Network Manager IP Edition
4.2

Guía de administración

2021-4212-01

Nota

Antes de utilizar esta información y el producto que soporta, lea la información de “Avisos” en la página 651.

Esta edición se aplica a la versión 4.2 de IBM Tivoli Network Manager IP Edition (número de producto 5724-S45) y a todos los releases y las modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Contenido

Acerca de esta publicación

El *IBM Tivoli Network Manager IP Edition Administration Guide* describe tareas de administración como iniciar y detener el producto, descubrir la red, sondear la red, gestionar sucesos, administrar procesos y consultar bases de datos. Esta publicación está destinada a administradores responsables del mantenimiento y disponibilidad de Network Manager.

Publicaciones

Esta sección lista publicaciones en la biblioteca de Network Manager y documentos relacionados. La sección también describe cómo acceder a publicaciones de IBM en línea y cómo solicitar publicaciones.

Su biblioteca de Network Manager

La siguiente documentación está disponible en la biblioteca de Network Manager:

- El *IBM Tivoli Network Manager IP Edition Release Notes* proporciona información importante y de última hora sobre Network Manager. Esta publicación está destinada a gestores de despliegue y administradores y debe leerse primero.
- La publicación *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*describe cómo instalar Network Manager. También describe tareas obligatorias y opcionales de configuración posteriores a la instalación. Esta publicación está destinada a administradores que deben instalar y configurar Network Manager.
- El *IBM Tivoli Network Manager IP Edition Administration Guide* describe tareas de administración como iniciar y detener el producto, descubrir la red, sondear la red, gestionar sucesos, administrar procesos y consultar bases de datos. Esta publicación está destinada a administradores responsables del mantenimiento y disponibilidad de Network Manager.
- El *Referencia de IBM Tivoli Network Manager* tiene información de referencia, inclusive el lenguaje del sistema, las bases de datos, y el API de Perl utilizado por Network Manager. Esta publicación está destinada a usuarios avanzados que necesitan personalizar el funcionamiento de Network Manager.

Publicaciones de requisito previo

Para utilizar la información de esta publicación de forma efectiva, debe tener algún conocimiento de requisito previo, que puede obtener desde las siguientes publicaciones:

- *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*

  Incluye procedimientos de instalación y actualización, y describe cómo configurar la seguridad y las comunicaciones de componentes. La publicación también contiene ejemplos de las arquitecturas de Tivoli Netcool/OMNIbus y describe cómo implementarlas.
- *IBM Tivoli Netcool/OMNIbus User's Guide*

  Proporciona una visión general de las herramientas de escritorio y describe las tareas del operador relacionadas con la gestión de sucesos utilizando estas herramientas.
- *IBM Tivoli Netcool/OMNIbus Administration Guide*

  Describe cómo realizar tareas administrativas utilizando la GUI de administrador de Tivoli Netcool/OMNIbus, herramientas de la línea de mandatos y control de procesos. Esta publicación también contiene descripciones y ejemplos de sintaxis y automatizaciones de ObjectServer SQL.
- *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*

  Contiene información de introducción y referencia acerca de sondas y pasarelas, lo que incluye la sintaxis de archivo de reglas de sonda y mandatos de pasarela.
- *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*

Describe cómo realizar tareas administrativas y de visualización de sucesos mediante la GUI web de Tivoli Netcool/OMNIbus.

Acceso a la terminología en línea

El sitio web de terminología de IBM consolida la terminología desde las bibliotecas de productos de IBM en una ubicación conveniente. Puede acceder al Sitio web de terminología en la siguiente dirección web:

http://www.ibm.com/software/globalization/terminology

Acceso a las publicaciones en línea

IBM publica publicaciones para este y todos los demás productos, en cuanto están disponibles y siempre que se actualizan, en el sitio web de IBM Knowledge Center en:

http://www.ibm.com/support/knowledgecenter/

La documentación de Network Manager está ubicada en el nodo **Cloud & Smarter Infrastructure** en ese sitio web.

Nota: Si imprime documentos PDF en papel distinto a tamaño de carta, establezca la opción en la ventana **Archivo** > **Imprimir** que permite a su aplicación de lectura de PDF imprimir páginas de tamaño de carta en su papel local.

Solicitud de publicaciones

Puede solicitar muchas publicaciones de IBM en línea en el siguiente sitio web:

http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss

También puede pedir por teléfono llamando a uno de estos números:

- En Estados Unidos: 800-879-2755
- En Canadá: 800-426-4968

En otros países, póngase en contacto con el representante de cuentas de software para pedir publicaciones de IBM. Para ubicar el número de teléfono de su representante local, realice los pasos siguientes:

1. Vaya al siguiente sitio web:

   http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss
2. Seleccione el país en la lista y pulse **Go** (Ir). La página **Bienvenido al Centro de publicaciones de IBM** se muestra para su país.
3. En el lado izquierdo de la página, haga clic en **Acerca de este sitio** para ver una página de información que incluya el número de teléfono de su representante local.

Accesibilidad

Las características de accesibilidad ayudan a los usuarios con una discapacidad física, como movilidad restringida o visión limitada, para utilizar productos de software satisfactoriamente.

Características de accesibilidad

Network Manager incluye las siguientes funciones de accesibilidad principales:

- Operaciones que utilizan un lector de pantalla.

Network Manager utiliza IBM Installation Manager para instalar el producto. Puede obtener información acerca de las funciones de accesibilidad para IBM Installation Manager en https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Network Manager utiliza el último estándar W3C, http://www.w3.org/TR/wai-aria/, para garantizar el cumplimiento de http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) y http://www.w3.org/TR/WCAG20/. Para aprovechar las funciones de accesibilidad, utilice el release más reciente de su lector de pantalla en combinación con el navegador web más reciente que admita este producto.

La documentación del producto en línea Network Manager en IBM Knowledge Center está habilitada para la accesibilidad. Las funciones de accesibilidad de IBM Knowledge Center se describen en https://www.ibm.com/support/knowledgecenter/v1/content/about/releasenotes.html#accessibility.

Navegación por teclado

Este producto utiliza teclas de navegación estándar.

Información de interfaz

Network Manager proporciona las siguientes características adecuadas para usuarios con poca visión:

- Todo el contenido no textual utilizado en la GUI tiene texto alternativo asociado.
- Los usuarios de visión baja pueden ajustar los valores de visualización del sistema, incluida la modalidad de alto contraste, y pueden controlar los tamaños de fonts utilizando los valores del navegador.
- El color no se utiliza como el único medio visual para transmitir información, indicar una acción, solicitar una respuesta o distinguir un elemento visual.

Network Manager proporciona las siguientes características adecuadas para usuarios epilépticos fotosensibles:

- Las interfaces de usuario de Network Manager no tienen contenido que parpadee más de dos veces en un periodo de un segundo.

La interfaz de usuario de web de Network Manager incluye puntos de referencia de navegación WAI-ARIA, que puede utilizar para navegar rápidamente a áreas funcionales en la aplicación.

Pasos extra para configurar Internet Explorer para la accesibilidad

Si utiliza Internet Explorer como su navegador web, puede que necesite realizar pasos de configuración extra para habilitar las características de accesibilidad.

Para habilitar la modalidad de alto contraste, realice los pasos siguientes:

1. Haga clic en **Herramientas** > **Opciones de Internet** > **Accesibilidad**.
2. Marque todos los recuadros de selección de la sección Formato.

Si al hacer clic en **Vista** > **Tamaño del texto** > **El más grande** no aumenta el tamaño de la font, haga clic en **Ctrl +** y **Ctrl -**.

Información relacionada sobre accesibilidad

Además de los sitios web de soporte y atención al cliente de IBM estándar, IBM ha establecido un servicio de teléfono de texto (TTY) especial para personas sordas o con deficiencias auditivas, para que puedan acceder a los servicios de soporte y ventas:

Servicio TTY
800-IBM-3383 (800-426-3383)
(en Norteamérica)

IBM y la accesibilidad

Para obtener más información sobre el compromiso de IBM con la compatibilidad, consulte https://www.ibm.com/able.

Formación técnica de Tivoli

Para obtener más información sobre la formación técnica de Tivoli, consulte el siguiente sitio web de educación de IBM Tivoli:

https://www.ibm.com/training/search?query=tivoli

Información de soporte y comunidad

Utilice el soporte de IBM, Service Management Connect y los grupos de usuarios de Tivoli para conectar con IBM y obtener la ayuda y la información que necesita.

Soporte de IBM

Si tiene un problema con el software de IBM, debe resolverlo lo antes posible. IBM proporciona las siguientes maneras para que obtenga el soporte que necesita:

En línea
Vaya al sitio web de Soporte de software de IBM en https://www.ibm.com/support/home/ y siga las instrucciones.

IBM Support Assistant
El IBM Support Assistant (ISA) es un área de trabajo gratuita de facilidad de mantenimiento de software local que ayuda a resolver preguntas y problemas con los productos de software de IBM. El ISA proporciona un acceso rápido a herramientas de facilidad de mantenimiento y a información relacionada con el soporte para la determinación de problemas. Para instalar el software ISA, vaya a https://www.ibm.com/support/knowledgecenter/SSLLVC/welcome/isa_welcome.html.

Service Management Connect

Acceda a Service Management Connect en https://www.ibm.com/developerworks/community/groups/service/html/communitystart?communityUuid=cdd16df5-7bb8-4ef1-bcb9-cefb1dd40581. Utilice Service Management Connect de las siguientes maneras:

- Implíquese en el desarrollo transparente, para fomentar la participación abierta y continua de otros usuarios y desarrolladores de IBM de productos de Tivoli. Puede acceder a diseños preliminares, demostraciones rápidas, hojas de ruta de productos y código previo al release.
- Póngase en contacto de forma privada con los expertos para colaborar y trabajar en red con Tivoli y la comunidad.
- Lea los blogs para beneficiarse de la experiencia de otros.
- Utilice los wikis y foros para colaborar con la comunidad de usuarios más amplia.

Parte 1. Administración de Network Manager

Para administrar el producto, debe iniciarlo y detenerlo. Podrá administrar procesos, registros, puertos, usuarios, contraseñas, informes y bases de datos.

Acerca de esta tarea

Las tareas de configuración generalmente se hacen una sola vez para configurar el producto.

Las tareas de configuración están descritas en el *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

En comparación, las tareas de administración se llevan a cabo según sea necesario, de manera continua. Las tareas de configuración están descritas en esta sección.

Tareas relacionadas

Administración de sondeo de red
Utilice la interfaz de línea de mandatos para realizar una amplia gama de tareas de administración de sondeo, incluidas la gestión de varias características de sondeador, la copia de sondeos de red en dominios de red, la suspensión de sondeo de red, la habilitación e inhabilitación de sondeos, la recuperación del estado de sondeo y la renovación de sondeos.

Capítulo 1. Inicio y detención de Network Manager

Sus opciones para iniciar y detener Network Manager se explican aquí.

Acerca de esta tarea

Establecimiento de variables de entorno

Antes de iniciar cualquier componente o de trabajar con un archivo de configuración, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Acerca de esta tarea

Los scripts de entorno establecen las siguientes variables de entorno necesarias. Los scripts de entorno se configuran automáticamente con las ubicaciones correctas en las que se han instalado los componentes. Otras variables del entorno se establecen automáticamente cuando es necesario mediante componentes de Network Manager.

$NCHOME
La ubicación de inicio de Netcool que se establece de forma predeterminada en el directorio `netcool` debajo del directorio de instalación:

- `/opt/IBM/netcool/core`

$NMGUI_HOME
La ubicación en la que se han instalado los componentes de la GUI de Network Manager. De forma predeterminada, esta ubicación es `/opt/IBM/netcool/gui/precision_gui`.

$ITNMHOME y $PRECISION_HOME
La ubicación de inicio de Network Manager toma como valor predeterminado `$NCHOME/precision`:

- `/opt/IBM/netcool/core/precision`

Nota: El script también establece $PRECISION_HOME. De forma predeterminada, $PRECISION_HOME se establece en la misma ubicación que $ITNMHOME, pero la utilizan otros componentes del producto.

$DASH_HOME
La ubicación de instalación de Dashboard Application Services Hub. De forma predeterminada, esta ubicación es `/opt/IBM/JazzSM/ui`.

$JazzSM_HOME
La ubicación de instalación de Jazz for Service Management. De forma predeterminada, esta ubicación es `/opt/IBM/JazzSM`.

Para establecer las variables de entorno de Network Manager, ejecute el script adecuado para los componentes que ha instalado. Existen scripts diferentes en el servidor en el que se han instalado los componentes principales y el servidor en el que se han instalado los componentes de la GUI.

Importante: Si ha instalado los componentes principales y los componentes de la GUI en un servidor, ejecute ambos scripts.

Procedimiento

- Ejecute el script de entorno adecuado:

  En el servidor en el que se han instalado los componentes principales de Network Manager, el script de entorno es `directorio_instalación/netcool/core/env.sh`.

  Por ejemplo, en los shells Bash, Bourne y Korn, obtenga el script env.sh mediante un mandato similar al siguiente:

```
. /opt/IBM/netcool/core/env.sh
```

En el servidor en el que se han instalado los componentes de la GUI De Network Manager, el script es `directorio_instalación/nmgui_profile.sh`, por ejemplo, `/opt/IBM/netcool/nmgui_profile.sh`.

Por ejemplo, en los shells Bash, Bourne y Korn, obtenga el script nmgui_profile.sh mediante un mandato similar al siguiente:

```
. /opt/IBM/netcool/nmgui_profile.sh
```

Qué hacer a continuación

Una vez que haya establecido las variables de entorno, inicie Network Manager y asegúrese de que se esté ejecutando correctamente.

Tareas relacionadas

Inicio de Network Manager

Puede iniciar Network Manager utilizando los métodos descritos aquí. Desde Network Manager V4.2 y posterior, debe iniciar Tivoli Netcool/OMNIbus por separado, utilizando los mandatos de Tivoli Netcool/OMNIbus.

Inicio de Network Manager

Puede iniciar Network Manager utilizando los métodos descritos aquí. Desde Network Manager V4.2 y posterior, debe iniciar Tivoli Netcool/OMNIbus por separado, utilizando los mandatos de Tivoli Netcool/OMNIbus.

Acerca de esta tarea

Importante: Tivoli Netcool/OMNIbus y la base de datos de topología deben iniciarse ambas antes que Network Manager.

Tareas relacionadas

Establecimiento de variables de entorno

Antes de iniciar cualquier componente o de trabajar con un archivo de configuración, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Inicio de todos los componentes de Network Manager (solo UNIX)

Puede iniciar Network Manager y todos sus componentes utilizando el mandato **`itnm_start`**. Este mandato también se puede utilizar para iniciar el sistema de cálculo en tiempo real Apache Storm, que se utiliza para agregar datos de sondeo sin formato a los datos de sondeo históricos.

Antes de empezar

Antes de trabajar con los procesos, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Acerca de esta tarea

En el caso de Network Manager, el mandato **`itnm_start`** inicia el controlador del proceso maestro, **`ncp_ctrl`**, que inicia todos los procesos de Network Manager.

Para ejecutar el mandato **`itnm_start`**:

Procedimiento

1. Si no ha configurado el entorno de UNIX, cambie al directorio `$NCHOME/precision/bin`.
2. Escriba el mandato siguiente: `itnm_start -domain` *`NCOMS`*.

Este mandato inicia todos los componentes de Network Manager que estén instalados en el servidor en el dominio NCOMS de ejemplo.

Tareas relacionadas

Establecimiento de variables de entorno
Antes de iniciar cualquier componente o de trabajar con un archivo de configuración, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Inicio de los procesos de Network Manager utilizando la consola de mandatos

Puede iniciar los procesos de Network Manager iniciando el controlador del proceso maestro, **ncp_ctrl**, utilizando la consola del mandato.

Antes de empezar

Antes de comenzar esta tarea, compruebe lo siguiente:

- Si desea que distintas dependencias de los procesos sean las predeterminadas, asegúrese de que en primer lugar estén configuradas.
- Asegúrese de que el entorno de UNIX esté configurado.

Acerca de esta tarea

Si inicia los procesos de Network Manager utilizando el controlador de procesos maestro, solo se inician los procesos que pertenecen a los componentes principales de Network Manager.

Para iniciar Network Manager utilizando la consola de mandatos

Procedimiento

Escriba el mandato siguiente:

```
ncp_ctrl -domain DOMAIN &
```

donde *DOMAIN* es el dominio en el que desea iniciar los componentes principales.

Detención de Network Manager

Puede detener Network Manager utilizando los métodos descritos aquí. A partir de Network Manager V4.2 y posteriores, debe detener Tivoli Netcool/OMNIbus por separado, utilizando los mandatos Tivoli Netcool/OMNIbus.

Detención de todos los componentes de Network Manager (solo UNIX)

También puede detener Network Manager y todos sus componentes, utilizando el mandato **itnm_stop**. Este mandato también se puede utilizar para detener el sistema de cálculo en tiempo real de Apache Storm, que se utiliza para agregar datos de sondeo sin formato a los datos de sondeo históricos.

Antes de empezar

Antes de trabajar con los procesos, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Acerca de esta tarea

En todos los sistemas operativos soportados , puede utilizar el script **itnm_stop** para detener el controlador de procesos del dominio de Network Manager, el proceso **ncp_ctrl** (el cual detiene, a continuación, todos los procesos necesarios).

Para ejecutar el mandato **itnm_stop**, realice los pasos siguientes.

Procedimiento

1. Vaya al directorio de $NCHOME/precision/bin.
2. Escriba el mandato siguiente: `itnm_stop -domain` *NCOMS*

   Este mandato detiene todos los componentes de Network Manager que están instalados en el servidor en el dominio de ejemplo NCOMS.

Tareas relacionadas

Establecimiento de variables de entorno
Antes de iniciar cualquier componente o de trabajar con un archivo de configuración, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Detención de los procesos de Network Manager utilizando la consola de mandatos

Puede detener todos los procesos de Network Manager deteniendo el controlador del proceso maestro, el proceso `ncp_ctrl`.

Acerca de esta tarea

Si detiene los procesos de Network Manager utilizando el controlador de proceso maestro, sólo se detienen los procesos que pertenecen a los componentes principales de Network Manager.

Para detener el proceso `ncp_ctrl`:

Procedimiento

1. Seleccione la ventana de la consola donde se está ejecutando el proceso `ncp_ctrl` .
2. Pulse Ctrl+C.

Resultados

El proceso `ncp_ctrl` se detiene y también todos sus procesos gestionados.

Reinicio del servidor Dashboard Application Services Hub

Tras las actividades de personalización y configuración, es posible que deba reiniciar Dashboard Application Services Hub.

Acerca de esta tarea

Fix Pack 7 Normalmente no es necesario reiniciar el servidor Dashboard Application Services Hub si cambia un archivo `.properties` que pertenece a Network Manager. Tales cambios se leen automáticamente.

Al reiniciar Dashboard Application Services Hub se reinician todas las aplicaciones de GUI que estén en ejecución en el servidor Dashboard Application Services Hub.

Las aplicaciones que se reinician incluyen las aplicaciones de GUI de Network Manager y las aplicaciones de GUI web.

Para reiniciar el servidor:

Procedimiento

1. En el Dashboard Application Services Hub adecuado, abra una ventana de mandatos.
2. Cambie al directorio $JazzSM_HOME/profile/bin.

3. Detenga el servidor emitiendo el siguiente mandato:

```
stopServer.sh server1
```

   Nota: Se le solicitará que proporcione el nombre de usuario y la contraseña del usuario administrativo.

4. Espere unos instantes a que el servidor concluya completamente y confirme que se ha detenido la ejecución de todos los procesos de Java™.

   Los mensajes siguientes confirman que el servidor está apagado:

```
ADMU3201I: Se ha emitido una petición de detención del servidor. Esperando el estado de
detención.
ADMU4000I: Detención del servidor server1 completada.
```

5. Inicie el servidor emitiendo el siguiente mandato:

```
startServer.sh server1
```

Capítulo 2. Administración de procesos

Puede iniciar, detener e investigar procesos individuales de Network Manager.

Acerca de esta tarea

Acerca del control del proceso

Puede comprobar el estado de los procesos de Network Manager utilizando el controlador del proceso maestro, el proceso **ncp_ctrl**.

De forma predeterminada, el proceso **ncp_ctrl** iniciará todos los procesos de Network Manager en el orden adecuado, en correspondencia con las dependencias configuradas del proceso. También puede utilizar el proceso **ncp_ctrl** para iniciar procesos de Network Manager individuales.

El proceso **ncp_ctrl** es el único componente de Network Manager que puede iniciar otro proceso. También lo utilizan otros procesos de Network Manager que necesitan iniciar y gestionar sus subprocesos.

El proceso **ncp_ctrl** es el proceso maestro y debe ejecutarse antes del resto de los procesos. El proceso **ncp_ctrl** se iniciará y gestionará los procesos adecuados cuando sus dependencias se hayan satisfecho.

Procesos de Network Manager

Se puede hacer referencia a los procesos en documentación mediante su nombre ejecutable (que comienza con ncp_) o mediante un nombre descriptivo.

La siguiente tabla describe los procesos de Network Manager.

Tabla 1. Procesos de Network Manager

Nombre ejecutable	Nombre descriptivo	Descripción
ncp_brokerd	Daemon de Really Small Message Broker	Daemon del intermediario de mensajes que inicia el Really Small Message Broker. La comunicación entre los componentes principales de Network Manager se gestiona mediante Really Small Message Broker. ncp_brokerd se inicia automáticamente cuando se inicia cualquier proceso de Network Manager.
ncp_class	Gestor de clases de objetos activos, CLASS	Sistema de gestión de bibliotecas dinámico responsable de gestionar las clases de objetos activos (AOC). Es el único componente que tiene contacto directo con las definiciones de AOC, y distribuye estas definiciones a cualquier componente que las necesite. Puede editar AOC utilizando un editor de texto. Reinicie el proceso **ncp_class** después de modificar los archivos AOC. Después de reiniciar y ejecutar ncp_class, reinicie el proceso **ncp_model**. **Nota:** Asegúrese de que realiza una copia de seguridad de cualquier AOC original antes de editarlos. Si sobrescribe la copia original, la copia de seguridad se puede restaurar.

Tabla 1. Procesos de Network Manager (continuación)

Nombre ejecutable	Nombre descriptivo	Descripción
`ncp_config`	Servidor de archivos de configuración de la GUI de Network Manager, CONFIG	Servidor de archivos de configuración que proporciona un medio para que los GUI de Network Manager lean y escriban en archivos de esquema.
`ncp_ctrl`	Controlador del proceso maestro, CTRL	Controlador del proceso maestro que inicia todos los procesos de Network Manager en el orden adecuado, en correspondencia con las dependencias configuradas del proceso. También puede utilizar el proceso `ncp_ctrl` para iniciar procesos de Network Manager individuales.
`ncp_crypt`	Programa de utilidad de cifrado de contraseña	Programa de utilidad para el cifrado manual de contraseñas.
`ncp_disco`	Motor de descubrimiento	Gestiona el proceso de la interconectividad y la existencia del dispositivo de descubrimiento. Los subprocesos de ncp_disco incluyen los siguientes procesos de buscadores, que son responsables de la determinación de existencia de dispositivos: • ncp_df_ping (Buscador de ping): Realiza una solicitud de eco de ICMP simple para las direcciones de difusión o multidifusión, direcciones IP individuales o todos los dispositivos de la subred. • ncp_df_file (Buscador de archivos): Analiza un archivo, como por ejemplo `/etc/hosts`, para recuperar una lista de dispositivos para buscar dispositivos en la red. • ncp_df_dbentry (Buscador de base de datos): Lee una base de datos para recuperar una lista de dispositivos a buscar en la red. • ncp_df_collector (Buscador de recopiladores): Recupera una lista de dispositivos gestionada por sistemas de gestión de elementos (EMS) en la red
`ncp_dla`	adaptador de biblioteca de descubrimiento	Recopila datos en relaciones y recursos de red desde Network Manager para su importación en la Tivoli Change and Configuration Management Database (CCMDB).

Tabla 1. Procesos de Network Manager (continuación)

Nombre ejecutable	Nombre descriptivo	Descripción
ncp_d_helpserv	Servidor de ayudantes	Los ayudantes recuperan información de la red durante un descubrimiento. El Servidor de ayudantes gestiona los ayudantes y almacena la información recuperada de la red. Los agentes de descubrimiento recuperan su información mediante el Servidor de ayudantes para reducir la carga en la red. El Servidor de ayudantes puede dar servicio a las solicitudes directamente con datos en memoria caché o pasar la solicitud al ayudante apropiado. El Servidor de ayudantes gestiona los siguientes ayudantes: • ncp_dh_arp (ayudante de ARP): realiza la resolución de la dirección IP en la dirección MAC • ncp_dh_dns (ayudante de DNS): realiza la resolución de la dirección IP en el nombre del dispositivo • ncp_dh_ping (ayudante de ping): hace ping a cada dispositivo de una subred, una dirección IP individual o una dirección de difusión o de multidifusión • ncp_dh_snmp (ayudante de SNMP): devuelve los resultados de una solicitud de SNMP, como Get, GetNext y GetBulk • ncp_dh_telnet (ayudante de telnet): devuelve resultados de una operación de telnet en un dispositivo especificado • ncp_dh_xmlrpc (ayudante de recopilador): proporciona funciones de comunicaciones con recopiladores de EMS mediante la interfaz XML-RPC
ncp_g_event	Pasarela de sucesos	Proporciona una interfaz bidireccional entre Network Manager y Tivoli Netcool/OMNIbus. La Pasarela de sucesos también reenvía sucesos a conectores que se suscriben a tipos específicos de sucesos y que realizan más acciones o más sucesos enriquecidos según los datos de sucesos.
ncp_mib	Programa de utilidad de administración de actualización de MIB	Utilice el programa de utilidad de administración de actualización de MIB para actualizar sus datos de MIB para su uso con el Navegador de MIB de SNMP.

Tabla 1. Procesos de Network Manager (continuación)

Nombre ejecutable	Nombre descriptivo	Descripción
`ncp_model`	Gestor de topología	Almacena los datos de topología tras un descubrimiento y envía los datos de topología a la base de datos de topología (NCIM), donde se pueden consultar utilizando SQL. Los GUI de visualización de topología recuperan los datos de topología desde NCIM para mostrar en operadores de red.
`nco_p_ncpmonitor`	Sonda para Tivoli Netcool/ OMNIbus	Habilita que los sucesos generados por el sondeo de Network Manager se envíen al ObjectServer de Tivoli Netcool/OMNIbus. El proceso `nco_p_ncpmonitor` convierte estos sucesos al formato ObjectServer.
`ncp_poller`	Motor de sondeo	Controla el sondeo del dispositivo de red.
`ncp_oql`	Proveedor de servicios de OQL	Interfaz de línea de mandatos que habilita a los administradores para consultar y actualizar datos en las bases de datos de Network Manager.
`ncp_trapmux`	Multiplexor de condiciones de excepción de SNMP	En la mayoría de las redes, las condiciones de excepción llegan a un único puerto predeterminado. El multiplexor de condiciones de excepción de SNMP resuelve este problema escuchando un puerto único y reenviando todas las condiciones de excepción que recibe a un conjunto de pares de host/socket.
`ncp_virtualdomain`	Dominio virtual	El dominio virtual se utiliza al ejecutar Network Manager con la migración tras error. Cualquier conexión a este dominio virtual se direcciona al servidor de Network Manager, que se ejecuta como el servidor principal en la arquitectura de migración tras error.
`ncp_webtool`	Herramientas web	Proporciona el alojamiento de WebTools en el servidor de fondo para que se pueda acceder a ellas en entornos distribuidos donde Topoviz se ejecute en un servidor distinto a los procesos de fondo de Network Manager y donde haya un cortafuegos entre los dos.

Procesos gestionados y no gestionados

El proceso ncp_ctrl inicia dos tipos de procesos: gestionados y no gestionados.

Procesos gestionados

Procesos de los que el proceso ncp_ctrl es totalmente responsable. El proceso ncp_ctrl no sólo inicia y detiene estos procesos, sino que también realiza un seguimiento de sus actividades y los reinicia si se detienen.El número de veces que ncp_ctrl reiniciará un proceso gestionado se puede configurar utilizando el campo retryCount de la base de datos services.inTray.

Procesos no gestionados
Procesos de los que el proceso ncp_ctrl sólo es responsable de iniciar o detener. El proceso ncp_ctrl no es responsable del seguimiento de procesos no gestionados independientes y no intenta reiniciar estos procesos cuando se detienen. Los procesos no gestionados pueden dividirse en dos tipos:

Procesos no gestionados independientes
Un proceso no gestionado independiente continúa ejecutándose si otros procesos terminan.

Procesos no gestionados dependientes
Ncp_ctrl detiene los procesos no gestionados dependientes si el proceso padre termina. Un ejemplo de los procesos no gestionados dependientes son los agentes de descubrimiento iniciados por el proceso del motor de descubrimiento padre, ncp_disco.

Los procesos principales de Network Manager (es decir, los que se encargan del descubrimiento, supervisión, análisis de causas raíz y datos de topología) se manejan como procesos gestionados. Los procesos como los scripts deben iniciarse como procesos no gestionados.

Acerca de los dominios de Network Manager

Un dominio es una parte de la red que se descubre y gestiona de forma independiente. Muchos procesos de Network Manager ejecutan una instancia por dominio. Cada dominio tiene un nombre exclusivo.

La ejecución de varios dominios permite descubrir, visualizar y supervisar varias topologías de red. Se pueden ejecutar varios procesos de Network Manager e forma independiente el uno del otro en el mismo servidor, si pertenecen a diferentes dominios.

La división de la red en dominios permite al usuario descubrir su red en secciones. Es posible que desee hacer esto por razones de escalabilidad: la red podría ser demasiado grande para ser descubierta de una vez. También, puede desear descomponer la red en regiones geográficas, y hacer que cada región se corresponda con un dominio.

De forma predeterminada, Network Manager se ejecuta en un único dominio.

El dominio en el que se ejecuta un componente viene determinado por el argumento de línea de mandatos -domain, el cual es obligatorio para todos los componentes, con la excepción del proceso **ncp_mib**, que gestiona la importación de MIB en todos los dominios utilizando la misma base de datos de Netcool Common Inventory Model (NCIM).

Los archivos de configuración que son específicos de un dominio particular tienen el nombre del dominio anexado al nombre del archivo. Por ejemplo, el archivo de configuración del proceso ncp_ctrl en ejecución en el dominio NCOMS sería `CtrlServices.NCOMS.cfg`

Restricción: Utilice únicamente caracteres alfanuméricos y subrayados (_) para los nombres de dominio. Todos los demás caracteres, como el guión (-), están prohibidos.

.

Archivos de configuración específicos del dominio

Puede utilizar distintos valores de configuración para diferentes dominios mediante las versiones guardadas específicas del dominio de los archivos de configuración que edite.

Si se encuentra un archivo de configuración específico del dominio, los procesos relevantes del dominio utilizan esos valores de configuración. Si no se encuentra ningún archivo de configuración específico del dominio, se utilizan los valores del archivo de configuración no específico.

Para guardar una versión específica del dominio de un archivo de configuración, añada el nombre del dominio al final del nombre de archivo inmediatamente antes de la extensión de archivo. Por ejemplo, el archivo de configuración para el proceso `ncp_ctrl` del dominio NCOMS se denomina `CtrlServices.NCOMS.cfg`.

Aunque en la práctica hay más archivos de que probablemente tiene que alterar, en principio, todo los tipos de archivo siguientes pueden ser específicos de dominio:

- Archivos de configuración, es decir, todos los archivos que terminan en `.cfg`

- Archivos del agente de descubrimiento, es decir, todos los archivos que terminan en `.agnt`
- Archivos de clase de objetos activos, es decir, todos los archivos que terminan en `.aoc`
- Archivos del agrupador basados en texto, todos los archivos del directorio `stitchers` que terminan en `.stch`

En la documentación de Network Manager, se hace referencia a estos archivos para utilizar sus nombres predeterminados a menos que se indique lo contrario.

Comprobación del estado del proceso

Puede comprobar el estado de IBM Tivoli Netcool/OMNIbus, y de los procesos individuales de Network Manager.

Comprobación del estado del proceso mediante la ejecución del mandato itnm_status

En los sistemas operativos UNIX, puede comprobar el estado de Network Manager con el mandato **`itnm_status`**.

Antes de empezar

Antes de trabajar con los procesos, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Acerca de esta tarea

Para comprobar el estado de todos los componentes de Network Manager en el servidor actual, complete los siguientes pasos:

Procedimiento

1. Vaya al directorio de `$NCHOME/precision/bin`.
2. Escriba el siguiente mandato: `itnm_status`

   Este mandato muestra el estado de todos los componentes de Network Manager que están instalados en el servidor.

Tareas relacionadas

Establecimiento de variables de entorno
Antes de iniciar cualquier componente o de trabajar con un archivo de configuración, establezca las variables de entorno adecuadas ejecutando los scripts del entorno.

Supervisión de mensajes de estado de proceso

Puede ver mensajes de estado en Network Manager para comprender el estado del producto.

Acerca de esta tarea

Los procesos de Network Manager envían mensajes a IBM Tivoli Netcool/OMNIbus cuando se inician y se detienen. Puede ver estos mensajes para conocer qué procesos se han iniciado o se ha detenido y para ver el estado de migración tras error.

Para obtener más información sobre sucesos de estado de Network Manager, consulte *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Para visualizar los mensajes de estado de proceso, complete las siguientes tareas.

Procedimiento

1. Añadir un widget de **Visor de sucesos** a un panel de control.
2. Aplicar un filtro a **Visor de sucesos** para que se visualicen sólo los sucesos con un `Alert Group` de `ITNM Status`.

Comprobar el estado del proceso mediante la consulta de bases de datos ncp_ctrl

En todos los sistemas operativos, puede comprobar el estado de procesos de Network Manager individuales consultando las bases de datos del proceso **ncp_ctrl**.

Acerca de esta tarea

El proceso **ncp_ctrl** también se debe estar ejecutando para el dominio que desea interrogar.

Identificación de qué procesos de Network Manager están en ejecución

Para identificar los procesos que se iniciaron mediante el proceso **ncp_ctrl**, han terminado de iniciarse y están actualmente en ejecución, emita una consulta a la tabla de base de datos services.inTray.

Acerca de esta tarea

Para identificar qué procesos están en ejecución:

Procedimiento

1. Inicie sesión en el servicio Ctrl utilizando la página Proveedor de servicios de OQL o la página Acceso a la base de datos de gestión:
   - Inicie el Proveedor de servicios de OQL escribiendo un mandato similar al siguiente:

     ```
     ncp_oql -domain NCOMS -service Ctrl
     ```

     donde *NCOMS* es el nombre del dominio. Si se ha configurado la autenticación para el Proveedor de servicios de OQL, escriba su nombre de usuario y su contraseña.
   - Inicie sesión en la página Acceso a la base de datos de gestión y seleccione el servicio Ctrl.
2. Emita el mandato siguiente:

   ```
   select serviceName, binaryName, domainName, processId
   from services.inTray
   where serviceState = 4 ;
   go
   ```

   Nota:

   Pueden transcurrir algunos minutos para que algunos procesos se inicien completamente después de que ncp_ctrl los haya iniciado. Mientras se inicia un proceso, no se devuelve en la consulta.

Ejemplo

La salida de ejemplo siguiente muestra que se iniciaron 12 procesos mediante el proceso **ncp_ctrl** y que se están ejecutando actualmente:

```
...........
{
        binaryName='ncp_store';
        domainName='SCO099';
        processId=12129;
        serviceName='ncp_store';
}
{
        binaryName='ncp_class';
        domainName='SCO099';
```

```
        processId=12130;
        serviceName='ncp_class';
}
{
        binaryName='ncp_model';
        domainName='SCO099';
        processId=12384;
        serviceName='ncp_model';
}
{
        binaryName='ncp_disco';
        domainName='SCO099';
        processId=12488;
        serviceName='ncp_disco';
}
{
        binaryName='ncp_d_helpserv';
        domainName='SCO099';
        processId=12131;
        serviceName='ncp_d_helpserv';
}
{
        binaryName='ncp_config';
        domainName='SCO099';
        processId=12132;
        serviceName='ncp_config';
}
{
        binaryName='ncp_poller';
        domainName='SCO099';
        processId=12906;
        serviceName='ncp_poller_default';
}
{
        binaryName='ncp_poller';
        domainName='SCO099';
        processId=12907;
        serviceName='ncp_poller_admin';
}
{
        binaryName='nco_p_ncpmonitor';
        domainName='SCO099';
        processId=12133;
        serviceName='nco_p_ncpmonitor';
}
{
        binaryName='ncp_g_event';
        domainName='SCO099';
        processId=12552;
        serviceName='ncp_g_event';
}
{
        binaryName='ncp_webtool';
        domainName='SCO099';
        processId=12134;
        serviceName='ncp_webtool';
}
{
        binaryName='ncp_virtualdomain';
        domainName='SCO099';
        processId=13182;
        serviceName='ncp_virtualdomain';
}
( 12 record(s) : Transaction complete )
```

Identificación de los procesos que se inician automáticamente

Para identificar los procesos que se inician automáticamente mediante el proceso **ncp_ctrl**, emita una consulta a la tabla de base de datos services.inTray.

Acerca de esta tarea

Para identificar qué procesos se inician automáticamente:

Procedimiento

1. Inicie sesión en el servicio Ctrl utilizando la página Proveedor de servicios de OQL o la página Acceso a la base de datos de gestión:
   - Inicie el Proveedor de servicios de OQL escribiendo un mandato similar al siguiente:

     ```
     ncp_oql -domain NCOMS -service Ctrl -username admin
     ```

     donde *NCOMS* y *admin* son su nombre de dominio y nombre de usuario.
   - Inicie sesión en la página Acceso a la base de datos de gestión y seleccione el servicio Ctrl.
2. Emita el mandato siguiente:

   ```
   select * from services.inTray;
   go
   ```

Ejemplo

La siguiente salida de ejemplo muestra los procesos configurados para iniciarse mediante el proceso **ncp_ctrl**:

```
{
        serviceName='ncp_disco';
        binaryName='ncp_disco';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin';
        domainName='NCOMS';
        argList=['-domain','$PRECISION_DOMAIN','-discoOnStartup',
                 '0','-latency','100000','-debug','0','-messagelevel',
                 'warn'];
        dependsOn=['ncp_d_helpserv','ncp_model'];
        retryCount=5;
        serviceId=4;
        traceLevel=0;
        logLevel='warn';
        serviceKey='ncp_disco_NCOMS';
        serviceState=4;
        interval=10;
        processId=2622;
}
.....
.....
{
        serviceName='ncp_model';
        binaryName='ncp_model';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin';
        domainName='NCOMS';
        argList=['-domain','$PRECISION_DOMAIN','-latency','100000',
                 '-debug','0','-messagelevel','warn'];
        dependsOn=['ncp_config','ncp_store','ncp_class'];
        retryCount=5;
        serviceId=3;
        traceLevel=0;
        logLevel='warn';
        serviceKey='ncp_model_NCOMS';
        serviceState=4;
        interval=10;
        processId=2542;
}
```

Identificación de procesos no gestionados

Para identificar los procesos iniciados automáticamente, pero no gestionados, mediante el proceso **ncp_ctrl**, emita una consulta a la tabla de base de datos services.unManaged.

Acerca de esta tarea

Las inserciones en la tabla `services.unManaged` se realizan por otros componentes de Network Manager para iniciar o detener sus subprocesos; por ejemplo, el proceso **ncp_disco** utiliza el proceso **ncp_ctrl** para iniciar los buscadores.

Para identificar procesos no gestionados:

Procedimiento

1. Inicie sesión en el servicio Ctrl utilizando el Proveedor de servicios de OQL o el Área de trabajo OQL:
   - Inicie el Proveedor de servicios de OQL escribiendo un mandato similar al siguiente:

     ```
     ncp_oql -domain DOMAIN_NAME -service Ctrl
     ```

   - Inicie sesión en el Área de trabajo OQL y seleccione el servicio Ctrl.
2. Emita uno de los siguientes mandatos para obtener una lista de los procesos no gestionados:
   a) Emita el siguiente mandato para obtener una lista de todos los procesos no gestionados:

      ```
      select * from services.unManaged;
      go
      ```

   b) Emita el siguiente mandato para obtener una lista de sólo los procesos no gestionados dependientes:

      ```
      select * from services.unManaged
      WHERE dependency is not NULL;
      go
      ```

Ejemplo

El siguiente ejemplo de salida muestra procesos sin gestionar que fueron iniciados por el proceso **ncp_ctrl**:

```
{
        serviceName='ncp_df_ping';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        dependency=19803;
        argList=['-domain','LNX39024','-server','ncp_disco.2622'];
        binaryName='ncp_df_ping';
        serviceId=14;
        logLevel='warn';
        traceLevel=0;
        domainName='NCOMS';
        processId=19869;
}
{
          serviceName='ncp_df_collector';
          servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
          dependency=19803;
          argList=['-domain','COLT45','-server','ncp_disco.19803'];
          binaryName='ncp_df_collector';
          serviceId=13;
          logLevel='warn';
          traceLevel=0;
          domainName='NCOMS';
          processId=19870;
}
{
          serviceName='ncp_df_file';
          servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
          dependency=19803;
          argList=['-domain','COLT45','-server','ncp_disco.19803'];
          binaryName='ncp_df_file';
          serviceId=14;
          logLevel='warn';
          traceLevel=0;
          domainName='NCOMS';
          processId=19871;
}
{
         serviceName='ncp_agent';
         servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
         dependency=19803;
          argList=['-domain','COLT45','-agent','Details','-server',
'ncp_disco.19803','-threads','100','-messagelevel','warn'];
           endSignal=2;
```

```
          binaryName='ncp_agent';
          serviceId=17;
          logLevel='warn';
          traceLevel=0;
          domainName='NCOMS';
           processId=28352;
}{
        serviceName='ncp_dh_snmp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        dependency=19646;
        argList=['-domain','LNX39024'];
        binaryName='ncp_dh_snmp';
        serviceId=19;
        logLevel='warn';
        traceLevel=0;
        domainName='NCOMS';
        processId=28460;
}
( 5 record(s) : Transaction complete )
```

Gestión de dependencias de procesos

Los procesos gestionados por ncp_ctrl en la configuración predeterminada no se pueden iniciar hasta que se hayan iniciado completamente los procesos de los que dependen. Las dependencias del proceso configuradas incorrectamente pueden dar lugar a problemas al iniciar procesos.

Acerca de esta tarea

Listado de dependencias de procesos

Puede emitir una consulta a la base de datos services.inTray para identificar qué procesos tienen dependencias de otros procesos.

Acerca de esta tarea

Para identificar dependencias de proceso:

Procedimiento

1. Inicie sesión en las bases de datos de control del proceso.
2. Emita el mandato siguiente:

```
select serviceName, dependsOn
from services.inTray;
go
```

3. La siguiente salida de ejemplo muestra que **ncp_class** y **ncp_store** no tienen ninguna dependencia y que **ncp_model** depende de **ncp_class** and **ncp_store**:

```
.....
{
                serviceName='ncp_class';
                dependsOn=[];
}
{
                serviceName='ncp_store';
                dependsOn=[];
}
.....
.....
{
                serviceName='ncp_model';
                dependsOn=['ncp_class', 'ncp_store'];
}
( 4record(s) : Transaction complete )
```

Identificación de dependencias para un proceso concreto

Para identificar las dependencias para un proceso concreto, emita una consulta a la base de datos services.inTray.

Acerca de esta tarea

Para identificar las dependencias del proceso para un proceso concreto:

Procedimiento

1. Inicie sesión en las bases de datos de control del proceso.
2. Emita el mandato siguiente:

```
select serviceName, dependsOn
from services.inTray
where serviceName='SERVICE';
go
```

   Donde *PROCESS* es el nombre del proceso para el que desea consultar las dependencias; por ejemplo, `ncp_disco`.

Ejemplo

La siguiente salida de ejemplo muestra que **ncp_model** depende de **ncp_class** y **ncp_store:**

```
{
                serviceName='ncp_model';
                dependsOn=['ncp_class', 'ncp_store'];
}
( 1record(s) : Transaction complete )
```

Configuración de dependencias de proceso

Para configurar dependencias de proceso, edite el archivo de configuración `$NCHOME/etc/precision/CtrlServices.cfg`.

Acerca de esta tarea

Las dependencias de proceso definidas en el archivo de configuración `CtrlServices.cfg` especifican en el que el proceso **ncp_ctrl** inicia los procesos.

Consejo:

Las dependencias de proceso están configuradas de forma predeterminada y, normalmente, no es necesario cambiarlas.

Para configurar dependencias de proceso:

Procedimiento

1. Realice una copia de seguridad y edite el archivo de configuración `CtrlServices.`*DOMAIN*`.cfg`, donde *DOMAIN* es el nombre del dominio.
2. Busque la siguiente línea en el archivo para localizar la entrada del proceso cuyas dependencias desea configurar:

```
serviceName='process_name';
```

   donde *process_name* es el nombre del proceso.
3. Modifique las dependencias del proceso añadiendo o eliminando nombre de procesos a la siguiente línea, directamente debajo de la línea anterior:

```
dependsOn=['process_name', 'process_name2'];
```

4. Guarde el archivo de configuración **CtrlServices.cfg**.
5. Reinicie el controlador de proceso maestro, el proceso **ncp_ctrl** , para que los cambios surtan efecto.

Lista de dependencias de procesos

Los procesos de Network Manager gestionados por ncp_ctrl de forma predeterminada se deben iniciar en el orden correcto.

Las dependencias de los procesos se muestran en la tabla siguiente:

Tabla 2. Dependencias de los procesos de Network Manager

Proceso	**Dependencias**
ncp_class	Sin dependencias
ncp_config	Sin dependencias
ncp_ctrl	Sin dependencias
ncp_disco	**ncp_d_helpserv**, **ncp_model**
ncp_d_helpserv	Sin dependencias
ncp_g_event	**ncp_model**, Tivoli Netcool/OMNIbus ObjectServer
ncp_model	**ncp_config**, **ncp_class**, **ncp_store**
ncp_poller	**ncp_g_event**, **nco_p_ncpmonitor**
nco_p_ncpmonitor	Netcool/OMNIbus ObjectServer
ncp_store	Sin dependencias
ncp_virtualdomain	**ncp_g_event**, **ncp_poller**
ncp_webtool	Sin dependencias

Archivos de configuración de control de procesos

Utilice los siguientes archivos de configuración para configurar el proceso ncp_ctrl.

- $NCHOME/etc/precision/CtrlSchema.cfg contiene las definiciones de las bases de datos del proceso ncp_ctrl. No necesita editar este archivo.
- $NCHOME/etc/precision/CtrlServices.cfg contiene todas las inserciones necesarias en las bases de datos del proceso ncp_ctrl para indicarle al proceso ncp_ctrl qué procesos deben iniciarse y en qué orden.

Para configurar el proceso ncp_ctrl para que inicie y gestione los procesos correctos, debe anexar inserciones de OQL en el archivo de configuración del proceso ncp_ctrl, $NCHOME/etc/precision/CtrlServices.cfg.

Inicio y detención de procesos

Puede iniciar y detener los procesos individuales de forma manual o automática.

Acerca de esta tarea

Configuración de procesos gestionados

Puede configurar procesos gestionados, iniciados automáticamente por el proceso **ncp_ctrl**, editando el archivo $NCHOME/etc/precision/CtrlServices.cfg e iniciando o reiniciando ncp_ctrl. Puede elegir qué procesos se inician de este modo, y puede cambiar los parámetros de línea de mandatos.

Acerca de esta tarea

Los cambios entrarán en vigor cuando el proceso **ncp_ctrl** se detenga y se reinicie. Los cambios también se mantendrán si ncp_ctrl se detiene o se reinicia más adelante. Por este motivo, el inicio de procesos gestionados utilizando $NCHOME/etc/precision/CtrlServices.cfg tal como se describe aquí es más sólido que realizar las inserciones directamente en la tabla de base de datos services.inTray.

Es posible que sólo desee utilizar un subconjunto de las funciones de Network Manager. Por ejemplo, es posible que desee utilizar Network Manager para descubrir la red y visualizar la topología únicamente. En este caso, puede configurar el proceso **ncp_ctrl** para que no inicie los procesos que supervisan la red y ejecutan análisis de causa raíz en sucesos de red.

Para configurar los procesos que se iniciarán de forma automática, lleve a cabo los siguiente pasos:

Procedimiento

1. Haga una copia de seguridad del archivo $NCHOME/etc/precision/CtrlServices.cfg.
2. Guarde una copia del archivo CtrlServices.cfg con el nombre de dominio incluido en nombre de archivo; por ejemplo, CtrlServices.NCOMS.cfg.
3. Edite el archivo CtrlServices.MASTER.cfg. Por ejemplo, si desea descubrir la red y visualizar únicamente la topología, debe suprimir o comentar las entradas de los procesos **ncp_g_event**, **ncp_poller** y **ncp_virtualdomain** del archivo CtrlServices.NCOMS.cfg.
4. Realice cambios en los parámetros de línea de mandatos que desee utilizar para iniciar los procesos.
5. Inicie el proceso **ncp_ctrl** en el dominio NCOMS.

Resultados

El proceso **ncp_ctrl** inicia ahora el conjunto limitado de procesos en el dominio NCOMS en el orden que haya especificado.

Ejemplo Inicio de Network Manager solo con las funciones de descubrimiento y visualización

En este ejemplo se muestra cómo configurar el controlador de proceso maestro para iniciar solo los procesos que ejecutan y admiten la visualización y el descubrimiento de redes.

Para asegurarse de que los procesos de gestión de sucesos no se inicien en el servidor actual, debe eliminar las sentencias de inserción relacionadas con los procesos ncp_g_event, ncp_poller y ncp_virtualdomain del archivo CtrlServices.DOMAIN.cfg.

Nota: El analizador de Tivoli Netcool/OMNIbus, nco_p_ncpmonitor, debe dejarse en el archivo CtrlServices.DOMAIN.cfg, ya que se utilizará para pasar los sucesos de estado de Network Manager a ObjectServer.

En el caso del proceso ncp_g_event, las líneas que deben eliminarse son similares a esta:

```
insert into services.inTray
(
    serviceName,
    binaryName,
    servicePath,
    domainName,
    argList,
    dependsOn,
```

```
    retryCount
)
values
(
    "ncp_g_event",
    "ncp_g_event",
    "$NCHOME/precision/platform/$PLATFORM/bin",
    "DOMAIN",
    [ "-domain" , "DOMAIN", "-latency", "60000" , "-debug", "0", "-messagelevel",
 "warn" ],
    [ "ncp_model" ],
    5
);
```

Inicio de procesos no administrados

Puede iniciar un proceso como no gestionado realizando una inserción OQL en la tabla `services.inTray`.

Acerca de esta tarea

Los cambios se perderán si el proceso **ncp_ctrl** se detiene y se reinicia.

Para iniciar un proceso no gestionado:

Procedimiento

1. Compruebe que el proceso **ncp_ctrl** está en ejecución.
2. Inicie sesión en las bases de datos de control del proceso.
3. Emita un mandato similar a este:

```
insert into services.unmanaged
(
        serviceName, servicePath, argList
)
values
(
        "user_script",
        "/opt/netcool/precision/solaris2/scripts/",
        [ ]
);
```

Resultados

La inserción anterior inicia un script denominado user_script, ubicado en el directorio $NCHOME/`precision/scripts`.

Detención de procesos gestionados

Puede detener un proceso gestionado que se esté ejecutando si elimina el registro en la tabla services.inTray.

Acerca de esta tarea

Si detiene un proceso gestionado de cualquier modo que no sea suprimiendo su entrada en la tabla services.inTray, ncp_ctrl lo reiniciará. Si suprime un registro de la tabla services.inTray, el proceso se reinicia sólo si se reinicia el proceso **ncp_ctrl**.

Para detener un proceso gestionado:

Procedimiento

1. Compruebe que el proceso **ncp_ctrl** está en ejecución.
2. Inicie sesión en las bases de datos de control del proceso.

3. Emita un mandato similar a este:

```
delete from services.inTray
where serviceName = 'ncp_model' ;
go
```

Nota: La detención del proceso ncp_disco de este modo no detiene el descubrimiento de forma inmediata si está ocupado. La detención del proceso ncp_disco de manera forzada puede dañar el descubrimiento.

Ejecución de procesos de forma remota

Si desea que los procesos de Network Manager de un servidor los gestione **ncp_ctrl** en otro servidor, debe configurar ambas instancias de **ncp_ctrl**.

Procedimiento

1. Instale Network Manager en ambos servidores.
2. Configure Really Small Message Broker para permitir la comunicación entre el servidor maestro y el servidor esclavo.
3. En el servidor maestro, configure el archivo `CtrlServices.`*`DOMAIN`*`.cfg`.
   a) Realice copia de seguridad y edite el archivo `CtrlServices.`*`DOMAIN`*`.cfg`.
   b) Para cada uno de los procesos que desee ejecutar en el servidor remoto, establezca el parámetro **hostName** para el nombre host del servidor remoto. Asegúrese de que el nombre host es el nombre que se definió en el servidor remoto.

   El siguiente ejemplo configura el proceso **ncp_store** para que se ejecute en el servidor remoto denominado example.com en el dominio TARA.

```
insert into services.inTray
(
    serviceName,
    binaryName,
    servicePath,
    domainName,
    hostName,
    argList,
    retryCount
)
values
(
    "ncp_store",
    "ncp_store",
    "/opt/IBM/netcool/core/precision/platform/linux2x86/bin",
    "TARA",
    "example.com",
    [ "-domain" , "<DOMAIN>" , "-latency" , "100000", "-debug", "0" ],
    5
);
```

4. En el servidor remoto, asegúrese de que el archivo `CtrlServices.`*`DOMAIN`*`.cfg` esté vacío de contenido. A continuación, inicie el proceso **ncp_ctrl** en el servidor remoto en modo esclavo. El ejemplo siguiente inicia el proceso **ncp_ctrl** en modo esclavo en el dominio TARA.

```
ncp_ctrl -domain TARA -slave
```

5. Inicie el proceso **ncp_ctrl** en el servidor local en modalidad maestro utilizando las opciones de línea de mandatos normal. El siguiente ejemplo inicia el proceso ncp_ctrl en modalidad maestro en el dominio TARA.

```
ncp_ctrl -domain TARA
```

Resultados

Los procesos que configuró para que se ejecutaran en el servidor maestro se han iniciado y los controla el proceso **ncp_ctrl** en el servidor maestro. El proceso **ncp_ctrl** que está en el servidor maestro también se inicia y controla cualquier proceso que esté configurado para gestionar en el servidor maestro.

Capítulo 3. Administración de registros

Network Manager proporciona funciones de registro para sus componentes de interfaz gráfica de usuario y procesos back-end. Puede configurar el registro de Network Manager para generar archivos de registro o rastreo que puede utilizar para resolver problemas.

Tareas relacionadas

Resolución de problemas de Network Manager

Consulte estas notas de resolución de problemas para ayudarse a determinar la causa del problema y cómo solucionarlo.

Configuración de registros para GUI

Puede configurar Network Manager para crear archivos de registro o de rastreo que se pueden utilizar para resolver problemas de GUI. También puede ajustar el nivel de registro de cada componente, así como el tamaño máximo y el número de archivos de registro que guarda el sistema.

Descripción general del archivo de registro del componente de GUI

Los mensajes de registro generados por los componentes de la GUI de Network Manager se escriben en archivos de registro y de rastreo.

- Los archivos de registro proporcionan información de registro en un formato estándar que es compatible con el formato Common Base (CBE) de IBM®. Los mensajes en formato CBE se pueden utilizar en IBM Support Assistant Log Analyzer para análisis fuera de línea.

  Nota: IBM Support Assistant Log Analyzer no se suministra como parte de IBM Tivoli Network Manager IP Edition. Debe descargarlo e instalarlo por separado.
- Los archivo de rastreo capturan todos los mensajes que contiene un archivo de registro y también detalles técnicos adicionales de operación. Los archivos de rastreo están pensados para ayudar en la resolución de problemas y son útiles para proporcionarlos a su contacto del servicio de soporte de IBM si se lo solicita.

Formato del mensaje de registro

Los mensajes de registro de la GUI se registran en formato de texto del siguiente modo:

```
[<date>T<time>]:<severity>:<message_code_id>:[<thread_id>]:<message>
```

Por ejemplo:

```
[2010-09-02T04:50:57]:INFO:HNMOB0001I:[Deferrable Alarm : 0]:Initialising
Discovery GUI Server
```

Fecha y hora
La fecha y la hora están en formato ISO 8601.

Gravedad
Están disponibles los siguientes niveles de gravedad:

- `CONFIG`:

  Registra todos los sucesos hasta incluir los cambios de configuración.
- `INFO`:

  Registra únicamente los cambios al estado del sistema. Este es el valor predeterminado.
- `WARNING`:

  Registra errores del sistema recuperables.
- `SEVERE`:

  Registra errores del sistema irrecuperables.

ID de código de mensaje
El código de mensaje proporciona más información sobre el componente del sistema del que se origina el mensaje.

Tabla 3. IDs de códigos de mensajes

ID de código de mensaje	componente de GUI
HNM T *letra*	Componentes de visualización de topología
HNM T A	Cliente de topologías
HNM T B	Servidor de topologías
HNM T C	Topología común
HNM N *letra*	Componentes GUI de MIB:
HNM N A	Navegador MIB
HNM N B	Generador de grafos MIB
HNM O *letra*	Componentes GUI de descubrimiento:
HNM O A	GUI de configuración de descubrimiento
HNM O B	Base de datos de gestión (anteriormente llamada OQL Workbench)
HNM P *letra*	Componentes GUI de sondeo de red:
HNM P A	Configuración de sondeo de red (políticas de sondeo y definiciones)
HNM S *letra*	Componentes de vistas de estructuras:
HNM S A	Explorador de estructura
HNM X *letra*	Componentes GUI comunes:
HNM X A	interfaz OQL
HNM X B	Otros componentes, como: Herramientas, Generador de filtros, Widgets, Búsqueda de entidades, Expresiones, Tabla de árboles.
HNM Z *letra*	Interfaces de producto externas:
HNM Z A	GUI web de Tivoli Netcool/OMNIbus

ID del subproceso
El ID de subproceso indica la tarea asociada con la función de la que se origina el mensaje.

Mensaje
El propio mensaje de registro que ofrece una descripción del suceso que se está registrando.

Formato del mensaje de seguimiento

Los mensajes de seguimiento proporcionan detalles más granulares sobre la operación en el siguiente formato:

```
<date> <component_id>\n
<severity>: <message>
```

Por ejemplo:

```
Aug 24, 2010 3:34:30 AM com.micromuse.precision.disco.server.DiscoConfigLogger
FINE: Received unknown request from the network
```

Los registros de seguimiento no ofrecen un formato de mensaje estandarizado ya que están más pensados para utilizarlos en la resolución de problemas. Los niveles de gravedad disponibles para los mensajes de seguimiento son los siguientes:

- `FINE`:

  Nivel mínimo de rastreo. La mayoría de los rastreos de pila aparecen ya en este nivel y están escritos en el archivo de rastreo. El archivo de rastreo también incluye todos los mensajes de registro.
- `FINER`:

  Nivel medio de rastreo que proporciona mensajes de depuración más detallados.
- `FINEST`:

  Nivel máximo de rastreo que produce información técnica muy detallada.

Tareas relacionadas

Cambio del nivel de registro de las interfaces gráficas de usuario
Puede ajustar el nivel de los archivos de registro de detalle para los componentes de GUI en conjunto o especificar niveles sobre una base más granular para segmentos de aplicación de GUI específicos.

Ubicación de archivos de registro de GUI

Todos los archivos de registro generados por componentes de interfaz gráfica de usuario se guardan en el directorio `$NMGUI_HOME/profile/logs/tnm/`.

Acerca de esta tarea

El nombre predeterminado del archivo de registro o de seguimiento es `ncp_`*`nombre_componente`*`.`*`número`*`.log` o `ncp_`*`nombre_componente`*`.`*`número`*`.trace`, respectivamente.

Para ubicar el archivo de registro de un componente:

Procedimiento

1. Vaya a `$NMGUI_HOME/profile/logs/tnm/`.
2. Localice los archivos de registro y de rastreo que correspondan al componente de GUI cuyos mensajes de registro desea comprobar y abra el archivo.

Tabla 4. Correlación de archivos de registro de componentes de GUI

componente de GUI	Propiedades de registro establecidas en archivo	nombre de archivo .log y .trace
GUI de estado de descubrimiento	`discoconfig.properties`	`ncp_disco.0.log` `ncp_disco.0.trace`
GUI de configuración del descubrimiento	`discoconfig.properties`	`ncp_guiconfig.0.log` `ncp_guiconfig.0.trace`
Acceso a la base de datos de gestión (anteriormente llamada OQL Workbench)	`nmdb.properties`	`ncp_nmdb.0.log` `ncp_nmdb.0.trace`

Tabla 4. Correlación de archivos de registro de componentes de GUI (continuación)		
componente de GUI	**Propiedades de registro establecidas en archivo**	**nombre de archivo .log y .trace**
GUI de sondeo de red (políticas de sondeo y definiciones)	`monitorconfig.properties`	`ncp_monitor.0.log` `ncp_monitor.0.trace`
Gráfico de MIB de SNMP **Navegador de MIB de SNMP**	`itnmgraph.properties`	`ncp_mib.0.log` `ncp_mib.0.trace`
Navegador de estructura	`structurebrowser.properties`	`ncp_structureview.0.log` `ncp_structureview.0.trace`
GUI de visualización de topología: • **Vistas de red** • **Vista de saltos de red** • **GUI de las vistas de vías de acceso** • **GUI de Administración de la vista de vía de acceso**	`topoviz.properties`	`ncp_topoviz.0.log` `ncp_topoviz.0.trace`
Valores generales incluidas las propiedades de la base de datos para los componentes de la GUI	`tnm.properties` **Nota:** No se debe confundir con el archivo de registro del mismo nombre, ubicado en `$NMGUI_HOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties`. Este último archivo se utiliza por el motor de sondeo, `ncp_poller`, para activar actualizaciones en las vistas de red para que el ámbito de la política de sondeo se mantenga actualizado.	`ncp_guiconfig.0.log` `ncp_guiconfig.0.trace`

Nota: Cuando el archivo de registro alcance el límite de tamaño máximo especificado, se le cambiará el nombre y se creará uno nuevo. El primer archivo de registro se denomina `ncp_`*`nombre_componente`*`.0.log`, y los mensajes de registro más recientes están siempre en este archivo. Los archivos de registro anteriores se guardan con un incremento del número (por ejemplo, `ncp_nmdb.1.log`, `ncp_nmdb.2.log`, etc.).

Cambio del nivel de registro de las interfaces gráficas de usuario

Puede ajustar el nivel de los archivos de registro de detalle para los componentes de GUI en conjunto o especificar niveles sobre una base más granular para segmentos de aplicación de GUI específicos.

Configuración del nivel de registro para componentes de la GUI

Puede configurar la cantidad de captura de archivos de registro de información para cada componente de la GUI. Los cambios se pueden realizar antes del inicio del sistema o durante el funcionamiento. Los cambios son persistentes, y no están afectados por los reinicios del sistema.

Acerca de esta tarea

Para establecer el comportamiento de registro, necesita modificar el correspondiente archivo de configuración.

Procedimiento

1. Vaya a `$NMGUI_HOMEprofile/etc/tnm/`.
2. Abra el archivo `.properties` del componente de la GUI para el que desee establecer el nivel de registro:

Opción	Descripción
discoconfig.properties	GUI de configuración de descubrimiento
itnmgraph.properties	Creación de gráficos de MIB Navegador de MIB
monitorconfig.properties	Configuración de sondeo de red (políticas de sondeo y definiciones)
nmdb.properties	Base de datos de gestión (anteriormente llamada OQL Workbench)
nm_rest.properties	API REST y consultas de SQL
structurebrowser.properties	Explorador de estructura
tnm.properties	Valores generales incluidas las propiedades de la base de datos para los componentes de la GUI
topoviz.properties	GUI de visualización de topología

3. Edite la línea *nombre*`.log.level` para establecer el nivel del mensaje:

Opción	Descripción
CONFIG	Registra todos los sucesos hasta incluir los cambios de configuración.
INFO	Registra únicamente los cambios al estado del sistema. Este es el valor predeterminado.
AVISO	Registra errores del sistema recuperables.
SEVERE	Registra errores del sistema irrecuperables.
FINE	Nivel mínimo de rastreo. La mayoría de los rastreos de pila aparecen ya en este nivel y están escritos en el archivo de rastreo. El archivo de rastreo también incluye todos los mensajes de registro. **Nota:** Al establecer el nivel de registro a FINE, FINER, FINEST, o ALL, tanto los archivos de registro como los archivos de rastreo contendrán información, y los archivos de rastreo incluirán todos los mensajes desde los archivos de registro aparte de más detalles técnicos del funcionamiento. Si se establece cualquier otro nivel de registro, los archivos de rastreo permanecerán vacíos.
FINER	Nivel medio de rastreo que proporciona mensajes de depuración más detallados.
FINEST	Nivel máximo de rastreo que produce información técnica muy detallada.

Opción	Descripción
TODOS	Habilita el registro y rastreo en todos los niveles para la aplicación.
DESAC.	Inhabilita todo el registro y el rastreo para la aplicación.

4. Guarde y cierre el archivo `.properties`.

   Nota: Los cambios tendrán efecto de forma inmediata si se realizan antes de comenzar Network Manager. Si los cambios se realizan cuando el sistema ya se está ejecutando, Network Manager leerá los archivos de configuración cada 60 segundos y aplicará cualquier cambio de forma inmediata.

Ejemplo

El ejemplo siguiente muestra la sección del archivo `structurebrowser.properties` que determina el nivel de registro:

```
structurebrowser.log.filename=ncp_structureview.%g.log
structurebrowser.log.level=INFO
structurebrowser.log.maxsize=10
structurebrowser.log.count=1

structurebrowser.trace.filename=ncp_structureview.%g.trace
structurebrowser.trace.maxsize=10
structurebrowser.trace.count=1
```

Los valores que aparecen aquí muestran el valor **INFO** predeterminado para los archivos de registro. Ello significa que los archivos de registro se rellenan con información acerca de los cambios del estado del sistema y que los archivos de rastreo permanecen vacíos.

Para cambiar el nivel de registro para que tenga todos los mensajes de registro y habilite los mensajes de rastreo, cambie **INFO** al menos a **FINE** (o FINER, o FINEST, en función del nivel de detalle que requiera en los archivos de rastreo). Esto significará que tanto los archivos de registro como los archivos de rastreo contendrán información. El ejemplo siguiente refleja este cambio:

```
structurebrowser.log.filename=ncp_structureview.%g.log
structurebrowser.log.level=FINE
structurebrowser.log.maxsize=10
structurebrowser.log.count=1

structurebrowser.trace.filename=ncp_structureview.%g.trace
structurebrowser.trace.maxsize=10
structurebrowser.trace.count=1
```

Establecimiento del nivel de registro de segmentos de aplicación

Cuando un área específica requiere una mejora en la solución de problemas, puede habilitar el registro de segmentos de aplicaciones GUI.

Antes de empezar

Póngase en contacto con el servicio de soporte de IBM para identificar qué segmentos de aplicación requieren establecer el registro para la determinación de problemas.

Nota: Estos cambios no son permanentes. Si se reinicia el sistema, todos los valores de registro de determinados segmentos de aplicación de la GUI se eliminarán. Los niveles de registro establecidos para la totalidad del componente de la GUI no se ven afectados.

Procedimiento

1. En el panel de navegación, haga clic en **Configuración** > **Consola de administración de Websphere**.
2. Haga clic en **Iniciar Consola de administración de WebSphere** para iniciar la consola del servidor de aplicaciones de WebSphere.
3. En la consola de administración, haga clic en **Resolución de problemas** > **Registros y rastreo**.

4. En la lista, haga clic en el nombre del servidor en el que se está ejecutando Network Manager.
5. Haga clic en **Cambiar niveles de detalle de registro** y, a continuación, en el separador **Tiempo de ejecución**.
6. Localice el nombre del segmento de aplicación específico desplazándose por la lista y ampliando los elementos en caso necesario.
7. Haga clic en el nombre del segmento y seleccione el nivel de registro requerido en el menú desplegable. Las opciones de nivel de registro y de rastreo son los mismos que para los componentes de la GUI.

   Nota: De forma predeterminada, cualquier configuración que se realice en el archivo `.properties` del componente de la GUI será el nivel de registro y de rastreo de todos los segmentos pertinentes de ese componente de la GUI.
8. Consulte el archivo de registro del componente de la GUI correspondiente para revisar los mensajes cargados para el segmento. Por ejemplo, consulte los archivos `ncp_disco.0.log` o `ncp_disco.0.trace` para los segmentos de la GUI de descubrimiento.

Tareas relacionadas

Ubicación de archivos de registro de GUI
Todos los archivos de registro generados por componentes de interfaz gráfica de usuario se guardan en el directorio `$NMGUI_HOME/profile/logs/tnm/`.

Establecimiento del tamaño del archivo de registro

Puede configurar el aumento de tamaño de un archivo de registro en MB y determinar el número de archivos de registro que el sistema conservará.

Acerca de esta tarea

Siga estos pasos para configurar el tamaño máximo de los archivos de registro en MB. Cuando el archivo alcance el tamaño máximo, se le cambiará el nombre y se creará uno nuevo. También puede establecer el número de archivos que se almacenarán después de que se alcance el límite de tamaño.

Procedimiento

1. Vaya a `$NMGUI_HOMEprofile/etc/tnm/` y abra el archivo `.properties` del componente GUI para que el que desea establecer el tamaño.
2. En el archivo de propiedades, lleve a cabo los siguientes pasos:
   a) Localice la línea *nombre_componente*`.log.maxsize` y establezca el tamaño máximo que puede alcanzar un archivo en MB. Por ejemplo, **`nmdb.log.maxsize = 20`** significa que el tamaño máximo permitido del archivo de registro de la base de datos de gestión es de 20 MB. El valor predeterminado es 10 MB.
   b) Localice la línea *nombre_componente*`.log.count`y establezca el número máximo de archivos que se puede almacenar. Por ejemplo, **`nmdb.log.count=2`** significa que los 2 últimos archivos de registro se mantendrán separados del que se esté escribiendo en ese momento. El valor predeterminado es 1, lo que significa que solo se guardarán el archivo actual y un archivo anterior.

      Nota: Cuando el archivo de registro alcance el límite de tamaño máximo especificado, se le cambiará el nombre y se creará uno nuevo. El primer archivo de registro se denomina `ncp_`*`nombre_componente`*`.0.log`, y los mensajes de registro más recientes están siempre en este archivo. Los archivos de registro anteriores se guardan con un incremento del número (por ejemplo, `ncp_nmdb.1.log`, `ncp_nmdb.2.log`, etc.).
3. Lleve a cabo los mismos pasos para los archivos de rastreo localizando y editando las líneas *nombre_componente*`.trace.maxsize` y *nombre_componente*`.trace.count`.
4. Guarde el archivo `.properties`.

Configuración de registros de procesos

Puede solucionar problemas con los procesos buscando información en los archivos de registro. Puede configurar Network Manager para registrar los archivos de registro o de rastreo de los procesos. También puede configurar el nivel de depuración de los procesos.

Acerca de esta tarea

Descripción general de archivos de registro de proceso

Network Manager puede crear archivos de registro y de rastreo para sus procesos.

Los archivos de registro proporcionan información acerca de sucesos importantes del proceso, tales como cambios de estado, advertencias o errores, en un formato estándar que es compatible con el formato (CBE) Common Base Event de IBM. Los archivos de registro ayudan a los administradores a supervisar sus sistemas y son útiles para proporcionarlos a su contacto del servicio de soporte de IBM si se lo solicita.

Los archivo de rastreo capturan salidas del sistema de nivel bajo y detalles técnicos. Están pensados para ayudar en la resolución de problemas y son útiles para proporcionarlos a su contacto del servicio de soporte de IBM si se lo solicita.

Los archivos de registro se pueden identificar por el sufijo .log y tienen las siguientes características:

- Los mensajes de registro tienen marcas de tiempo.
- Los mensajes de registro se clasifican por nivel; por ejemplo, error, aviso, información y depuración.
- Los mensaje de registro se formatean para ser compatibles con el formato Common Base Event de IBM.
- Los archivos de registro se pueden borrar y volver a crear para permitir la rotación de los archivos de registro.

Los archivos de registro se pueden identificar por el sufijo .trace. Puede capturar diferentes niveles de detalle, también conocidos como niveles de depuración. El nivel de depuración 4 es el más detallado. Los archivos de rastreo establecidos en los niveles de depuración más altos pueden consumir rápidamente el espacio en disco y, por lo tanto, deben utilizarse solo cuando se necesite información muy detallada para resolver un problema.

Ubicación de archivos de registro para un proceso

Ubique archivos de registro para un proceso para obtener información que pueda ser útil para resolver problemas en el proceso.

Acerca de esta tarea

El nombre predeterminado del archivo de registro es el nombre de proceso seguido por el nombre de dominio y, a continuación, la extensión de archivo `.log` o `.trace`.

Para ubicar un archivo de registro para un proceso:

Procedimiento

1. Navegue hasta la ubicación predeterminada para los archivos de rastreo y de registro de proceso, `$NCHOME/log/precision`.
2. Ubique los archivos de rastreo y de registro que corresponden con el nombre de proceso.
   Por ejemplo, una instancia del proceso **ncp_disco** en ejecución en el dominio de NCOMS genera los siguientes archivos:

   ncp_disco.*DOMINIO*.log
   ncp_disco.*DOMINIO*.trace

3. Para ver los archivos de registro de los procesos que no empiezan por `ncp_`, por ejemplo, para las bases de datos o los componentes de terceros, consulte los directorios `$NCHOME/PD/core/component_name`.

Cambio del nivel de registro para los procesos

Cambie el nivel de registro de un proceso antes de iniciar el proceso o mientras este se está ejecutando.

Cambio del nivel de registro antes de iniciar un proceso

Cambie le valor del argumento de línea de mandatos que corresponda en el archivo de configuración para cambiar el nivel de registro que utilizará un proceso cuando se inicie o se reinicie.

Acerca de esta tarea

Los argumentos de línea de mandatos –debug y –logdir se utilizan con la información de rastreo y los argumentos de línea de mandatos -messagelevel y -messagelog se utilizan con la información de registro.

El nivel de mensaje predeterminado es `warn`, que significa de forma predeterminada que los archivos de registro no contienen mensajes `info` o `debug`.

Para cambiar el nivel de registro:

Procedimiento

1. Navegue hasta el archivo `CtrlServices.cfg`. El archivo se encuentra en el siguiente directorio:

   ```
   NCHOME/etc/precision/CtrlServices.domain_name.cfg
   ```

   domain_name es el nombre del dominio para el que se va a modificar el nivel de registro.
2. En el archivo `CtrlServices.cfg`, cambie el argumento especificado en el archivo a –debug para el rastreo o –messagelevel para el registro.
   El siguiente ejemplo muestra cómo se puede configurar el proceso **ncp_webtool** en este archivo.

   ```
   insert into services.inTray
   (
       serviceName,
       binaryName,
       servicePath,
       domainName,
       argList,
       retryCount
   )
   values
   (
       "ncp_webtool",
       "ncp_webtool",
       "$PRECISION_HOME/platform/$PLATFORM/bin",
       "$PRECISION_DOMAIN",
       [ "-domain" , "$PRECISION_DOMAIN" , "-latency" , "100000", "-debug", "0",
    "-messagelevel", "warn"],
       5
   );
   ```

3. Inicie o reinicie el proceso **ncp_ctrl**.

   El proceso **ncp_ctrl** se utiliza para detener e iniciar el resto de los procesos. También puede reiniciar Network Manager mediante el mandato `itnm_start ncp`.

Cambio del nivel de registro de un proceso en ejecución

Modifique el nivel de registro de un proceso en ejecución para proporcionar archivos de registro o de seguimiento más detallados para ayudar a realizar la depuración.

Acerca de esta tarea

Puede cambiar el nivel de registro o de seguimiento (también denominado nivel de depuración) de un proceso en ejecución mediante el envío de una señal USR1 o USR2 al proceso. El envío de una señal USR1 cambia el nivel de registro y el envío de una señal USR2 cambia el nivel de seguimiento. La información adicional proporcionada por el aumento de los niveles de registro o de seguimiento puede ayudar en la depuración de un problema con un proceso.

Los archivos de rastreo tienen cinco niveles de depuración (0 a 4) cuyo ciclo puede ejecutar para ofrecer mayores niveles de detalles sobre un proceso. Por ejemplo, si un proceso se encuentra en el nivel 3, el envío de una señal USR2 aumentará el nivel al 4; si el proceso está en el nivel 4, una señal USR2 lo transferirá al nivel 0.

Los archivos de registro tienen cuatro niveles de mensaje cuyo ciclo se puede ejecutar para incrementar el nivel de detalle capturado: error, aviso, información y depuración.

El siguiente procedimiento describe cómo aumentar el nivel de seguimiento de un proceso. Para aumentar el nivel de registro de un proceso, realice el mismo procedimiento utilizando la señal USR1 en lugar de USR2.

Para aumentar el nivel de seguimiento de un proceso, realice el siguiente procedimiento:

Procedimiento

1. Localice el ID de proceso (*PID*) del proceso que va a investigar:
   a) En los sistemas operativos Unix y Linux®, especifique `ps -ef | grep ncp` en la línea de mandatos.
2. Para aumentar el nivel de depuración en un nivel:
   a) En los sistemas operativos Unix y Linux, especifique `kill -USR2` *PID* en la línea de mandatos.

Cómo evitar los errores de proceso con archivos de registro o rastreo grandes utilizando la rotación de archivos de registro

Si los archivos de registro o rastreo llegan a tener un tamaño demasiado grande, es posible que los procesos salgan inesperadamente. Si se crean demasiados archivos, puede quedarse sin espacio de disco. Configure el número y el tamaño de los archivos de rastreo y registro configurando la rotación de archivos de registro.

Puede controlar el tamaño de los archivos de registro y rastreo utilizando uno de los siguientes criterios:

- Tamaño máximo
- Hora del día

Puede configurar el número de archivos de registro configurando una agrupación de archivos, es decir, un número de archivos que se graban en una sucesión. El proceso de utilización de archivos nuevos cuando se desencadena se denomina rotación de archivo de registro. Todos los archivos de registro se pueden rotar, pero no todos los componentes tienen archivos de registro. Algunos componentes solo tienen archivos de rastreo, que se pueden rotar también.

Restricción: Sólo los procesos gestionadas por el controlador de proceso de dominio, **`ncp_ctrl`**, pueden tener los archivos de registro rotados.

Establecimiento del tamaño máximo de los archivos de registro y rastreo

Los archivos de registro o rastreo grandes pueden producir errores de proceso. El tamaño máximo predeterminado para un archivo de registro es 1 GB en los sistemas UNIX. Como cálculo orientativo para los archivos de registro, suponiendo que cada archivo de registro tenga 1 GB de tamaño y se establezcan seis procesos en el nivel de depuración completo, necesitará 24 GB de espacio de disco. (6 procesos x 4 archivos de registro o rastreo cada uno = 24 archivos de registro o rastreo x 1 GB = 24 GB).

Establezca la variable de entorno NDE_LOGFILE_MAXSIZE para determinar el tamaño máximo que puede alcanzar un archivo de registro o rastreo para un proceso. Este valor se aplica a todos los procesos de Network Manager. Cuando el archivo de registro alcanza el tamaño máximo, se utiliza el siguiente archivo de registro.

- Si se desactiva la rotación de archivos de registro para un proceso, sólo se utilizan dos archivos.
- Si se activa la rotación de archivos de registro para un proceso, se utiliza el número de archivos configurados en la agrupación.

Puede rotar los archivos de registro de acuerdo con el tamaño de archivo o la hora del día. Si se ha configurado la rotación de archivos de registro de acuerdo con la hora del día, los valores del tamaño de archivo se ignoran.

El siguiente ejemplo muestra cómo establecer el tamaño máximo de archivo de registro en 1 GB (el valor está en bytes).

```
setenv NDE_LOGFILE_MAXSIZE 1073741824
```

Nota: No establezca un tamaño máximo de menos de 1000000 (1 MB). Establezca un tamaño máximo de menos de 1000000 (1 MB) puede hacer que los procesos ncp_g_event y nco_p_monitor fallen.

Debe reiniciar los procesos de Network Manager después de cambiar las variables de entorno de rotación de archivo de registro para que los procesos utilicen las variables actualizadas.

Importante: En sistemas UNIX, asegúrese de establecer las variables de entorno de registro en los archivos de perfil de shell adecuados para la cuenta que Network Manager está ejecutando. No las establezca en el archivo `NCHOME/env.sh`, ya que este archivo no se utiliza cuando se inicia Network Manager.

Establecimiento de una hora del día para la rotación de archivos de registro

Para establecer la rotación de archivos de registro que se produce a una determinada hora del día, establezca la variable de entorno NDE_LOGFILE_ROTATION_TIME en la hora necesaria y establezca la variable de entorno NDE_LOGFILE_ROTATION_FORMAT en el formato de denominación necesario. Si establece una hora del día, este valor tiene prioridad sobre el valor de tamaño de archivo máximo.

La variable de entorno NDE_LOGFILE_ROTATION_TIME especifica la hora después de la cual se produce una rotación de archivos de registro cada día. Los archivos de registro se rotan cuando se realiza la primera grabación en el archivo después de la hora establecida por la variable de entorno NDE_LOGFILE_ROTATION_TIME. Esta variable de entorno es un entero, con un valor predeterminado de 0000.

El siguiente ejemplo especifica la rotación de archivos de registro en la primera grabación después de medianoche cada día:

```
setenv NDE_LOGFILE_ROTATION_FORMAT "%Y%m%d-%H%M"
setenv NDE_LOGFILE_ROTATION_TIME 0000
```

El siguiente ejemplo muestra cómo rotar los archivos de registro a medianoche cada día y añadir el nombre de archivo de registro antiguo con la serie de caracteres literales `"old"`

```
setenv NDE_LOGFILE_ROTATION_FORMAT \'old\'
setenv NDE_LOGFILE_ROTATION_TIME 0000
```

Restricción: Los caracteres literales deben tener como carácter de escape las comillas (' ') como se describe en http://userguide.icu-project.org/formatparse/datetime.

La variable de entorno NDE_LOGFILE_ROTATION_FORMAT configura cómo se crean los archivos de registro.

- Si NDE_LOGFILE_ROTATION_FORMAT se establece en "old" y no se ha configurado una agrupación de archivos de registro para el proceso en cuestión, se utilizan dos archivos.

- Si se configura una agrupación de archivos de registro para un proceso, se utiliza el número de archivos de la agrupación.
- Si NDE_LOGFILE_ROTATION_FORMAT se establece en un formato de indicación de fecha y hora soportado y no se ha configurado una agrupación de archivos de registro para el proceso en cuestión, se crea un nuevo archivo cada día. Si se utiliza un formato de indicación de fecha y hora sin configurar una agrupación de archivos de registro, el número ilimitado de archivos de registro puede ser ilimitado.

  Restricción: El único formato de indicación de fecha y hora soportado para el uso por parte de los procesos de Network Manager es el formato POSIX. Se soportan las opciones siguientes:

  %a
  Nombre de día de la semana abreviado, por ejemplo Jue

  %A
  Nombre de día de la semana completo, por ejemplo Jueves

  %b
  Nombre de mes abreviado, por ejemplo Ago

  %B
  Nombre de mes completo, por ejemplo Agosto

  %d
  Día del mes, rellenado con ceros, (01-31), por ejemplo 23

  %e
  Día del mes, rellenado con espacios, (1-31), por ejemplo, 23

  %h
  Equivalente a %b.

  %H
  Hora en formato de 24 horas (00-23), por ejemplo 14

  %I
  Hora en formato de 12 h (01-12), por ejemplo, 02

  %j
  Día del año (001-366), por ejemplo 235

  %m
  Mes como número decimal (01-12), por ejemplo 08

  %M
  Minuto (00-59), por ejemplo 55

  %p
  Designación AM o PM, por ejemplo PM

  %R
  Hora de 24 horas HH:MM, equivalente a %H:%M, por ejemplo 14:55

  %S
  Segundo (00-61), por ejemplo 02

  %T
  Formato de hora ISO 8601 (HH:MM:SS), equivalente a %H:%M:%S, por ejemplo 14:55:02

  %u
  Día de la semana ISO 8601 como número con lunes como 1 (1-7), por ejemplo 4

  %V
  Número de semana ISO 8601 (00-53), por ejemplo 34

  %y
  Año, dos últimos dígitos (00-99), por ejemplo 01

  %Y
  Año, por ejemplo 2001

  %Z
  Nombre de huso horario.

Por ejemplo, %Y%m%d-%H%M genera archivos de registro de rotación con el año, mes, día, hora y minuto añadidos. Un ejemplo de archivo es ncp_model.NCOMS.log_20100430-0000.

Debe reiniciar los procesos de Network Manager después de cambiar las variables de entorno de rotación de archivo de registro para que los procesos utilicen las variables actualizadas.

Importante: En sistemas UNIX, asegúrese de establecer las variables de entorno de registro en los archivos de perfil de shell adecuados para la cuenta que Network Manager está ejecutando. No las establezca en el archivo NCHOME/env.sh, ya que este archivo no se utiliza cuando se inicia Network Manager.

Configuración del número de archivos de registro creados por proceso

El número de archivos de registro creados por un proceso lo determinan para cada proceso las variables de línea de mandatos -logfileusepool y -logfilepoolsize. Si se inicia un proceso de Network Manager con la opción de línea de mandatos -logfileusepool, el proceso utiliza una agrupación de archivos de registro. El número de archivos de la agrupación lo define el valor de la opción de línea de mandatos -logfilepoolsize. Si no se especifica la opción de línea de mandatos -logfilepoolsize, se utiliza el valor predeterminado de 10. El valor mínimo de -logfilepoolsize es 2 y el valor máximo es 99.

Los archivos de registro de la agrupación se suprimen cada vez que el usuario o el sistema reinicia el proceso. Si desea mantener registros históricos, necesita para utilizar NDE_LOGFILE_ROTATION_FORMAT sin una agrupación de registros.

Importante: Si tiene muchos procesos que se han configurado para crear una agrupación de sus propios archivos de registro y rastreo, el número total de archivos de registro creados puede ser grande. Asegúrese de que tiene suficiente espacio de disco. Asegúrese de que el sistema operativo permite abrir simultáneamente suficientes archivos. En los sistemas operativos UNIX y Linux, asegúrese de que hay suficientes descriptores de archivos permitidos.

Restricción:

No inicie los procesos ncp_g_event o nco_p_ncpmonitor con la opción de línea de mandatos -logfileusepool si ha establecido la variable de entorno NDE_LOGFILE_ROTATION_FORMAT. No se soporta el uso conjunto de la agrupación de archivos de registro y de la rotación de archivos de registro temporizada para estos procesos.

Ejemplo de inicio de un proceso con la agrupación de archivos de registro especificada

El siguiente extracto de ejemplo del archivo de configuración CtrlServices.cfg configura el proceso **ncp_disco** para utilizar una agrupación de 5 archivos de registro:

```
insert into services.inTray
    (
        serviceName,
        binaryName,
        servicePath,
        domainName,
        argList,
        dependsOn,
        retryCount
    )
    values
    (
        "ncp_model",
        "ncp_model",
        "$PRECISION_HOME/platform/$PLATFORM/bin",
        "$PRECISION_DOMAIN",
        [
            "-domain" , "$PRECISION_DOMAIN", "-latency" ,
            "100000" , "-debug", "1", "-messagelevel", "debug", "-logfileusepool",
            "-logfilepoolsize", "5"
        ],
        [ "ncp_disco" ],
        1
    );
```

Qué ocurre cuando se rotan los archivos de registro

Si se configura una agrupación de archivos de registro para un proceso, la rotación de archivos de registro se produce como se indica a continuación:

1. Se crean varios archivos de registro para ese proceso cuando éste se inicia. El número de archivos que se abren lo configura el valor de la opción de línea de mandatos `-logfilepoolsize`. El proceso mantiene los archivos de registro abiertos durante el tiempo que dura la ejecución del proceso. Por el contrario, los archivos `.trace` sólo se crean cuando son necesarios y no se mantienen abiertos. Los archivos de la agrupación se denominan utilizando el formato *proceso*`[.`*dominio*`].log_ID` o *proceso*`[.`*dominio*`].trace_ID`, donde `ID` es un número de dos dígitos que empieza en 01 y tiene un rango hasta el número máximo especificado para la opción `-logfilepoolsize`.
2. Si ya existen, los primeros N archivos .log se truncan (se establecen al tamaño de cero) y los primeros N archivos `.trace` se suprimen, donde N es el número de archivos de registro especificados para la opción `-logfilepoolsize` para el proceso. Si hay más de N archivos .log o .trace, por ejemplo de un momento anterior en que el tamaño de agrupación de registros era mayor, el resto de los archivos no resultan afectados. Si desea asegurarse de que se conservan todos los archivos . log o `.trace` anteriores, cópielos en una ubicación diferente antes de iniciar o reiniciar el proceso.

   Nota: Una excepción es el proceso ncp_disco. Cuando se reinicia el proceso ncp_disco (incluido en cada descubrimiento completo), los archivos `ncp_disco.`*DOMAIN*`.log_`n anteriores se renombran añadiendo una extensión `.old` al nombre de archivo
3. Se utiliza el archivo con el menor número de archivos disponibles para el registro, independientemente de cuál sea el archivo que se ha utilizado por última vez.
4. Cuando se cumplen los criterios para la rotación de registro, el sistema de registro graba en el siguiente archivo.
5. Cuando todos los archivos de la agrupación alcanzan el tamaño máximo, el sistema de registro trunca el primer archivo de la agrupación y empieza a escribir en él de nuevo.

Si no se ha configurado una agrupación de archivos de registro, se produce la rotación de archivos de registro como se indica a continuación:

1. El proceso ncp_ctrl cambia el nombre del archivo de registro de *logfilename.log* al formato establecido por la variable de entorno NDE_LOGFILE_ROTATION_FORMAT o a *logfilename.log_old* si no se ha establecido la variable de entorno NDE_LOGFILE_ROTATION_FORMAT.
2. El proceso ncp_ctrl genera un nuevo archivo de registro denominado *logfilename.log*.
3. Cuando el nuevo archivo *logfilename.log* alcanza el tamaño máximo, el proceso ncp_ctrl sobrescribe *logfilename.log_old*.

Capítulo 4. Administración de puertos

Si hay conflictos con los puertos que están en uso en su sistema, cambie algunos de los puertos predeterminados.

Acerca de esta tarea

Si está desplegando Network Manager en un entorno seguro, puede que necesite saber qué puertos utilizan distintos procesos para configurar un cortafuegos u otra aplicación de seguridad.

Nota: Al acceder a un ObjectServer de Tivoli Netcool/OMNIbus protegido por un cortafuegos, debe especificar un puerto IDUC y proporcionar acceso a ese puerto utilizando el cortafuegos.Para obtener más información sobre cómo especificar un puerto IDUC para ObjectServer, consulte *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Acerca de la comunicación entre procesos

Los procesos de Network Manager se comunican a través de conexiones TCP, multidifusión y Really Small Message Broker.

Acerca de Really Small Message Broker

La comunicación entre los componentes principales de Network Manager se gestiona mediante Really Small Message Broker. Para asegurar el correcto funcionamiento de Network Manager, Really Small Message Broker debe estar en ejecución en todo momento.

Varios componentes principales de Network Manager pasan información a otros componentes del mismo servidor, y a cualquier componente principal de Network Manager en servidores distintos.

Esta comunicación se gestiona mediante Really Small Message Broker.

Really Small Message Broker se instala e inicia automáticamente mediante el proceso de instalación de Network Manager.

Si detiene Really Small Message Broker mientras los procesos principales de Network Manager como el Motor de descubrimiento, ncp_disco, están en ejecución, los procesos principales reiniciarán Really Small Message Broker automáticamente.

Nota: La ejecución de varios dominios en paralelo puede sobrecargar el intermediario de mensajes en algunos sistemas. Si desea ejecutar varios dominios bajo carga en paralelo, es una buena idea ejecutar un intermediario de mensajes separado para cada dominio.

Tareas relacionadas

Ejecución de un intermediario de mensajes independiente para cada dominio
Si desea ejecutar varios dominios bajo carga en paralelo, es una buena idea ejecutar un intermediario de mensajes separado para cada dominio.

Acerca de multidifusión

Los procesos que utilizan la comunicación TCP directa utilizan en primer lugar la multidifusión para localizarse entre ellos y, después, para configurar sockets TCP.

Cambio de los valores del host y del puerto para Really Small Message Broker

Puede cambiar los valores del host y del puerto para Really Small Message Broker modificando el archivo de configuración de Really Small Message Broker y, a continuación, deteniendo el intermediario.

Actualización del archivo de configuración de Really Small Message Broker

Puede configurar el host y el puerto para Really Small Message Broker.

Antes de empezar

Antes de actualizar el archivo de configuración deReally Small Message Broker (`precision.broker.cfg`), debe detener todos los procesos ncp.

Acerca de esta tarea

Para configurar el host y el puerto para Really Small Message Broker, complete los pasos siguientes en cada servidor donde están instalados los componentes principales de Network Manager.

Procedimiento

1. Asegúrese de que se han detenido todos los procesos ncp.
2. Suprima el siguiente archivo:

   ```
   $NCHOME/etc/precision/broker_1883.cfg
   ```

   Importante: `Broker_1883.cfg` se genera automáticamente desde `precision.broker.cfg` cuando se inicia Really Small Message Broker. Si este archivo no se suprime antes de que se edite el archivo Really Small Message Broker, se puede producir una discordancia entre las dos versiones del archivo. Esto puede impedir que se inicia Network Manager.
3. Edite el archivo siguiente:

   ```
   $NCHOME/etc/precision/Precision.broker.cfg
   ```
4. Localice la siguiente sección en el archivo:

   ```
   broker session =
     {
       'service' = '1883',
       'network' = '127.0.0.1'
     };
   ```

   Nota: Los valores de `broker session` utilizan la dirección IP de la interfaz de bucle de retorno. Esto le garantiza que sólo puede acceder el intermediario del servidor local. Si desea permitir conexiones externas debe enlazarlas a la dirección IP del servidor. Tenga en cuenta que permitir conexiones externas al intermediario puede constituir un riesgo de seguridad.
5. Cambie el valor de `'service'` para el puerto que desea utilizar. Asegúrese de que no entre en conflicto con ningún otro puerto del sistema.
6. Cambie el valor de `'network'` a la dirección del servidor actual.
7. Guarde y cierre el archivo.

Detención de Really Small Message Broker

Una vez que ha cambiado el archivo de configuración de Really Small Message Broker, debe detenerReally Small Message Broker para que sus cambios surtan efecto.

Acerca de esta tarea

Para detener Really Small Message Broker, ejecute el siguiente script.

```
$NCHOME/precision/scripts/perl/scripts/stop_broker.pl
```

Los procesos principales de Network Manager que se están ejecutando como el motor de descubrimiento, ncp_disco reiniciará Really Small Message Broker automáticamente. La nueva instancia de Really Small Message Broker recogerá los cambios de configuración.

Ejecución de un intermediario de mensajes independiente para cada dominio

Si desea ejecutar varios dominios bajo carga en paralelo, es una buena idea ejecutar un intermediario de mensajes separado para cada dominio.

Acerca de esta tarea

Para ejecutar un intermediario de mensajes independiente para cada dominio, haga lo siguiente.

Procedimiento

1. Asegúrese de que se han detenido todos los procesos ncp.
2. Cree un archivo de configuración `Precision.broker.cfg` específico de dominio.

   Para ello, copie el siguiente archivo:`$NCHOME/etc/precision/Precision.broker.cfg` en una copia específica de dominio: `$NCHOME/etc/precision/Precision.broker.`*DOMAIN_NAME*`.cfg`

   Donde *DOMAIN_NAME* es el nombre de uno de sus dominios.
3. Localice la siguiente sección en el archivo:

```
broker session =
  {
    'service' = '1883',
    'network' = '127.0.0.1'
  };
```

4. Cambie el valor de `'service'` para el puerto que desea utilizar. Asegúrese de que no entre en conflicto con ningún otro puerto del sistema.
5. Guarde y cierre el archivo.
6. Repita los pasos “2” en la página 43 a “5” en la página 43 para crear un intermediario de mensajes independiente para cada uno de los dominios.
7. Reinicie todos los procesos ncp.

Comprobación de uso de los puertos

Puede comprobar qué puertos están en uso en el servidor actual, para investigar o prevenir conflictos en el puerto.

Acerca de esta tarea

Para comprobar qué puertos están en uso en el servidor actual, escriba el siguiente mandato:

```
netstat -a
```

El mandato devuelve una lista de daemons de escucha y las conexiones establecidas.

Definición de un puerto TCP fijo

Para los procesos que utilizan conexiones basadas en socket TCP, puede definir un puerto fijo en lugar de utilizar el puerto predeterminado asignado de forma aleatoria.

Acerca de esta tarea

Para evitar problemas de cortafuegos o conflictos de puertos, es posible que tenga que definir un puerto TCP específico para un proceso. Por ejemplo, puede que tenga que realizar esto si los ayudantes y el servidor ayudante `ncp_d_helpserv`, se están ejecutando en un host distinto al del motor de descubrimiento, `ncp_disco`, y los hosts están detrás de un cortafuegos. También puede necesitar definir un puerto TCP fijo como parte de una configuración de migración tras error. Para obtener más información

sobre cómo definir un puerto TCP fijo específicamente para una migración tras error, consulte *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Para definir un puerto TCP fijo, lleve a cabo los siguientes pasos:

Procedimiento

1. Inicie el proceso en el primer servidor.
2. Realice una copia de seguridad del archivo `ServiceData.cfg`.
3. Edite el archivo `ServiceData.cfg` y copie la línea correspondiente al proceso para el que desee definir un puerto.

   La línea existente podría ser similar a la de este ejemplo:

   ```
   -SERVICE: Helper DOMAIN: DEMO ADDRESS: 192.168.31.8 PORT: 51153
   SERVERNAME: britanicus DYNAMIC: SÍ
   ```

   En este ejemplo, `DYNAMIC: YES` muestra que el puerto del Servidor ayudante se ha asignado de forma dinámica.
4. Cambie el valor `PORT` al valor requerido.
5. Cambie la cadena `DYNAMIC:YES` a `DYNAMIC:NO`. Esto obligará al proceso a utilizar la misma dirección y puerto la próxima vez que se inicie.
6. Guarde el archivo `ServiceData.cfg`.
7. En el segundo servidor, realice una copia de seguridad del archivo `ServiceData.cfg`.
8. Copie la línea que corresponda del archivo `ServiceData.cfg` en el primer servidor al archivo `ServiceData.cfg` en el segundo servidor.
9. Guarde el archivo `ServiceData.cfg`.

Definición de una dirección de multidifusión fija

Puede definir qué dirección y puerto utilizarán los procesos para las comunicaciones multidifusión editando el archivo de configuración `ServiceData.cfg`.

Acerca de esta tarea

Si un proceso Network Manager necesita saber en qué otro puerto se está ejecutando otro proceso, buscará el puerto TCP/IP definido en ese proceso en el archivo `ServiceData.cfg`. Si no hay un puerto definido para un servicio específico, el proceso emitirá una solicitud de dirección mediante multidifusión. Podrá definir la dirección que se utilizará en esta solicitud de dirección de multidifusión.

La dirección de multidifusión debe ser la misma en todos los servidores que tengan procesos Network Manager que se comuniquen entre sí.

Para definir la dirección para la comunicación multidifusión, lleve a cabo los siguientes pasos.

Procedimiento

1. Haga una copia de seguridad y edite el archivo `ServiceData.cfg`.
2. Edite la línea que contiene `SERVICE: MulticastService`. Establezca las variables ADDRESS y PORT.
3. Establezca `DOMAIN` en `ANY_PRECISION_DOMAIN`. Esto significa que el servicio utilizará la misma dirección de multidifusión para todos los dominios en los que se ejecute.
   La línea debe ser similar a la de este ejemplo:

   ```
   SERVICE: MulticastService DOMAIN: ANY_PRECISION_DOMAIN
   ADDRESS: 224.0.0.108 PORT: 33000
   ```
4. Guarde y cierre el archivo `ServiceData.cfg`.

Lista de puertos utilizados por el producto

Network Manager utiliza diferentes puertos de comunicación: algunos fijos, algunos definidos por archivos de configuración y otros asignados por el sistema operativo.

La siguiente tabla describe los puertos predeterminados que utiliza Network Manager.

Tabla 5. Puertos predeterminados utilizados por Network Manager

Puerto	Protocolo	Descripción
22	SSH a través de TCP/IP	Si se habilita el soporte de SSH, el ayudante de telnet utiliza este puerto para comunicarse con dispositivos de red.
23	Telnet a través de TCP / IP	Si no se habilita el soporte de SSH, el ayudante de telnet utiliza este puerto para comunicarse con dispositivos de red.
161	SNMP	El puerto 161 es el puerto predeterminado de los dispositivos de red a los que se envían consultas SNMP durante los procesos de descubrimiento y supervisión. Se encuentra definido en la columna m_SnmpPort de la tabla de base de datos snmpStack.verSecurityTable.
162	UDP	Puerto de condición de excepción predeterminado. Utilizado por el agente de sondeo de condiciones de excepción. Si varios procesos o aplicaciones necesitan acceder a este puerto, el multiplexor de condiciones de excepción SNMP, ncp_trapmux, se puede utilizar para reenviar condiciones de excepción. El multiplexor de condiciones de excepción SNMP, el agente de descubrimiento de condiciones de excepción y el agente de sondeo de condiciones de excepción se pueden configurar para utilizar un puerto distinto cada uno de ellos.
1883	Transporte de telemetría s de colas de mensajes (MQTT)	Puerto predeterminado que utiliza Really Small Message Broker con las comunicaciones entre procesos.
4100	TCP/IP	Puerto predeterminado de ObjectServer. Debe especificarse en el momento de la instalación. Se define en `interfaces.`*`Arch`* en la estación de trabajo de ObjectServer. Este puerto lo utiliza el proceso `ncp_g_event` para comunicarse con ObjectServer.
7968	TCP/IP	Puerto predeterminado de acceso al servidor de Network Manager desde Dashboard Application Services Hub. Lo utiliza la GUI de configuración de descubrimiento y se define en el archivo de configuración `ServiceData.cfg`. Si desea cambiar este puerto, edite el archivo de configuración `ServiceData.cfg` y reinicie los procesos ncp_model y ncp_config mediante CTRL.
16310	HTTP	Puerto predeterminado de Dashboard Application Services Hub. Dashboard Application Services Hub Asigna los siguientes trece puertos a partir el puerto especificado para Dashboard Application Services Hub durante la instalación para su propio uso. De forma predeterminada, este puerto redirige a 16316.
16311	HTTPS	Puerto seguro predeterminado de Dashboard Application Services Hub.

Tabla 5. Puertos predeterminados utilizados por Network Manager (continuación)		
Puerto	**Protocolo**	**Descripción**
33000	TCP/IP	De forma predeterminada, la dirección IP multidifusión 225.13.13.13 y el puerto 33000 se utilizan para habilitar los ayudantes de descubrimiento y los agentes de descubrimiento para ubicar el servidor ayudante. Esta dirección de multidifusión se especifica en el archivo `$NCHOME/etc/precision/ServiceData.cfg`. Cuando un proceso ha ubicado el servidor ayudante, se establece una conexión TCP en un puerto asignado por el sistema operativo.
50000	TCP/IP	Puerto de bases de datos Db2 predeterminado.
Asignado por SO	TCP/IP	Los puertos TCP son asignados por el sistema operativo para la comunicación TCP entre procesos; por ejemplo, la comunicación entre los agentes de descubrimiento y el servidor de ayuda. Si esto es un problema, debe asegurarse de que su cortafuegos sea externo al servidor Network Manager y que todos los procesos de descubrimiento se ejecuten en el mismo host.
1521	TCP/IP	Puerto predeterminado de bases de datos Oracle

archivo de configuración de ServiceData

El archivo de configuración `ServiceData` es un archivo dinámico que lista información de conexión TCP y de multidifusión para procesos de Network Manager.

Al inicio, cada servicio de Network Manager (es decir, componente o proceso) que utiliza un socket TCP agrega una línea al archivo de configuración de ServiceData. Esta línea contiene información acerca del servicio. La información siguiente se adjunta al archivo de configuración:

- El nombre del servicio
- El dominio del servicio
- La dirección IP del servicio
- El número de puerto del servicio
- El servidor en el que el proceso se ejecuta

En el siguiente archivo de configuración de ejemplo, el primer servicio llamado MulticastService muestra el número de puerto y la dirección de multidifusión. El segundo servicio muestra que el servicio del Ayudante se ejecuta en el dominio DEMO e incluye información acerca de la dirección IP, el número de puerto y el nombre del servidor donde se está ejecutando el servicio del Ayudante. DYNAMIC: YES significa que el puerto está asignado por el sistema operativo cada vez que se inicia el proceso. DYNAMIC: NO define un puerto fijo.

```
--
-- Server data file - contains info on servers and the general multicast
-- address to use.
--
SERVICE: MulticastService DOMAIN: ANY_PRECISION_DOMAIN ADDRESS: 225.13.13.13
PORT: 33000

SERVICE: Helper DOMAIN: DEMO ADDRESS: 192.168.31.8 PORT: 51153
SERVERNAME: britanicus DYNAMIC: SÍ
```

Capítulo 5. Administración de usuarios

Utilice las funciones de la consola web para proporcionar acceso a las interfaces basadas en web para usuarios, según los grupos de usuarios y los roles de usuarios predeterminados. Los usuarios y los perfiles para el Proveedor de servicios de OQL se gestionan de forma separada.

Acerca de esta tarea

Las interfaces de usuario se pueden categorizar del siguiente modo:

Aplicaciones web
Network Manager incluye las siguientes aplicaciones web:

- GUI de descubrimiento de red
- GUI de sondeo de red
- Vista de saltos Topoviz
- Vistas de red Topoviz
- Navegador de MIB de SNMP
- Navegador de estructura

Para añadir y gestionar usuarios, consulte la información sobre *Gestión de usuarios y grupos de Jazz for Service* en Jazz for Service Management IBM Knowledge Center at https://www.ibm.com/support/knowledgecenter/SSEKCU.

Proveedor de servicios de OQL
La autenticación de usuario para el proveedor de servicios OQL se gestiona aparte de los usuarios de las aplicaciones web. Consulte *Configuración de la autenticación del Proveedor de servicios de OQL* en *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Usuarios predeterminados

Se suministran varios usuarios con Network Manager.

Usuarios y sus grupos

La siguiente tabla describe a los usuarios que están presentes después de la instalación, junto con sus grupos.

Tabla 6. Usuarios presentes después de la instalación

Nombre de usuario	Grupo	Contraseña	Descripción
`smadmin`	Ninguno	Definido durante la instalación. El valor predeterminado de una instalación básica es netcool. El administrador debe cambiar esta contraseña.	El administrador de Dashboard Application Services Hub. En una instalación nueva, este usuario tiene permisos para administrar usuarios, grupos, roles y páginas. Definido en el repositorio de usuarios basado en archivos.

Tabla 6. Usuarios presentes después de la instalación (continuación)			
Nombre de usuario	**Grupo**	**Contraseña**	**Descripción**
`itnmadmin`	Network_Manager_IP_Admin	Definido durante la instalación.	El administrador de Network Manager. En una instalación nueva, este usuario tiene permisos para administrar todas las aplicaciones web de Network Manager. Definido en el repositorio de usuarios elegido durante la instalación. Este usuario tiene también los siguientes roles Dashboard Application Services Hub de forma predeterminada. • administrador • chartAdministrator • chartCreator
`itnmuser`	Network_Manager_User	Definido durante la instalación.	Un usuario operador de ejemplo de Network Manager. Definido en el repositorio de usuarios elegido durante la instalación.

Roles de usuario de Network Manager

Network Manager define un número de roles predeterminados, que proporcionan a los usuarios la capacidad de realizar un conjunto de actividades predefinidas dentro de las aplicaciones web.

El acceso a las aplicaciones web y a las funciones dentro de las aplicaciones web depende de los roles asignados a los usuarios. Los roles de Network Manager se asignan, por lo general, a los usuarios mediante grupos. Los usuarios también pueden tener roles asignados a ellos desde otros productos. Después de que el administrador añada o elimine los roles, la función revisada no estará disponible para otros usuarios hasta que no cierren la sesión y vuelvan a iniciarla en Dashboard Application Services Hub.

Nota: Para obtener información sobre los roles de usuario que están definidos por Cognos Analytics, visite el Knowledge Center de Cognos Analytics en la siguiente dirección web: https://www.ibm.com/support/knowledgecenter/SSEP7J.

La tabla siguiente muestra todos los roles predeterminados que se definen en Network Manager.

Tabla 7. Roles de usuario de Network Manager		
Rol	**Asignado al grupo**	**Descripción**
`ncp_bookmark_admin`	`Network_Manager_IP_Admin`	El usuario puede modificar los permisos de los marcadores de vista de red.
`ncp_config`	`Network_Manager_IP_Admin`	El usuario puede guardar los cambios de configuración que haya realizado.

Tabla 7. Roles de usuario de Network Manager (continuación)

Rol	Asignado al grupo	Descripción
ncp_config_editor	Network_Manager_IP_Admin	El usuario puede editar los siguientes widgets. Configuración del descubrimiento de red Configuración del acceso a la base de datos NCIM
ncp_disco_config	Network_Manager_IP_Admin	El usuario puede ver y editar los valores de configuración de descubrimiento.
ncp_disco_config_alter_domain	Network_Manager_IP_Admin	El usuario puede cambiar el dominio para el que va a configurar un descubrimiento.
ncp_disco_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Estado del descubrimiento de red.
ncp_disco_status	Network_Manager_IP_Admin	El usuario puede ver el estado de un descubrimiento durante su ejecución.
ncp_disco_status_control	Network_Manager_IP_Admin	El usuario puede iniciar o detener el descubrimiento o ejecutar un descubrimiento con la misma configuración. Este rol no tiene ningún efecto sin el rol de Network Manager IP Discovery Status.
ncp_disco_status_alter_domain	Network_Manager_IP_Admin	El usuario puede cambiar el dominio del que obtiene el estado de descubrimiento. **Nota:** No elimine este rol de los administradores de descubrimientos.
ncp_event_analytics	No asignado a un grupo de forma predeterminada	Habilita las herramientas de Event Analytics que se activan con el botón derecho en los dispositivos del gráfico de topología.
ncp_gis	No asignado a un grupo de forma predeterminada	El usuario puede abrir vistas geográficas.
ncp_gis_admin	No asignado a un grupo de forma predeterminada	El usuario puede editar preferencias de diseño de portlets en las vistas geográficas.
ncp_hopview	Network_Manager_User	El usuario puede acceder a la Vista de saltos.
ncp_hopview_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Vista de saltos de red.

Tabla 7. Roles de usuario de Network Manager (continuación)		
Rol	**Asignado al grupo**	**Descripción**
ncp_manage_unmanage	Network_Manager_IP_Admin	El usuario puede establecer el estado de los dispositivos como gestionado o no gestionado.
ncp_mibbrowser	Network_Manager_User	El usuario puede acceder al navegador MIB.
ncp_mibbrowser_config	Network_Manager_User	El usuario puede acceder al navegador MIB con fines de configuración.
ncp_mibbrowser_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Navegador de MIB de SNMP.
ncp_mibgraph_default_properties_config	Network_Manager_IP_Admin	El usuario puede modificar las propiedades predeterminadas del gráfico MIB. Este rol no tiene efecto sin los roles de grupo Network_Manager_User: ncp_mibgraph_user, ncp_mibgraph_config, ncp_mibbrowser.
ncp_mibgraph_config	Network_Manager_IP_Admin, Network_Manager_User	Habilita el acceso al widget Gráfico de MIB de SNMP y a las herramientas de clic con el botón derecho.
ncp_mibgraph_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Gráfico de MIB de SNMP.
ncp_mibgraph_user	Network_Manager_User	El usuario puede acceder al gráfico MIB SNMP.
ncp_monitor_policy	Network_Manager_IP_Admin	Habilita el acceso al widget Configurar políticas de sondeo, así como el acceso a la herramienta de clic con botón derecho Crear política de sondeo.
ncp_monitor_editor	Network_Manager_IP_Admin	El usuario puede editar los siguientes widgets. Configuración de definiciones de sondeo Configuración de políticas de sondeo
ncp_monitor_policy_alter_domain	Network_Manager_IP_Admin	El usuario puede seleccionar un dominio que no sea el predeterminado para las políticas de sondeo.
ncp_monitor_template	Network_Manager_IP_Admin	El usuario puede crear una definición nueva de política de sondeo.
ncp_networkhealth_dashboard	Network_Manager_User	El usuario puede acceder al Panel de control de estado de red.

Tabla 7. Roles de usuario de Network Manager (continuación)		
Rol	**Asignado al grupo**	**Descripción**
ncp_networkhealth_ dashboard_admin	Network_Manager_IP_Admin	El usuario puede editar los widgets de Panel de control de estado de red.
ncp_networkview	Network_Manager_User	El usuario puede acceder a la Vista de red y mostrar cualquiera de las siguientes vistas: • Vistas de usuarios: Las vistas de red creadas por el usuario. • Vistas de grupos: Las vistas asignadas al grupo o grupos a los que este usuario pertenece. • Vistas globales: Vistas accesibles a todos los usuarios independientemente del grupo al que pertenezcan. Los usuarios con este rol no pueden cambiar el diseño de la vista, a menos que el administrador les dé acceso a los botones del formato Jerárquico, Simétrico, Circular y Tabular. Para permitir a los usuarios cambiar (pero no guardar) el diseño, establezca la opción topoviz.networkview.readonly. enablelayout=true en el archivo $NMGUI_HOMEprofile/etc/tnm/topoviz.properties. Para conceder más permisos a los usuarios, asigne un rol diferente, como ncp_networkview_admin_user.
ncp_networkview_admin_global	Network_Manager_IP_Admin	El usuario puede crear, editar, particionar y suprimir vistas globales. A estas vistas podrán acceder todos los usuario, independientemente del grupo al que pertenezcan. El usuario también podrá realizar operaciones de transferencia en las vistas de red dentro de las vistas globales.

Tabla 7. Roles de usuario de Network Manager (continuación)		
Rol	**Asignado al grupo**	**Descripción**
ncp_networkview_admin_group	Network_Manager_IP_Admin	El usuario puede crear, editar, particionar y suprimir vistas de grupo. Se trata de vistas asignadas al grupo o grupos a los que pertenece el usuario. Este rol permite al usuario realizar operaciones de movimiento en las vistas de red dentro de una colección de vistas de grupo.
ncp_networkview_admin_user	Network_Manager_User	El usuario puede crear, editar, particionar y suprimir su propio conjunto de vistas de red. Este rol permite al usuario realizar operaciones de movimiento en las vistas de red dentro de una vista de usuario.
ncp_networkview_admin_all_users	Network_Manager_IP_Admin	El usuario puede crear, editar, particionar y suprimir vistas privadas. Se trata de vistas privadas creadas por usuarios que tienen las vistas de Vista de redes IP de Network Manager - Administrar para el rol de usuario. Este rol permite al usuario realizar operaciones de movimiento en las vistas de red dentro de una colección de vistas de grupo.
ncp_networkview_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Vistas de red.
ncp_oql	Network_Manager_IP_Admin	El usuario puede ejecutar y mostrar los resultados de las operaciones de selección de tipos mediante la página Acceso a la base de datos de gestión.
ncp_oql_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Acceso a la base de datos de gestión.
ncp_oql_update	Network_Manager_IP_Admin	El usuario puede ejecutar y mostrar los resultados de las operaciones de actualización de tipos mediante la página Acceso a la base de datos de gestión.
ncp_pathview	Network_Manager_IP_Admin, Network_Manager_User	El usuario puede crear, editar y eliminar vistas de ruta.
ncp_pathview_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Vistas de vía de acceso.

Tabla 7. Roles de usuario de Network Manager (continuación)		
Rol	**Asignado al grupo**	**Descripción**
ncp_reporting_user	Network_Manager_IP_Admin, Network_Manager_User	Añade el elemento de menú de Cognos Reporting.
ncp_reporting_admin	No asignado a un grupo de forma predeterminada	Este rol no se utiliza actualmente.
ncp_rest_api	Network_Manager_IP_User	Necesario para acceder a elementos de GUI que utilizan las API RESTful. Deje este rol asignado a todos los usuarios.
ncp_structurebrowser	Network_Manager_User	El usuario puede utilizar el navegador de estructura.
ncp_structurebrowser_editor	Network_Manager_IP_Admin	El usuario puede editar el widget Navegador de estructura.
ncp_structureview_entitysearch	Network_Manager_User	El usuario puede buscar entidades en el navegador de estructura.
ncp_structureview_interport_navigation	Network_Manager_User	El usuario puede navegar desde un puerto en un dispositivo a un puerto en otro dispositivo en el navegador de estructura.
ncp_topo_mgmt	Network_Manager_IP_Admin	El usuario puede añadir y eliminar dispositivos y conexiones a la topología utilizando la función de gestión de topologías, disponible en **Vista de saltos de red**.
ncp_webtools	Network_Manager_User	El usuario puede utilizar WebTools.
ncp_webtools_editor	Network_Manager_IP_Admin	El usuario puede editar las herramientas web, que es un conjunto de GUI disponibles en el menú que aparece al hacer clic con el botón derecho en un dispositivo del mapa de topología.
netcool_rw	No asignado a un grupo de forma predeterminada	El usuario puede usar los widgets Gestión de acceso de bases de datos y Sondeo de red.
noi_npi	Network_Manager_User	El usuario puede ver el **Panel de control de dispositivo** y, en concreto, el widget de **Performance Insights** que se utiliza en este panel de instrumentos.
Fix Pack 1 Fix Pack 1 noi_npi_admin	Network_Manager_IP_Admin	El usuario puede editar el **Panel de control de dispositivo** y, en concreto, el widget de **Performance Insights** que se utiliza en este panel de instrumentos.

Roles de usuario para la representación gráfica

Los usuarios deben tener los ID de usuario asignados a un rol de gráfico antes de ver y trabajar con las funciones de representación gráfica.

El administrador principal de Jazz for Service Management ya tiene el rol de chartAdministrator, y puede asignar usuarios a cualquiera de los tres roles de diagrama que están disponibles. Los usuarios registrados no tendrán privilegios de acceso a las funciones de representación gráfica si su ID de usuario no se ha asignado a un rol de gráfico. Estas son las posibilidades de los roles de gráficos:

chartAdministrator
Los usuarios con este rol pueden crear y suprimir conexiones de representación gráfica a los orígenes de datos, cargar gráficos y borrar la memoria caché de la representación gráfica (útil para la resolución de problemas).

chartCreator
Los usuarios con este rol pueden cargar gráficos, verlos y editarlos. No pueden crear ni suprimir conexiones de gráficos ni borrar la memoria caché de la representación gráfica.

chartViewer
Los usuarios que tienen asignado este rol pueden seleccionar y ver gráficos, pero no pueden modificarlos, ni tampoco sus preferencias. No pueden cargar gráficos, crear conexiones ni borrar la memoria caché de la representación gráfica.

Los roles se asignan mediante **Usuarios y grupos > Roles de usuario administrativo**.

Grupos de usuarios

Utilice grupos para organizar los usuarios en unidades con metas funcionales comunes. Se crean muchos grupos de Network Manager en la instalación.

Grupos de usuarios predeterminados

Los grupos siguientes se proporcionan con Network Manager. Los roles se asignan a estos grupos durante la instalación.

Network Manager IP Admin
Asigne a todos los administradores de Network Manager en este grupo para otorgar a los usuarios permisos administrativos para las aplicaciones web de Network Manager.

Usuario de Network Manager
Asigne a todos los usuarios finales y operadores de Network Manager en este grupo para otorgar a los usuarios permisos para utilizar las aplicaciones web de Network Manager.

Capítulo 6. Administración de contraseñas del sistema

Además de las contraseñas de usuario, Network Manager utiliza una serie de contraseñas internamente y cuando interactúa con la red.

Acerca de esta tarea

Todo el cifrado de contraseñas de Network Manager se realiza utilizando algoritmos compatibles con FIPS 140–2.

Restricción: Todas las contraseñas en un servidor determinado deben estar encriptadas con el mismo archivo `conf.key`. La forma más sólida de configurar las contraseñas de acceso a la línea de mandatos y SNMP es mediante el uso de **GUI de configuración del descubrimiento**. Si copia cualquier archivo que contenga contraseñas cifradas de un servidor a otro, también debe copiar el archivo `conf.key` que se utilizó para cifrarlos, y debe asegurarse de que todas las contraseñas del servidor se cifren con esa clave. Puede verificar las contraseñas utilizadas en el descubrimiento al validarlas con **GUI de configuración del descubrimiento**, antes de ejecutar un descubrimiento.

Restricción: Todas las contraseñas utilizadas en Network Manager deben ajustarse a las políticas de contraseñas del servidor o del entorno del sistema.

Cifrado o descifrado de una contraseña de forma manual

Si establece una contraseña utilizando un archivo de configuración, debe cifrar o descifrar la contraseña manualmente. De forma predeterminada, el mandato **`ncp_crypt`** cifra la contraseña proporcionada. Sin embargo, si especifica la opción de descifrado, la contraseña se descifrará.

Acerca de esta tarea

Siga estos pasos para cifrar o descifrar una contraseña del archivo de configuración.

Nota: Todo el cifrado de contraseñas de Network Manager se realiza utilizando algoritmos compatibles con FIPS 140–2.

Procedimiento

1. Detenga Network Manager.
2. Cifre o descifre la contraseña necesaria desde la línea de mandatos utilizando el programa de utilidad **`ncp_crypt`** del directorio `ITNMHOME/bin`.

   ncp_crypt -password *contraseña* [-decrypt] [-help] [-version]
3. Configure una inserción en el archivo de configuración correspondiente.
   a) Utilice la salida del programa de utilidad de cifrado **`ncp_crypt`**.
   b) Establezca el valor del campo `m_EncryptedPwd` en 1.
4. Reinicie Network Manager.

Ejemplo

Para cifrar la contraseña, escriba el siguiente mandato.

```
ncp_crypt -password mypassword
```

Para descifrar una contraseña utilice el mismo programa de utilidad que para cifrar la contraseña, pero con un argumento de línea de mandatos adicional.

```
ncp_crypt -decrypt -password @44:xXd7WUIC8teZDhLs8RQ1VjArw8HmUtNCwWs/VrVIxqI=@
```

Tareas relacionadas

Inicio y detención de Network Manager
Sus opciones para iniciar y detener Network Manager se explican aquí.

Cambio de la clave de cifrado

Puede cambiar la clave de cifrado que utiliza Network Manager al realizar el cifrado de contraseña.

Antes de empezar

Antes de cambiar la clave de cifrado, debe descifrar todas las contraseñas usadas actualmente en los archivos de configuración mediante el programa de utilidad **ncp_crypt** en el directorio `ITNMHOME/bin`:

```
ncp_crypt -password password -decrypt
```

Donde *password* es la contraseña a descifrar.

Acerca de esta tarea

Durante la instalación de Network Manager, se generará una clave de cifrado de 128 bits y se almacenará en la siguiente ubicación: `$NCHOME/etc/security/keys/conf.key`. Puede cambiar la clave de cifrado utilizando **nco_keygen** del programa de utilidad de Tivoli Netcool/OMNIbus.

Nota: Si desea cambiar la longitud del código de cifrado, consulte *Configuración de la longitud y tipo de cifrado* en *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Para cambiar la clave de cifrado:

Procedimiento

1. Cierre todos los procesos Network Manager.

   Puede utilizar el comando `itnm_stop`.
2. Si ha cambiado la longitud del código de cifrado, edite el archivo `$NCHOME/etc/precision/ConfigSchema.cfg` y cambie el valor que se inserta en `config.settings.m_KeyLength` por la longitud del nuevo código en bits. Los valores permitidos son 128, 192 y 256.
3. Utilice el programa de utilidad **nco_keygen** para generar una nueva clave de cifrado. Asegúrese de que especifica el archivo de salida como `$NCHOME/etc/security/keys/conf.key`.
4. Reinicie todos los procesos Network Manager.

   Puede utilizar el comando `itnm_start`.
5. Al utilizar la nueva clave de cifrado, vuelva a cifrar todas las contraseñas utilizadas actualmente en los archivos de configuración utilizando el programa de utilidad **ncp_crypt** escribiendo el mandato siguiente:

   ```
   ncp_crypt -password password
   ```

   Donde *password* es la contraseña a cifrar.

Desactivar el cifrado de contraseñas

Puede configurar Network Manager para desactivar el cifrado de contraseñas. Si realiza esta acción, las contraseñas introducidas en las interfaces gráficas de usuario se escribirán en el disco en texto sin formato.

Acerca de esta tarea

Para desactivar el cifrado de contraseñas:

Procedimiento

1. Edite el archivo de configuración **ncp_config**, `ConfigSchema.cfg`.
2. Configure la siguiente inserción en la tabla config.settings:

```
insert into config.settings
(
        m_EncryptPasswords,
        m_EncryptionKeyFile,
)
values
(
        0,
        ""
);
```

La inserción anterior especifica que no hay ningún cifrado (`m_EncryptPasswords = 0`) y que debe utilizarse la clave de cifrado predeterminada.

Lista de contraseñas de Network Manager

Cualquier cambio de contraseña debe hacerse utilizando las GUI de Network Manager siempre que sea posible.

De forma predeterminada, Network Manager cifra todas las contraseñas introducidas con las GUI de Network Manager. Algunas contraseñas no se pueden cambiar usando una interfaz gráfica de usuario y sólo se pueden cambiar configurando declaraciones de inserción en el archivo de configuración correspondiente. Si establece una contraseña utilizando un archivo de configuración, debe cifrar la contraseña manualmente.

La siguiente tabla muestra todas las contraseñas de Network Manager, y especifica cómo cambiar la contraseña.

Tabla 8. Contraseñas de Network Manager

Acceso necesario a	Tipo de contraseña	Descripción	Cambio de uso de
Telnet	Contraseña de modo privilegiado	Configurada como parte de la configuración de descubrimiento. Network Manager necesita esta contraseña para acceder a un dispositivo de red mediante Telnet.	GUI de descubrimiento de red
Telnet	Contraseña	Configurada como parte de la configuración de descubrimiento. Network Manager necesita esta contraseña para acceder a un dispositivo de red mediante Telnet.	GUI de descubrimiento de red
SNMP	Cadena de comunidad	Configurada como parte de la configuración de descubrimiento. Network Manager necesita esta contraseña para acceder a un dispositivo de red mediante SNMP.	GUI de descubrimiento de red

Tabla 8. Contraseñas de Network Manager (continuación)

Acceso necesario a	Tipo de contraseña	Descripción	Cambio de uso de
SNMP	Contraseña de autenticación de nivel 3	Configurada como parte de la configuración de descubrimiento. Network Manager necesita esta contraseña para acceder a un dispositivo de red mediante SNMP.	GUI de descubrimiento de red
SNMP	Contraseña privada de nivel 3	Configurada como parte de la configuración de descubrimiento. Network Manager necesita esta contraseña para acceder a un dispositivo de red mediante SNMP.	GUI de descubrimiento de red
Base de datos NCIM	Contraseña de acceso de línea de mandatos a la base de datos de topología	Proporciona acceso a la base de datos de topología NCIM.	Los archivos de configuración `$NCHOME/etc/precision/DbLogins.`*`DOMAIN`*`.cfg` y `$NCHOME/etc/precision/MibDbLogin.cfg`.
Base de datos NCIM	Parámetros de acceso utilizados por las aplicaciones web de Network Manager	Necesita la contraseña de la base de datos de topología NCIM para poder utilizar las interfaces gráficas de usuario que realizan consultas a la base de datos NCIM.	GUI de configuración de acceso a bases de datos
Tivoli Netcool/OMNIbusObjectServer	Contraseña segura de ObjectServer	La Pasarela de sucesos necesita esta contraseña para poder acceder al ObjectServer de las actividades de enriquecimiento de sucesos.	Inserción de archivo de configuración
Aplicaciones web	Contraseña `tnm.properties`	Permite a la GUI acceder a la base de datos de topología NCIM.	Aplicaciones web

Capítulo 7. Administración de bases de datos de gestión

Utilice la página de acceso a bases de datos de gestión basadas en GUI o el proveedor de servicios OQL para acceder a las bases de datos de cualquier proceso.

Acerca de esta tarea

Consulta de bases de datos de gestión mediante la página Acceso a la base de datos de gestión

Utilice la página Acceso a la base de datos de gestión para realizar consultas sobre las bases de datos de componente de Network Manager.

Acerca de esta tarea

Inicio de sesión en la página Acceso a la base de datos de gestión

Para iniciar sesión en la página Acceso a la base de datos de gestión:

Procedimiento

Pulse el icono **Administración** y seleccione **Red** > **Acceso a la base de datos de gestión**.

Emisión de una consulta mediante la página Acceso a la base de datos de gestión

Utilice la página Acceso a la base de datos de gestión para emitir consultas simples y complejas en bases de datos Network Manager.

Acerca de esta tarea

Para emitir una consulta de base de datos utilizando la página Acceso a la base de datos de gestión:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Acceso a la base de datos de gestión**.
2. Especifique un valor para los siguientes campos.

   Dominio
   Seleccione el dominio en el que emitir la consulta OQL.

   Servicio
   Seleccione el servicio que desea consultar.
3. Para emitir una consulta de una sola línea, escriba la consulta en el campo **Consulta** y haga clic en **Ir**  .
4. Para emitir una consulta de varias líneas:

   a) Haga clic en **Consulta OQL avanzada**  .

   b) Escriba la consulta en el campo **Mandato OQL** y haga clic en **Aceptar**.

c) Haga clic en **Ir**  .

Consejo: To skip clicking **Go**, append ; go to multiple-line queries.

Resultados

Listado de las bases de datos y tablas del servicio actual

Puede explorar las bases de datos de un servicio, las tablas de dichas bases de datos y las columnas de esas bases de datos.

Acerca de esta tarea

Listado de las bases de datos de un servicio utilizando el Área de trabajo OQL

Para mostrar una lista de las bases de datos de los servicios en los que ha iniciado la sesión, utilice el mandato **`show databases`**.

Acerca de esta tarea

Para listar las bases de datos de un servicio:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Acceso a la base de datos de gestión**.
2. Especifique un valor para los siguientes campos.

   Dominio
   Seleccione el dominio en el que emitir la consulta OQL.

   Servicio
   Seleccione el servicio que desea consultar.

3. Haga clic en **Consulta OQL avanzada**  . En el campo **Mandato OQL**, escriba la siguiente consulta:

```
show databases ;
```

Salida de ejemplo

La siguiente salida de ejemplo muestra las bases de datos del servicio de ncp_model:

```
[ 'dbModel', 'master', 'model', 'ncimCache' ]
```

Listado de las tablas de base de datos mediante la página Acceso a la base de datos de gestión

Para mostrar una lista de las tablas de una base de datos, utilice el mandato **`show tables from`**.

Acerca de esta tarea

Para listar las tablas de una base de datos:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Acceso a la base de datos de gestión**.
2. Especifique un valor para los siguientes campos.

Dominio
Seleccione el dominio en el que emitir la consulta OQL.

Servicio
Seleccione el servicio que desea consultar.

3. Haga clic en **Consulta OQL avanzada**  . En el campo **Mandato OQL**, escriba la siguiente consulta:

```
show tables from
 database_name ;
```

Salida de ejemplo

La siguiente salida de ejemplo muestra las tablas de la base de datos `master`:

```
[ 'entityByName', 'entityByNeighbor', 'containers' ]
```

Listado de las columnas de una tabla de base de datos mediante la página Acceso a la base de datos de gestión

Puede mostrar una lista de las columnas en una base de datos utilizando el mandato **show table**.

Acerca de esta tarea

Para listar las columnas de una tabla de base de datos:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Acceso a la base de datos de gestión**.
2. Especifique un valor para los siguientes campos.

   Dominio
   Seleccione el dominio en el que emitir la consulta OQL.

   Servicio
   Seleccione el servicio que desea consultar.

3. Haga clic en **Consulta OQL avanzada**  . En el campo **Mandato OQL**, escriba la siguiente consulta:

```
show table
database_name.table_name;
```

database_name es el nombre de la base de datos, y *table_name* es el nombre de la tabla requerida.

Consultas de bases de datos de gestión desde la línea de mandatos

Utilice el Proveedor de servicios OQL para realizar consultas en bases de datos de componentes de Network Manager.

Acerca de esta tarea

Una vez iniciada sesión en el Proveedor de servicios OQL, podrá emitir sentencias OQL para que actúen en las bases de datos del servicio en el que ha iniciado sesión. Debe terminar las sentencias con un punto y coma (;) y la palabra clave **go**. También puede utilizar la palabra clave **send** en lugar de **go**.

Puede configurar el Proveedor de servicios OQL para requerir autenticación en NCIM u ObjectServer. Para obtener más información, consulte la publicación *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Inicio del proveedor de servicios OQL

Inicie el Proveedor de servicios de OQL para acceder a las bases de datos de un determinado proceso Network Manager.

Acerca de esta tarea

Ingrese el mandato siguiente:

```
ncp_oql -domain DOMAIN_NAME -service SERVICE_NAME [-username USERNAME ] [-password
 PASSWORD ] [ -latency LATENCY ]
```

En este mandato:

- *DOMAIN_NAME* es el nombre del dominio para consultar.
- *SERVICE_NAME* es el nombre del proceso Network Manager para consultar.
- *USERNAME* es el nombre de usuario con el que autenticarse. Este argumento sólo es necesario si el proveedor de servicios OQL se ha configurado para requerir autenticación.
- *PASSWORD* es la contraseña con la que autenticarse. Este argumento sólo es necesario si el proveedor de servicios OQL se ha configurado para requerir autenticación.
- *LATENCY* es el máximo de tiempo en milisegundos (ms) que el proveedor de servicios espera para conectarse a otro proceso de Network Manager a través del bus de mensajería. Esta opción es útil para redes de gran tamaño y con mucho tráfico donde los valores predeterminados pueden hacer que los procesos presupongan que existe un problema cuando en realidad el retraso en las comunicaciones se debe al tráfico de red. El valor predeterminado es 3000 (equivalente a 3 segundos). Es posible que desee aumentar este valor ya que el valor predeterminado puede que no sea lo suficientemente largo para obtener una respuesta desde una base de datos OQL grande u ocupada.

Listado de las bases de datos y las tablas del servicio actual mediante el Proveedor de servicios de OQL

Puede explorar las bases de datos de un servicio, las tablas de dichas bases de datos y las columnas de esas bases de datos.

Listado de las bases de datos de un servicio utilizando el Proveedor de servicios OQL

Para mostrar una lista de las bases de datos de los servicios en los que ha iniciado la sesión, utilice el mandato **show databases**.

Acerca de esta tarea

Para listar las bases de datos de un servicio utilizando el Proveedor de servicios OQL

Procedimiento

1. Inicie el Proveedor de servicios OQL.
2. Escriba la siguiente consulta:

```
show databases;
go
```

Salida de ejemplo

La siguiente salida de ejemplo muestra las bases de datos del servicio de ncp_model:

```
{
        databases = [ 'master', 'translations' ]
}
```

Tareas relacionadas

Inicio del proveedor de servicios OQL
Inicie el Proveedor de servicios de OQL para acceder a las bases de datos de un determinado proceso Network Manager.

Listado de las tablas de una base de datos utilizando el Proveedor de servicios OQL

Para mostrar una lista de las tablas de una base de datos, utilice el mandato **show tables from**.

Acerca de esta tarea

Para listar las tablas de una base de datos utilizando el Proveedor de servicios OQL:

Procedimiento

1. Inicie el Proveedor de servicios OQL.
2. Escriba la siguiente consulta:

```
show tables from
database_name;
go
```

Salida de ejemplo

La siguiente salida de ejemplo muestra las tablas de la base de datos `master`:

```
{
        tables = [ 'entityByName', 'entityByNeighbor', 'containers' ]
}
```

Tareas relacionadas

Inicio del proveedor de servicios OQL
Inicie el Proveedor de servicios de OQL para acceder a las bases de datos de un determinado proceso Network Manager.

Listado de las columnas de una tabla de base de datos utilizando el Proveedor de servicios OQL

Puede mostrar una lista de las columnas de una tabla de bases de datos utilizando el mandato **show table**.

Acerca de esta tarea

Para emitir una consulta de base de datos utilizando el Proveedor de servicios OQL:

Procedimiento

1. Inicie el Proveedor de servicios OQL.
2. Escriba la siguiente consulta:

```
show table
database_name.table_name;
go
```

database_name es el nombre de la base de datos, y *table_name* es el nombre de la tabla requerida.

Tareas relacionadas

Inicio del proveedor de servicios OQL
Inicie el Proveedor de servicios de OQL para acceder a las bases de datos de un determinado proceso Network Manager.

Uso de consultas OQL en scripts

Puede iniciar el proveedor de servicios en un modo especial que ejecuta una sola consulta especificada y se desconecta del proveedor de servicios.

Acerca de esta tarea

Esto permite utilizar consultas OQL en scripts.

El siguiente ejemplo muestra la opción `-query` en uso.

```
ncp_oql -domain NCOMS -service Disco -query "select * from disco.status;"
```

El ejemplo anterior realiza una sola consulta en la tabla de base de datos `disco.status` y se desconecta del proveedor de servicios de OQL. Para llevar a cabo esta consulta, el proceso **ncp_disco** tendría que estar en ejecución en el dominio `NCOMS` y ser válidos el nombre de usuario y la contraseña.

Cualquier consulta OQL aceptable puede especificarse con la opción `-query`. La consulta debe terminar con un punto y coma, pero no con la palabra clave **go**.

Salir del proveedor de servicios OQL

Cuando haya terminado de emitir consultas OQL, salga del proveedor de servicios OQL.

Acerca de esta tarea

Para salir del proveedor de servicios, escriba el siguiente mandato:

```
quit
```

Sugerencias del Proveedor de servicios de OQL

El Proveedor de servicios de OQL proporciona cierto número de mandatos para facilitar la interacción con la línea de mandatos.

Restricción: Estos mandatos sólo funcionan en el Proveedor de servicios de OQL. No funcionan en la página Acceso a la base de datos de gestión.

Consejo: De forma predeterminada, los valores nulos no se muestran en los resultados devueltos. Para mostrar valores nulos, utilice la opción de línea de mandatos `-displayNulls` cuando inicie **ncp_oql**.

Mostrar historial de mandatos

Utilice el mandato `hist` para mostrar los mandatos más recientes.

Con el uso del mandato `hist` puede mostrar hasta los mil (1000) mandatos más recientes.

Ejemplo

Este ejemplo muestra cómo utilizar el mandato `hist`:

```
history

        1:      select * from services.unManaged;
        2:      select * from services.unManaged where serviceName like 'dh';
        3:      select count(*) from services.unManaged;
```

Ejecutar un mandato anterior

Utilice el mandato `!` junto con un número desde la lista de historial de mandatos para repetir un mandato reciente. Utilice el mandato `!!` para repetir el mandato más reciente.

Ejemplo

Este ejemplo muestra cómo utilizar el comando `!`:

```
history

        1:      select * from services.unManaged;
        2:      select * from services.unManaged where serviceName like 'dh';
        3:      select count(*) from services.unManaged;

!2
```

Esto ejecuta el segundo mandato de la lista de historial y produce la salida siguiente:

```
{
        serviceName='ncp_dh_dns';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=23;
        processId=10734;
}
{
        serviceName='ncp_dh_snmp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=24;
        processId=10750;
}
{
        serviceName='ncp_dh_arp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=25;
        processId=10872;
}
{
        serviceName='ncp_dh_telnet';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=52;
        processId=11424;
}
{
        serviceName='ncp_dh_ping';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=67;
        processId=13399;
}
( 5 record(s) : Transaction complete )
```

Activar la modalidad de visualización tabular

Utilice el mandato `tabon` para activar la modalidad de visualización tabular.

Ejemplo

Este ejemplo muestra cómo utilizar el mandato `tabon`:

```
tabon
select * from services.unManaged where serviceName like 'dh';
go
```

Esto crea la salida siguiente:

```
+---------------+----------------------------------------+--------------------
| serviceName   | servicePath                            | argList
+---------------+----------------------------------------+--------------------
| ncp_dh_dns    | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_snmp   | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_arp    | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_telnet | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_ping   | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
+---------------+----------------------------------------+--------------------
```

```
----+-----------+-----------+
    | serviceId | processId |
----+-----------+-----------+
    | 23        | 10734     |
    | 24        | 10750     |
    | 25        | 10872     |
    | 52        | 11424     |
    | 67        | 13399     |
----+-----------+-----------+

( 5 record(s) : Transaction complete )
```

Desactivar la modalidad de visualización tabular

Utilice el mandato `taboff` para desactivar la modalidad de visualización tabular.

Ejemplo

Este ejemplo muestra cómo utilizar el mandato `tabon`:

```
taboff
select * from services.unManaged where serviceName like 'dh';
go
```

Esto crea la salida siguiente:

```
{
        serviceName='ncp_dh_dns';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=23;
        processId=10734;
}
{
        serviceName='ncp_dh_snmp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=24;
        processId=10750;
}
{
        serviceName='ncp_dh_arp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=25;
        processId=10872;
}
{
        serviceName='ncp_dh_telnet';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=52;
        processId=11424;
}
{
        serviceName='ncp_dh_ping';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=67;
        processId=13399;
}
( 5 record(s) : Transaction complete )
```

Capítulo 8. Administrar la base de datos de topología de NCIM

Los datos de topología de red se almacenan en la base de datos NCIM.

Acerca de esta tarea

Cambio de los detalles de acceso de NCIM

Si cambia el nombre de host, puerto, contraseña o nombre de base de datos de la base de datos NCIM, debe completar algunas tareas de configuración para permitir que Network Manager se conecte a la base de datos.

Acerca de esta tarea

Para cambiar los detalles de acceso de NCIM, complete los pasos siguientes.

Procedimiento

Cambie el nombre de host, puerto, contraseña o nombre de base de datos en la base de datos.

Para cambiar el nombre de host, puerto, contraseña o nombre de base de datos, consulte la documentación de configuración para la versión de la base de datos de topología adecuada:

- Para obtener información sobre la instalación y configuración de Oracle, consulte la documentación de Oracle en http://docs.oracle.com/en/database/.
- Para obtener información acerca de cómo instalar y configurar Db2, consulte la documentación de Db2 en http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome
- Para obtener información sobre el cambio de contraseña, consulte "Actualización de los valores de acceso de NCIM para las aplicaciones web" en la página 67.

Qué hacer a continuación

Después de cambiar los detalles de acceso en la base de datos, actualice los valores en los componentes de Network Manager que se conectan a la base de datos NCIM.

Tareas relacionadas

Script de resolución de problemas de acceso de bases de datos

En el caso de que haya problemas de acceso a la base de datos de topología, la base de datos de sondeo histórica o la base de sondeo, ejecute el script **ncp_db_access.pl**. Este script comprueba la configuración de la base de datos y determina si los cortafuegos están bloqueando el acceso a las bases de datos.

Actualización de los valores de acceso de NCIM para las aplicaciones web

Si ha modificado los valores de NCIM, debe configurar el acceso de NCIM para las aplicaciones web de Network Manager.

Acerca de esta tarea

Los valores de acceso de NCIM para las aplicaciones web se establecen como parte de la instalación del producto. Solo actualice los valores si ha modificado los detalles de acceso de NCIM.

Si cambia los valores con la GUI existen menos posibilidades de errores. Si no puede utilizar la GUI para cambiar los valores, puede editar los detalles de acceso en el archivo `$NMGUI_HOMEprofile/etc/tnm/tnm.properties`.

Para configurar los valores de acceso de NCIM con la GUI, siga estos pasos:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Configuración del acceso a base de datos**.
   Se muestra el widget **Configurar acceso a base de datos de NCIM**.
2. Escriba el host en que está instalada la base de datos en el campo **Host de base de datos**. De forma predeterminada, este host es el mismo host en el que está instalado Network Manager.
3. Escriba el puerto que utiliza la base de datos en el campo **Puerto de base de datos**.
4. Escriba el nombre de usuario que se escribió durante la instalación de la base de datos en el campo **Nombre de usuario**.
5. Escriba la contraseña que se escribió durante la instalación de la base de datos en el campo **Contraseña**.
6. Confirme la contraseña.

Referencia relacionada

La pantalla de Topoviz está en blanco
Si Topoviz no se inicia, o se inicia con una pantalla en blanco, actualice la ventana del navegador. Si la pantalla inicial de Network Manager no aparece, compruebe los parámetros de acceso a la base de datos de topología.

Actualización de los detalles de acceso de NCIM utilizados por Reporting Services

Si cambia los detalles de acceso de NCIM configure Cognos Analytics para utilizar los nuevos detalles.

Antes de empezar

Necesita una contraseña para el usuario administrador Dashboard Application Services Hub (normalmente el usuario smadmin).

Acerca de esta tarea

Para configurar Cognos Analytics para utilizar diferentes detalles de acceso para la base de datos de NCIM, complete los pasos siguientes.

Procedimiento

1. Cambie la contraseña utilizada por Cognos Analytics a través de la configuración de las propiedades de la fuente de datos para los informes y para todas las fuentes de datos. Consulte el Centro de conocimiento de Cognos Analytics en https://www.ibm.com/support/knowledgecenter/SSEP7J.
2. En cada origen de datos, utilice la GUI de Cognos para cambiar el nombre de usuario o la contraseña.
   a) Haga clic en el icono **Informes** y seleccione **Informe de Cognos**. Dentro del widget, seleccione **Administrar** > **consola de administración**.
   b) Haga clic en el separador **Configuración**.
   c) Pulse **NCIM** y, a continuación, vuelva a pulsar **NCIM**.
      La indicación de ruta en la parte superior de la GUI debe indicar **Directorio** > **Cognos** > **NCIM** > **NCIM**.
   d) Seleccione la casilla de verificación al lado de **ncim** y pulse **Más** > **Establecer propiedades**
   e) En la pestaña de **Inicio de sesión**, haga clic en **Editar inicio de sesión** y escriba el nombre de usuario y la nueva contraseña de la base de datos.

Actualización de los valores de acceso de NCIM en los componentes principales de Network Manager

Si cambia los detalles de acceso de NCIM configure los componentes principales de Network Manager para utilizar los nuevos detalles.

Acerca de esta tarea

Para configurar los componentes principales de Network Manager para utilizar los nuevos detalles, complete los pasos siguientes.

Procedimiento

1. Si sólo desea cambiar la contraseña, ejecute el script **ncp_password_update.pl**. Para obtener información sobre la ejecución de este script de Perl, consulte *ncp_password_update.pl* en *Referencia de IBM Tivoli Network Manager*.
2. Opcional: Si no está seguro de que la contraseña sea correcta, desactive el cifrado estableciendo `tnm.database.password.encrypted=false` en el `tnm.properties`, e introduzca la contraseña en texto simple. Hágalo sólo para fines de resolución de problemas y recuerde activar de nuevo el cifrado después.
3. Para cambiar otros valores de acceso, como el nombre de host o puerto, ejecute el script **set_db_details.pl**. Para obtener información sobre la ejecución de este script, consulte *set_db_details.pl* en *Referencia de IBM Tivoli Network Manager*.

Resultados

Después de cambiar la contraseña, puede utilizar el scriptNCHOME/`precision/scripts/perl/scripts/ncp_db_access.pl` para verificar el acceso. Para obtener más información sobre el script `ncp_db_access.pl`, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Recreación de las vistas de red

Si crea un esquema de base de datos NCIM y desea que la GUI de Network Manager utilice el nuevo esquema, deben configurar la GUI para acceder a la nueva base de datos. También necesita volver a crear las vistas de red.

Antes de empezar

Asegúrese de que ha configurado el acceso de la GUI a la nueva base de datos de topología.

Acerca de esta tarea

Las vistas de red son suministradas automáticamente por los archivos `default.xml` y `itnmuser.xml` al instalar Network Manager y después se crean en la base de datos. Sin embargo, si no crea esquemas de bases de datos de topología durante la instalación o posteriormente cambia la base de datos, tendrá que volver a crear las vistas.

Para volver a crear vistas de red:

Procedimiento

1. Vaya a `$NMGUI_HOME/profile/etc/tnm/autoprovision/`.
2. Cambie el nombre de los archivos denominados *`filename`*`.xml.processed` a *`filename`*`.xml`.
3. Guarde y cierre los archivos.

Creación de los esquemas de la base de datos de topología

Puede configurar la base de datos de topología durante la instalación. Si necesita configurar una base de datos después de la instalación para un Network Managerexistente, podrá hacerlo de forma manual utilizando los scripts suministrados.

Acerca de esta tarea

Debe crear la base de datos de topología antes de poder utilizar Network Manager.

Para obtener información sobre la creación de las bases de datos de topología, consulte el tema ***Instalación y configuración de una base de datos de topología*** en *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Creación de esquemas de la base de datos de topología de Db2 en UNIX

Puede utilizar los scripts para crear los esquemas de base de datos de topología en una base de datos de Db2 en UNIX. Se requieren usuarios diferentes para ejecutar los diferentes scripts.

Acerca de esta tarea

Para crear la base de datos de topología:

Procedimiento

1. Asegúrese de que ha seguido los requisitos previos para instalar Db2 e instale y configure la base de datos Db2.
2. Asegúrese de que los scripts de creación de base de datos estén disponibles en el servidor de base de datos.
   - Si la base de datos Db2 está en el mismo servidor que Network Manager y ya se ha instalado Network Manager, los scripts de creación de base de datos están disponibles en `$ITNMHOME/scripts/sql`.
   - Si la base de datos Db2 está en un servidor distinto, copie el contenido de `$ITNMHOME/scripts/sql` en el servidor Db2 o localice el archivo `db2_creation_scripts.tar.gz` en el nivel superior, que está disponible desde IBM Installation Manager como un paquete independiente.
3. Como usuario, administrativo, por ejemplo, el usuario `db2inst1`, ejecute el script `create_db2_database.sh` como el usuario administrativo de Db2 escribiendo el mandato siguiente en el servidor Db2:

   `./create_db2_database.sh` *`nombre_base_datos nombre_usuario`* `-force`

   Donde:

   `nombre_base_datos`
   Es el nombre de la base de datos.

   `nombre_usuario`

   Es el usuario de Db2 que se ha de utilizar para conectar con la base de datos.

   Importante: Este usuario no debe ser el usuario de administración. Este usuario debe ser un usuario de un sistema operativo existente y de Db2.

   `-force`
   Es un argumento que fuerza la salida de cualquier usuario de Db2 de la instancia antes de que se cree la base de datos.

   Por ejemplo, para crear una base de datos Db2 denominada `ITNM` para el usuario de Db2 `ncim`, escriba:

   ```
   ./create_db2_database.sh ITNM ncim
   ```

Después de ejecutar `create_db2_database.sh`, reinicie la base de datos como el usuario administrativo de Db2 de la siguiente manera: ejecute **db2stop** y, a continuación, ejecute **db2start**.

4. Cree el esquema de base de datos. Para crear el esquema de base de datos, utilice uno de los métodos siguientes (no es posible utilizar ambos métodos).
   a) Para crear el esquema de base de datos desde el servidor de Network Manager, ejecute el mandato `$ITNMHOME/scripts/sql/create_all_schemas.sh` en el servidor Network Manager como usuario administrativo, de este modo:

      `./create_all_schemas.sh` *`tipo_base_datos nombre_base_datos host nombre_usuario contraseña puerto`*

      Donde:

      tipo_base_datos
      Identifica el tipo de base de datos para crear. En este caso, es db2.

      nombre_base_datos
      Especifica el nombre de la base de datos.

      host
      Especifica el nombre de host de servidor o la dirección IP donde está instalada la base de datos.

      nombre_usuario
      Identifica al usuario de Db2 que se ha de utilizar para conectar con la base de datos.

      Importante: Este usuario no debe ser el usuario de administración. Este usuario debe ser un usuario de un sistema operativo existente y de Db2.

      contraseña
      Proporciona la contraseña del usuario.

      puerto
      Especifica el puerto que utiliza la base de datos.

      El ejemplo siguiente crea los esquemas NCIM en una base de datos Db2 que tiene el nombre de servicio DB_123 en un host remoto con el nombre samplehost, en el puerto 9088. La combinación de usuario/contraseña para conectar a la base de datos es ncim/password.

      ```
      $NCHOME/precision/scripts/sql/create_all_schemas.sh db2 DB_123 samplehost
      ncim password 9088
      ```

   b) Si lo prefiere, para crear el esquema de base de datos en el servidor de base de datos, vaya a la ubicación del servidor de base de datos donde ha descomprimido el archivo `db2_creation_scripts.tar.gz`. Como usuario administrativo, ejecute el siguiente script para rellenar las bases de datos:

      ```
      ./populate_db2_database.sh database_name user_name password > db2.log 2>&1
      ```

5. Examine el archivo `db2.log` en busca de errores.
6. Inicie sesión como el administrador de Db2 en el cliente de Db2 que se ejecuta en el servidor de Dashboard Application Services Hub.
7. Ejecute el mandato `$ITNMHOME/bin/ncp_mib` para asegurarse de que la base de datos `ncmib` se ha rellenado por completo con datos SNMP de los MIB antes de que se ejecute un descubrimiento.
8. Si desea que la GUI de Network Manager utilice el esquema de base de datos que ha creado, tendrá que configurar el acceso al nuevo esquema de base de datos de topología y volver a crear las vistas de red.

Tareas relacionadas

Actualización de los valores de acceso de NCIM para las aplicaciones web
Si ha modificado los valores de NCIM, debe configurar el acceso de NCIM para las aplicaciones web de Network Manager.

Recreación de las vistas de red

Si crea un esquema de base de datos NCIM y desea que la GUI de Network Manager utilice el nuevo esquema, deben configurar la GUI para acceder a la nueva base de datos. También necesita volver a crear las vistas de red.

Creación de esquemas de bases de datos de topología Oracle en UNIX

Utilice los scripts para crear los esquemas de base de datos de topología en una base de datos Oracle en UNIX.

Acerca de esta tarea

Para crear la base de datos de topología, siga estos pasos en el servidor en el que está instalada la base de datos Oracle. Se requieren usuarios diferentes para ejecutar los diferentes scripts.

Procedimiento

1. Compruebe que ha seguido todos los requisitos previos de instalación de Oracle e instale y configure la base de datos de Oracle.

   Para obtener información sobre la instalación y configuración de Oracle, consulte la documentación de Oracle en http://docs.oracle.com/en/database/.
2. Asegúrese de que los scripts de creación de base de datos estén disponibles en el servidor de base de datos.
   - Si la base de datos de Oracle está en el mismo servidor que Network Manager y ya se ha instalado Network Manager, los scripts de creación de base de datos están disponibles en `$ITNMHOME/scripts/sql`.
   - Si la base de datos de Oracle está en un servidor distinto, copie el contenido de `$ITNMHOME/scripts/sql` en el servidor de Oracle o localice el archivo `oracle_creation_scripts.tar.gz` en el nivel superior, que está disponible desde IM como un paquete independiente.
3. Ejecute el script `create_oracle_ncadmin_user.sh` en el servidor donde está instalada la base de datos. Inicie sesión en el host de Oracle como administrador de base de datos de Oracle y ejecute el script `create_oracle_ncadmin_user.sh` proporcionando el usuario `sys` y la contraseña. Ejecute el script como en el ejemplo siguiente:

   ```
   $NCHOME/precision/scripts/sql/oracle/create_oracle_ncadmin_user.sh
   sys
   password [-pdb pluggable_database_name]
   ```

   Donde se aplican los parámetros siguientes:

   contraseña
   Especifica la contraseña del usuario `sys`.

   -pdb *nombre_basedatos_conectable*
   Opcional: Si está ejecutando Oracle 12c con RAC, debe utilizar una base de datos conectable. En este caso, utilice este parámetro para especificar el nombre de la base de datos conectable Oracle 12c.
4. Para crear la base de datos, ejecute el script `./create_oracle_database.sh`. Como administrador de base de datos de Oracle, ejecute el script `./create_oracle_database.sh` proporcionando el usuario `system` y la contraseña. En el servidor de Network Manager, el script se encuentra en el directorio `$ITNMHOME/scripts/sql/oracle`. Ejecute el script en el servidor donde se ha instalado la base de datos. Ejecute el script como en el ejemplo siguiente:

   ```
   ./create_oracle_database.sh system password [-asm]
   [-pdb pluggable_database_name]
   ```

   Donde se aplican los parámetros siguientes:

   contraseña
   Especifica la contraseña del usuario `system`.

-asm
Especifique `-asm` si la base de datos de Oracle utiliza ASM.

-pdb *nombre_basedatos_conectable*
Opcional: Si está ejecutando Oracle 12c con RAC, debe utilizar una base de datos conectable. En este caso, utilice este parámetro para especificar el nombre de la base de datos conectable Oracle 12c.

5. Cree el esquema de base de datos. Para crear el esquema de base de datos, utilice uno de los métodos siguientes (no es posible utilizar ambos métodos).
   a) Para crear el esquema de base de datos desde el servidor de Network Manager, ejecute el mandato `$ITNMHOME/scripts/sql/create_all_schemas.sh` en el servidor Network Manager como usuario administrativo, de este modo:

   `./create_all_schemas.sh` *`tipo_base_datos nombre_base_datos host nombre_usuario contraseña puerto`*

   Donde:

   tipo_base_datos
   Identifica el tipo de base de datos para crear. En este caso, es `oracle`.

   nombre_base_datos
   Especifica el nombre de la base de datos. En Oracle, este nombre debe ser la base de datos conectable.

   host
   Especifica el nombre de host de servidor o la dirección IP donde está instalada la base de datos.

   nombre_usuario
   Identifica el usuario que se utilizará para conectarse a la base de datos.

   contraseña
   Proporciona la contraseña del usuario.

   puerto
   Especifica el puerto de base de datos.

   b) Para crear el esquema de base de datos en el servidor de base de datos, vaya a la ubicación del servidor de base de datos donde ha descomprimido el archivo `oracle_creation_scripts.tar.gz`. Como usuario administrativo, ejecute el script `populate_oracle_database.sh`. Ejecute el script como en el ejemplo siguiente:

   ```
   ./populate_oracle_database.sh database_user_name password
   [-pdb pluggable_database_name]
    > oracle.log 2>&1
   ```

   Donde se aplican los parámetros siguientes:

   database_user_name
   El valor puede ser `system` o `ncim`. Ha creado el usuario `ncim` en un paso anterior.

   contraseña
   Proporciona la contraseña del usuario.

   -pdb *nombre_basedatos_conectable*
   Opcional: Si está ejecutando Oracle 12c con RAC, debe utilizar una base de datos conectable. En este caso, utilice este parámetro para especificar el nombre de la base de datos conectable Oracle 12c.

6. Examine el archivo `oracle.log` en busca de errores.
7. Ejecute el mandato `$ITNMHOME/bin/ncp_mib` para asegurarse de que la base de datos `ncmib` se ha rellenado por completo con datos SNMP de los MIB antes de que se ejecute un descubrimiento.
8. Si desea que la GUI de Network Manager utilice el esquema de base de datos que ha creado, tendrá que configurar el acceso al nuevo esquema de base de datos de topología y volver a crear las vistas de red.

Tareas relacionadas

Actualización de los valores de acceso de NCIM para las aplicaciones web
Si ha modificado los valores de NCIM, debe configurar el acceso de NCIM para las aplicaciones web de Network Manager.

Recreación de las vistas de red
Si crea un esquema de base de datos NCIM y desea que la GUI de Network Manager utilice el nuevo esquema, deben configurar la GUI para acceder a la nueva base de datos. También necesita volver a crear las vistas de red.

Eliminación de dominios de la base de datos de topología

Cuando ya no hace falta un dominio, utilice el script `domain_drop.pl` para eliminarlo de la base de datos de topología NCIM. La topología completa del dominio se elimina así como todas las políticas de sondeo para dicho dominio. La información de configuración para la memoria caché del dominio y la topología no se ven afectadas.

Procedimiento

1. Detenga el dominio ejecutando el mandato **`itnm_stop`**.
   Por ejemplo, para eliminar el dominio OLDDOMAIN:

   ```
   itnm_stop ncp -domain OLDDOMAIN
   ```

   Para comprobar que los procesos del dominio se han detenido, ejecute el mandato **`itnm_status`**.
2. En `$NCHOME/precision/scripts/perl/scripts`, ejecute el script `domain_drop.pl`.
   Por ejemplo, para eliminar el dominio que se detuvo en el paso anterior:

   ```
   NCHOME/precision/bin/ncp_perl domain_drop.pl -domain OLDDOMAIN
   -password password
   ```

Eliminación de todas las entidades de los dominios

Como alternativa a descartar dominios de la base de datos NCIM, puede utilizar una sentencia SQL DELETE para eliminar todas las entidades de los dominios. A diferencia de cuando se descartan los dominios, si elimina todas las entidades, la correlación entre los entityID y los entityName persiste.

Procedimiento

Para eliminar todas las entidades de un dominio, utilice la sentencia DELETE como se muestra en el siguiente ejemplo.

```
delete from ncim.entityData where entityId in (select a.entityId from
ncim.entityData a inner join ncim.domainMembers b on
a.entityid=b.entityid and b.domainMgrId=domainMgrId;)
```

Donde *domainMgrId* es el valor de domainMgrId del dominio.

Resultados

Las entidades se eliminan del dominio. Como la correlación entre los entityID y entityName persiste, si se redescubren entidades que tienen el mismo nombre, se les asigna el mismo entityID que antes de la supresión.

Eliminación de la base de datos de topología

Puede eliminar la base de datos de topología de si ya no es necesaria.

Acerca de esta tarea

Antes de eliminar la base de datos de topología, debe detener todos los procesos que se conectan con la base de datos.

Eliminación de una base de datos de topología Db2 en UNIX

Puede eliminar la base de datos Db2 en UNIX mediante un script.

Acerca de esta tarea

Para eliminar una base de datos Db2, lleve a cabo los siguientes pasos:

Procedimiento

1. Cambie al directorio de scripts con el siguiente mandato:

```
cd $NCHOME/precision/scripts/sql/db2
```

2. Ejecute el script con el siguiente mandato:

```
drop_db2_database.sh NCIM [ force ]
```

Resultados

Si utiliza la opción de forzado opción, el script forzará a los usuarios de Db2 a salir de la instancia antes de intentar eliminar la base de datos.

Eliminación de una base de datos de topología Oracle en UNIX

Puede eliminar la base de datos Oracle en UNIX mediante un script.

Acerca de esta tarea

Para eliminar una base de datos Oracle, lleve a cabo los siguientes pasos:

Procedimiento

1. Compruebe que ha iniciado sesión como usuario `system`.
2. Cambie al directorio de scripts con el siguiente mandato:

```
cd $NCHOME/precision/scripts/sql/oracle
```

3. Ejecute el script con el siguiente mandato:

```
drop_oracle_database.sh system password [ -pdb pluggable_db]
```

Eliminación de una base de datos de topología Oracle en Windows

Puede eliminar la base de datos Oracle en Windows mediante un script.

Acerca de esta tarea

Para eliminar una base de datos Oracle, lleve a cabo los siguientes pasos:

Procedimiento

1. Compruebe que ha iniciado sesión como usuario `system`.
2. Cambie al directorio de scripts con el siguiente mandato:

```
cd %NCHOME%\precision\scripts\sql\oracle
```

3. Ejecute el script con el siguiente mandato:

```
sqlplus system/password < drop_oracle_database.sql
```

Resultados

Si utiliza la opción de forzado opción, el script forzará a los usuarios de Oracle a salir de la instancia antes de intentar eliminar la base de datos.

Capítulo 9. Informes de administración

Puede crear informes nuevos, modificar los informes existentes y configurar el acceso del usuario a los informes.

Acerca de esta tarea

Los orígenes de datos para Cognos Analytics se establecen durante la instalación. Si los detalles de la base de datos cambian, configure de nuevo la fuente de datos utilizando las funciones administrativas de Cognos Analytics. Consulte el Centro de conocimiento de Cognos Analytics en https://www.ibm.com/support/knowledgecenter/SSEP7J.

Creación y edición de informes

Puede editar los informes existentes y crear sus propios informes con las herramientas de Cognos Analytics.

Acerca de esta tarea

Puede crear informes nuevos utilizando Cognos Query Studio, que se describe en la *Query Studio - Guía de usuario*, disponible en el menú **Ayuda** en el widget **Informes** > **Common Reporting**.

Puede editar informes existentes con Cognos Report Studio, descrito en *Report Studio Professional Authoring - Guía de usuario*, disponible en el menú **Ayuda** en el widget **Informes** > **Common Reporting**.

Consejo: Si tiene una red grande y compleja, los informes detallados pueden incluir potencialmente grandes cantidades de datos. Puede ser difícil utilizar informes con cientos de miles de líneas y pueden producir que los componentes de elaboración de informes se queden sin memoria. Asegúrese de que los informes están optimizados para devolver datos que le resulten útiles.

Si crea o edita informes personalizados basados en Cognos, el procedimiento de creación o de edición de informes requerirá la selección de vistas y atributos del Modelo de datos comunes (CDM) de IBM. Para obtener más información sobre las vistas de CDM consulte *Referencia de IBM Tivoli Network Manager*.

Creación de una URL para ejecutar informes

Puede crear una URL para abrir directamente un informe en una ventana de navegador. Otras aplicaciones pueden utilizar estas URL para ejecutar informes.

Acerca de esta tarea

Para construir una dirección URL para abrir un informe, lleve a cabo los siguientes pasos.

Procedimiento

1. Localice el informe que desea utilizar y anote los parámetros requeridos.
2. Cree una URL similar a esta:

```
https://hostname:port/tarf/servlet/dispatch?
b_action=cognosViewer&ui.action=run&ui.object=/content/package[@name=
'Network Manager']/folder[@name='report_group_name']
/report[@name='report_name']&ui.name=report_name
&run.outputFormat=HTML&domainName=AUTO&report_parameter=
"value"
```

Donde

- *nombre_host* es el nombre del servidor donde se ha instalado Dashboard Application Services Hub.

- *puerto* es el número de puerto utilizado para Dashboard Application Services Hub.
- *nombre_grupo_informe* es el nombre del grupo al que pertenece el informe.
- *nombre_informe* es el nombre del informe que desea abrir.
- *parámetro_informe* es un parámetro que se pasa el informe.
- *valor* es el valor del parámetro.

La siguiente URL de ejemplo abre el informe Información de direccionamiento IP, que pertenece al grupo de informes de vistas de rutas, que muestra la ruta 3323 y el dispositivo 13.

```
https://10.10.10.108:16311/tarf/servlet/dispatch?b_action=cognosViewer
&ui.action=run&ui.object=/content/package[@name='Network Manager']
/folder[@name='Path Views Reports']/report[@name='IP Routing Info']&ui.name
=IP Routing Info&run.outputFormat=HTML&domainName
=AUTO&pathEntityId=3323&entityId=13
```

Modificación del nivel de aislamiento del origen de datos

El nivel de aislamiento predeterminado del origen de datos ODBC de Cognos está establecido como de lectura confirmada. Si tiene varios dominios o varios sondeos en ejecución, o ambas cosas, es posible que necesite cambiar el nivel de aislamiento a lectura no confirmada por motivos de rendimiento o para evitar bloqueos de tabla que originen errores.

Acerca de esta tarea

Para establecer el nivel de aislamiento como de lectura no confirmada, cambie la configuración del origen de datos NCPOLLDATA del siguiente modo:

Procedimiento

1. Haga clic en el icono **Informes** y seleccione **Informe de Cognos**. Dentro del widget, seleccione **Administrar** > **consola de administración**.
2. Haga clic en el separador **Configuración**.
3. Haga clic en NCPOLLDATA.
4. Haga clic en el icono **Establecer propiedades** y seleccione el separador **Conexión**.
5. Seleccione **Lectura no confirmada** en el menú desplegable **Especificar un valor**.

   Nota: Algunos proveedores de base de datos utilizan diferentes nombres para los niveles de aislamiento. Consulte la ayuda Cognos Analytics y escriba "niveles de aislamiento" para obtener más información sobre los niveles disponibles y sus correspondientes nombres en distintas clases de base de datos.
6. Haga clic en **Aceptar**.

Capítulo 10. Resolución de problemas y ayuda

Utilice esta información para ayudarle a resolver problemas con el producto.

Resolución de problemas de Network Manager

Consulte estas notas de resolución de problemas para ayudarse a determinar la causa del problema y cómo solucionarlo.

Tareas relacionadas

Administración de registros
Network Manager proporciona funciones de registro para sus componentes de interfaz gráfica de usuario y procesos back-end. Puede configurar el registro de Network Manager para generar archivos de registro o rastreo que puede utilizar para resolver problemas.

Resolución de problemas de descubrimiento
Puede solucionar problemas de descubrimiento supervisando los sucesos de descubrimiento y ejecutando informes de descubrimiento. También puede configurar sus propios agentes de descubrimiento.

Resolución de problemas del sondeo ping de la red
Utilice esta información para que le ayude a asegurarse de que el sondeo ping de las direcciones IP importantes de la red realizado por Network Manager es el previsto o, en caso contrario, para proporcionar información para solucionar el problema.

Resolución de problemas e instalación

Utilice esta información para saber cómo solucionar errores que se pueden producir durante la instalación de Network Manager.

Los temas siguientes describen los tipos de mensajes de error que puede encontrar durante el proceso de instalación y las acciones que puede realizar para resolver estos problemas.

Visualización de los registros de instalación

La visualización de los registros de instalación puede ser útil para la resolución de problemas.

Acerca de esta tarea

La información sobre el éxito del proceso de instalación se registra en IBM Installation Manager. Para ver la información de registro de instalación, proceda de la siguiente manera. Podrá encontrar más información en IBM Installation Manager Knowledge Center en: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Nota: Para ver los valores generales de la instalación de Network Manager como, por ejemplo, información sobre la versión instalada de Network Manager, la ubicación de inicio de los componentes e información sobre la conexión de base de datos, consulte el archivo `NCHOME/etc/itnm.cfg`.

Procedimiento

1. Revise el historial de instalación. En IBM Installation Manager pulse **Archivo** > **Historial de instalación**.
   a) En IBM Installation Manager pulse **Archivo** > **Historial de instalación**.
   b) Revise el estado de los paquetes instalados.
      La columna **Nombre de grupo de paquetes** lista los paquetes instalados y la columna **Estado** lista los resultados de la instalación de dicho paquete.
   c) Pulse **Ver registro** para ver el archivo de registro para cualquier paquete seleccionado.

2. También puede filtrar los diversos archivos de registro por tipo de suceso. Para ello, en IBM Installation Manager, pulse **Archivo** > **Ver registro**.

   Puede filtrar información en los archivos de registro por los siguientes tipos de suceso:

   - Error
   - Aviso
   - Nota
   - Información
3. Si es necesario, puede exportar un conjunto completo de datos de registro para que IBM lo analice. Para ello, en IBM Installation Manager pulse **Ayuda** > **Exportar datos para análisis de problemas**.

Comprobación de la URL de inicio de sesión y de los puertos predeterminados

Si tiene problemas para iniciar sesión, asegúrese de que comprueba el formato de URL y los puertos que utiliza tras la instalación.

formato de la URL

Compruebe que el formato de la URL entrado es como sigue (muestra los puertos predeterminados):

- `https://localhost:16311/ibm/console` (acceso seguro).
- `http://localhost:16310/ibm/console` (acceso no seguro).

Donde *localhost* es el nombre de host completo o la dirección IP del servidor de Dashboard Application Services Hub.

Puertos predeterminados

16310 es el número de puerto no seguro predeterminado y 16311 es el número de puerto seguro predeterminado. Si su entorno estaba configurado durante la instalación con un número de puerto distinto al predeterminado, indique ese otro número.

Resolución de problemas de Dashboard Application Services Hub

Podrá encontrar información sobre la resolución de problemas de Dashboard Application Services Hub en el Knowledge Center de Jazz for Service Management.

El Knowledge Center de Jazz for Service Management está ubicado en https://www.ibm.com/support/knowledgecenter/SSEKCU

Resolución de problemas de aplicaciones web

Utilice esta información de resolución de problemas para ayudarle a resolver los problemas comunes que pueden surgir al administrar las aplicaciones web.

No se ha encontrado el dispositivo

Un error `No se ha encontrado el dispositivo` se puede producir al hacer clic con el botón derecho del ratón en un suceso en GUI web de Tivoli Netcool/OMNIbus y seleccionar **Buscar en vista de saltos**.

Este error aparece por uno de los siguientes motivos:

- No existe un dispositivo correspondiente en la topología. Si este es el caso, debe comprobar que:
  - Ha configurado el ámbito del descubrimiento para que incluya este dispositivo.
  - Dispone el agente de descubrimiento adecuado para descubrir este dispositivo.
  - El dispositivo es un dispositivo de red admitido.

  - Se ha descubierto el dispositivo, dado que es posible que se haya conectado recientemente y sea necesario descubrirlo.
- El suceso procede de un analizador que no se ha configurado para incluir los campos que Network Manager requiere para localizar el dispositivo. Esta es la causa de error más probable si el dispositivo se encuentra en la topología.

La pantalla de Topoviz está en blanco

Si Topoviz no se inicia, o se inicia con una pantalla en blanco, actualice la ventana del navegador. Si la pantalla inicial de Network Manager no aparece, compruebe los parámetros de acceso a la base de datos de topología.

Tareas relacionadas

Actualización de los valores de acceso de NCIM para las aplicaciones web

Si ha modificado los valores de NCIM, debe configurar el acceso de NCIM para las aplicaciones web de Network Manager.

No se puede acceder al dominio

Si la lista desplegable **Dominio** no muestra el dominio esperado, compruebe la configuración del acceso a la base de datos de topología. Asimismo, consulte los archivos del directorio `$NMGUI_HOME/profile/logs/tnm/` para obtener información relevante sobre la GUI, especialmente los archivos `ncp_topoviz.0.log` y `ncp_topoviz.0.trace` para obtener información relevante sobre Topoviz.

No se pueden ejecutar las herramientas de clic con el botón derecho del ratón en Visor de sucesos

Si las opciones de menú contextual **Mostrar causa raíz** o **Mostrar sucesos suprimidos** fallan durante la ejecución y se devuelve un mensaje de error, esto podría deberse a los scripts CGI, que se ejecutan cuando se eligen estas opciones de menú que no pueden encontrar la ruta a Perl.

Si ha instalado Perl en una ubicación no estándar, compruebe que ha especificado la ruta correcta a Perl en todos los scripts CGI.

El dispositivo en Topoviz aparece como nodo genérico

Si se sabe que un dispositivo es un conmutador o direccionador pero aparece en **Vista de saltos de red** o in the **Vistas de red** como icono de nodo genérico, es posible que el dispositivo no esté correctamente correlacionado al icono del archivo de clase de objetos activos (AOC).

Causa

El dispositivo se descubrió correctamente y se correlaciona a un archivo de AOC. Una forma de comprobar esto es asegurarse de que en **Vistas de red**, se puede ubicar el dispositivo en una de las vistas de red de la clase de dispositivo.

Resolución del problema

Ciertos archivos de AOC no proporcionan un icono visual pero en lugar de eso utilizan la sentencia `visual_icon = ' ';`. En este caso, el archivo de AOC (y el dispositivo correspondiente) toma visual_icon de super_class del AOC.

Ejemplo

Un ejemplo son el archivo Extreme.aoc y ExtremeSummit.aoc. La super_class para Extreme.aoc es el archivo Device.aoc, que utiliza el icono 'Device'. Si desea un dispositivo creado como instancia como Extreme.aoc para verlo en **Vista de saltos de red** en **Vistas de red** como conmutador o direccionador, edite el archivo AOC y utilice la sentencia `visual_icon = 'Switch';;` or `visual_icon = 'Router;` en lugar de `visual_icon = ' ';`.

Repercusión del rendimiento en vistas de red cuando hay presentes muchos túneles MPLS-TE

El proceso `Path View Engine` se ejecuta como proceso de fondo para compilar todas las vistas necesarias para la topología de red. Cuando la topología contiene muchos túneles MPLS-TE, el proceso `Path View Engine` es muy activo mientras el proceso está compilando las vistas y, en algunos casos, el proceso puede tener repercusión en el rendimiento de la GUI de Network Manager.

Si es necesario, puede inhabilitar el proceso `Path View Engine`. Para inhabilitar el proceso `Path View Engine`, vaya a `$NMGUI_HOME/profiles/etc/topoviz.properties` y establezca la propiedad `topoviz.pathviewengine.enabled` en `FALSE`.

Las GUI no aparecen

Si integra aplicaciones web Network Manager en el producto y determinadas aplicaciones web no aparecen, es posible que se deba al filtro de clickjacking. Este filtro se aplica de forma predeterminada a la GUI de acceso de bases de datos y la GUI de configuración de descubrimiento.

Acerca de esta tarea

Para resolver este problema, consulte *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Mensaje de error de no autorización al iniciar sesión en Network Manager

Es posible que se cierre de forma inesperada su sesión en ITNM, o podría recibir mensajes de error inesperado acerca de que no tiene permiso al iniciar sesión, por ejemplo, al intentar acceder a la ayuda en línea de Network Manager. Una solución a este problema es cambiar el nombre de la cookie de inicio de sesión único de WebSphere Application Server para garantizar que los usuarios que han iniciado sesión en Network Manager serán siempre reconocidos y autenticados por Network Manager, independientemente de cualquier otra cookie de SSO establecida en las sesiones de inicio de sesión simultáneas en otros servidores como, por ejemplo, los inicios de sesión en la intranet.

Para cambiar el nombre de la cookie de inicio de sesión único (SSO) de WebSphere Application Server, lleve a cabo los siguientes pasos:

1. Inicie sesión en la consola de administración de WebSphere como usuario smadmin.

   ```
   https://hostname:port/ibm/console
   ```

   Donde:

   - *nombre_host* es el nombre del WebSphere Application Server.
   - *puerto* es el número de puerto asociado con el WebSphere Application Server. De forma predeterminada, este es el número de puerto del servidor de Dashboard Application Services Hub + 5, el cual es 16316.
2. En el árbol de navegación de la izquierda, pulse **Seguridad** > **Seguridad global**.
3. En la página **Seguridad global**, haga clic en **Seguridad web y SIP** y, a continuación, pulse **Inicio de sesión único (SSO)**.
4. En el campo **Nombre de cookie LTPA V2**, escriba el nombre de la cookie SSO deseado; por ejemplo, `ITNMLtpaToken`.

   Este campo está en blanco de forma predeterminada y si deja en blanco el nombre de la cookie, adopta de forma predeterminada el valor `LtpaToken2`. Por lo tanto, es importante cambiar el nombre de cookie por otro que no sea `LtpaToken2`.
5. Haga clic en **Aceptar**.
6. Pulse **Guardar directamente en la configuración maestra**.
7. Reinicie el servidor Dashboard Application Services Hub.

Resolución de problemas de creación de informes

Si tiene problemas con Cognos Analytics, repase la información relativa a la resolución de problemas.

Los informes de datos de sondeo contienen valores nulos

Si los informes sobre los datos de sondeo contienen valores nulos, es posible que tenga que eliminar los datos de sondeo.

Acerca de esta tarea

Con el tiempo, debido a la adición o la eliminación de entidades, la tabla ncmonitor.monitoredInstance puede contener instancias de entityIds que se han eliminado desde entonces desde la tabla ncim.entity. Esto puede producir como resultado que los informes de los datos de sondeo contengan información nula. Lleve a cabo los pasos siguientes para solucionar este problema:

Procedimiento

1. Ejecute las siguientes consultas para determinar si su base de datos contiene valores nulos:

   ```
   select count(*) from ncpolldata.monitoredInstance where instanceType =
   'ifIndex' and entityId is null;
   ```

   ```
   select count(*) from ncpolldata.monitoredInstance where instanceType =
   'ifIndex' and entityId not in (select entityId from ncim.interface);
   ```

2. Si la consulta indicada más arriba devuelve algún valor, use `itnm_stop` para detener el dominio y ejecute el siguiente script para eliminar los datos de sondeo de un dominio:

   ```
   $NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/domain_drop.pl -domain
   domain -clearPollData
   ```

   Donde *domain* es el dominio para el que desea eliminar los datos de sondeo.

Cambio del nivel de registro para los informes

Para obtener información sobre cómo establecer el registro y cómo cambiar el nivel de registro para Cognos Analytics, consulte Centro de conocimiento de Cognos Analytics en https://www.ibm.com/support/knowledgecenter/SSEP7J.

Información relacionada

Página de bienvenida de Cognos Business IntelligencePara obtener más información sobre la configuración del registro para informes, consulte la documentación en línea de Cognos Business Intelligence.

Resolución de problemas del acceso a base de datos

Para resolver problemas de acceso a base de datos, compruebe el acceso de usuario o ejecute el script de resolución de problemas de la base de datos.

Script de resolución de problemas de acceso de bases de datos

En el caso de que haya problemas de acceso a la base de datos de topología, la base de datos de sondeo histórica o la base de sondeo, ejecute el script **ncp_db_access.pl**. Este script comprueba la configuración de la base de datos y determina si los cortafuegos están bloqueando el acceso a las bases de datos.

Acerca de esta tarea

El script **ncp_db_access.pl** comprueba el acceso a la base de datos y los problemas de cortafuegos de las siguientes bases de datos:

- base de datos de topología NCIM

- Base de datos de sondeo NCMONITOR
- Base de datos de sondeo histórica de MIB

Procedimiento

1. Cambie al directorio `$NCHOME/precision/scripts/perl/scripts` y localice el programa ncp_db_access.pl.
2. Emita el mandato siguiente.

   `perl ncp_db_access.pl -domain` *`domain_name`*
   Donde:

   - *`domain_name`* es el nombre del dominio necesario.

   Para cada base de datos, el script indica si la conexión es correcta o hay problemas de acceso.

Tareas relacionadas

Cambio de los detalles de acceso de NCIM
Si cambia el nombre de host, puerto, contraseña o nombre de base de datos de la base de datos NCIM, debe completar algunas tareas de configuración para permitir que Network Manager se conecte a la base de datos.

Resolución de problemas del agente de ITM

Para resolver un problema con IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, reúna información sobre el problema para el Soporte de software de IBM, utilice el registro de datos y consulte las listas de problemas identificados y métodos alternativos.

Para obtener información general sobre la resolución de problemas, consulte la *IBM Tivoli Monitoring: Guía de resolución de problemas*.

Para obtener información sobre los problemas conocidos con esta versión de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, consulte *IBM Tivoli Network Manager IP Edition Release Notes*.

Puede resolver algunos problemas asegurándose de que el sistema cumpla los requisitos del sistema. Los requisitos más actualizados se encuentran en los https://www.ibm.com/software/reports/compatibility/clarity/ (http://www.ibm.com/software/reports/compatibility/clarity/index.jsp).

Recopilación de información del producto para el Servicio de soporte de software de IBM

Antes de ponerse en contacto con el soporte técnico de software de IBM acerca de un problema que está experimentando con este producto, reúna la información que aparece en Tabla 9 en la página 84.

Tabla 9. Información que debe recopilar antes de contactar con el servicio de soporte de software de IBM

Tipo de información	**Descripción**
Archivos de registro	Recopile los archivos de registro de rastreo de los sistemas que presentan anomalías. La mayoría de los registros se encuentran en un subdirectorio `logs` del host.
Network ManagerInformación de	Número de versión y nivel de parche
Sistema operativo	Número de versión y nivel de parche del sistema operativo
mensajes	Mensajes y otra información que se muestra en la pantalla

Tabla 9. Información que debe recopilar antes de contactar con el servicio de soporte de software de IBM (continuación)	
Tipo de información	**Descripción**
Números de versión de IBM Tivoli Monitoring	Número de versión y niveles de parche para IBM Tivoli Monitoring y IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
Capturas de pantalla	Capturas de pantalla de la salida incorrecta, en caso de existir.
(Solo sistemas UNIX) Archivos de volcado del núcleo	Si el sistema se detiene en los sistemas UNIX, recopile el archivo de volcado de núcleo del directorio *dir_instalación*/bin, donde *dir_instalación* es el directorio en el que ha instalado el agente de supervisión.

Para obtener información sobre cómo trabajar con IBM Software Support, visite https://www.ibm.com/support/home/ (https://www.ibm.com/support/servicerequest/Home.action).

Utilización del registro cronológico

El registro es la característica principal de resolución de problemas del agente de supervisión. *Registro* hace referencia a los mensajes de texto y datos de rastreo generados por el agente. Los mensajes y los datos de rastreo se envían a un archivo.

Los datos de rastreo capturan información transitoria sobre el entorno operativo actual cuando un componente o una aplicación no funcionan como está previsto. Los técnicos del soporte de software de IBM utilizan la información de rastreo capturada para determinar cuál es el origen de un error o una condición inesperada.

Consulta de las listas de soluciones temporales y problemas identificados

Los problemas conocidos están organizados en tipos como los de la siguiente lista para facilitar su localización:

- Instalación, configuración y desinstalación
- Despliegue remoto
- Agente
- Espacio de trabajo
- Situación
- Mandatos de actuación

Registro cronológico de rastreo

Los registros cronológicos de rastreo se utilizan para capturar información sobre el entorno operativo cuando el software de componente no funciona del modo previsto.

El tipo de registro principal es el registro de rastreo RAS (fiabilidad, disponibilidad y capacidad de servicio). Estos registros solo están en inglés. El mecanismo de registro de rastreo RAS está disponible para todos los componentes de IBM Tivoli Monitoring. La mayor parte de los registros se encuentran en un subdirectorio `logs` del host.

Nota: En la documentación se hace referencia al recurso RAS en IBM Tivoli Monitoring como "RAS1."

El personal de soporte de software de IBM utiliza la información capturada por el registro de rastreo para rastrear un problema hasta su origen o para determinar por qué se ha producido un error. Todos los componentes del entorno de IBM Tivoli Monitoring tienen un nivel de rastreo predeterminado. El nivel de rastreo se puede cambiar en el nivel de componente para ajustar el tipo de información de rastreo

recopilada, el grado de detalle de rastreo, el número de registros de rastreo que se van a conservar y la cantidad de espacio en disco utilizada para el rastreo.

Visión general sobre gestión de archivos de registro

El conocimiento de los convenios de denominación de los archivos de registro le ayuda a encontrar los archivos.

Convenciones de nomenclatura de los archivos de registro de un agente

Los nombres de archivos de registro de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition siguen este convenio de denominación:

Sistemas Linux y UNIX
*nombre_host*_np_*programa_fecha_hora_HEX-nn*.log

Ubicación de los archivos de registro de rastreo

Los archivos de registro de rastreo están ubicados en distintos sistemas.

Las siguientes tablas contienen ubicaciones, nombres de archivo y descripciones de algunos registros de rastreo que pueden ayudarle a determinar el origen de los problemas con los agentes.

Consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* para obtener más información sobre todos los registros de rastreo que se mantienen en el servidor de supervisión.

Tabla 10. Archivos de registro de rastreo ubicados en el Tivoli Enterprise Monitoring Server

Nombre y vía de acceso del archivo	Descripción
• **Windows:** El archivo IBM Tivoli Monitoring *timestamp*.log en la vía de acceso *install_dir*\InstallITM • **UNIX:** El archivo candle_installation.log en la vía de acceso *install_dir*/logs • **Linux:** El archivo candle_installation.log en la vía de acceso *install_dir*/logs	Proporciona detalles sobre los productos que están instalados. **Nota:** El registro de rastreo está habilitado de forma predeterminada. No se precisa ninguna tarea de configuración para habilitar este rastreo.
El nombre del archivo RAS tiene el formato siguiente: • **Windows:** *dir_instalación*\logs*nombre_host*_ms_*indicación_fecha_hora-nn*.log • **UNIX:** *dir_instalación*/logs/*nombre_host*_ms_*fecha_hora-nn*.log • **Linux:** *dir_instalación*/logs/*nombre_host*_ms_*indicación_fecha_hora-nn*.log **Nota:** Los nombres de archivo de los registros de RAS1 contienen una indicación de fecha y hora hexadecimal. Asimismo, en sistemas UNIX, se proporciona una indicación de fecha y hora decimal: *nombre_host*_np_*fecha_hora*.log y *nombre_host*_np_*fecha_hora*.pid*nnnnn* en la vía de acceso de *dir_instalación*/logs, donde *nnnnn* es el número de ID de proceso.	Rastrea la actividad del servidor de supervisión.

Tabla 10. Archivos de registro de rastreo ubicados en el Tivoli Enterprise Monitoring Server (continuación)	
Nombre y vía de acceso del archivo	**Descripción**
El nombre del archivo RAS tiene el formato siguiente: • **Windows:** *install_dir*\logs\ *hostname*_cq_HEXtimestamp-nn.log • **UNIX:** *install_dir*/logs/ *hostname*_cq_HEXtimestamp-nn.log • **Linux:** *install_dir* /logs/ *hostname*_cq_HEXtimestamp-nn.log **Nota:** Los nombres de archivo de los registros de RAS1 contienen una indicación de fecha y hora hexadecimal. Asimismo, en sistemas UNIX, se proporciona una indicación de fecha y hora decimal: *nombre_host*_np_*fecha_hora*.log y *nombre_host*_np_*fecha_hora*.pid*nnnnn* en la vía de acceso de *dir_instalación*/logs, donde *nnnnn* es el número de ID de proceso.	Rastrea la actividad en el servidor del portal.

En la tabla siguiente se incluyen los archivos de registro de rastreo que se encuentran en el servidor de Tivoli Enterprise Portal.

Tabla 11. Archivos de registro de rastreo ubicados en el servidor de Tivoli Enterprise Portal	
Nombre y vía de acceso del archivo	**Descripción**
El nombre del archivo RAS tiene el formato siguiente: • **Windows:** *install_dir*\logs\ *hostname*_cq_HEXtimestamp-nn.log • **UNIX:** *install_dir*/logs/ *hostname*_cq_HEXtimestamp-nn.log • **Linux:** *install_dir* /logs/ *hostname*_cq_HEXtimestamp-nn.log **Nota:** Los nombres de archivo de los registros de RAS1 contienen una indicación de fecha y hora hexadecimal. Asimismo, en sistemas UNIX, se proporciona una indicación de fecha y hora decimal: *nombre_host*_np_*fecha_hora*.log y *nombre_host*_np_*fecha_hora*.pid*nnnnn* en la vía de acceso de *dir_instalación*/logs, donde *nnnnn* es el número de ID de proceso.	Rastrea la actividad en el servidor del portal.

Tabla 12. Archivos de registro de rastreo ubicados en el servidor de Network Manager

Nombre y vía de acceso del archivo	**Descripción**
Los archivos de registro RAS1 son los siguientes: • **UNIX:** *hostname*_np_*instance_name*_knpagent_HEXtimestamp-nn.log en el directorio *install_dir*/logs • Linux **Linux:** *hostname*_np_*instance_name*_knpagent_HEXtimestamp-nn.log en el directorio *install_dir*/logs Estos archivos de registro están situados en los directorios siguientes: • **UNIX:** *dir_instalación*/logs • Linux **Linux:** *dir_instalación*/logs En los sistemas Linux se proporcionan los siguientes registros adicionales: – *nombre_host*_np_timestamp.log – *hostname*_np_timestamp.pidnnnnn en la vía de acceso *install_dir*/logs, donde *nnnnn* es el número de ID de proceso	Rastrea actividad del agente de supervisión.
Los archivos de registro de operaciones del agente son los siguientes: *instance_hostname_NP*.LG0 es el registro actual creado cuando se inicia el agente. *instance_hostname_NP*.LG1 es la copia de seguridad del registro anterior. Estos registros están en el directorio siguiente dependiendo del sistema operativo que esté utilizando: • Linux **Linux:** *dir_instalación*/logs • **UNIX:** *dir_instalación*/logs	Muestra si el agente pudo conectar con el servidor de supervisión. Muestra qué situaciones se han iniciado y detenido, y además muestra otros sucesos mientras el agente se está ejecutando. Se genera una nueva versión de este archivo cada vez que se reinicia el agente. Se genera una copia de seguridad del archivo *.LG0 con la etiqueta .LG1. Vea la etiqueta .LG1 para ver los detalles siguientes relativos a la sesión de supervisión *anterior*: • Estado de la conectividad con el servidor de supervisión • Situaciones que estaban en ejecución. • El estado de resultado satisfactorio o anomalía de los mandatos de Actuación
Los archivos de registro del comando de actuación son los siguientes: • *host*_np_*instance*_*takeactioncommand*.log Los registros se encuentran en los directorios siguientes: • **UNIX:** *dir_instalación*/logs • Linux **Linux:** *dir_instalación*/logs	Rastrea la actividad cada vez que se ejecuta un mandato de Actuación. Por ejemplo, cuando se ejecuta un mandato de actuación **start_command** hipotético, se genera un archivo start_command.log.

Tabla 12. Archivos de registro de rastreo ubicados en el servidor de Network Manager (continuación)	
Nombre y vía de acceso del archivo	**Descripción**
Los archivos de registro del comando de actuación son los siguientes: • knp_data_provider_actions_*instance_n*.log Los registros se encuentran en los directorios siguientes: • **UNIX**: *dir_instalación*/logs • Linux **Linux**: *dir_instalación*/logs	Rastrea la actividad cada vez que se ejecuta un mandato de Actuación. Todos los mandatos de actuación predefinidos se registran en este archivo.
Los archivos de registro de actuación son los siguientes: • knp_*instance_takeactioncommand*.log • knp_*instancia*_control_*dominioplanificador*.log	Rastrea la actividad cada vez que se ejecuta un mandato de Actuación. Por ejemplo, cuando se ejecuta un mandato de actuación **stop_scheduler**, se generan los siguientes mensajes de registro: • kp9_*instancia*_stop_log Este registro contiene cierta información básica sobre cómo el mandato de actuación ha invocado a continuación y proceso denominado Control Scheduler. • kp9_*instance*_control_scheduler.log Este registro contiene la salida de registro de toda la salida de la CLI psadmin de PeopleSoft recopilada al ejecutar mandatos de Actuación específicos.
Archivos de registro de proveedor de datos: • knu_data_provider_instance_startup.log • knu_data_provider_instance_n.log Los registros se encuentran en los directorios siguientes: • **Windows:** *dir_instalación*\tmaitm6\logs • **Linux:** *dir_instalación*/logs	Rastrea el estado y las operaciones del proveedor de datos del agente.

Definiciones de las variables:

- *indicación_fecha_hora* es una indicación de la fecha y hora con un formato que incluye año (a), mes (m), día (d), hora (h) y minuto (m), como el siguiente: **aaaammdd hhmm**
- *indicación_fecha_hora_HEX* es una representación hexadecimal de la hora a la que se ha iniciado el proceso.
- *install_dir* representa la vía de acceso del directorio donde instaló el componente correspondiente. *install_dir* puede representar una vía de acceso del sistema que contiene el sistema de supervisión, el agente de supervisión o el portal.
- *instancia* hace referencia al nombre de la instancia de base de datos que está supervisando.
- *nombre_instancia* hace referencia al nombre de la instancia de agente.
- *nombre_host* hace referencia al nombre del sistema en el que se ejecuta el componente correspondiente.

- *nn* representa la secuencia circular en la cual rotan los registros. Este valor incluye un rango de 1 - 5, de manera predeterminada. El primero siempre se conserva porque incluye parámetros de configuración.

Consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* para obtener más información sobre todos los registros de rastreo que se mantienen en el servidor de supervisión.

Ejemplos: Utilización de registros de rastreo

Puede abrir registros de rastreo en un editor de texto para conocer algunos datos sobre el entorno de IBM Tivoli Monitoring.

Los siguientes ejemplos pertenecen al registro de Tivoli Enterprise Monitoring Server.

Ejemplo uno

Este extracto muestra el registro típico de una conexión fallida entre un agente de supervisión y un servidor de supervisión con el nombre de host **server1a**:

```
(Thursday, August 11, 2005, 08:21:30-{94C}kdcl0cl.c,105,"KDCL0_ClientLookup")
 status=1c020006, "location server unavailable", ncs/KDC1_STC_SERVER
_UNAVAILABLE (Thursday, August 11, 2005, 08:21:35-{94C}kraarreg.cpp,
1157,"LookupProxy") Unable to connect to broker at ip.pipe:: status=0,
 "success", ncs/KDC1_STC_OK (Thursday, August 11, 2005, 08:21:35-{94C}
kraarreg.cpp,1402,"FindProxyUsingLocalLookup") Unable to find running
 CMS on CT_CMSLIST <IP.PIPE:#server1a>
```

Ejemplo dos

Los extractos siguientes procedentes del archivo de registro de rastreo *correspondiente al servidor de supervisión* muestran el estado de un agente, identificado aquí como "Nodo remoto". El nombre del sistema donde se ejecuta el agente es **SERVER5B**:

```
(42C039F9.0000-6A4:kpxreqhb.cpp,649,"HeartbeatInserter")
 Remote node SERVER5B:NP is ON-LINE.
. . .
(42C3079B.0000-6A4:kpxreqhb.cpp,644,"HeartbeatInserter")
 Remote node SERVER5B:NP is OFF-LINE.
```

Consulte los siguientes puntos clave sobre los extractos precedentes:

- El servidor de supervisión añade el código de producto de dos caracteres al nombre de servidor para formar un nombre exclusivo (por ejemplo, SERVER5B: VM) para esta instancia del agente. Mediante este nombre exclusivo, puede distinguir entre varios productos de supervisión que puede haber en ejecución en **SERVER5B**.
- El registro muestra el inicio del agente (ON-LINE) y su posterior detención (OFF-LINE) en el entorno.
- Para abreviar, los puntos suspensivos (...) representan la serie de entradas de registro cronológico de rastreo que se han generado durante la ejecución del agente.
- Entre las entradas de registro ON-LINE y OFF-LINE, el agente se comunicaba con el servidor de supervisión.
- Las entradas ON-LINE y OFF-LINE del archivo de registro siempre están disponibles en el archivo de registro de rastreo.

Parámetros de rastreo RAS

Identifique un problema estableciendo el rastreo detallado de los componentes individuales del agente de supervisión y de los módulos.

Consulte el apartado "Visión general sobre gestión de archivos de registro" en la página 86 para asegurarse de que conoce la rotación de registros y puede hacer referencia a los archivos de registro correctos cuando gestione la generación de archivos de registro.

Establecimiento de los parámetros de rastreo de RAS mediante la GUI

En sistemas Windows, puede utilizar la interfaz gráfica de usuario para establecer las opciones de rastreo.

Acerca de esta tarea

El nivel de rastreo predeterminado de RAS1 es ERROR, pero puede cambiarlo. Para cambiar los valores de rastreo RAS1, realice los siguientes pasos:

Procedimiento

1. Abra la ventana **Manage Tivoli Enterprise Monitoring Services**.
2. Seleccione **Avanzado** > **Editar parámetros de rastreo**. Se muestra la ventana **Parámetros de rastreo de Tivoli Enterprise Monitoring Server**.
3. Seleccione un nuevo valor de rastreo en el menú desplegable del campo **Especificar filtros de RAS1** o escriba una serie válida.
   - Rastreo de errores general. KBB_RAS1=ERROR
   - Rastreo de errores intensivo. KBB_RAS1=ERROR (UNIT:knp ALL)
   - Rastreo de errores máximo. KBB_RAS1=ERROR (UNIT:knp ALL) (UNIT:kra ALL)

     Nota: Como muestra este ejemplo, puede definir varias opciones de rastreo de RAS en una sola sentencia.
4. Modifique el valor de Tamaño de registro máximo por archivo (MB) para cambiar el tamaño del archivo de registro (cambia el valor LIMIT).
5. Modifique el valor del Número máximo de archivos de registro por sesión para modificar el número de archivos de registro por arranque de un programa (cambia el valor de COUNT).
6. Modifique el valor del número máximo total de archivos de registro para cambiar el número de archivos de registro para todos los arranques de un programa (cambia el valor de MAXFILES).
7. Opcional: Pulse S (Sí) en el menú **Valor KDC_DEBUG** para registrar la información que puede ayudarle a diagnosticar los problemas de comunicaciones y conectividad entre el agente de supervisión y el servidor de supervisión. El valor **KDC_DEBUG** y el valor **Rastreo máximo de errores** pueden generar una gran cantidad de registros de rastreo. Utilice estos valores sólo temporalmente mientras realiza la resolución de los problemas. De lo contrario, los registros pueden ocupar demasiado espacio de disco duro.
8. Haga clic en **Aceptar**. Aparece un mensaje que indica que debe reiniciarse el agente de supervisión para que los cambios entren en vigor.

Qué hacer a continuación

Supervise el tamaño del directorio `logs`. El comportamiento predefinido puede generar un total de 45 a 60 MB para cada agente que se ejecuta en un sistema. Por ejemplo, cada instancia de base de datos que supervise puede generar de 45 a 60 MB de datos de registro.

Pode regularmente los archivos de registro que no sean los archivos de registro RAS1 del directorio `logs`. A diferencia de los archivos de registro RAS1 que se borran automáticamente, otros tipos de registro pueden crecer de forma indefinida, por ejemplo, los registros que incluyen un número de ID de proceso (PID).

Utilice los registros de rastreo de recopilador como una fuente adicional de información para la resolución de problemas.

Nota: El valor **KDC_DEBUG** y el valor **Rastreo máximo de errores** pueden generar una gran cantidad de registros de rastreo. Utilice estos valores únicamente de manera temporal, mientras resuelve los problemas. De lo contrario, los registros pueden ocupar demasiado espacio de disco duro.

Configuración manual de los parámetros de rastreo de RAS

Puede editar manualmente los parámetros de registro de rastreo RAS1.

Acerca de esta tarea

El nivel de rastreo de RAS1 predeterminado es ERROR. Para cambiar los valores de rastreo, realice los siguientes pasos.

Procedimiento

1. Abra el archivo de opciones de rastreo:

   install_dir /config/np.config
2. Edite la línea que empieza por **KBB_RAS1=** para establecer las preferencias de registro de rastreo. Por ejemplo, si desea utilizar el registro de rastreo detallado, establezca la opción **Rastreo máximo**: KBB_RAS1=ERROR (UNIT:knp ALL) (UNIT:kra ALL)
3. Edite la línea que empieza con **KBB_RAS1_LOG=** para gestionar la generación de archivos de registro:
   - **MAXFILES**: El número total de archivos que se van a mantener para todos los inicios de un programa específico. Una vez superado este valor, los archivos de registro más antiguos se eliminarán. El valor predeterminado es 9.
   - **LIMIT**: Tamaño máximo, en megabytes (MB) de un archivo de registro de RAS1. El valor predeterminado es 5.
   - El servicio de soporte de software de IBM puede ayudarle a modificar los parámetros siguientes:
     - **COUNT** El número de archivos de registro que se deben conservar durante el ciclo acumulado de un inicio de programa. El valor por omisión es 3.
     - **PRESERVE**: El número de archivos que no se han de reutilizar en el ciclo acumulado de un inicio de programa. El valor predeterminado es 1.

     Nota: El parámetro **KBB_RAS1_LOG** también permite la especificación del directorio del archivo de registro, el nombre del archivo de registro, y el nombre y directorio del archivo de control de inventario. No modifique estos valores; en caso contrario, se puede perder la información de registro.
4. Reinicie el agente de supervisión para que los cambios entren en vigor.

Qué hacer a continuación

Supervise el tamaño del directorio `logs`. El comportamiento predefinido puede generar un total de 45 a 60 MB para cada agente que se ejecuta en un sistema. Por ejemplo, cada instancia de base de datos que supervise puede generar de 45 a 60 MB de datos de registro.

Pode regularmente los archivos de registro que no sean los archivos de registro RAS1 del directorio `logs`. A diferencia de los archivos de registro RAS1 que se borran automáticamente, otros tipos de registro pueden crecer de forma indefinida, por ejemplo, los registros que incluyen un número de ID de proceso (PID).

Utilice los registros de rastreo de recopilador como una fuente adicional de información para la resolución de problemas.

Nota: El valor **KDC_DEBUG** y el valor **Rastreo máximo de errores** pueden generar una gran cantidad de registros de rastreo. Utilice estos valores únicamente de manera temporal, mientras resuelve los problemas. De lo contrario, los registros pueden ocupar demasiado espacio de disco duro.

Problemas y soluciones temporales

Los problemas conocidos y las soluciones temporales se organizan en tipos de problemas que pueden producirse con un agente, por ejemplo, problemas de instalación y configuración y problemas con el espacio de trabajo.

Puede resolver algunos problemas asegurándose de que el sistema cumpla los requisitos para instalar el agente de supervisión. Vea *Requisitos para la instalación del agente de supervisión* en *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración* para obtener información adicional.

Resolución de problemas de instalación y configuración

Se pueden producir problemas durante la instalación, configuración y desinstalación del agente.

Las tablas siguientes proporcionan información sobre los problemas y soluciones.

Tabla 13. Problemas y soluciones de la instalación y configuración

Problema	**Solución**
(*Solo UNIX*) Durante una instalación de línea de mandatos, elige instalar un componente que ya está instalado y ve el aviso siguiente: `AVISO - está a punto de instalar la MISMA versión de "component_name"` donde *component_name* es el nombre del componente que está intentando instalar. Este problema afecta a instalaciones de la línea de mandatos de UNIX.	Deberá salir y reiniciar el proceso de instalación. No puede volver a la lista donde seleccionó los componentes que deseaba instalar. Al volver a ejecutar el instalador, no intente instalar ningún componente que esté instalado actualmente.
Tal y como se describe en el siguiente ejemplo, se pueden producir problemas si instala y configura un nuevo agente de supervisión en un sistema en el que ya se están ejecutando otros agentes: • Hay agentes que se ejecutan en un sistema y se comunican con un Tivoli Enterprise Monitoring Server, denominado **TEMS1**. • Instala un nuevo agente en el mismo sistema y desea que este agente se comunique con otro servidor de supervisión, denominado **TEMS2**. • Al configurar el nuevo agente para comunicarse con **TEMS2**, todos los agentes ya existentes se vuelven a configurar para comunicarse con **TEMS2**.	Debe volver a configurar los agentes que ya existían para restaurar su conexión de comunicación con **TEMS1**. Por ejemplo, puede pulsar con el botón derecho en la fila para un agente específico en Manage Tivoli Enterprise Monitoring Services y seleccionar **Reconfigurar**. Para obtener más información sobre la reconfiguración, consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
Aparece un mensaje que indica que no se ha podido encontrar CMS en ejecución en CT_CMSLIST en el archivo de registro.	Si se visualiza un mensaje similar a "`No se ha podido encontrar CMS en ejecución en CT_CMSLIST`" en el archivo de registro, el agente no podrá establecer la conexión con el servidor de supervisión. Confirme si se cumplen estas condiciones: • ¿Existen varias tarjetas de interfaz de red (NIC) en el sistema? • Si existen varias NIC en el sistema, averigüe cuál está configurada para el servidor de supervisión. Compruebe que especifica los valores de puerto y nombre de host correctos para la comunicación en el entorno de IBM Tivoli Monitoring.

Tabla 13. Problemas y soluciones de la instalación y configuración (continuación)	
Problema	**Solución**
El sistema experimenta un uso elevado de la CPU.	**Proceso de agente:** Vea el uso de memoria del proceso KNPCMA. Si el uso de la CPU parece excesivo, reinicie el agente de supervisión. **Tarjetas de red:** Las configuraciones de tarjetas de red pueden deteriorar el rendimiento de un sistema. Cada secuencia de paquetes que recibe una tarjeta de red (suponiendo que se trate de una difusión o que esté destinada al sistema con bajo rendimiento) debe generar una interrupción de CPU y transferir los datos mediante el bus de E/S. Si la tarjeta de red en cuestión es una tarjeta de maestro de bus, el trabajo se puede descargar y una transferencia de datos entre la memoria y la tarjeta de red puede continuar sin utilizar la potencia de proceso de la CPU. Las tarjetas de maestro de bus son de 32 bits y están basadas en las arquitecturas de bus PCI o EISA.

Tabla 14. Problemas generales y soluciones para la desinstalación	
Problema	**Solución**

En sistemas Windows, la desinstalación de IBM Tivoli Monitoring no puede desinstalar todo el entorno.	Asegúrese de seguir el proceso de desinstalación general descrito en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*:
	
	1. Elimine el soporte de Tivoli Enterprise Monitoring Server Application completando los pasos siguientes:
	   a. Utilice Manage Tivoli Enterprise Monitoring Services.
	   b. Seleccione **Tivoli Enterprise Monitoring Server**.
	   c. Pulse con el botón derecho del ratón y seleccione **Avanzadas**.
	   d. Seleccione **Eliminar soporte de aplicación de TEMS**.
	   e. Seleccione el agente para eliminar su soporte de la aplicación.
	2. Desinstale primer los agentes de supervisión, tal como se muestra en los ejemplos siguientes:
	   • Desinstale el único agente de supervisión de una base de datos específica.
	   -o-
	   • Desinstale todas las instancias de un producto de supervisión, por ejemplo, IBM Tivoli Monitoring para bases de datos.
	3. Desinstale IBM Tivoli Monitoring.

Tabla 14. Problemas generales y soluciones para la desinstalación (continuación)	
Problema	**Solución**
La forma de eliminar los sistemas gestionados inactivos (sistema cuyo estado es fuera de línea (OFFLINE)) del árbol del navegador del portal no es obvia.	Siga los pasos siguientes para eliminar, pero no desinstalar, un sistema gestionado fuera de línea del árbol de navegación: 1. Pulse el icono **Enterprise** en el árbol de Navigator. 2. Pulse con el botón derecho del ratón y, a continuación, pulse **Espacio de trabajo** > **Estatus de sistemas gestionados**. 3. Pulse el botón derecho del ratón en el sistema gestionado fuera de línea y seleccione **Borrar entrada fuera de línea**. Para desinstalar el agente de supervisión, utilice el procedimiento descrito en *IBM Tivoli Monitoring: Guía de instalación y configuración*.
Tras la eliminación remota desde el Tivoli Enterprise Portal de una instancia en ejecución, el nombre de instancia sigue figurando en la lista de inicio.	Abra la lista de configuración para eliminar el nombre de instancia en la Lista de inicio.

Tabla 14. Problemas generales y soluciones para la desinstalación (continuación)	
Problema	**Solución**
IBM Tivoli Monitoring puede no generar un nombre exclusivo para los componentes de supervisión debido al truncamiento de nombres que el producto genera automáticamente.	Si el agente admite varias instancias, IBM Tivoli Monitoring crea automáticamente un nombre para cada componente de supervisión concatenando el nombre de subsistema, el nombre de host y el código de producto separados por dos puntos (*nombre_subsistema*: *nombre_host*: KNP). **Nota:** Cuando supervisa un sistema de múltiples nodos, por ejemplo, una base de datos, IBM Tivoli Monitoring añade un nombre de subsistema al nombre concatenado, generalmente un nombre de instancia de base de datos. La longitud del nombre que genera IBM Tivoli Monitoring puede ser de 32 caracteres como máximo. El truncamiento puede hacer que varios componentes tengan el mismo nombre de 32 caracteres. Si se produce este problema, acorte la porción del nombre correspondiente a *nombreHost*, de esta manera: 1. Abra el archivo de configuración para el agente de supervisión, que se encuentra en la siguiente vía de acceso: • **En UNIX y Linux:** `itm_home/config/`*`código_producto`*`.ini` y *`código_producto`*`.config`. Por ejemplo, los nombres de archivo para el agente de supervisión del SO de UNIX son `ux.ini` y `ux.config`. 2. Localice la línea que empiece por `CTIRA_HOSTNAME=`. 3. Escriba un nuevo nombre para el nombre de host que sea un nombre exclusivo más corto para el sistema principal. El nombre concatenado final con el nombre de subsistema, el nombre de host nuevo y KNP no puede tener más de 32 caracteres. **Nota:** Compruebe que el nombre obtenido sea exclusivo en relación con los componentes de supervisión existentes que se hayan registrado anteriormente en el Tivoli Enterprise Monitoring Server. 4. Guarde el archivo. 5. Reinicie el agente.

Resolución de problemas con el despliegue remoto

Se pueden producir problemas con el despliegue y la eliminación remotos del software de agente utilizando el proceso de despliegue remoto de agente.

La siguiente tabla contiene problemas y soluciones relacionados con el despliegue remoto.

Tabla 15. Problemas y soluciones para el despliegue remoto	
Problema	**Solución**
Mientras utiliza la función de despliegue remoto para instalar el agente de supervisión, aparece una ventana de mandatos vacía en el sistema destino. Este problema se produce cuando el destino del despliegue remoto es un sistema Windows. (Para obtener más información sobre la función de despliegue remoto, consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.)	No cierre ni modifique esta ventana. Forma parte del proceso de instalación y desaparecerá automáticamente.
No se puede eliminar un agente de supervisión cuando se utiliza el proceso de eliminación remoto en el navegador o el escritorio de Tivoli Enterprise Portal.	Este problema puede producirse al intentar efectuar el proceso de eliminación remota inmediatamente después de reiniciar el Tivoli Enterprise Monitoring Server. Debe dejar tiempo para que el agente de supervisión renueve su conexión con el Tivoli Enterprise Monitoring Server antes de iniciar el proceso de eliminación remota.

Resolución de problemas relacionados con los espacios de trabajo

Se pueden producir problemas relacionados con los espacios de trabajo generales y con espacios de trabajo específicos de un agente.

La siguiente tabla contiene problemas y soluciones relacionados con los espacios de trabajo.

Tabla 16. Problemas y soluciones de los espacios de trabajo

Problema	**Solución**
Los componentes de la aplicación de proceso están disponibles, pero el estado Disponibilidad muestra PROCESS_DATA_NOT_ AVAILABLE.	Este problema se produce porque el objeto de rendimiento PerfProc está inhabilitado. Cuando se da esta condición, IBM Tivoli Monitoring no puede recopilar datos de rendimiento para este proceso. Siga estos pasos para confirmar que este problema existe y para solucionarlo: 1. En el menú **Iniciar** de Windows, pulse **Ejecutar**. 2. Especifique `perfmon.exe` en el campo **Abrir** de la ventana **Ejecutar**. Se abre la ventana **Rendimiento**. 3. Pulse el signo de suma (+) de la barra de herramientas. Se visualiza la ventana **Agregar contadores**. 4. Busque **Proceso** en el menú **Objeto de rendimiento**. 5. Realice una de las acciones siguientes: • Si ve **Proceso** en el menú, el objeto de rendimiento PerfProc está habilitado y el problema procede de un origen diferente. Es posible que necesite ponerse en contacto con el Soporte de software de IBM. • Si no ve **Proceso** en el menú, utilice el programa de utilidad de Microsoft del Sitio web de operaciones de Microsoft.com para habilitar el objeto de rendimiento PerfProc. El objeto de rendimiento **Proceso** se hace visible en el menú **Objeto de rendimiento** de las ventanas **Agregar contadores** e IBM Tivoli Monitoring es capaz de detectar datos de disponibilidad. 6. Reiniciar el agente de supervisión.
El nombre del atributo no aparece en una vista de diagrama de barras o gráfico.	Cuando una vista de diagrama o gráfico que incluye el atributo se visualiza con un tamaño pequeño, se muestra un espacio en blanco en lugar de un nombre truncado. Para ver el nombre del atributo, expanda la vista del diagrama hasta que haya espacio suficiente para mostrar todos los caracteres del nombre del atributo.
En la parte inferior de cada una de las vistas, aparece el siguiente error KFWITM220E del espacio de trabajo histórico: `La solicitud ha fallado durante la ejecución`.	Compruebe que configura todos los grupos que proporcionan datos a la vista. En la vista Configuración histórica, asegúrese de que la recopilación de datos está configurada para todos los grupos que suministran datos a la vista.
Cuando se utiliza un nombre de proceso largo en la situación, el nombre del proceso se trunca.	El comportamiento previsto es que se trunquen los nombres de proceso o de servicio para las situaciones de la tabla Disponibilidad en la visualización del portal. La longitud máxima del nombres es 100 bytes.

Tabla 16. Problemas y soluciones de los espacios de trabajo (continuación)	
Problema	**Solución**
No se muestran los datos de supervisión normales (no históricos).	Compruebe la formación de las consultas que utiliza para recopilar los datos. Por ejemplo, busque sentencias de SQL no válidas.
No se visualiza ninguna fila de datos para aplicaciones de 64 bits en los espacios de trabajo cuando el agente de supervisión se ejecuta en un sistema operativo de 64 bits.	Tivoli Enterprise Portal Muestra datos únicamente para aplicaciones de 32 bits. No hay ninguna solución disponible para este problema en este momento.

Resolución de problemas de situaciones

Se pueden producir problemas con las situaciones y la configuración de situaciones.

La siguiente tabla contiene problemas y soluciones para las situaciones.

Tabla 17. Problemas y soluciones de situaciones	
Problema	**Solución**
La supervisión de actividades requiere demasiado espacio de disco.	Compruebe los valores de registro de rastreo RAS. Por ejemplo, los registros de rastreo crecen rápidamente cuando se aplica la opción de registro ALL(TODO).
Una fórmula que utiliza operadores matemáticos parece ser incorrecta. Por ejemplo, si supervisa un sistema Linux, la fórmula que realiza el cálculo cuando el valor de **Memoria libre** está por debajo del 10 por ciento del valor de **Memoria total** no funciona: `LT #'Linux_VM_Stats.Total_Memory' / 10`	Esta fórmula es incorrecta porque los predicados de situación sólo soportan operadores lógicos. Las fórmulas no pueden tener operadores matemáticos. **Nota:** El Editor de situaciones ofrece soluciones alternativas a los operadores matemáticos. En este ejemplo, puede seleccionar el atributo **% Memoria libre** y evitar el uso de operadores matemáticos.
Desea cambiar el aspecto de las situaciones cuando se visualizan en el árbol de navegación.	1. Pulse con el botón derecho del ratón en un elemento del árbol de Navegación. 2. Pulse **Situaciones** en el menú. Se visualiza la ventana **Editor de situaciones**. 3. Seleccione la situación que desee modificar. 4. Utilice el menú **Estado** para establecer el estado y el aspecto de la situación cuando se desencadene. **Nota:** el valor **Estado** no está relacionado con valores de gravedad en IBM Tivoli Enterprise Console.

Tabla 17. Problemas y soluciones de situaciones (continuación)	
Problema	**Solución**
Cuando se desencadena una situación en el grupo de atributos Registro de sucesos, permanece en la consola de sucesos de situaciones mientras la entrada de ID de suceso esté presente en el espacio de trabajo del registro de sucesos. Cuando se elimina esta entrada de ID de suceso del espacio de trabajo Registro de sucesos en Tivoli Enterprise Portal, también se borra la situación aun cuando el problema real que ha producido el suceso no esté resuelto y la entrada de ID de suceso también está presente en el Visor de sucesos de Windows.	Se produce un error de tiempo de espera en la memoria caché de sucesos para el grupo Registro de sucesos de NT. Aumente el tiempo de memoria caché de la recopilación de registro de sucesos para satisfacer los requisitos añadiendo la siguiente variable y valor de tiempo de espera en el archivo K*pc*ENV para el agente (donde *pc* es el código de producto de dos letras): `CDP_NT_EVENT_LOG_CACHE_TIMEOUT=3600` Esta variable determina durante cuánto tiempo se mantienen los sucesos del registro de sucesos NT.
La situación de un agente en particular no es visible en Tivoli Enterprise Portal.	Abra el Editor de situaciones. Acceda a la vista de todos los servidores gestionados. Si no se visualiza la situación, confirme que el servidor de supervisión se ha inicializado para el agente.
El intervalo de supervisor es demasiado largo.	Acceda a la vista del Editor de situaciones para la situación que desea modificar. Examine el área **Intervalo de muestreo** de la pestaña **Fórmula**. Ajuste el intervalo de tiempo según sea necesario.
La situación no se ha activado al inicio.	Recicle manualmente la situación tal como se indica a continuación: 1. Pulse el botón derecho sobre la situación y seleccione **Detener la situación**. 2. Pulse con el botón derecho del ratón la situación y seleccione **Iniciar situación**. **Nota:** Se puede evitar esta situación de forma permanente seleccionando la casilla de verificación **Ejecutar al inicio** de la vista Editor de situación para una situación concreta.
La situación no aparece.	Pulse el separador **Acción** y compruebe si la situación tiene una acción correctora automatizada. Dicha acción se puede producir directamente o a través de una política. Es posible que la situación se resuelva tan rápidamente que no sea posible ver el suceso o la actualización en la interfaz gráfica de usuario.
No se ha producido un suceso de alerta aunque el predicado se ha especificado correctamente.	Compruebe los registros, informes y espacios de trabajo.
Una situación se activa en un objeto gestionado inesperado.	Confirme que ha distribuido e iniciado la situación en el sistema gestionado correcto.
El producto no ha distribuido la situación a un sistema gestionado.	Pulse el separador **Distribución** y compruebe la configuración de distribución de la situación.

Tabla 17. Problemas y soluciones de situaciones (continuación)

Problema	**Solución**

La situación no se activa.	Este problema puede deberse a que haya predicados incorrectos en la fórmula que define la situación. Por ejemplo, el objeto gestionado muestra un estado que normalmente desencadena un suceso de supervisión, pero la situación no es verdadera porque se ha especificado el atributo incorrecto en la fórmula.
	
	En la pestaña **Fórmula**, analice los predicados de la manera siguiente:
	
	1. Pulse en el icono **fx** del área **Fórmula**. Se visualiza la ventana **Mostrar fórmula**.
	   a. Confirme los datos siguiente en el área **Fórmula** de la ventana:
	   • Los atributos que desea supervisar están especificados en la fórmula.
	   • Las situaciones que desea supervisar están especificadas en la fórmula.
	   • Los operadores lógicos en la fórmula coinciden con el objetivo de supervisión.
	   • Los valores numéricos de la fórmula coinciden con su objetivo de supervisión.
	   b. (Opcional) Marque el recuadro de selección **Mostrar fórmula detallada** para ver los nombres originales de los atributos de la aplicación o del sistema operativo que está supervisando.
	   c. Pulse **Aceptar** para cerrar la ventana **Mostrar fórmula**.
	2. (Opcional) En el área **Fórmula** del separador **Fórmula**, asigne temporalmente valores numéricos que desencadenen de inmediato un suceso de supervisión. Si se desencadena un suceso, se confirmará que el resto de predicados en la fórmula son válidos.
	
	Nota: Tras efectuar esta prueba, debe restaurar los valores numéricos a los niveles válidos a fin de no generar datos de supervisión excesivos en función de los valores temporales.

Los sucesos de situación no aparecen en la vista Consola de sucesos en el espacio de trabajo.	Asocie la situación con un elemento de Navigator. **Nota:** No es necesario visualizar la situación en el espacio de trabajo. Es suficiente que la situación se asocie con cualquier elemento del Navegador.

Tabla 17. Problemas y soluciones de situaciones (continuación)	
Problema	**Solución**
No dispone de acceso a una situación.	**Nota:** Debe tener privilegios de administrador para realizar estos pasos. 1. Pulse **Editar** > **Administrar usuarios** para acceder a la ventana **Administrar usuarios**. 2. En el área **Usuarios**, seleccione el usuario cuyos privilegios desea modificar. 3. En el separador **Permisos**, el separador **Aplicaciones** y el separador **Vistas del navegador**, seleccione los permisos o privilegios correspondientes al rol del usuario. 4. Haga clic en **Aceptar**.

Solución de problemas relacionados con los mandatos de actuación

Se pueden producir problemas con los mandatos de actuación.

La siguiente tabla contiene problemas y soluciones que pueden producirse con los mandatos de actuación.

Tabla 18. Problemas y soluciones de mandatos de situación	
Problema	**Solución**
Los mandatos de actuación a menudo tardan varios minutos en completarse.	Espere varios minutos. Si no ve un mensaje avisándole de que el mandato se ha completado, intente ejecutar el mandato manualmente.
Las situaciones no activan los mandatos de Actuación.	Intente ejecutar manualmente el mandato de Actuación en Tivoli Enterprise Portal. Si el mandato de actuación funciona, busque problemas de configuración en la situación.

Referencia de agente de ITM

El agente de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition proporciona espacios de trabajo, atributos y situaciones predefinidos. Se puede ampliar con mandatos y políticas Take Action.

Referencia de espacios de trabajo

Un espacio de trabajo es el área de trabajo de la ventana de aplicación de Tivoli Enterprise Portal. El Navegador contiene una lista de los espacios de trabajo proporcionados por el agente.

Acerca de los espacios de trabajo

Utilice el navegador para seleccionar el espacio de trabajo que desea ver. Como parte de la ventana de aplicación, la barra de estado muestra el nombre y número de puerto del servidor de Tivoli Enterprise Portal al que se aplica la información visualizada y el ID del usuario actual.

Cuando seleccione un elemento en el navegador, se visualizará un espacio de trabajo predeterminado. Si pulsa el botón derecho del ratón sobre un elemento de navegador, se mostrará un menú que incluirá un elemento Espacio de trabajo. El elemento Espacio de trabajo contiene una lista de espacios de trabajo para dicho elemento de navegador. Todos los espacios de trabajo tienen al menos una vista. Algunas vistas tienen enlaces a otros espacios de trabajo. También puede utilizar la herramienta Galería de espacios de trabajo como se describe en *Tivoli Enterprise Portal: Guía del usuario* para abrir espacios de trabajo.

Los espacios de trabajo del navegador se muestran en una vista Física que muestra la empresa como una correlación física o una vista lógica llenada dinámicamente que es específica del agente. También puede crear una vista Lógica. La vista Física es la vista predeterminada.

Este agente de supervisión proporciona espacios de trabajo predefinidos. No puede modificar ni suprimir los espacios de trabajo predefinidos, pero puede crear espacios de trabajo nuevos editándolos y guardando los cambios con un nombre diferente.

El IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition proporciona varios espacios de trabajo predeterminados. Estos espacios de trabajo se visualizan en el navegador bajo los nodos y subnodos siguientes para este agente de supervisión:

IBM Tivoli Monitoring for Tivoli Network Manager
Corresponde a una instancia de agente y contiene espacios de trabajo de nivel de instancia de agente.

Cuando se define una única instancia del agente de supervisión en un sistema, el nodo de nivel superior es IBM Tivoli Monitoring for Tivoli Network Manager - *Instancia*:*Nombre_host*:NP. El espacio de trabajo IBM Tivoli Monitoring for Tivoli Network Manager está definido en este nodo. Cuando en un sistema se definen varias instancias del agente de supervisión, el nodo de nivel superior pasa a ser IBM Tivoli Monitoring for Tivoli Network Manager. El espacio de trabajo IBM Tivoli Monitoring for Tivoli Network Manager no está definido en este nodo. Se crea una instancia para cada nodo denominada *Instancia*:*Nombre_host*:NP. Un espacio de trabajo denominado *Instancia*: *Nombre_host*: NP se asocia con el nodo de instancia. Este espacio de trabajo es comparable con el espacio de trabajo IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.

Las vistas del espacio de trabajo pueden ser cualquier combinación de vistas basadas en consulta, vistas de sucesos y vistas de propósito especial.

Información adicional acerca de espacios de trabajo

Para obtener más información sobre cómo crear, personalizar y trabajar con espacios de trabajo, consulte "Uso de espacios de trabajo" en *Tivoli Enterprise Portal: Guía del usuario*.

Algunos grupos de atributos para este agente de supervisión no pueden estar representados en los espacios de trabajo predefinidos o en vistas para este agente.

Espacios de trabajo predefinidos

El agente de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition proporciona espacios de trabajo predefinidos, que están organizados por elemento de navegador.

Elementos de Navegador a nivel de agente

- Elemento de navegador de IBM Tivoli Monitoring for Tivoli Network Manager
  - Espacio de trabajo de IBM Tivoli Monitoring for Tivoli Network Manager
- Elemento de navegador Disponibilidad
  - Espacio de trabajo Disponibilidad.
- Elemento de navegador Descubrimiento
  - Espacio de trabajo Descubrimiento.
- Elemento de navegador Red
  - Espacio de trabajo Red.

Descripciones de espacios de trabajo

Cada descripción de espacio de trabajo proporciona información sobre éste, como por ejemplo la finalidad, y una lista de vistas en el espacio de trabajo.

Los espacios de trabajo se listan bajo los elementos de navegador.

Elemento de navegador de IBM Tivoli Monitoring for Tivoli Network Manager
Las descripciones de espacios de trabajo están organizadas por el elemento de navegador para el que son pertinentes los espacios.

Espacio de trabajo de IBM Tivoli Monitoring for Tivoli Network Manager
Este espacio de trabajo muestra el estado general de la aplicación Tivoli Network Manager.

Este espacio de trabajo contiene las siguientes vistas:

Disponibilidad
Muestra el estado de los procesos de Tivoli Network Manager.

Descubrimiento
Muestra el estado de Tivoli Network Manager.

Red
Muestra las métricas de Tivoli Network Manager.

Elemento de navegador Disponibilidad
Las descripciones de espacios de trabajo están organizadas por el elemento de navegador para el que son pertinentes los espacios.

Espacio de trabajo Disponibilidad
El espacio de trabajo Disponibilidad muestra del estado general de la aplicación.

Este espacio de trabajo contiene las siguientes vistas:

Disponibilidad
Muestra el estado de cada componente en la aplicación. Cada proceso se muestra con un nombre descriptivo, el nombre del proceso en ejecución y el estado del proceso (UP, DOWN o PROCESS_DATA_NOT_AVAILABLE). Si el estado del componente es DOWN (para un proceso o servicio), éste se resalta con un fondo de color rojo.

Procesador
Muestra la cantidad de CPU utilizada por cada proceso que sea un componente de la aplicación. Muestra los dos componentes principales del uso de CPU: el tiempo de privilegio, que es el tiempo que el proceso ha invertido en el kernel, y el tiempo de modalidad de usuario, que es el tiempo invertido en la ejecución del código del proceso.

Hebras
Muestra los hebras utilizados por cada proceso que sea un componente de la aplicación.

Memoria
Muestra la cantidad de memoria consumida por cada proceso que es un componente de la aplicación. Se muestran este tamaño (virtual) total del proceso y el tamaño del proceso en memoria (conjunto de trabajo).

Elemento de navegador Descubrimiento
Las descripciones de espacios de trabajo están organizadas por el elemento de navegador para el que son pertinentes los espacios.

Espacio de trabajo Descubrimiento
El espacio de descubrimiento muestra el estado del descubrimiento de red realizado por Tivoli Network Manager y recopila las métricas utilizadas para generar informes.

Este espacio de trabajo contiene las siguientes vistas:

Current_Discovery
Esta vista muestra una instantánea del descubrimiento actual. Los valores están todos establecidos en cero, no hay ningún descubrimiento disponible de momento.

Duración del último descubrimiento
Muestra una instantánea de la duración de cada fase de último descubrimiento.

Utilización de la memoria en KBytes del último descubrimiento
Muestra una instantánea de la utilización de la memoria para procesar el último descubrimiento completado.

Objetos descubiertos
Muestra una instantánea de los objetos descubiertos durante el último descubrimiento completado.

Estado del agente
Muestra una instantánea del estado de cada agente configurado en el sistema.

Elemento de navegador Supervisión
Las descripciones de espacios de trabajo están organizadas por el elemento de navegador para el que son pertinentes los espacios.

Espacio de trabajo Supervisión
Este espacio de trabajo muestra información relacionada con la supervisión de Tivoli Network Manager. Este espacio de trabajo recopila métricas de supervisión de red utilizados para sondear Tivoli Network Manager y a generar informes.

Este espacio de trabajo contiene las siguientes vistas:

Muestra el número total de objetos de MIB recuperados por segundo.

Número de dispositivos sondeados por tipo de definición de sondeo
Muestra el número total de dispositivos de sondeo por el tipo de definición de sondeo.

Paquetes enviados por el sondeador
Muestra el número total de paquetes enviados por el sondeador.

Paquetes procesados por el sondeador
Muestra el número total de paquetes procesados por el sondeador.

Errores y respuestas de tiempo de espera excedido de SNMP
Muestra el número total de errores y tiempos de espera excedidos de SNMP.

Elemento de navegador Red
Las descripciones de espacios de trabajo están organizadas por el elemento de navegador para el que son pertinentes los espacios.

Espacio de trabajo Red
Este espacio de trabajo muestra información relacionada con una red supervisada por Tivoli Network Manager. El espacio de trabajo recopila métricas de descubrimiento de red utilizadas para supervisar la red y generar informes.

Este espacio de trabajo contiene las siguientes vistas:

Elementos de red
Muestra el número total de elementos de red listados por tipo en la red supervisada.

Dispositivos con y sin acceso SNMP
Muestra el número total de dispositivos con y sin acceso SNMP.

Interfaces activas e inactivas
Muestra un contador del estado operativo de la interfaz que puede estar en UP o DOWN.

Referencia de atributos

Los atributos son las propiedades de aplicación que son medidas y notificadas por el agente.

Acerca de los atributos

Los atributos están organizados en grupos de atributos. Los atributos de un grupo de atributos están relacionados con un único objeto como, por ejemplo, una aplicación o a un único tipo de datos, como por ejemplo información de estado.

Los atributos de un grupo se pueden utilizar en consultas, vistas basadas en consultas, situaciones, flujos de trabajo de política, definiciones de actuación, y definiciones de inicio de aplicación. Las vistas de diagrama o de tabla y las situaciones son dos ejemplos de la forma en que los atributos de un grupo se pueden utilizar:

- Vistas de diagrama o tabla

  Los atributos se visualizan en vistas de diagramas y tablas. Las vistas de gráfico y tabla utilizan consultas para especificar los valores de atributos que se solicitan de un agente de supervisión. Puede utilizar el Editor de propiedades para aplicar filtros y establecer estilos para definir el contenido y el aspecto de una vista en base a una consulta existente.
- Situaciones

  Los atributos permiten crear situaciones que supervisan el estado del sistema operativo, la base de datos o la aplicación. Una situación describe una condición que desea someter a prueba. Cuando inicie una situación, los valores que asigne a los atributos de situación se comparan con los valores recopilados por el agente y se registra un *suceso* si la condición se cumple. Los iconos de indicador que se muestran en el navegador alertan sobre los sucesos.

Información adicional sobre los atributos

Para obtener más información sobre la utilización de los atributos y de grupos de atributos, consulte la publicación *Tivoli Enterprise Portal: Guía del usuario*.

Grupos de atributos del agente de supervisión

El agente contiene los siguientes grupos de atributos.

- Nombre de grupo de atributos: Estado del agente
  - Nombre de tabla: KNPAGTSTS
- Nombre de grupo de atributos: Disponibilidad
  - Nombre de tabla: KNPAVAIL
- Nombre de grupo de atributos: Descubrimiento actual
  - Nombre de tabla: KNPCURDISC
- Nombre de grupo de atributos: Dispositivos sondeados
  - Nombre de tabla: KNPDEVPOLL
- Nombre de grupo de atributos: Dispositivos con acceso SNMP
  - Nombre de tabla: KNPSNMPAC
- Nombre de grupo de atributos: Entidades en BD de modelo
  - Nombre de tabla: KNPTOTENT
- Nombre de grupo de atributos: Interfaces activas e inactivas
  - Nombre de tabla: KNPNODETO
- Nombre de grupo de atributos: Último descubrimiento
  - Nombre de tabla: KNPLSTDISC
- Nombre de grupo de atributos: Objetos de MIB recuperados
  - Nombre de tabla: KNPMIBOBJ
- Nombre de grupo de atributos: Elementos de red
  - Nombre de tabla: KNPNETELEM
- Nombre de grupo de atributos: Objetos descubiertos
  - Nombre de tabla: KNPOBJDISC
- Nombre de grupo de atributos: Paquetes enviados y procesados por sondeador

  - Nombre de tabla: KNPPACPROC
- Nombre de grupo de atributos: Estado de objeto de rendimiento
  - Nombre de tabla: KNPPOBJST
- Nombre de grupo de atributos: Capacidad de sondeo
  - Nombre de tabla: KNPCAPPACT
- Nombre de grupo de atributos: Errores y tiempos de espera excedidos de SNMP
  - Nombre de tabla: KNPSNMPERR
- Nombre de grupo de atributos: Cola de elemento de trabajo
  - Nombre de tabla: KNPWORKQUE

Atributos en cada grupo de atributos

Los atributos en cada grupo de atributos recopilan datos que el agente utiliza para supervisar.

Grupo de atributos Estado de agente
Esta vista muestra una instantánea del estado de cada agente configurado en el sistema.

Descripciones de atributo

La lista siguiente contiene información sobre cada atributo del grupo de atributos Estado del agente:

atributo Conexiones de agentes

Descripción
Muestra el número total de conexiones de agente.

Tipo
Entero (indicador de 32 bits)

Nombre de agente de atributo Este atributo es un atributo clave.

Descripción
Muestra el nombre de agente configurado en el sistema.

Tipo
Serie

Atributo Estado del agente

Descripción
Muestra el estado de los agentes utilizados por el descubrimiento.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: Estado inactivo (0), No iniciado todavía (1), Iniciándose (2), Recibiendo y enviando datos (3), Proceso activo pero finalizado (4), Estaba activo pero ha concluido (5). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Nodo Este atributo es un atributo de clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Disponibilidad
El conjunto de datos Disponibilidad contiene los datos de disponibilidad de todos los procesos y servicios que componen esta aplicación.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Disponibilidad:

Atributo Componente de aplicación Este atributo es un atributo de clave.

Descripción
Nombre descriptivo de un componente de la aplicación.

Tipo
serie

Atributo Línea de mandatos

Descripción
El nombre de programa y cualquier argumento especificado en la línea de mandatos al iniciarse el proceso. Para una prueba de funcionalidad o servicio, este atributo tiene un valor N/A.

Tipo
Cadena con valores enumerados. Se definen los valores siguientes: N/A (N/A). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Nombre completo

Descripción
Nombre completo del proceso, incluida la ruta.

Tipo
cadena con valores enumerados. Se definen los valores siguientes: N/A (N/A). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Mensaje de prueba de funcionalidad

Descripción
Mensaje de texto que corresponde al Estatus de prueba de funcionalidad. Este atributo sólo es válido para las pruebas de funcionalidad.

Tipo
Cadena con valores enumerados. Se definen los valores siguientes: N/A (N/A). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Estado de prueba de funcionalidad

Descripción
Código de retorno de la prueba de funcionalidad. Cuando la aplicación supervisada se ejecuta correctamente, aparece 'SUCCESS'. Se visualiza 'NOT_RUNNING' cuando no se ejecuta correctamente. Se visualiza 'N/A' cuando la fila no representa una prueba de funcionalidad.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: SUCCESS (0), N/A (1), GENERAL ERROR (2), WARNING (3), NOT RUNNING (4), DEPENDENT NOT RUNNING (5), ALREADY RUNNING (6), PREREQ NOT RUNNING (7), TIMED OUT (8), DOESNT EXIST (9), UNKNOWN (10), DEPENDENT STILL RUNNING (11), INSUFFICIENT USER AUTHORITY (12). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Nombre

Descripción
El nombre del proceso, servicio o prueba de funcionalidad. Este nombre coincide con el nombre ejecutable del proceso, el nombre abreviado del servicio o el nombre del proceso utilizado para probar la aplicación.

Tipo
Cadena con valores enumerados. Se definen los valores siguientes: N/A (N/A). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Errores de página por segundo

Descripción
La tasa de anomalías de página del proceso medida en anomalías por segundo. Este atributo solo contiene datos válidos para procesos.

Tipo
Entero (indicador de 32 bits)

Atributo Porcentaje de tiempo con privilegios

Descripción
Porcentaje del tiempo de CPU disponible que este proceso utiliza para la operación privilegiada.

Tipo
Entero (indicador de 32 bits)

Atributo Porcentaje de tiempo de procesador

Descripción
El porcentaje del tiempo transcurrido que este proceso ha utilizado el procesador para ejecutar instrucciones.

Tipo
Entero (indicador de 32 bits)

Atributo Porcentaje de tiempo en modalidad de usuario

Descripción
Porcentaje del tiempo de CPU utilizado por este proceso para operación en modo de usuario.

Tipo
Entero (indicador de 32 bits)

Atributo PID

Descripción
ID de proceso asociado con el proceso. Este atributo solo contiene datos válidos para procesos.

Tipo
Entero (indicador de 32 bits)

Atributo Estado

Descripción
Estado del componente de la aplicación.

- Para los procesos 'UP', 'DOWN', 'WARNING' o 'PROCESS_DATA_NOT_AVAILABLE': Se visualizará 'PROCESS_DATA_NOT_AVAILABLE' para un proceso cuando el proceso correspondiente está en ejecución, pero no se puede recopilar la información sobre uso de recursos para ese proceso.
- Para los servicios 'UP', 'DOWN' o 'UNKNOWN': Se visualizará 'UNKNOWN' cuando el servicio no esté instalado.
- Para pruebas de funcionalidad: Se visualiza 'PASSED' o 'FAILED'.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: DOWN (0), UP (1), WARNING (2), UNKNOWN (3), PASSED (4), FAILED (5), PROCESS DATA NOT AVAILABLE (6). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Recuento de hebras

Descripción
Número de hebras que este proceso ha asignado actualmente. Este atributo solo contiene datos válidos para procesos.

Tipo
Entero (indicador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Atributo Tipo

Descripción
El tipo del componente de la aplicación. Los componentes son procesos, servicios o pruebas de funcionalidad.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: PROCESS (0), SERVICE (1), FUNCTIONALITY TEST (2). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Tamaño virtual

Descripción
El tamaño virtual (en MB) del proceso.

Tipo
Entero (indicador de 32 bits)

Atributo Tamaño de conjunto de trabajo

Descripción
Tamaño del conjunto de trabajo del proceso en MB. Este atributo solo contiene datos válidos para procesos.

Tipo
Entero (indicador de 32 bits)

Grupo de atributos Descubrimiento actual
Esta vista muestra una instantánea del descubrimiento actual. Si no hay un descubrimiento actual, todos los valores serán establecidos en cero.

Descripciones de atributo

La lista siguiente contiene información sobre cada atributo del grupo de atributos Descubrimiento actual:

Atributo Estado de apagón

Descripción
Estado de apagón

Tipo
Entero con valores enumerados. Se definen los valores siguientes: False (0), True (1). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Número de ciclos

Descripción
El número de ciclos de descubrimiento.

Tipo
Entero (indicador de 32 bits)

Atributo Modalidad de descubrimiento

Descripción
Modalidad de descubrimiento.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: Full (0), Partial (1). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Fase de descubrimiento

Descripción
Fase de descubrimiento

Tipo
Entero con valores enumerados. Se definen los valores siguientes: Phase 0 (Not Running) (0), Phase 1 (1), Phase 2 (2), Phase 3 (3), Phase 4 (4). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Proceso necesario

Descripción
El proceso de descubrimiento necesario.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: No (0), Yes (1). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Dispositivos sondeados
Esta vista muestra el número total de dispositivos sondeados por el tipo de definición de sondeo.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Dispositivos sondeados:

Atributo Direcciones

Descripción
Muestra el número total de direcciones que están siendo sondeadas.

Tipo
Entero (indicador de 32 bits)

Atributo Entidades

Descripción
Muestra el número total de entidades supervisadas.

Tipo
Entero (indicador de 32 bits)

Atributo Nodo Este atributo es un atributo de clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Nombre de política

Descripción
Muestra el nombre de política que está sondeando los dispositivos.

Tipo
Serie

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Dispositivos con acceso SNMP
Muestra el número total de dispositivos con y sin acceso SNMP.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Dispositivos con acceso SNMP:

Atributo Sin acceso SNMP

Descripción
Muestra el número total de dispositivos sin acceso SNMP.

Tipo
Entero (indicador de 32 bits)

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Acceso SNMP

Descripción
Muestra el número total de dispositivos con acceso SNMP.

Tipo
Entero (indicador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Entidades en BD de modelo
Muestra el número total de entidades definidas en la base de datos modelo.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Entidades en BD modelo:

Atributo Entidades

Descripción
Muestra el número total de entidades definidas en la base de datos modelo.

Tipo
Entero (indicador de 32 bits)

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Interfaces activas e inactivas
Muestra un contador del estado operativo de las interfaces, que pueden estar en estado ACTIVO e INACTIVO.

Descripciones de atributo

La lista siguiente contiene información sobre cada atributo del grupo de atributos Interfaces activas e inactivas:

Atributo Inactiva

Descripción
Muestra el número total de interfaces inactivas.

Tipo
Entero (indicador de 32 bits)

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Atributo Activo

Descripción
Muestra el número total de interfaces activas.

Tipo
Entero (indicador de 32 bits)

Grupo de atributos Último descubrimiento

Esta vista muestra una instantánea de la duración y utilización de memoria de cada fase del último descubrimiento completado.

Descripciones de atributo

La lista siguiente contiene información sobre cada atributo del grupo de atributos Último descubrimiento:

Atributo Memoria de finalización

Descripción
Muestra la memoria de finalización del descubrimiento.

Tipo
Entero (indicador de 32 bits)

Atributo Hora de finalización

Descripción
Muestra la hora de finalización del descubrimiento.

Tipo
Serie

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Memoria de la fase uno

Descripción
Muestra el uso de memoria de la fase uno.

Tipo
Entero (indicador de 32 bits)

Atributo Inicio de la fase uno

Descripción
Muestra la hora de inicio de la fase uno.

Tipo
Serie

Atributo Memoria de la fase tres

Descripción
Muestra el uso de memoria de la fase tres.

Tipo
Entero (indicador de 32 bits)

Atributo Inicio de la fase tres

Descripción
Muestra la hora de inicio de la fase tres.

Tipo
Serie

Atributo Memoria de la fase dos

Descripción
Muestra el uso de memoria de la fase dos.

Tipo
Entero (indicador de 32 bits)

Atributo Inicio de la fase dos

Descripción
Muestra la hora de inicio de la fase dos.

Tipo
Serie

Atributo Hora de inicio de proceso

Descripción
Muestra la hora de inicio del proceso de datos.

Tipo
Serie

Atributo Memoria inicial

Descripción
Muestra el tamaño inicial de la memoria de descubrimiento.

Tipo
Entero (indicador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Atributo Tiempo de descubrimiento total

Descripción
Muestra el tiempo total empleado por el descubrimiento.

Tipo
Serie

Grupo de atributos Objetos de MIB recuperados
Muestra el número total de objetos de MIB recuperados por segundo.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Objetos de MIB recuperados:

Atributo Nodo Este atributo es un atributo de clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Atributo Total

Descripción
Muestra el número total de objetos de MIB recuperados por segundo.

Tipo
Entero (indicador de 32 bits)

Grupo de atributos Elementos de red
Esta vista muestra el número total de elementos listados por tipo en una red supervisada.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Elementos de red:

Atributo Tarjeta

Descripción
Muestra el número total de tarjetas.

Tipo

Entero (indicador de 32 bits)

Atributo Chasis

Descripción
Muestra el número total de chasis.

Tipo
Entero (indicador de 32 bits)

Atributo Interfaces

Descripción
Muestra el número total de interfaces.

Tipo
Entero (indicador de 32 bits)

Atributo Interfaz lógica

Descripción
Muestra el número total de interfaces lógicas.

Tipo
Entero (indicador de 32 bits)

Atributo Módulo

Descripción
Muestra el número total de módulos.

Tipo
Entero (indicador de 32 bits)

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo PSU

Descripción
Muestra el número total de PSU.

Tipo
Entero (indicador de 32 bits)

Atributo Subred

Descripción
Muestra el número total de subredes.

Tipo
Entero (indicador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo

Serie

Atributo Desconocido

Descripción
Muestra el número total de Desconocido.

Tipo
Entero (indicador de 32 bits)

Atributo Objetos de VLAN

Descripción
Muestra el número total de objetos de VLAN.

Tipo
Entero (indicador de 32 bits)

Grupo de atributos Objetos descubiertos
Esta vista muestra una instantánea de los objetos descubiertos durante el último descubrimiento completado.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Objetos descubiertos:

Atributo Dispositivos

Descripción
Muestra el número total de dispositivos.

Tipo
Entero (indicador de 32 bits)

Atributo Interfaces

Descripción
Muestra el número total de interfaces.

Tipo
Entero (indicador de 32 bits)

Atributo Nodo Este atributo es un atributo de clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Direccionadores

Descripción
Muestra el número total de direccionadores.

Tipo
Entero (indicador de 32 bits)

Atributo Conmutadores

Descripción
Muestra el número total de conmutadores.

Tipo

Entero (indicador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Paquetes enviados y procesados por sondeador
Muestra el número de paquetes enviados y procesados por el sondeador por segundo.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Paquetes enviados y procesados por sondeador:

Atributo Nodo Este atributo es un atributo de clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Procesados

Descripción
Muestra el número total de paquetes procesados por el sondeador por segundo.

Tipo
Entero (indicador de 32 bits)

Atributo Enviados

Descripción
Muestra el número total de paquetes enviados por el sondeador por segundo.

Tipo
Entero (indicador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Estado de objeto de rendimiento
El conjunto de datos Estado del objeto de rendimiento contiene información que refleja el estado de otros conjuntos de datos para que pueda ver el estado de todos los objetos de rendimiento que componen esta aplicación de una sola vez. Cada uno de estos otros conjuntos de datos de rendimiento se representa mediante una fila de esta tabla (u otro tipo de vista). El estado de un conjunto de datos refleja el resultado del último intento de recopilar datos para ese conjunto de datos de modo que pueda ver si el agente está recopilando datos correctamente. A diferencia de otros conjuntos de datos, el conjunto de datos de estado de objeto de rendimiento no refleja el estado de la aplicación supervisada. Este conjunto de datos se utiliza con más frecuencia para determinar por qué no están disponibles los datos para uno de los conjuntos de datos de rendimiento.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Estado de objeto de rendimiento:

Atributo Promedio de duración de recopilación

Descripción
Duración media de todas las recopilaciones de datos de este grupo en segundos.

Tipo
Número real (contador de 32 bits) con dos posiciones decimales de precisión con valores enumerados. Se definen los valores siguientes: NO DATA (-100). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Porcentaje de aciertos de memoria caché

Descripción
Porcentaje de solicitudes de datos externas para este grupo que se han satisfecho desde la memoria caché.

Tipo
Número real (contador de 32 bits) con dos posiciones decimales de precisión

Atributo Aciertos de memoria caché

Descripción
Número de veces que se ha satisfecho una solicitud de datos externa para este grupo desde la memoria caché.

Tipo
Entero (contador de 32 bits)

Atributo Errores de memoria caché

Descripción
Número de veces que una solicitud de datos externa para este grupo no estaba disponible en la memoria caché.

Tipo
Entero (contador de 32 bits)

Atributo Código de error

Descripción
Código de error asociado a la consulta.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: NO ERROR (0), GENERAL ERROR (1), OBJECT NOT FOUND (2), COUNTER NOT FOUND (3), NAMESPACE ERROR (4), OBJECT CURRENTLY UNAVAILABLE (5), COM LIBRARY INIT FAILURE (6), SECURITY INIT FAILURE (7), PROXY SECURITY FAILURE (9), NO INSTANCES RETURNED (10), ASSOCIATOR QUERY FAILED (11), REFERENCE QUERY FAILED (12), NO RESPONSE RECEIVED (13), CANNOT FIND JOINED QUERY (14), CANNOT FIND JOIN ATTRIBUTE IN QUERY 1 RESULTS (15), CANNOT FIND JOIN ATTRIBUTE IN QUERY 2 RESULTS (16), QUERY 1 NOT A SINGLETON (17), QUERY 2 NOT A SINGLETON (18), NO INSTANCES RETURNED IN QUERY 1 (19), NO INSTANCES RETURNED IN QUERY 2 (20), CANNOT FIND ROLLUP QUERY (21), CANNOT FIND ROLLUP ATTRIBUTE (22), FILE OFFLINE (23), NO HOSTNAME (24), MISSING LIBRARY (25), ATTRIBUTE COUNT MISMATCH (26), ATTRIBUTE NAME MISMATCH (27), COMMON DATA PROVIDER NOT STARTED (28), CALLBACK REGISTRATION ERROR (29), MDL LOAD ERROR (30), AUTHENTICATION FAILED (31), CANNOT RESOLVE HOST NAME (32), SUBNODE UNAVAILABLE (33), SUBNODE NOT FOUND IN CONFIG (34), ATTRIBUTE ERROR (35), CLASSPATH ERROR (36), CONNECTION FAILURE (37), FILTER SYNTAX ERROR (38), FILE NAME MISSING (39), SQL QUERY ERROR (40), SQL FILTER QUERY ERROR (41), SQL DB QUERY ERROR (42), SQL DB FILTER QUERY ERROR (43), PORT OPEN FAILED (44), ACCESS DENIED (45), TIMEOUT (46), NOT IMPLEMENTED (47), REQUESTED A BAD VALUE (48),

RESPONSE TOO BIG (49), GENERAL RESPONSE ERROR (50), SCRIPT NONZERO RETURN (51), SCRIPT NOT FOUND (52), SCRIPT LAUNCH ERROR (53), CONF FILE DOES NOT EXIST (54), CONF FILE ACCESS DENIED (55), INVALID CONF FILE (56), EIF INITIALIZATION FAILED (57), CANNOT OPEN FORMAT FILE (58), FORMAT FILE SYNTAX ERROR (59), REMOTE HOST UNAVAILABLE (60), EVENT LOG DOES NOT EXIST (61), PING FILE DOES NOT EXIST (62), NO PING DEVICE FILES (63), PING DEVICE LIST FILE MISSING (64), SNMP MISSING PASSWORD (65), DISABLED (66), URLS FILE NOT FOUND (67), XML PARSE ERROR (68), NOT INITIALIZED (69), ICMP SOCKETS FAILED (70), DUPLICATE CONF FILE (71). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Intervalos omitidos

Descripción
Número de veces que se ha saltado una recopilación de datos de segundo plano para este grupo porque la recopilación anterior aún se estaba ejecutando cuando se debía iniciar la siguiente.

Tipo
Entero (contador de 32 bits)

Atributo Duración de última recopilación

Descripción
Duración de la recopilación de datos completada más recientemente de este grupo en segundos.

Tipo
Número real (contador de 32 bits) con dos posiciones decimales de precisión

Atributo Última recopilación finalizada

Descripción
Hora más reciente en que ha finalizado una recopilación de datos de este grupo.

Tipo
Indicación de fecha y hora con valores enumerados. Se definen los valores siguientes: NOT COLLECTED (0691231190000000), NOT COLLECTED (0000000000000001). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Último inicio de recopilación

Descripción
Hora más reciente en que se ha iniciado una recopilación de datos de este grupo.

Tipo
Indicación de fecha y hora con valores enumerados. Se definen los valores siguientes: NOT COLLECTED (0691231190000000), NOT COLLECTED (0000000000000001). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Nodo Este atributo es un atributo de clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Número de recopilaciones

Descripción
El número de recopilaciones de datos de este grupo desde que se inició el agente.

Tipo

Entero (contador de 32 bits)

Atributo Nombre de objeto

Descripción
El nombre del objeto de rendimiento.

Tipo
Serie

Atributo Estado del objeto

Descripción
Estado del objeto de rendimiento.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: ACTIVE (0), INACTIVE (1). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Tipo de objeto

Descripción
El tipo del objeto de rendimiento.

Tipo
Entero con valores enumerados. Se definen los valores siguientes: WMI (0), PERFMON (1), WMI ASSOCIATION GROUP (2), JMX (3), SNMP (4), SHELL COMMAND (5), JOINED GROUPS (6), CIMOM (7), CUSTOM (8), ROLLUP DATA (9), WMI REMOTE DATA (10), LOG FILE (11), JDBC (12), CONFIG DISCOVERY (13), NT EVENT LOG (14), FILTER (15), SNMP EVENT (16), PING (17), DIRECTOR DATA (18), DIRECTOR EVENT (19), SSH REMOTE SHELL COMMAND (20). Cualquier valor que no tenga una definición aquí, se visualiza en la interfaz de usuario.

Atributo Nombre de consulta **Este atributo es un atributo de clave.**

Descripción
Nombre del grupo de atributos.

Tipo
Serie

Atributo Intervalo de renovación

Descripción
Intervalo con el que se renueva este grupo, en segundos.

Tipo
Entero (contador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Capacidad de sondeo
Muestra la capacidad de sondeo de supervisión.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Capacidad de sondeo:

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Atributo Total

Descripción
Muestra el número total de hebras disponibles para utilizarse.

Tipo
Entero (indicador de 32 bits)

Grupo de atributos Errores y tiempos de espera excedidos de SNMP
Muestra el número total de respuestas de errores y tiempos de espera excedidos de SNMP.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Errores y tiempos de espera excedidos de SNMP:

Atributo Errores

Descripción
Muestra el número total de errores SNMP por segundo.

Tipo
Entero (indicador de 32 bits)

Atributo Nodo **Este atributo es un atributo de clave.**

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Tiempos de espera excedidos

Descripción
Muestra el número total de tiempos de espera excedidos de SNMP por segundo.

Tipo
Entero (indicador de 32 bits)

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Grupo de atributos Cola de elemento de trabajo
Muestra el número de elementos de trabajo en la cola que procesar.

Descripciones de atributo
La lista siguiente contiene información sobre cada atributo del grupo de atributos Cola de elemento de trabajo:

Atributo Nodo Este atributo es un atributo de clave.

Descripción
Nombre del sistema gestionado del agente.

Tipo
Serie

Atributo Indicación de fecha y hora

Descripción
Hora local en el agente a la que se recopilaron los datos.

Tipo
Serie

Atributo Total

Descripción
Muestra el número total de elementos de trabajo en la cola.

Tipo
Entero (indicador de 32 bits)

Referencia de situaciones

Una situación es una expresión lógica en la que intervienen una o más condiciones del sistema. Las situaciones se utilizan para supervisar la condición de los sistemas en la red. Puede gestionar situaciones desde el Tivoli Enterprise Portal utilizando el Editor de situaciones o desde la interfaz de línea de mandatos utilizando los mandatos tacmd para situaciones. Puede gestionar situaciones privadas en el archivo XML de configuración privada.

Acerca de las situaciones

Los agentes de supervisión que utiliza para supervisar el entorno del sistema incluyen un conjunto de situaciones que puede utilizar tal cual. Puede también crear nuevas situaciones para satisfacer sus requisitos.

Las situaciones predefinidas contienen atributos que comprueban condiciones del sistema comunes a muchas empresas. Las situaciones predefinidas le pueden ayudar a comenzar a utilizar más rápidamente el producto IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. Puede cambiar las condiciones o valores que se están supervisando utilizando una situación predefinida en las condiciones o valores que mejor se adecuen a su empresa.

El Editor de situaciones permite visualizar las situaciones predefinidas y crear situaciones propias del usuario. El editor de situaciones lista inicialmente las situaciones asociadas con el elemento de navegador que ha seleccionado. Al pulsar en un nombre de situación o crear una situación, se abrirá un panel con los siguientes separadores:

Fórmula
Fórmula que describe la condición que se prueba.

Distribución
Lista de los sistemas gestionados (sistemas operativos, subsistemas o aplicaciones) a los que puede distribuirse la situación. Todos los sistemas gestionados se asignan de forma predeterminada.

Consejo experto
Comentarios e instrucciones a leer en el espacio de trabajo de sucesos.

Acción
Mandato a enviar al sistema.

EIF
Personalizar el reenvío del suceso a un receptor de Event Integration Facility. (Disponible cuando Tivoli Enterprise Monitoring Server está configurado para reenviar sucesos.)

Hasta
Opciones para cerrar el suceso tras un período de tiempo o cuando otra situación pasa a ser verdadera (true).

Más información sobre situaciones

El manual *Tivoli Enterprise Portal: Guía del usuario* contiene más información sobre situaciones predefinidas y personalizadas y cómo utilizarlas para responder a las alertas.

Situaciones predefinidas

El agente de supervisión contiene situaciones predefinidas, que están organizados por el elemento del Navegador.

Elementos de Navigator de nivel de agente

- IBM Tivoli Monitoring for Tivoli Network Manager
  - No aplicable
- Disponibilidad
  - No aplicable
  - KNP_NCPMONITOR_Process_Down
  - KNP_NCP_CONFIG_Process_Down
  - KNP_NCP_D_HELPSRV_Process_Down
  - KNP_NCP_G_EVENT_Process_Down
  - KNP_NCP_MODEL_Process_Down
  - KNP_NCP_POLLER_Process_Down
  - KNP_NCP_STORE_Process_Down
  - KNP_NCP_VIRTUAL_Process_Down
  - KNP_NCP_WEBTOOL_Process_Down
  - KNP_Process_CPU_Critical
  - KNP_Process_CPU_High
- Descubrimiento
  - No aplicable
- Supervisión
  - No aplicable
  - KNP_Polling_Capacitiy_Critical
  - KNP_Polling_Capacitiy_Warning
  - KNP_Work_Item_Queue_Warning
- Red
  - No aplicable
  - KNP_Total_Entities_Critical
  - KNP_Total_Entities_Warning

Descripciones de las situaciones

Cada descripción de situación proporciona información sobre la situación que puede utilizar para supervisar la condición de los sistemas de la red.

Las descripciones de situación proporcionan la siguiente información:

Descripción
Información sobre las condiciones que la situación comprueba.

Fórmula
Sintaxis que contiene una o varias expresiones lógicas que describen las condiciones de la situación que debe supervisarse.

Distribución
Si la situación se distribuye automáticamente a las instancias del agente o si está disponible para una distribución manual.

Ejecutar al iniciar
Si la situación comienza a supervisar cuando se inicia el agente.

Intervalo de muestreo
Número de segundos que transcurre entre una muestra de datos que el agente de supervisión recopila para el servidor y la siguiente muestra.

Permanencia de la situación
Si las condiciones especificadas en la situación se evalúan como verdaderas para el número definido de apariciones en una fila antes de que se genere la situación. El valor predeterminado de uno significa que no se lleva a cabo ninguna comprobación de persistencia.

Gravedad
Gravedad de los sucesos predefinidos: Aviso, Informativo o Crítico.

Condiciones de cierre
Controla cuándo se cierra una situación verdadera: transcurrido un periodo, cuando otra situación es verdadera o lo que suceda en primer lugar si se seleccionan ambas.

Elemento de navegador de IBM Tivoli Monitoring for Tivoli Network Manager
No se incluyen situaciones predefinidas para este elemento del navegador.

Elemento de navegador Disponibilidad
Las descripciones de situación están organizadas por el elemento de navegador para el que son pertinentes las situaciones.

Situación KNP_NCPMONITOR_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula

```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'nco_p_ncpmonitor' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_CONFIG_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_config' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_D_HELPSRV_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_d_helpserv' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_G_EVENT_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_g_event' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_MODEL_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_model' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_POLLER_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_poller' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_STORE_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_store' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_VIRTUAL_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_virtualdomain' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_NCP_WEBTOOL_Process_Down

Descripción
El proceso de Network Manager no se está ejecutando.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ DOWN ) *AND ( *VALUE
KNP_AVAILABILITY.Application_Component *EQ 'ncp_webtool' ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_Process_CPU_Critical

Descripción
Un proceso de Network Manager en ejecución tiene una alta utilización de la CPU.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ UP ) *AND ( *VALUE
KNP_AVAILABILITY.Percent_Processor_Time *GE 80 ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_Process_CPU_High

Descripción
La utilización de CPU por parte del proceso de ITNM es alta.

La situación se evalúa para cada valor diferente del atributo COMPONENT.

Fórmula
```
*IF ( ( *VALUE KNP_AVAILABILITY.Status *EQ UP ) *AND ( *VALUE
KNP_AVAILABILITY.Percent_Processor_Time *LT 80 ) *AND ( *VALUE
KNP_AVAILABILITY.Percent_Processor_Time *GE 20 ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Aviso

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Elemento de navegador Descubrimiento
No se incluyen situaciones predefinidas para este elemento del navegador.

Elemento de navegador Supervisión
Las descripciones de situación están organizadas por el elemento de navegador para el que son pertinentes las situaciones.

Situación KNP_Polling_Capacitiy_Critical

Descripción
El sondeador supervisor está cerca de alcanzar la capacidad de sondeo.

La situación se evalúa para cada valor diferente del atributo TOTAL.

Fórmula
```
*IF *VALUE KNP_POLLING_CAPACITY.Total *GE 60
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_Polling_Capacitiy_Warning

Descripción
El supervisor está cerca de la capacidad de sondeo.

La situación se evalúa para cada valor diferente del atributo TOTAL.

Fórmula
```
*IF *VALUE KNP_POLLING_CAPACITY.Total *GE 50
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Aviso

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_Work_Item_Queue_Warning

Descripción
El número de elementos en la cola de sondeador es alto.

La situación se evalúa para cada valor diferente del atributo TOTAL.

Fórmula
```
*IF *VALUE KNP_WORK_ITEM_QUEUE.Total *GT 0
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
5 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Aviso

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Elemento de navegador Red
Las descripciones de situación están organizadas por el elemento de navegador para el que son pertinentes las situaciones.

Situación KNP_Total_Entities_Critical

Descripción
El número total de entidades en la base de datos MODEL es crítico.

La situación se evalúa para cada valor diferente del atributo ENTITIES.

Fórmula
```
*IF ( ( *VALUE KNP_ENTITIES_ON_MODEL_DB.Entities *GE 225000 ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
15 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Grave

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Situación KNP_Total_Entities_Warning

Descripción
El número total de entidades en la base de datos MODEL es alto.

La situación se evalúa para cada valor diferente del atributo ENTITIES.

Fórmula
```
*IF ( ( *VALUE KNP_ENTITIES_ON_MODEL_DB.Entities *GE 200000 ) *AND
( *VALUE KNP_ENTITIES_ON_MODEL_DB.Entities *LE 225000 ) )
```

Distribución
Esta situación se distribuye automáticamente entre las instancias de este agente.

Ejecutar al iniciar
Sí

Intervalo de muestreo
15 minutos

Permanencia de la situación
El número de veces que deben producirse las condiciones de la situación para que la situación sea verdadera es de 1.

Condiciones de error
Aviso

Condiciones de cierre
La situación se borra cuando la condición pasa a ser falsa.

Referencia de mandatos de actuación

Los mandatos de Actuación se pueden ejecutar desde el cliente de portal o se pueden incluir en una situación o en una política.

Acerca de los mandatos de Actuación

Cuando se incluye en una situación, el mandato se ejecuta cuando la situación pasa a ser verdadera. Un mandato de actuación en una situación también se denomina *automatización de reflejo*. Cuando se habilita un mandato de Actuación en una situación, se automatiza una respuesta a las condiciones del sistema. Por ejemplo, puede utilizar un mandato de actuación para enviar un mandato para reiniciar un proceso en el sistema gestionado o para enviar un mensaje de texto a un teléfono móvil.

En la automatización avanzada, las políticas se utilizan para realizar acciones, planificar trabajo y automatizar tareas manuales. Una política consta de una serie de pasos automatizados, denominados actividades, que están conectados para crear un flujo de trabajo. Una vez finalizada una actividad, Tivoli

Enterprise Portal recibe un código de retorno y la lógica de automatización avanzada responde con actividades prescritas por el código de retorno.

Un mandato Actuación básico muestra el código de retorno de la operación en un recuadro de mensaje que se muestra una vez completada la acción, o en un archivo de registro. Después de cerrar esta ventana, no hay más información disponible para esta acción.

IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition no proporciona mandatos de Actuación predefinidos.

Información adicional sobre los mandatos de actuación

Para obtener más información sobre cómo trabajar con mandatos de actuación, consulte la sección "Mandatos de actuación" de la publicación *Tivoli Enterprise Portal: Guía del usuario*.

Referencia de políticas

Las políticas se utilizan como técnicas avanzadas de automatización para la implementación de estrategias de flujo de trabajo más complejas que las que se puedan crear mediante una simple automatización. El agente de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition no proporciona políticas predefinidas, pero los usuarios podrán crear políticas para cualquier agente.

Una *política* es un conjunto de procesos automatizados del sistema que puede realizar acciones, planificar trabajos para usuarios o automatizar tareas manuales. Se utiliza el Editor de flujos de trabajo para diseñar políticas. Puede controlar el orden en el que la política ejecuta una serie de pasos automáticos, que también se llaman *actividades*. Las políticas están conectadas para crear un flujo de trabajo. Una vez finalizada una actividad, Tivoli Enterprise Portal recibe un código de retorno y la lógica de automatización avanzada responde con actividades prescritas por el código de retorno.

Para obtener más información sobre la utilización de políticas, consulte "Automatización con políticas" en la publicación *Tivoli Enterprise Portal: Guía del usuario*.

Para obtener información sobre cómo utilizar el Editor de flujos de trabajo, consulte la *IBM Tivoli MonitoringGuía del administrador de*o la Tivoli Enterprise Portalayuda en línea para .

Parte 2. Descubrimiento de la red

El descubrimiento de la red implica la creación de la topología de red realizando una serie de descubrimientos iniciales y, a continuación, asegurándose de que siempre tendrá una topología de red actualizada mediante descubrimientos regulares.

Acerca de esta tarea

Los siguientes temas describen cómo descubrir la red y mantener actualizado el descubrimiento.

Capítulo 11. Acerca del descubrimiento

Configure el descubrimiento estableciendo los parámetros que gobiernan cómo se realiza el descubrimiento.

Acerca de los tipos de descubrimiento

Se utilizan distintos términos para describir el descubrimiento de red, en función de lo que se descubra y cómo se haya configurado el descubrimiento. Puede ejecutar descubrimientos, redescubrimientos y descubrimientos completos y parciales.

Descubrimiento y redescubrimiento

Descubrimiento
El término descubrimiento se utiliza generalmente para dar a entender cualquier tipo de descubrimiento. Técnicamente, sólo el primer descubrimiento que se ejecuta después de que se inicie el motor de descubrimiento, ncp_disco, se puede llamar propiamente un descubrimiento, y cada descubrimiento después de ese es un redescubrimiento. Dado que aún no hay datos de descubrimiento en la memoria, los descubrimientos llevan algo más de tiempo que los redescubrimientos.

Redescubrimiento
Una vez que se ha ejecutado un descubrimiento, cualquier descubrimiento posterior que se ejecuta es un redescubrimiento. Los redescubrimientos utilizan un flujo de datos distinto a los descubrimientos, con algunos agrupadores y tablas de base de datos distintos. Si se reinicia ncp_disco, el siguiente descubrimiento es de nuevo sólo un descubrimiento, y los descubrimientos posteriores después de esos son redescubrimientos. A menos que esté ejecutando descubrimientos avanzados o modificando el flujo de datos de descubrimiento, la diferencia entre un descubrimiento y un redescubrimiento normalmente no es importante y, para facilidad de lectura, las instrucciones de esta información no distinguen entre descubrimiento y redescubrimiento a menos que sea necesario.

Descubrimiento completo y parcial

Descubrimiento completo
Un descubrimiento completo es una ejecución de descubrimiento con un gran ámbito, pensado para descubrir todos los dispositivos de red que desea gestionar. Los descubrimientos completos normalmente se llaman solamente descubrimientos, a menos que se comparen con los descubrimientos parciales.

Descubrimiento parcial
Un descubrimiento parcial es un redescubrimiento posterior de una sección de una red ya descubierta previamente. La sección de la red normalmente se define con un ámbito de descubrimiento que consiste en un rango de direcciones, un dispositivo único o un grupo de dispositivos. Un descubrimiento parcial depende de los resultados del último descubrimiento completo y sólo puede ejecutarse si el motor de descubrimiento, el proceso **ncp_disco**, no se ha detenido desde el último descubrimiento completo. Un descubrimiento parcial es, por tanto, un tipo de redescubrimiento.

Descubrimiento planificado

Puede planificar un descubrimiento completo para que se inicie a una hora determinada. Por ejemplo, puede planificar un descubrimiento completo para que se ejecute todas las noches a la misma hora o a la misma hora de un día concreto de la semana o a la misma hora el mismo día del mes.

Ámbitos

Defina las zonas de la red (es decir, rangos de subred) que desee incluir en el descubrimiento y las zonas que desee excluir del mismo. Las áreas de la red a incluir en el proceso de descubrimiento, o a excluir del mismo, son conocidas colectivamente como el ámbito del descubrimiento.

Hay muchos beneficios en la limitación del ámbito de descubrimiento:

- Es importante limitar el ámbito del descubrimiento dado que el rango de las direcciones IP tenidas en cuenta por el proceso de descubrimiento predeterminado es potencialmente ilimitado. Sin un ámbito, el descubrimiento intentará reconocer cada dispositivo de red. Al limitar el ámbito, puede concentrarse en las áreas importantes de su red.

  Atención: Si existen rutas desde la red a Internet, un descubrimiento sin ámbito encontrará estas rutas y procederá a descubrir partes de Internet.
- Puede que también desee restringir el ámbito del descubrimiento para controlar el descubrimiento de dispositivos sensibles que no desee sondear. Un dispositivo se puede considerar como sensible debido a que haya un riesgo de seguridad implicado en el sondeo del dispositivo, o porque el sondeo haya sobrecargado el dispositivo. Puede especificar que dispositivos concretos se descubran pero no se instancien en una definición de AOC (tales dispositivos se descubren pero *no* se representan en la topología de red y sus detalles *no* se envían a MODEL). También puede restringir dispositivos de que se descubran (el acceso SNMP a cualquiera de tales dispositivos no se intentará).
- Otro motivo para el ámbito del descubrimiento es que restringe la cantidad de datos que Network Manager intenta descargar desde las tablas de direccionamiento de direccionadores individuales. Sin dicha restricción, si Network Manager encuentra un direccionador que conoce la tabla de direccionamiento para toda Internet, el descubrimiento llevará mucho tiempo en completarse.

Restricción: Network Manager no soporta el formato IPv4–mapped IPv6 y espera que todas las direcciones IPv6 estén en un formato IPv6 estándar separado por dos puntos. Por ejemplo, Network Manager no soporta una dirección IPv6 correlacionada con IPv4 como `::ffff:192.0.2.128`. En su lugar, esta dirección debe especificarse como `::ffff:c000:280` (formato estándar IPv6 separado por dos puntos).

Tipos de ámbitos

Network Manager ofrece varios tipos de ámbitos.

Puede habilitar los siguientes tipos de ámbitos:

- Puede incluir o excluir áreas de su red (ya sean rangos de subred o dispositivos específicos) en el descubrimiento. Se hará referencia a cada área configurada como una *zona*.

  Consejo: Si su subred se ha rellenado dispersamente, incluidos los direccionadores individuales, lo más normal es que dé como resultado un descubrimiento posterior que incluir toda la subred.
- Las zonas se pueden especificar dentro de zonas: dentro de una zona de inclusión determinada, puede especificar dispositivos o subredes que no se detectarán. El Buscador de pings no hace ping en estos dispositivos ni los agentes de descubrimiento interrogan los mismos. Por ejemplo, puede definir una zona de ámbito de inclusión formada por la subred de clase B 1.2.0.0/16 y, dentro de esa zona, puede especificar una zona de ámbito de exclusión formada por la red de clase C 1.2.3.0/24. Finalmente, dentro de la zona de ámbito de exclusión, podría especificar una zona de ámbito de inclusión 1.2.3.128/26.
- Puede incluir o excluir dispositivos que no sean IP, como los dispositivos ópticos de capa 1, mediante un filtro.
- Puede configurar un filtro que determine si un dispositivo descubierto se interroga para información de conectividad.
- Puede configurar ámbitos de multidifusión. Esto le permite configurar las subredes de multidifusión que se deben utilizar como ámbitos para el descubrimiento multidifusión.

Definición de zonas de descubrimiento para restringir el descubrimiento

Para restringir el descubrimiento, debe definir las zonas de descubrimiento. Puede definir zonas de descubrimiento de varias formas.

Seleccione uno de los métodos siguientes para definir una zona de descubrimiento:

- Definir zonas de descubrimiento utilizando la GUI Configuración del descubrimiento.
- Construir zonas agregando una inserción OQL en la tabla `scope.zones` con el archivo de configuración `DiscoScope.cfg`. Este método es para usuarios más experimentados.

Nota: Si no se especifica nada en la tabla `scope.zones`, se considerará que todo está en el ámbito.

Para cada zona, debe especificar la información siguiente:

- El tipo de protocolo de red utilizado por la zona, aunque actualmente sólo está soportado IP. Puede definir tantas zonas como sea necesario. También se pueden definir varias zonas dentro de la misma inserción.
- La acción a llevar a cabo para la zona, donde `m_Action=1` significa incluir en el descubrimiento, y `m_Action=2` significa excluir. Puede definir ambas zonas de inclusión y exclusión. La acción a llevar a cabo en la zona más pequeña sustituye las acciones de las zonas más grandes.
- Una lista de varbinds (`name=value`) que define la zona de descubrimiento actual.

Ejemplos de zonas de descubrimiento

Utilice esta información para entender cómo las zonas de inclusión y exclusión define los dispositivos que están incluidos y excluidos del descubrimiento. Los diagramas de esta sección muestran que la zona más pequeña tiene prioridad.

Zona de inclusión

Utilice esta información para entender cómo trabaja una zona de inclusión.

La figura siguiente muestra una zona de inclusión, 172.18.1.0/24.

- Una entidad con dirección IP 172.18.1.33 está dentro de la zona de inclusión y, por lo tanto, está descubierta.
- Una entidad con dirección IP 172.18.2.33 está fuera de la zona de inclusión y, por lo tanto, no está descubierta.

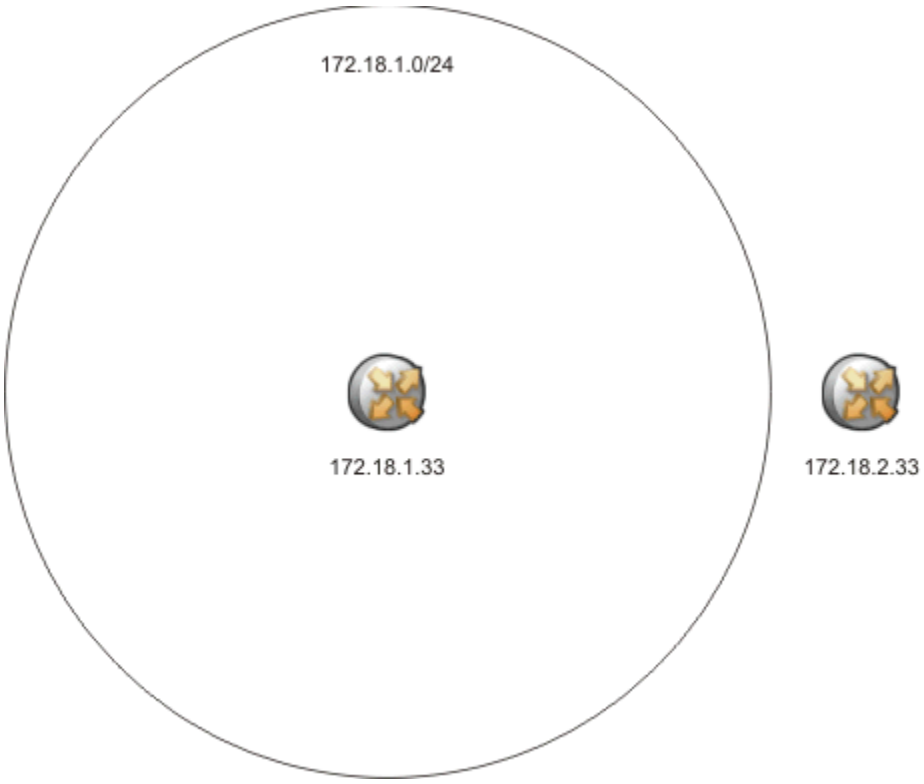


Figura 1. Zona de inclusión, con un dispositivo dentro y fuera de la zona.

Zona de exclusión dentro de una zona de inclusión

Utilice esta información para entender cómo trabaja el ámbito para una zona de exclusión dentro de una zona de inclusión.

La figura siguiente muestra una zona de exclusión dentro de una zona de inclusión.

- Una entidad con dirección IP 172.18.1.33 está dentro de la zona de exclusión y, por lo tanto, no está descubierta.
- Una entidad con dirección IP 172.18.2.33 está dentro de la zona de inclusión y, por lo tanto, está descubierta.
- Una entidad con dirección IP 172.19.3.2 está fuera de la zona de inclusión y, por lo tanto, no está descubierta.

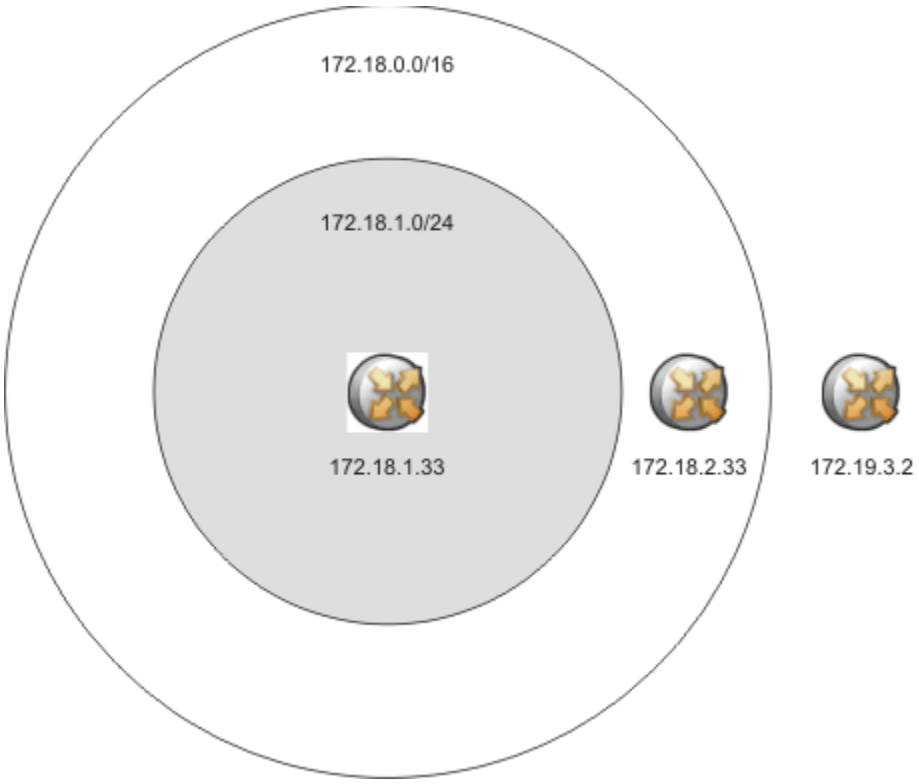


Figura 2. Zona de exclusión dentro de una zona de inclusión

Inclusión, exclusión y zona de inclusión

Utilice esta información para entender cómo trabaja el ámbito del dispositivo para una zona de inclusión dentro de una zona de exclusión dentro de una zona de inclusión.

La figura siguiente muestra una zona de inclusión dentro de una zona de exclusión dentro de una zona de inclusión.

- Una entidad con dirección IP 172.18.1.33 está dentro de la zona de inclusión y, por lo tanto, está descubierta.
- Una entidad con dirección IP 172.18.2.33 está dentro de la zona de exclusión y, por lo tanto, no está descubierta.
- Una entidad con dirección IP 172.19.3.2 está dentro de la zona de inclusión y, por lo tanto, está descubierta.
- Una entidad con dirección IP 172.19.3.2 está fuera de la zona de inclusión y, por lo tanto, no está descubierta.

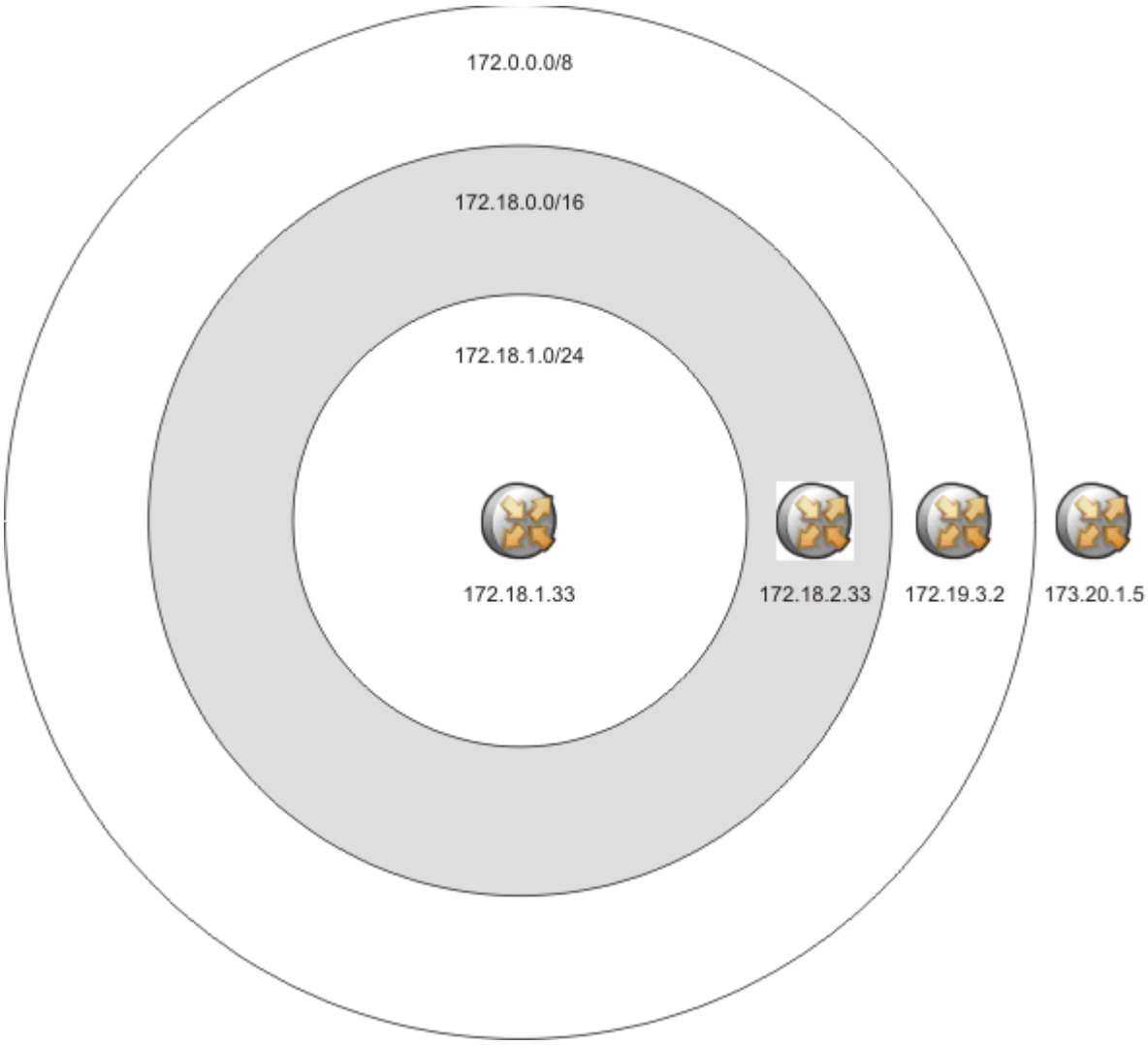


Figura 3. Zona de inclusión dentro de una zona de exclusión dentro de una zona de inclusión.

Zona de exclusión

Utilice esta información para entender cómo trabaja el ámbito para los trabajos de una zona de exclusión.

La figura siguiente muestra una zona de exclusión, 172.18.1.0/24.

- Una entidad con dirección IP 172.18.1.33 está dentro de la zona de exclusión y, por lo tanto, no está descubierta.
- Una entidad con dirección IP 172.18.2.33 está fuera de la zona de exclusión y, por lo tanto, está descubierta.

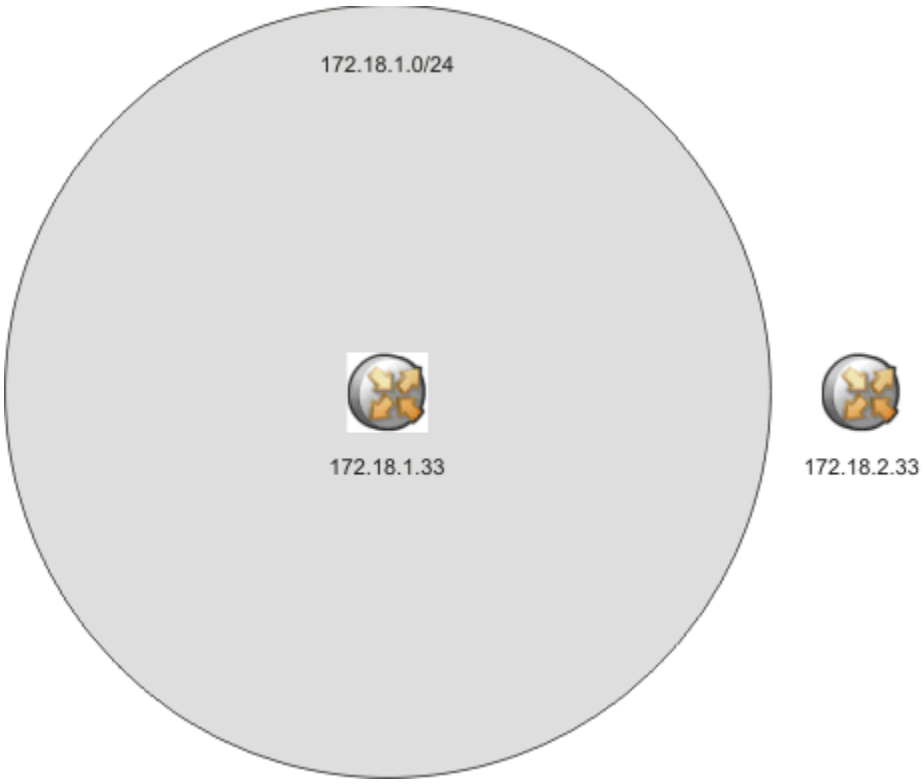


Figura 4. Zona de exclusión

Zona de inclusión dentro de la zona de exclusión

Utilice esta información para entender cómo trabaja el ámbito para una zona de inclusión dentro de una zona de exclusión.

La figura siguiente muestra una zona de inclusión dentro de una zona de exclusión.

- Una entidad con dirección IP 172.18.1.33 está dentro de la zona de inclusión y, por lo tanto, está descubierta.
- Una entidad con dirección IP 172.18.2.33 está dentro de la zona de exclusión y, por lo tanto, no está descubierta.
- Una entidad con dirección IP 172.19.3.2 está fuera de la zona de exclusión y, por lo tanto, está descubierta.

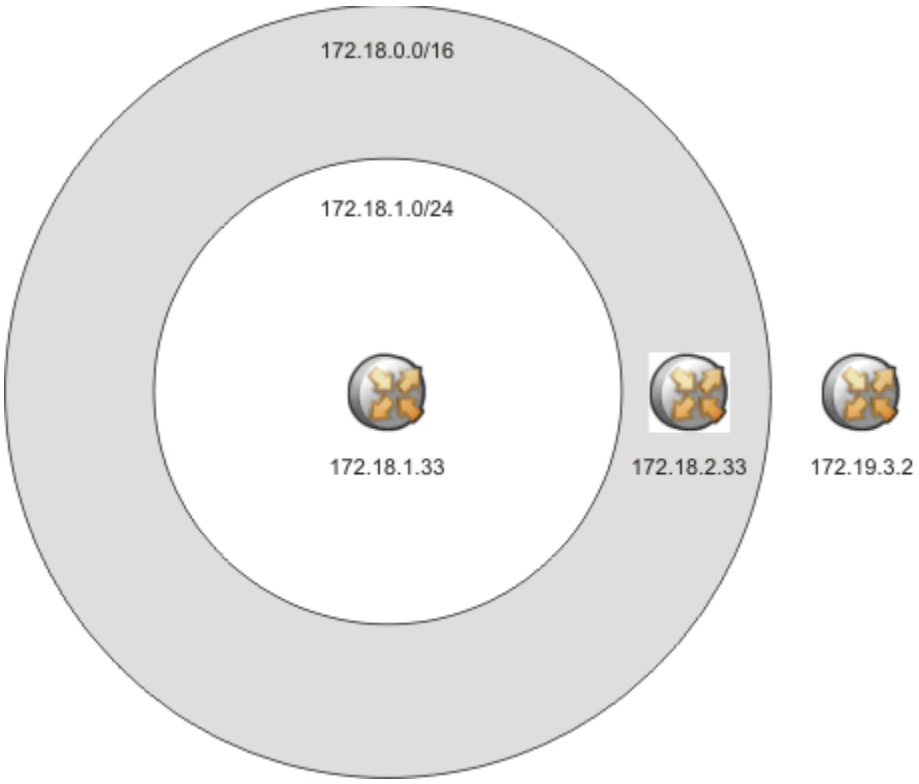


Figura 5. Zona de inclusión dentro de una zona de exclusión

Exclusión, inclusión y zona de exclusión

Utilice esta información para entender cómo trabaja el ámbito del dispositivo para una zona de exclusión dentro de una zona de inclusión dentro de una zona de exclusión.

La figura siguiente muestra una zona de exclusión dentro de una zona de inclusión dentro de una zona de exclusión.

- Una entidad con dirección IP 172.18.1.33 está dentro de la zona de exclusión y, por lo tanto, no está descubierta.
- Una entidad con dirección IP 172.18.2.33 está dentro de la zona de inclusión y, por lo tanto, está descubierta.
- Una entidad con dirección IP 172.19.3.2 está dentro de la zona de exclusión y, por lo tanto, no está descubierta.
- Una entidad con dirección IP 173.20.1.5 está fuera de la zona de exclusión y, por lo tanto, está descubierta.

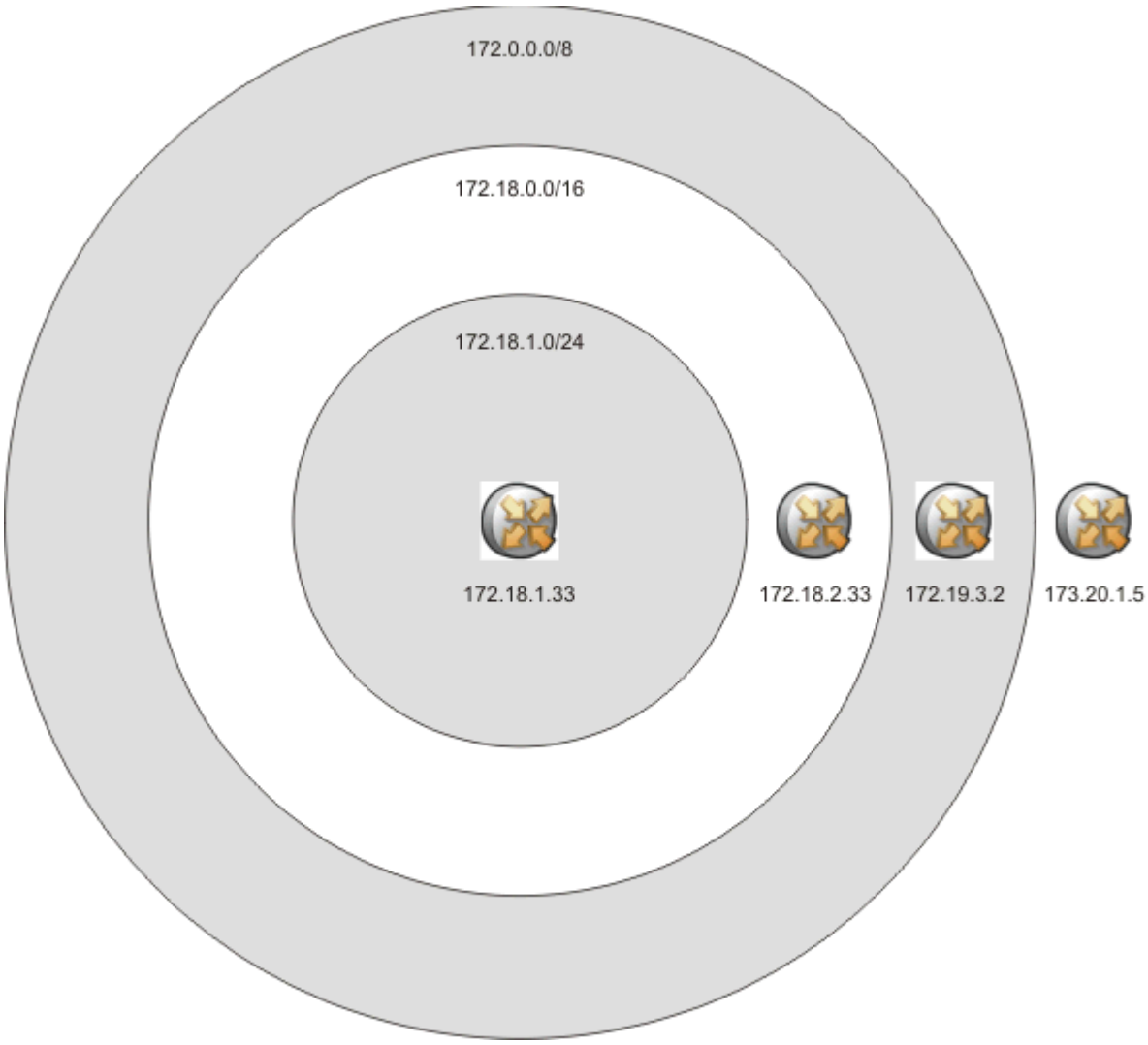


Figura 6. Zona de exclusión dentro de una zona de inclusión dentro de una zona de exclusión.

Definición de una zona de inclusión única

Utilice esta información para entender cómo definir una zona de inclusión única.

Acerca de esta tarea

Una zona de inclusión es cualquier zona que desea que descubra el motor de descubrimiento, ncp_disco. La siguiente inserción de ejemplo define una única zona de inclusión para el protocolo de IP y asocia la zona con una subred. Esta zona se aplica a todos los dispositivos dentro de la dirección de subred especificada.

```
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        1,
        [
            {
                m_Subnet="172.16.1.0",
                m_NetMask=24
            }
```

```
        ]
);
```

La inserción superior define una zona de inclusión IP para la subred 172.16.1.0 con una máscara de red de 24.

Definición de varias zonas de inclusión

Puede definir varias zonas de inclusión en la tabla scope.zones.

Acerca de esta tarea

En el siguiente ejemplo, se definen tres zonas de inclusión de IP diferentes dentro de una única inserción.

```
insert into scope.zones
(
    m_Protocol,
    m_Action,
    m_Zones
)
values
(
        1,
        1,
        [
              {
                    m_Subnet="172.16.1.0",
                    m_NetMask=24
              },
              {
                    m_Subnet="172.16.2.*"
              },
              {
                    m_Subnet="172.16.3.0",
                    m_NetMask=255.255.255.0
              }
        ]
);
```

El ejemplo anterior define tres zonas de inclusión de IP diferentes y cada una utiliza una sintaxis diferente para definir la máscara de subred. Network Manager descubre:

Procedimiento

- Cualquier dispositivo dentro de la subred 172.16.1.0 (con una máscara de subred de 24, es decir, 24 bits activados y 8 bits desactivados, lo que implica una máscara de red de 255.255.255.0).
- Cualquier dispositivo con una dirección IP que empiece por "172.16.2", es decir, en la subred 172.16.2.0 con una máscara 255.255.255.0.
- Cualquier dispositivo dentro de la subred 172.16.3.0 con una máscara de 255.255.255.0.

Definición de zonas de exclusión

Utilice esta información para entender cómo definir las zonas de exclusión.

Acerca de esta tarea

Una zona de exclusión es cualquier zona que no desea que descubra el motor de descubrimiento, ncp_disco. Se pueden crear varias zonas de exclusión dentro de la misma inserción de la misma forma que las zonas de inclusión. La siguiente inserción de ejemplo define una única zona de exclusión para el protocolo de IP y asocia la zona con una subred.

```
insert into scope.zones
(m_Protocol, m_Action, m_Zones)
values (1, 2,[{m_Subnet="172.16.1.0", m_NetMask=24]);
```

Definición de zonas para espacios de direcciones de NAT

Utilice esta información para entender cómo definir zonas para espacios de direcciones de NAT.

Acerca de esta tarea

Las zonas de inclusión y exclusión se pueden personalizar para dominios de NAT, utilizando la columna m_AddressSpace de la tabla scope.zones. La siguiente inserción de ejemplo define una zona de inclusión dentro de un dominio NAT particular.

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="172.16.2.*",
            }
        ],
        "NATDomain1"
);
```

Restricción de la detección de dispositivos específicos

Puede especificar subredes o dispositivos individuales al que el buscador de pings no va a hacer ping. Como el buscador de pings no ha detectado su existencia, estos dispositivos o subredes no son interrogados por agentes de descubrimiento.

Restricción de la interrogación de dispositivos específicos

Puede excluir dispositivos específicos desde el descubrimiento especificando que después de una detección inicial esos dispositivos no se van a interrogar más para obtener información de conectividad.

Acerca de esta tarea

Para especificar dispositivos que no se deben detectar, debe añadir una inserción OQL en la tabla scope.detectionFilter para el archivo de configuración DiscoScope.cfg. Solo puede haber una inserción por protocolo en la tabla scope.detectionFilter. Se deben definir varias condiciones dentro de una única inserción.

Dentro de la tabla scope.detectionFilter, debe especificar:

- El tipo de protocolo de red. Actualmente, solo la IP es soportada.
- Las condiciones de filtro. Solo a los dispositivos que pasen este filtro, es decir, a los que el filtro evalúa como true, se interrogan en mayor medida. Si no se especifica ningún filtro, se pasan todos los dispositivos por el filtro de detección.

Un agrupador prueba cada dispositivo que se ha descubierto en la condición de filtro en la tabla scope.detectionFilter y el resultado de esta prueba determina si se ha descubierto el dispositivo. Ya que el flujo de proceso del descubrimiento es completamente configurable, puede configurar este agrupador para actuar en cualquier momento durante el proceso de descubrimiento. De forma predeterminada, el agrupador realiza la prueba de condición en los detalles del dispositivo que devuelve el agente Detalles. Por lo tanto, el filtro debe estar basado en las columnas de la tabla Details.returns. Los siguientes ejemplos muestran cómo puede configurar el filtro de detección.

Atención: Se muestran varios ejemplos únicamente con fines ilustrativos. En la práctica, debe asegurarse de que solo existe una inserción por protocolo en la tabla scope.detectionFilter.

Ejemplo

Evitando la interrogación de un dispositivo basado en la dirección IP

En este ejemplo, solo se interroga en mayor medida a aquellos dispositivos que no tienen la dirección IP 10.10.63.234.

```
insert into scope.detectionFilter
(
        m_Protocol, m_Filter
)
values
(
        1,
        "( ( m_UniqueAddress <> '10.10.63.234' ) )"
);
```

Restricción de interrogación basada en el ID de objeto

El siguiente ejemplo muestra cómo debe impedir una mayor interrogación de dispositivos que coinciden con un ID de objeto determinado. La cláusula not like de OQL indica que solo se interroga en mayor medida a los dispositivos que pasen el filtro (es decir, los dispositivos para los que el OID no es como 1.3.6.1.4.1.*).

```
insert into scope.detectionFilter
(
        m_Protocol,
        m_Filter
)
values
(
        1,
        "(
                ( m_ObjectId not like '1\.3\.6\.1\.4\.1\..*' )
        )"
);
```

Se debe utilizar la barra inclinada invertida en la inserción superior para que escape el ., que de otro modo se tratará como un comodín.

Combinando varias condiciones de filtro

El siguiente ejemplo muestra cómo puede combinar condiciones de filtro dentro de una única inserción OQL. Este ejemplo asegura que solo se detectan los dispositivos que no tienen el OID especificado ni la dirección IP especificada:

```
insert into scope.detectionFilter
(
        m_Protocol,
        m_Filter
)
values
(
        1,
        "(
                ( m_ObjectId not like '1\.3\.6\.1\.4\.1\..*' )
                AND
                ( m_UniqueAddress <> '10.10.63.234' )
        )"
);
```

Configuración de la condición de filtro

Aunque puede configurar la condición de filtro para probar cualquiera de las columnas de la tabla Details.returns, será necesario que utilicé la dirección IP como base para el filtro si tienen que restringir la detección de un dispositivo en particular. Si el dispositivo no otorga acceso SNMP al agente Detalles, el agente Detalles no podrá recuperar las variables MIB, como el ID de objeto. Sin embargo, se le garantiza al menos la devolución de la dirección IP cuando se detecta el dispositivo.

Fuentes

Configure fuentes para especificar las ubicaciones desde las que comenzar a descubrir dispositivos. Las fuentes del descubrimiento pueden ser direcciones IP, o direcciones de subred.

Puede especificar fuentes de varias formas:

- Utilizando el buscador de pings: Especifique las direcciones IP o las direcciones de subred a descubrir en primer lugar.
- Uso del buscador de archivos: Proporcione uno o varios archivos en el que cada uno contenga una lista de direcciones IP o direcciones de subred.
- Uso del buscador de base de datos: Especifique detalles de conexión para una base de datos interna o externa que contenga detalles de los dispositivos a descubrir. Especifique también la ejecución de una consulta SQL para obtener los detalles de dispositivo de la base de datos. Una ventaja de utilizar el buscador de bases de datos en lugar del buscador de archivos es que puede extraer los datos directamente de una base de datos de terceros sin tener que extraer los datos de dispositivo como un archivo plano.

  Nota: El método buscador de bases de datos solo se puede configurar desde la línea de mandatos.
- Uso del buscador de recopiladores: Especifique uno o más puertos utilizados para acceder a procesos de recopilador independientes.

Consejo: Para restringir el descubrimiento a una lista de dispositivos específicos, propague el descubrimiento con una lista de dispositivos utilizando el Buscador de archivos o el Buscador de pings, e inhabilite la retroalimentación en el separador **Avanzado** de la **GUI de configuración de descubrimiento de red**.

Acceso a dispositivos

Configure el acceso a dispositivos especificando cadenas de comunidad SNMP y parámetros Telnet para que el sistema pueda acceder a dispositivos de red.

Configure el acceso a dispositivos como sigue:

- Especificar las cadenas de comunidad SNMP para que Network Manager pueda acceder e interrogar a los dispositivos de red que utilizan SNMP. Network Manager soporta SNMP v1, v2 y v3,
- Especificar parámetros Telnet para que Network Manager pueda acceder e interrogar a los dispositivos de red que utilizan Telnet.

Agentes

Utilice agentes de descubrimiento para recuperar información acerca de dispositivos en la red. Seleccione los agentes correctos para su descubrimiento en función del tipo de red.

Los agentes de descubrimiento recuperan los detalles de descubrimiento e investigan la conectividad de los dispositivos. También informan de la existencia de nuevos dispositivos buscando nuevas conexiones al investigar la conectividad de los dispositivos. Los agentes de descubrimiento se pueden utilizar para tareas especializadas. Por ejemplo, el agente de descubrimiento de caché ARP rellena la base de datos del servidor ayudante con correlaciones de dirección IP a dirección MAC.

Se proporcionan agentes predeterminados para el tipo de descubrimiento que desee realizar, por ejemplo, un descubrimiento de capa 2 ó 3. Puede seleccionar distintos conjuntos de agentes para descubrimientos completos y para descubrimientos parciales. Los agentes varían porque la información de conectividad varía según la tecnología del hardware en la red.

Filtros de dispositivos

Utilice filtros de predescubrimiento para aumentar la eficiencia del descubrimiento.

Una vez que haya definido el ámbito del descubrimiento utilizando el separador **Ámbito**, es posible restringir el ámbito con filtros. Por ejemplo, puede que desee mantener las zonas del ámbito que definió anteriormente, pero restringir el ámbito según la ubicación (por ejemplo, sólo hardware de Nueva York) o según el proveedor de hardware (por ejemplo, sólo dispositivos de Cisco).

Puede filtrar dispositivos basándose en una variedad de criterios, lo que incluye ubicación, tecnología y fabricante.

De forma predeterminada, los filtros de descubrimiento no filtran el host de Network Manager porque normalmente también sirve como estación de sondeo para análisis de la causa raíz. Para que el análisis de la causa raíz funcione correctamente, la estación de sondeo y la máquina host de Network Manager, deben formar parte de la topología.

Para obtener más información sobre el análisis de la causa raíz, consulte la publicación *IBM Tivoli Network Manager IP Edition Administration Guide* y la publicación *Guía del usuario de IBM Tivoli Network Manager*.

Si tiene que filtrar el host de Network Manager, necesita modificar los siguientes agrupadores y eliminar las secciones de código, indicadas por comentarios, que impiden que el host de Network Manager se filtre. Los agrupadores son DetectionFilter.stch e InstantiationFilter.stch.

Filtro de predescubrimiento

Puede que desee aplicar este filtro a dispositivos sensibles que no desee sondear. Un dispositivo se puede considerar como sensible debido a que haya un riesgo de seguridad implicado en el sondeo del dispositivo, o porque el sondeo pueda causar que el dispositivo se sobrecargue.

Los filtros de predescubrimiento impiden que el descubrimiento recupere datos detallados o datos de conectividad del dispositivo e impide que los dispositivos descubiertos se sondeen para información de conectividad. Sólo los dispositivos que coincidan con el filtro de predescubrimiento se descubrirán completamente. Si no se define ningún filtro de predescubrimiento, se descubrirán todos los dispositivos del ámbito.

Los filtros de predescubrimiento proporcionan un mecanismo para basar el descubrimiento en rangos de IP complejos que no se pueden definir de forma sencilla en el separador **Ámbito**. Se pueden utilizar para filtrar dispositivos según su valor sysObjectId. Los filtros predeterminados existen para filtrar nodos finales, impresoras y dispositivos similares. Puede crear varios filtros bastante similares, que hacen a esta característica muy potente, pero intente asegurar que los filtros estén diseñados para que se puedan mantener de forma sencilla. El filtro actúa en los campos de la tabla de OQL `Details.returns` en el servicio de descubrimiento (Disco), para que pueda utilizar campos distintos a las direcciones IP, como por ejemplo m_ObjectId (equivalente a sysObjectId). Un dispositivo debe pasar todos los filtros que se descubrirán.

Importante: Diseñe la lógica de filtro para que no necesite modificar los filtros de predescubrimiento cada vez que añada nuevos ámbitos.

Puede configurar la condición de filtro para probarla en cualquiera de las columnas de la tabla Details.returns. Pero también será necesario que utilice la dirección IP (m_UniqueAddress) como base para el filtro para restringir la detección de un dispositivo en particular. Si el dispositivo no otorga acceso SNMP al agente Detalles, el agente Detalles no podrá recuperar las variables MIB, como el ID de objeto. Sin embargo, se le garantiza al menos la devolución de la dirección IP cuando se detecta el dispositivo.

Puede definir varios filtros de predescubrimiento. Los filtros se combinan automáticamente utilizando una expresión booleana AND. Deben coincidir todos los criterios definidos en todos los filtros.

Filtro de postdescubrimiento

El filtro de postdescubrimiento no se encuentra disponible cuando el descubrimiento se ejecuta en la modalidad dNCIM.

Filtrado de interfaz SNMP

Puede filtrar los datos SNMP recuperados de los dispositivos por el proceso de descubrimiento mediante la configuración de filtros de interfaz SNMP. Sólo puede configurar filtros de interfaz SNMP desde la línea de mandatos.

Por qué utilizar el filtrado de interfaz SNMP

En ocasiones, un dispositivo o una clase de dispositivos devuelve demasiados datos de MIB. Por ejemplo, si los dispositivos virtuales tienen un gran número de interfaces, descubrirlas puede tardar bastante tiempo. Para acelerar el descubrimiento de estos dispositivos, puede utilizar filtros de interfaz SNMP para reducir el número de interfaces recuperadas por el ayudante de SNMP.

Cómo funciona el filtrado de interfaz SNMP

Cuando los agentes de descubrimiento, scripts de Perl o el **Navegador de MIB de SNMP** solicitan información SNMP, el ayudante de SNMP recupera la información de los dispositivos de red. Los filtros de interfaz SNMP definen filas en las tablas de MIB que recupera el ayudante de SNMP. El ayudante de SNMP recupera un subconjunto de la información que se habría devuelto sin filtro y la envía al proceso que ha solicitado la información SNMP. Los filtros de interfaz SNMP también pueden definir tablas completas que no deben ser recuperadas por el ayudante de SNMP.

Los filtros de interfaz SNMP sólo se aplican a solicitudes de recorridos completos de tablas de MIB. Las solicitudes Get o GetNext de SNMP de interfaces específicas dentro de una tabla de MIB no se filtran.

Los dispositivos que deberían tener el filtro aplicado se definen en el *filtro de dispositivos*. Si hay un filtro de dispositivos definido, las solicitudes de información SNMP para un dispositivo se comprueban primero en el filtro de dispositivos. Únicamente los dispositivos que pasen el filtro se comprueban a continuación para el filtrado de interfaz.

El filtro puede filtrar varias filas de una tabla. La primera vez que se accede a una tabla filtrada, se recorren una o más columnas de la tabla. Todas las solicitudes posteriores de recorridos SNMP de dicha tabla devuelven sólo las interfaces que coinciden con el filtro.

Inclusión de varias tablas con filtros dependientes

También puede definir *filtros dependientes*. Si se define un filtro de interfaz SNMP *Filtro 1* en la Tabla A, puede definirse un segundo filtro dependiente *Filtro 2* en la Tabla B. La información SNMP en la Tabla B que esté relacionada con la misma interfaz también se recupera.

Para definir un filtro dependiente, además de definir un filtro en la Tabla A, deben ser ciertas una o más de las condiciones siguientes:

- Tabla A y Tabla B tienen índices equivalentes.
- El índice de Tabla A es un valor de Tabla B.

Si Tabla A y Tabla B tienen exactamente el mismo índice, no es necesario definir un filtro dependiente. La información de Tabla B se recupera automáticamente en función del filtro definido en Tabla A.

Cuándo puede utilizar el filtrado de interfaz SNMP

Puede utilizar el filtrado de interfaz SNMP en cualquier tabla de MIB SNMP que tenga una clave en ifIndex. Por ejemplo, al filtrar en ifTable o ifXTable se permite el filtrado en valores como ifType e ifDescr.

Restricción: No se admite el filtrado sobre cualquier variable de MIB SNMP distinta de las interfaces. Sin embargo, puede acceder en bloque a cualquier tabla utilizando la opción m_InstanceFilterTable.

El fragmento de ejemplo siguiente muestra la definición para la ipAddrTable del archivo `NCHOME/precision/mibs/RFC1213.mib`:

```
          -- the IP address table

          -- The IP address table contains this entity's IP addressing
          -- information.

          ipAddrTable OBJECT-TYPE
              SYNTAX  SEQUENCE OF IpAddrEntry
              ACCESS  not-accessible
              STATUS  mandatory
              DESCRIPTION
                      "The table of addressing information relevant to
```

```
                        this entity's IP addresses."
                ::= { ip 20 }
```

La sintaxis "SEQUENCE OF" define esto como una tabla. Puede averiguar qué tablas están definidas en el MIB buscando esta cadena. El ejemplo siguiente muestra la salida de la ejecución de una búsqueda en UNIX:

```
% grep 'SEQUENCE OF'  RFC1213.mib
               SYNTAX  SEQUENCE OF IfEntry
               SYNTAX  SEQUENCE OF AtEntry
               SYNTAX  SEQUENCE OF IpAddrEntry
               SYNTAX  SEQUENCE OF IpRouteEntry
               SYNTAX  SEQUENCE OF IpNetToMediaEntry
               SYNTAX  SEQUENCE OF TcpConnEntry
               SYNTAX  SEQUENCE OF UdpEntry
               SYNTAX  SEQUENCE OF EgpNeighEntry
```

Sistema de nombres de dominio

Configure DNS para habilitar el descubrimiento para acceder a servicios DNS que se utilizan para realizar búsquedas de nombres de dominio.

Puede configurar tres tipos de Sistema de nombres de dominio:

Servidor DNS
Un servidor en la red dedicado a realizar la resolución de nombres de dominio.

Archivo
El nombre de un archivo en el host de Network Manager que contiene direcciones IP y nombres de host en el formato de tabla de búsqueda.

Sistema
El sistema DNS local en la máquina de Network Manager.

Conversión de direcciones de red

Configure los datos para las pasarelas NAT en su red.

Las pasarelas NAT proporcionan correlaciones entre la dirección IP privada de su red y las direcciones IP del dispositivo públicas. Puede habilitar el sistema para descubrir dispositivos dentro de espacios de direcciones privadas configurando datos para pasarelas NAT.

Configuración avanzada

Configure valores de descubrimiento avanzados para aumentar la velocidad del descubrimiento y equilibrar la velocidad con la carga en el servidor. Generalmente, un descubrimiento más rápido resulta en mayor utilización de memoria en el servidor. La configuración avanzada controla características del descubrimiento como procesos simultáneos y tiempos de espera.

Nota: Modifique la configuración avanzada sólo si es un usuario experimentado de Network Manager.

Puede configurar los siguientes valores de descubrimiento avanzados:

Parámetros del buscador:
Los buscadores son subsistemas de descubrimiento que descubren dispositivos en la red. Puede configurar parámetros como los tiempos de espera, el número de reintentos y el número de hebras para los buscadores.

Parámetros del ayudante
Los ayudantes son aplicaciones de descubrimiento utilizadas por los agentes para recuperar información de los dispositivos. Puede configurar los parámetros como los tiempos de espera, el número de reintentos y el número de hebras para los ayudantes.

Otros parámetros

Puede configurar valores de descubrimiento complejos, como la habilitación del almacenamiento en caché de tablas de descubrimiento, el modelado de VLAN, la verificación de buscador de archivos y los parámetros que afectan a la velocidad del descubrimiento parcial.

La mayoría de los parámetros avanzados de descubrimiento son opcionales.

Descubrimiento sensible al contexto

Si necesita descubrir dispositivos que soportan varios contextos, debe ejecutar un descubrimiento sensible al contexto. Por ejemplo, un dispositivo que utiliza contextos SNMP separados para proporcionar acceso a sus direccionadores virtuales. El descubrimiento sensible al contexto garantiza la correcta representación de direccionadores virtuales que pueden acceder al contexto. Compruebe siempre que el tipo de dispositivo particular está soportado para el descubrimiento.

En un descubrimiento sensible al contexto, se pasa información sobre un dispositivo de la tabla `returns` del agente Detalles a la tabla `despatch` del agente de contexto relevante.

Los agentes de contexto utilizan los filtros de los archivos `.agnt` de los agentes para determinar qué dispositivos procesar. Este enfoque es verdadero para todos los agentes de descubrimiento. Si el dispositivo no es de un tipo que soporte los dispositivos virtuales que pueden acceder al contexto, es decir, no necesita procesamiento sensible al contexto, se pasa directamente al agente de dirección asociada.

Ayudantes

Los ayudantes son aplicaciones especializadas que recuperan información de la red a petición. La configuración del ayudante predeterminada es suficiente para la mayoría de las redes. Sin embargo, puede decidir alterar la configuración por varias razones.

La configuración del Sistema del ayudante puede acelerar el descubrimiento de red, pero se recomienda para usuarios experimentados.

Aunque los agentes de descubrimiento recuperan información de conectividad, no tienen ninguna interacción directa con la red. En su lugar, recuperan información de conectividad a través del Sistema del ayudante, que consta de un Servidor del ayudante y de varios ayudantes.

Entre las razones para configurar los ayudantes se incluyen:

- Para acelerar el proceso de descubrimiento, puede reducir los tiempos de espera del ayudante y el número de reintentos.
- Si tiene una red muy fiable en la que los dispositivos responden rápidamente, puede especificar un tiempo de espera predeterminado pequeño.
- Puede que desee cambiar los tiempos de espera predeterminados para los ayudantes SNMP y Telnet si tiene muchos dispositivos que o no responden a SNMP y Telnet o que están configurados para no responder al acceso Telnet o SNMP. Un gran tiempo de espera predeterminado podría significar, por lo tanto, que los ayudantes esperan un largo tiempo respuestas que nunca reciben.
- Para reducir la cantidad de tráfico de red causado por un descubrimiento, puede aumentar el tiempo de espera e inhabilitar el ping de difusión y de multidifusión.

Recopiladores

Los recopiladores son como agentes, excepto que no descubren información de los dispositivos, pero la recopilan desde los Sistemas de gestión de elementos (EMS). Habilite y configure los recopiladores correctos para su descubrimiento si utiliza un EMS.

Los recopiladores son procesos separados que se inician independientemente del proceso ncp_disco. Los recopiladores se conectan a un EMS o analizan archivos desde un EMS para recopilar datos sobre los dispositivos gestionados por EMS.

Cada recopilador que tenga que ejecutar debe configurarse para conectarse al EMS adecuado.

Descubrimientos especializados

Puede configurar el sistema para realizar descubrimientos más complejos, como el descubrimiento MPLS (Multiprotocol Label Switching) y NAT (Conversión de direcciones de red).

Los descubrimientos especializados incluyen:

Descubrimiento EMS (sistema de gestión de elementos)
Recopile datos de topología de sistemas de gestión de elementos e integre estos datos en la topología descubierta.

Descubrimientos MPLS
Descubra las redes privadas virtuales de capa 3 (VPN) y las VPN de capa 2 mejoradas que se ejecutan en redes principales de MPLS.

Descubrimientos de NAT
Descubra dispositivos de pasarela de NAT para recuperar datos en dispositivos en espacios de dirección privada.

Descubrimientos de terceros:
Descubra redes de proveedores participantes como un objeto de "terceros" en varias redes que se ejecutan en una red de proveedor (por ejemplo, VPN empresariales en una red troncal de MPLS de proveedor).

Capítulo 12. Configuración del descubrimiento de red

Configure la manera en que se descubre su red, incluidos los tipos de dispositivos que quiere descubrir y donde se deben situar los límites del descubrimiento.

Acerca de esta tarea

Network Manager proporciona herramientas para el descubrimiento de la red utilizando un enfoque por fases.

- Utilice el asistente de configuración de descubrimiento para realizar descubrimientos iniciales. El asistente proporciona un descubrimiento guiado y lleva a cabo elecciones de configuración basándose en las respuestas que proporciona a medida que trabaja con el asistente.
- Utilice la GUI de configuración de descubrimiento para realizar descubrimientos posteriores. Al utilizar la GUI puede configurar valores de descubrimiento detallados, incluido el ámbito, las fuentes, cadenas de comunidad, selección de agentes y muchos otros valores de configuración.

Nota: También puede configurar un descubrimiento utilizando los archivos de configuración de descubrimiento y la línea de mandatos. Sin embargo, debe configurar el descubrimiento de esta manera solo si es un usuario experimentado de Network Manager y si entiende los diferentes aspectos de descubrimiento, incluidos los procesos de descubrimiento, fases, etapas, ayudantes, agentes, agrupadores e interrupciones.

Para obtener información sobre cómo editar de forma manual una topología descubierta antes del descubrimiento, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*.

Planificación para el descubrimiento

Antes de configurar y ejecutar un descubrimiento, debe comprobar diferentes valores de sistema, parámetros y requisitos.

Acerca de esta tarea

Las siguientes notas le ayudan a planificar el descubrimiento.

Guardar cambios en la GUI de configuración de descubrimiento de red
Para guardar los cambios de configuración que ha realizado durante una sesión, acuérdese de hacer clic en el botón **Guardar** antes de que finalice sesión, cierre la ventana del navegador o cierre el separador de la configuración del descubrimiento de red. Es una buena idea hacer clic en **Guardar** a medida que pase de separador a separador.

Sistema operativo
Asegúrese de que el host en el que Network Manager se está ejecutando tiene todos los parches actualizados.

Ámbito del descubrimiento
Tenga en cuenta las siguientes preguntas y puntos relacionados con el ámbito del descubrimiento:

- ¿La posición del host de Network Manager se encuentra en la red?
- ¿El host está posicionado para interrogar todos los dispositivos que desea incluir en su descubrimiento?
- Tenga en cuenta todas las redes y subredes necesarias y determine las máscaras de red asociadas.
- ¿Hay algunas partes de la red que desee excluir?
- Recopile todas las cadenas de comunidad SNMP relevantes para los dispositivos en el ámbito

Direccionamiento
Asegúrese de que cada una de las redes y subredes que se van a descubrir se pueden alcanzar utilizando el proceso ICMP. Si fuese necesario, agregue rutas a la máquina host de Network Manager utilizando el mandato **route add**.

Listas de control de acceso
Network Manager utiliza varios protocolos que pueden pasar por los cortafuegos. Estos protocolos son ICMP, SNMP, DNS, ARP, SSH y TELNET. Para asegurarse de que Network Manager puede acceder a los dispositivos que están detrás de estos cortafuegos, aconseje a los administradores del cortafuegos relevante sobre cómo preparar los cortafuegos.

Análisis de la causa raíz
Para realizar el análisis de la causa raíz en dispositivos dentro de una topología, el descubrimiento debe identificar todos los dispositivos en los que desee realizar el análisis de la causa raíz. Además, la estación de sondeo de Network Manager debe ser conocida. Si la estación de sondeo, por lo general el servidor Network Manager, no se encuentra dentro del ámbito del dominio de red, para habilitar el conector RCA para realizar la supresión aislada, es necesario especificar la dirección IP o el nombre del DNS de la interfaz de ingreso como entidad de sondeo. Esta es la interfaz dentro del alcance del descubrimiento desde la que se transmiten los paquetes de red a y desde la estación de sondeo.Para obtener más información sobre el análisis de causa raíz, consulte la *Network ManagerGuía de RCA y supervisión*.

Configuración de descubrimientos estándar

Puede configurar el descubrimiento utilizando el asistente para la configuración del descubrimiento, la GUI de configuración del descubrimiento o la línea de mandatos.

Descubrimiento de la red utilizando el asistente

El asistente de configuración de descubrimiento es para aquellos usuarios con experiencia limitada configurando descubrimientos.

Acerca de esta tarea

Importante: Si desea mantener los valores de configuración de descubrimiento que ha definido anteriormente utilizando la GUI, no utilice el asistente. El asistente de configuración de descubrimiento sobrescribe todos los valores anteriores.

Inicio del asistente

Seleccione un dominio e inicie el asistente para empezar a configurar y a ejecutar el descubrimiento.

Acerca de esta tarea

Para iniciar el asistente, complete estos pasos.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la parte superior izquierda del separador de configuración de descubrimiento de red, seleccione el dominio en el que desea ejecutar un descubrimiento desde el menú **Dominio**.
3. Haga clic en el botón del asistente a la derecha del menú **Dominio**.

Elección de un descubrimiento con o sin ámbito

La ventana **Ámbito del descubrimiento** proporciona la opción de un descubrimiento con o sin ámbito.

Acerca de esta tarea

Para elegir un descubrimiento con o sin ámbito, siga estos pasos.

Restricción: Network Manager no soporta el formato IPv4–mapped IPv6 y espera que todas las direcciones IPv6 estén en un formato IPv6 estándar separado por dos puntos. Por ejemplo, Network Manager no soporta una dirección IPv6 correlacionada con IPv4 como `::ffff:192.0.2.128`. En su lugar, especifique esta dirección como `::ffff:c000:280` (formato IPv6 estándar separado por dos puntos).

Procedimiento

1. Seleccione **Con ámbito** o **Sin ámbito**.

   Con ámbito
   Un descubrimiento con ámbito restringe el descubrimiento a una parte determinada de su red. Para especificar un descubrimiento con ámbito, indique al asistente a que área de la red restringir el descubrimiento y asigne direcciones IP o subredes como fuentes de pings para comenzar el descubrimiento.

   Sin ámbito
   Un descubrimiento sin ámbito intenta descubrir toda la red. Seguirá teniendo que, sin embargo, asignar direcciones IP o subredes como fuentes para hacer ping para comenzar el descubrimiento.

   Atención: Si existen rutas desde la red a Internet, un descubrimiento sin ámbito encontrará estas rutas y empezará a descubrir partes de Internet.
2. Si ha seleccionado **Con ámbito**, especifique a qué área de la red restringir el descubrimiento.

   Especifique una o más subredes para utilizar con el ámbito y fuentes haciendo clic en **Nuevo** y escribiendo un dirección IP y una subred.

   Restricción: Por razones de rendimiento, sólo se hará ping a direcciones IPV4. Para hacer ping a direcciones IPV6 utilice el separador fuente en la GUI de la configuración del descubrimiento.
3. Si ha seleccionado la opción **Sin ámbito**, especifique las fuentes que va a utilizar para el descubrimiento sin ámbito.

   Pulse **Nuevo...** y especifique una o más direcciones IP.

Configuración del acceso SNMP utilizando el asistente

Especifique cadenas de comunidad específicas de dirección, específicas de red o globales en la ventana **Cadenas de comunidad SNMP**.

Acerca de esta tarea

Para SNMP versión 3, también puede especificar contraseñas para cadenas de comunidad.

Para configurar el acceso SNMP, siga estos pasos.

Procedimiento

1. Para cada cadena de comunidad SNMP y contraseña asociada que desee definir:
   a) Haga clic en el icono **Nuevo** en la parte superior de la tabla **Cadenas de comunidad SNMP** para visualizar la ventana **Propiedades de contraseña SNMP**.
   b) Especifique cadenas de comunidad SNMP específicas de dirección, específicas de subred o globales y proporcione contraseñas para estas cadenas de comunidad en el caso de SNMP V3.

      Puede que necesite especificar una cadena de comunidad más de una vez. Por ejemplo, especifique una cadena para SNMP V1, otra para SNMP V2 y una más para SNMP V3.

      Especificación de cadenas de comunidad por resultados de subredes mediante un descubrimiento más eficiente y rápido.

      Restricción: Es recomendable no utilizar el símbolo arroba (@) en cadenas de comunidad. La utilización de este símbolo en una cadena de comunidad puede provocar problemas de conexión a dispositivos durante el descubrimiento.

2. Utilice las flechas arriba y abajo para ordenar según la frecuencia de uso esperada. Sitúe las cadenas de comunidad utilizadas con mayor frecuencia en la parte superior.

Configuración de acceso a Telnet utilizando el asistente

En la ventana **Acceso a Telnet**, defina los parámetros de accesos a Telnet.

Acerca de esta tarea

Para configurar el acceso a Telnet, complete estos pasos.

Procedimiento

1. Después de haber especificado las cadenas de comunidad SNMP, haga clic en el icono **Nuevo** en la ventana **Acceso a Telnet**.
2. Para cada conjunto de dispositivos accesibles mediante Telnet para los que quiera definir solicitudes y contraseñas, haga clic en **Nuevo**.
3. En la ventana **Contraseñas de Telnet**, especifique un conjunto de dispositivos accesibles mediante Telnet (todos los dispositivos, todos los dispositivos con una subred determinada o una única dirección IP) junto con indicadores, ID de inicio de sesión y contraseñas de inicio de sesión para este conjunto de dispositivos.

Especificación del tipo de descubrimiento

En la ventana **Tipo de descubrimiento**, especifique el tipo de descubrimiento: de capa 3 o de capa 2.

Acerca de esta tarea

Un descubrimiento de capa 3 es más rápido, pero los resultados de un descubrimiento de capa 3 no se pueden utilizar para un análisis de la causa raíz. El descubrimiento de capa 2 es más detallado y los resultados pueden utilizarse para el análisis de causa raíz.

Para especificar el tipo de descubrimiento, siga estos pasos.

Procedimiento

1. En la ventana **Tipo de descubrimiento**, especifique un descubrimiento de capa 2 o de capa 3.
2. Si ha seleccionado **Capa 3**, aparecerá a ventana **Descubrimiento de nodos finales**.

   En la ventana **Descubrimiento de nodo final**, puede filtrar los dispositivos de nodo final como las estaciones de trabajo y las impresoras. Puede también filtrar aquellos dispositivos que no tenga acceso SNMP.

   Consejo: Filtrar los nodos finales en redes con un gran número de nodos finales puede conducir a mejoras en velocidad y rendimiento del descubrimiento.
3. Si ha seleccionado **Capa 2 y Capa 3**, aparecerá la ventana **Modelado de VLAN**.

   En la ventana **Modelado de VLAN** puede configurar el descubrimiento para modelar VLAN en la topología resultante. Esto permite tener en cuenta las VLAN al realizar el análisis de causa raíz. Las VLAN son un concepto de capa 2 y el modelado de VLAN sólo es necesario para los descubrimientos de capa 2. Especifique si desea modelar las VLAN. Cuando haya especificado una opción, haga clic en **Siguiente** para mostrar la ventana **Descubrimiento de nodos finales**.

Optimización del descubrimiento

En la ventana **Optimización del descubrimiento**, optimice la conectividad, riqueza de la información y velocidad del descubrimiento.

Acerca de esta tarea

Para optimizar el descubrimiento, siga estos pasos.

Procedimiento

1. Proporcione distintas cantidades de información de conectividad seleccionado una de las siguientes opciones.

   Mayor precisión y riqueza posible de información.
   Esta opción proporciona información de conectividad entre conmutadores, nodos finales y direccionadores, así como información detallada sobre cada dispositivo descubierto. Sin embargo, un descubrimiento puede tardar bastante tiempo en finalizar.

   Mayor precisión posible de conectividad pero prefiriendo velocidad a la riqueza de información
   Esta opción proporciona información de conectividad completa. El descubrimiento proporciona, sin embargo, menos información detallada sobre cada dispositivo descubierto para proporcionar un descubrimiento más rápido.

   Información detallada sobre dispositivos pero prefiriendo velocidad a conectividad precisa
   Esta opción proporciona información detallada sobre cada dispositivo descubierto. El descubrimiento proporciona, sin embargo, información de conectividad menos detallada para poder proporcionar un descubrimiento más rápido. Por ejemplo, el descubrimiento puede proporcionar información sobre cómo están conectados los conmutadores entre sí, pero puede que no proporcione información sobre la conectividad entre conmutadores y nodos finales o entre conmutadores y direccionadores.

   Nota: Esta opción es más adecuada si desea recopilar datos de inventario en lugar de realizar RCA (análisis de causa raíz). RCA depende de datos de conectividad precisos.

   Tiempo de descubrimiento más rápido
   Esta opción se centra en la velocidad del descubrimiento. Este descubrimiento proporciona, sin embargo, información limitada sobre conectividad así como información menos detallada sobre todos los dispositivos.
2. Si selecciona una de las dos primeras opciones, querrá decir que una conectividad precisa es importante. Aparecerá la ventana **Fiabilidad de red**.
3. Si selecciona cualquiera de las dos últimas opciones, querrá decir que prefiere comprometer la información sobre conectividad para garantizar un descubrimiento más rápido. En este caso, el asistente preguntará qué proporción de la red está compuesta de dispositivos Cisco. Si una gran parte de la red está compuesta de dispositivos Cisco, el asistente podrá desactivar aquellos agentes que descubren la conectividad de dispositivos no Cisco, acelerando por tanto el descubrimiento de manera significativa. Aparecerá la ventana **Hardware de Cisco**.
   a) Especifique qué proporción de la red se compone de hardware Cisco seleccionando una de estas opciones.

      Toda
      Esta opción indica al asistente que ejecute Cisco Discovery Protocol (CDP).

      La mayoría, parte, no lo sé
      Esta opción le indica al asistente que ejecute CDP. Sin embargo, si elige un descubrimiento de capa 2 o capa 3 o si ha indicado que desea excluir nodos finales del descubrimiento, esta opción invocará el STP (Protocolo de bucle de árbol) así como CDP.

      Ninguna
      Esta opción especifica que no se utilizan ni el protocolo CDP ni el STP.

   b) Cuando seleccione una de estas opciones, haga clic en **Siguiente**.

   c) Si su respuesta a la pregunta sobre el hardware de Cisco ha sido **Toda** o **Ninguna**, aparecerá la ventana **Fiabilidad de la red**.

   d) Si su respuesta a la pregunta de hardware de Cisco ha sido **La mayoría**, **Parte** o **No lo sé**, se mostrará la ventana **Protocolo de bucle de árbol**, en la que debe especificar si el protocolo de bucle de árbol se habilitará en todos los conmutadores de red.

Indicación de la fiabilidad de la red

En la ventana **Fiabilidad de la red**, seleccione una descripción de la fiabilidad de la red al responder a solicitudes de ping y SNMP. La descripción indica al asistente que establezca la longitud de los tiempos de espera.

Acerca de esta tarea

Para describir la fiabilidad de la red, seleccione la opción que corresponda con la fiabilidad de la red cuando responda a solicitudes de ping y SNMP.

Muy fiable
Esta descripción indica que la red debe ser fiable al responder a solicitudes de pings y SNMP. Seleccione esta opción para permitir que el asistente aplique tiempos de espera muy breves, sin ningún reintento. Esta opción es apropiada para una red muy fiable y da como resultado descubrimientos rápidos. Si ha solicitado el tiempo de descubrimiento más rápido en la ventana Optimización de descubrimiento, los tiempos de espera establecidos por esta opción serán aún más cortos.

Bastante fiable
Esta descripción indica que la red debe ser fiable en su mayoría al responder a solicitudes de pings y SNMP. Seleccione esta opción para permitir que el asistente aplique tiempos de espera ligeramente más largos con un único reintento para solicitudes de ping y SNMP.

No muy fiable
Esta descripción indica que la red no tiene que ser necesariamente fiable al responder a solicitudes de pings y SNMP. Seleccione esta opción para permitir que el asistente aplique tiempos de espera más largos, dos reintentos para solicitudes SNMP y de ping. Los tiempos de espera más largos son adecuados para redes menos fiables.

Revisión de la configuración

En la ventana **Resumen de configuración**, revise su configuración. Puede también guardar la configuración y, si lo desea, iniciar el descubrimiento con los valores configurados.

Acerca de esta tarea

Para revisar los valores de la configuración, siga estos pasos:

Procedimiento

1. Revise los valores en la ventana **Resumen de configuración**.

   Haga clic en cualquiera de los enlaces para regresar a la ventana relevante para poder modificar los valores según estime correspondiente.
2. Cuando esté satisfecho con los valores del descubrimiento, seleccione una de estas opciones.
   - Seleccione **Iniciar descubrimiento** para utilizar los valores de configuración del descubrimiento especificados y, a continuación, haga clic en **Finalizar** para iniciar el descubrimiento.
   - Si no selecciona **Iniciar descubrimiento**, se guardarán los valores del descubrimiento al hacer clic en **Finalizar**.

Descubrimiento de la red utilizando la GUI

Para realizar un descubrimiento personalizado, complete los separadores en la página **Configuración del descubrimiento de red**. En estos separadores puede configurar parámetros del descubrimiento más complejos que cuando se utiliza el **Asistente de configuración de descubrimiento**.

Antes de empezar

Recuerde: Para guardar los cambios de configuración que ha realizado durante una sesión, haga clic en el botón **Guardar** antes de que finalice sesión, cierre la ventana del navegador o renueve o cierre el

separador de la configuración del descubrimiento de red. Es una buena idea hacer clic en **Guardar** a medida que pase de separador a separador.

Acerca de esta tarea

Los parámetros que puede establecer en los separadores de **Configuración del descubrimiento de red** se describen en los siguientes temas.

La mayoría de los parámetros que puede establecer en la página **Configuración del descubrimiento de red** son opcionales.

Para que el descubrimiento se ejecute, deberá, como mínimo, ejecutar los siguientes parámetros:

- Un dispositivo fuente
- Las cadenas de comunidad SNMP correctas para descubrir la red.

Si alguno de los separadores contiene datos, estos datos serán de configuraciones anteriores. Los datos se mantienen en un archivo de configuración de descubrimiento correspondiente.

Definición del ámbito del descubrimiento

Para configurar el ámbito del descubrimiento para dispositivos basados en IP y subredes, defina las zonas de la red (es decir, los rangos de subredes) que desea incluir en el descubrimiento y las zonas que desea excluir.

Acerca de esta tarea

Puede definir tantas zonas como sea necesario. Puede agregar nuevas zonas o bien editar o suprimir las zonas existentes.

Nota: Este procedimiento solo se puede utilizar para configurar el ámbito de las entidades basadas en IP. La definición del ámbito de las entidades que no son IP, como los dispositivos ópticos de capa 1 y determinados dispositivos de red de acceso mediante radio, debe hacerse configurando un filtro de predescubrimiento en el separador **Filtros**.

Para definir el ámbito del descubrimiento:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en **Ámbito**.
4. Para agregar una nueva zona de ámbito, haga clic en **Nuevo**  .
   Aparecerá la página **Propiedades del ámbito**.
5. Complete los campos tal como se muestra a continuación y haga clic en **Aceptar**.

   Acción
   Defina el rango de subred como una zona de inclusión o de exclusión. Si el rango de subred es una zona de inclusión en la que ejecutará ping durante el descubrimiento, haga clic en **Agregar a lista de fuentes de ping**. Al hacer clic en esta opción, se agregan automáticamente los dispositivos en la zona del ámbito como dispositivos de fuente de descubrimiento.

   Restricción: La opción `Agregar a lista de fuente de ping` no está disponible para zonas de ámbito de IPv6. Esto evita los barridos de ping de subredes IPv6, que potencialmente pueden contener billones de dispositivos para hacer ping. Por lo tanto, un barrido de ping de redes IPv6 puede provocar un descubrimiento interminable.
6. Para editar una zona de ámbito existente, haga clic en la fila requerida. En la página **Propiedades del ámbito**, edite las propiedades tal como se describen en el paso “5” en la página 161.

7. Para suprimir una zona de ámbito existente, marque el recuadro de selección **Seleccionar** junto a la o las filas requeridas y haga clic en **Suprimir**  .
8. Haga clic en **Guardar**  .

Qué hacer a continuación

Si está realizando la correlación de direcciones NAT, deberá configurar las pasarelas NAT y regresar al separador **Ámbito** para configurar la correlación de direcciones.

Adición de fuentes a un descubrimiento

Para agregar fuentes al descubrimiento, proporcione los puntos de inicio desde los que buscar dispositivos.

Antes de empezar

Para que el descubrimiento se ejecute, deberá, como mínimo, ejecutar los siguientes parámetros:

- Un dispositivo fuente
- Las cadenas de comunidad SNMP correctas para descubrir la red.

Acerca de esta tarea

Utilice los siguientes métodos para agregar fuentes al descubrimiento:

Buscador de pings
Agregue fuentes al Buscador de pings con un dispositivo o dirección de subred en la que el buscador comience a buscar dispositivos. Puede especificar fuentes para el Buscador de pings y guardar dichas fuentes. Puede decidir por separado si activar el Buscador de pings para el descubrimiento.

Buscador de archivos
Agregue fuentes al Buscador de archivos mediante un archivo de texto en el host de Network Manager al que tenga acceso de lectura. El archivo debe ser un archivo de texto estructurado que contenga las fuentes en formato de direcciones IP y nombres de dispositivos en columnas. Generalmente se utiliza un archivo que ya exista en el host de Network Manager. Sin embargo, si desea crear un nuevo archivo para las fuentes, deberá tener permiso de escritura en el directorio donde desee escribir el archivo.

Nota: También es posible iniciar el descubrimiento utilizando el buscador de bases de datos; sin embargo, este método sólo está disponible desde la línea de mandatos. Inicie el buscador de base de datos especificando una consulta que lea una base de datos para recuperar una lista de dispositivos para buscar en la red.

Cuando se ejecute un descubrimiento IPv6, compruebe que se cumplen las condiciones siguientes:

- Existe al menos un dispositivo de fuente IPv6 dentro de cada ámbito de IPv6.
- Si especifica una subred de IPv6 como fuente, compruebe que la subred es pequeña especificando un valor elevado para la máscara de red.

De forma predeterminada, el Buscador de pings y el Buscador de archivos están activados.

Para agregar fuentes al descubrimiento:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en **Fuente**.
4. Opcional: Para desactivar el Buscador de pings o el Buscador de archivos, desmarque los recuadros de selección **Utilizar Buscador de pings en descubrimiento** o **Utilizar Buscador de archivos en descubrimiento**.

5. Agregar o editar una fuente de pings:

   - Para agregar una nueva fuente de pings, haga clic en **Nuevo**  .
   - Para editar una fuente de pings existente, haga clic en la entrada requerida en la lista.

   Aparecerá la página **Propiedades de fuente de ping**.
6. Rellene los campos tal como se muestra y haga clic en **Aceptar**.

   Agregar fuentes por:
   Seleccione una de las siguientes opciones:

   IP
   Escriba una dirección IP.

   Subred
   Especifique una subred y escriba el número de bits de máscara de red. El campo **Máscara de red** se actualiza automáticamente.

   Restricción: Network Manager no soporta el formato IPv4–mapped IPv6 y espera que todas las direcciones IPv6 estén en un formato IPv6 estándar separado por dos puntos. Por ejemplo, Network Manager no soporta una dirección IPv6 correlacionada con IPv4 como `::ffff:192.0.2.128`. En su lugar, especifique esta dirección como `::ffff:c000:280` (formato IPv6 estándar separado por dos puntos).

   Tiempo de espera excedido
   Especifique el tiempo en milisegundos que desea esperar a obtener de una dirección a la que ha hecho ping antes de exceder el tiempo de espera.

   Reintentos
   Especifique el número de veces que debe ejecutarse ping en un dispositivo.
7. Para suprimir una fuente de ping existente, marque el recuadro de selección **Seleccionar** junto a la fila requerida y haga clic en **Suprimir** .
8. Agregar o editar una fuente de archivos:

   - Para agregar una nueva fuente de archivos al Buscador de archivos, haga clic en **Nuevo**  .
   - Para editar una fuente de archivos existente, haga clic en la entrada requerida en la lista.

   Aparecerá la página **Propiedades de fuente de archivo**.
9. Rellene los campos tal como se muestra y haga clic en **Aceptar**.

   Nombre de archivo
   Especifique la vía de acceso del archivo en la estación de trabajo host que contiene los datos de la fuente.

   Delimitador
   Especifique el delimitador de columnas. Utilice una expresión regular si fuera necesario. Por ejemplo, si las columnas Nombre e IP están separadas por uno o más tabuladores, inserte `[ espacio_tabulador ]+`, donde *espacio_tabulador* es un carácter de tabulador real. Para producir este carácter de tabulador, inserte un tabulador en un editor de textos, copie el tabulador y péguelo en el campo.

   Columna IP
   Escriba el número de columna de la columna que contiene las direcciones IP de los dispositivos de fuente.

   Columna Nombre
   Escriba el número de columna en la columna que contiene los nombres de dispositivos de los dispositivos de fuente.
10. Para suprimir una fuente de archivos existente, marque el recuadro de selección **Seleccionar** junto a la fila requerida y haga clic en **Suprimir**  .
11. Haga clic en **Guardar**  .

Qué hacer a continuación

Puede agregar fuentes a un descubrimiento utilizando el *Buscador de recopiladores*. El buscador de recopiladores recupera datos de topología desde un EMS. Los datos de topología son recopilados por los recopiladores EMS, que son módulos de software que recuperan datos de topología de una base de datos EMS, los convierten a formato XML y pasan dichos datos a Network Manager para incluirlos en la topología. Debe agregar fuentes al Buscador de recopiladores para permitir que Network Manager encuentre uno o más recopiladores EMS.

Tamaños de la máscara de subred IPv6

Potencialmente, hay miles de millones de dispositivos en los que se puede hacer ping dentro de una única subred de IPv6. Para comprobar que el descubrimiento se completa, debe especificar una máscara de red lo suficientemente grande si especifica una subred IPv6 como una fuente de pings.

La siguiente tabla proporciona ejemplos de tamaños de máscara de subred IPv6 configurados dentro de fuentes de ping y el tiempo estimado correspondiente requerido para hacer ping en los dispositivos de la subred. Los tiempos estimados se basan en espaciar los pings por 100 ms entre pings. Esta tabla muestra que es mejor limitar el tamaño de las máscaras de subred IPv6 de sus fuentes de subred.

Tabla 19. Tiempos de respuesta de ping para máscaras de subred IPv6

Tamaño de la máscara de subred IPv6	Número de direcciones IPv6 en la subred	Tiempo de ping estimado para la subred
120	256	26 segundos
112	65536	1 hora 48 minutos
100	268 millones	Aproximadamente 8,5 años

Las estimaciones de tiempo mostrados en la tabla se refieren al tiempo que se tarda en hacer ping en todas las fuentes de una fuente de subred especificada para el Buscador de pings. Puede llevar más tiempo para que el descubrimiento se complete, ya que habrá muchos más dispositivos en los que hacer ping dentro del ámbito de descubrimiento.

Configuración del acceso a dispositivos

Especifique la información de cadenas de comunidad SNMP y acceso a Telnet para permitir que los ayudantes y Network Manager sondeen el acceso de los dispositivos en la red.

Antes de empezar

Tenga en cuenta la siguiente información sobre el ayudante de SNMP y el ayudante de Telnet:

Ayudante de SNMP
: Debe especificar cadenas de comunidad SNMP para el ayudante de SNMP y para las operaciones de sondeo en dispositivos en la red. Puede que necesite especificar una cadena de comunidad más de una vez. Por ejemplo, una vez para SNMP V1, una para SNMP V2 y una para SNMP V3.

ayudante de Telnet
: Especifique los indicadores de dispositivo relevantes, ID de inicio de sesión y contraseña para el ayudante de Telnet y los agentes de descubrimiento que utilizan Telnet. Puede configurar propiedades de acceso privilegiado a Telnet. La modalidad de acceso privilegiado permite ejecutar mandatos que pueden cambiar la configuración del dispositivo. De forma predeterminada, cuando el descubrimiento accede al dispositivo utilizando Telnet, el acceso se proporciona en modalidad de usuario. Esta modalidad permite solo la ejecución de mandatos básicos, como los mandatos que muestran el estado del sistema. Esta modalidad de acceso predeterminado es una característica de seguridad para impedir que el descubrimiento realice modificaciones en la configuración de los dispositivos sin realizar ningún cambio explícito en la modalidad privilegiada.

Las cadenas de comunidad y los datos de acceso a Telnet pueden ser *globales*, que significa que el descubrimiento prueba la cadena de comunidad para cada dispositivo que encuentra, o restringidos a subredes específicas (es decir, sólo se utilizan en dispositivos con una subred específica), o incluso

restringidos a dispositivos específicos. La especificación de cadenas de comunidad y datos de acceso a Telnet por subred permite un descubrimiento más eficiente y rápido. En general, cuanto más específicas son las credenciales, más rápido el descubrimiento determinará las credenciales correctas.

Nota: La velocidad de descubrimiento relacionada con los valores de cadena de comunidad de la GUI sólo afecta a los descubrimientos iniciales. Una vez que Network Manager ha identificado las cadenas de comunidad correctas, almacena esta información en la base de datos relacional NCMONITOR. Los descubrimientos posteriores acceden a esta base de datos para obtener las cadenas de comunidad SNMP y otra información de acceso a dispositivos relacionada con SNMP.

Acerca de esta tarea

Para que el descubrimiento se ejecute, deberá, como mínimo, ejecutar los siguientes parámetros:

- Un dispositivo fuente
- Las cadenas de comunidad SNMP correctas para descubrir la red.

Para configurar el acceso a dispositivos:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en **Contraseñas**.
4. Para agregar una nueva cadena de comunidad SNMP, haga clic en **Nuevo**  .
   Aparecerá la página **Propiedades de contraseña SNMP**.
5. Rellene los campos tal como se muestra a continuación y haga clic en **Aceptar**:

   Cadena de comunidad
   Escriba un nombre. Cuando guarde la cadena de comunidad, el nombre estará cifrado, pero en la GUI, el valor siempre se muestra sin cifrar. Para rapidez de descubrimiento, ordene las cadenas de SNMP por frecuencia, con las cadenas más comunes en primer lugar.

   Restricción: Es recomendable no utilizar el símbolo arroba (@) en cadenas de comunidad. La utilización de este símbolo en una cadena de comunidad puede provocar problemas de conexión a dispositivos durante el descubrimiento.

   Aplicar a
   El descubrimiento se completa más rápidamente si especifica el ámbito correcto de las cadenas de comunidad. Seleccione una de las siguientes opciones:

   Todos los dispositivos
   Seleccione esta opción si la cadena de la comunidad es global.

   Dirección IP
   Seleccione esta opción si la cadena de la comunidad es específica a una dirección IP y escriba la dirección IP.

   Subred
   Seleccione esta opción si la cadena de comunidad es específica a una subred. Escriba la subred requerida y especifique el número de bits de máscara de red. El campo **Máscara de red** se actualiza automáticamente.

   Versión de SNMP
   Especifique la versión de SNMP de esta comunidad SNMP. Si especifica SNMP V3, cumplimente los siguientes campos adicionales:

   Nombre de seguridad
   Escriba un nombre.

   Nivel
   Especifique el nivel requerido de autenticación y privacidad.

NoAuthNoPriv,
Seleccione esta opción para comunidades SNMP sin autenticación ni clave privada. En este caso, no es necesario especificar ninguna contraseña.

AuthNoPriv
Seleccione esta opción para comunidades SNMP con una clave de autenticación pero no una clave privada. A continuación, especifique una contraseña en el campo **Contraseña de autorización**.

AuthPriv
Seleccione esta opción para comunidades SNMP con una clave de autenticación y una clave privada. A continuación, especifique contraseñas en los campos **Contraseña de autorización** y **Contraseña privada**.

Tipo de autorización
Especifique el tipo de cifrado para la contraseña de autenticación.

Restricción:

La opción de cifrado de MD5 no está disponible si está ejecutando una instalación de FIPS 140–2 de Network Manager.

De forma predeterminada, la GUI no utiliza ninguna rutina criptográfica que esté excluida de una instalación de FIPS140-2, independientemente del estado de instalación del servidor central. Si desea configurar opciones de descubrimiento SNMP para habilitar MD5 y DES, establezca `tnm.fips.mode=false` en el archivo `tnm.properties`.

Tipo de privacidad
Especifique el tipo de cifrado para la contraseña de privacidad.

Restricción: La opción de cifrado de DES no está disponible si está ejecutando una instalación de FIPS 140–2 de Network Manager.

Puerto SNMP
Especifique el puerto requerido.

Tiempo de espera excedido
Especifique el tiempo, en milisegundos, que debe esperarse a obtener una respuesta antes de exceder dicho tiempo de espera.

Nota: El administrador puede controlar el tiempo de espera máximo que se puede establecer mediante este campo, al configurar la propiedad `discoconfig.oobl.passwords.snmp.timeout.max` en el archivo `discoconfig.properties`.

Reintentos
Especifica cuántas veces desea que el ayudante de SNMP y las operaciones de sondeo intenten acceder a un dispositivo.

Nota: El administrador puede controlar el número máximo de reintentos que se pueden establecer mediante este campo, al configurar la propiedad `discoconfig.oobl.passwords.snmp.retries.max` en el archivo `discoconfig.properties`.

6. Haga clic en **Subir** y en **Bajar** para ordenar las cadenas de comunidad de SNMP. Sitúe las cadenas que se utilizan con más frecuencia en la parte superior de la lista.
7. Haga clic en **Guardar**.
8. Para agregar información de acceso a Telnet, haga clic en **Nuevo.**
   Aparecerá la página **Propiedades de contraseña Telnet**.
9. Cumplimente los campos tal como se detalla a continuación:

Aplicar a
Seleccione una de las siguientes opciones:

Todos los dispositivos
Seleccione esta opción si los datos se aplican globalmente.

Dirección IP
Seleccione esta opción si la cadena es específica a un dispositivo y escriba la dirección IP del dispositivo.

Subred
Seleccione esta opción si la cadena es específica a una subred. Escriba la subred requerida y especifique el número de bits de máscara de red. El campo **Máscara de red** se actualiza automáticamente.

Indicador de nombre de usuario
Escriba el indicador que desea que aparezca durante el inicio de sesión. Si no sabe el formato exacto del indicador, utilice una expresión regular.

Nombre de usuario
Escriba el nombre de usuario.

Indicador de contraseña
Escriba el indicador que desea que aparezca cuando se requiere una contraseña durante el inicio de sesión. Si no sabe el formato exacto del indicador, utilice una expresión regular.

Contraseña
Escriba la contraseña.

Indicador de consola
Escriba el indicador que aparecerá al iniciar la sesión. Si no sabe el formato exacto del indicador, utilice una expresión regular.

Puerto de acceso
Especifique el puerto en el que el ayudante de Telnet y los agentes de descubrimiento intentan acceder a dispositivos.

Tiempo de espera excedido
Especifique el tiempo, en milisegundos, que debe esperarse a obtener una respuesta antes de exceder dicho tiempo de espera.

Nota: El administrador puede controlar el tiempo de espera máximo que se puede establecer mediante este campo, al configurar la propiedad `discoconfig.oobl.passwords.telnet.timeout.max` en el archivo `discoconfig.properties`.

Utilizar SSH
Seleccione esta opción para configurar el Ayudante de Telnet para utilizar el programa Secure Shell (SSH).

10. Opcional: Para configurar las propiedades de modalidad de acceso privilegiado a Telnet:
    a) Haga clic en **Avanzado**.
    Aparecerá la página **Propiedades de la modalidad de acceso privilegiado a Telnet**.
    b) Rellene los campos tal como se muestra a continuación y haga clic en **Aceptar**:

Mandato
Escriba el mandato requerido para especificar la modalidad de acceso privilegiado a Telnet. Este mandato es normalmente `enable`.

Indicador de contraseña
Escriba el indicador que desea que aparezca cuando se requiere una contraseña durante el inicio de sesión. Si no sabe el formato exacto del indicador, utilice una expresión regular.

Contraseña
Escriba la contraseña requerida para la modalidad privilegiada.

Indicador de consola
Escriba el indicador que aparecerá al iniciar la sesión. Si no sabe el formato exacto del indicador, utilice una expresión regular.

Mandatos que requieren modalidad:
Especifique los mandatos que desea que estén disponibles desde la modalidad privilegiada. Para agregar nuevos mandatos, haga clic en **Nuevo...** y escriba el mandato en el campo **Mandato priv**. Los siguientes mandatos son obligatorios para ejecutarse en modalidad `enable`:

- **`show run`**
- **`show mac-address-table`**
- **`show ip nat translation`**

11. Haga clic en **Aceptar**.

Resultados

Cuando guarde la configuración de la contraseña Telnet, se cifrarán automáticamente las siguientes contraseñas:

- Contraseña de Telnet
- Contraseña de modalidad privilegiada de Telnet (si se especifica)

Cuando guarde los valores de la contraseña, se cifrarán automáticamente las siguientes contraseñas:

- Cadena de comunidad SNMP
- Contraseña de autenticación SNMP
- Contraseña privada de SNMP

Qué hacer a continuación

Si fuese necesario, cambie la configuración del cifrado de SNMP y Telnet. Por ejemplo, puede cambiar el archivo de clave de cifrado o desactivar el cifrado.

Activación de agentes

Debe habilitar los agentes correspondientes al descubrimiento que desea realizar. Puede especificar agentes para un descubrimiento completo o para un descubrimiento parcial.

Acerca de esta tarea

Puede acelerar el tiempo de un descubrimiento parcial seleccionando sólo aquellos agentes esenciales para descubrir los dispositivos nuevos o modificados. Puede que desee ejecutar un descubrimiento parcial si sabe se han agregado nuevos dispositivos o que los ingenieros han estado trabajando en un dispositivo y que han agregado o eliminado componentes a dicho dispositivo.

Nota: Cuantos más agentes ejecute, más datos se recuperan de la red, y más lento es el descubrimiento.

Para activar los agentes:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en uno de los siguientes separadores, dependiendo de sus requisitos:

Separador	Descripción
Agentes de descubrimiento completo	Seleccione los agentes en este separador para ejecutar un descubrimiento completo.
Agentes de descubrimiento parcial	Seleccione los agentes en este separador para ejecutar un descubrimiento parcial.

Separador	Descripción
	Nota: El botón **Restablecer** de la ventana **Agentes de descubrimiento parcial** configura los agentes parciales de forma que coincidan con los valores definidos en la ventana **Agentes de descubrimiento completo**.

Aparecerá la **Lista de agentes**, que muestra todos los agentes de descubrimiento disponibles de la opción de descubrimiento seleccionada.

4. Marque los recuadros de selección junto a los agentes seleccionados.

   Para obtener descripciones de los agentes, seleccione un nombre de agente.

   Para seleccionar todos los agentes requeridos para un descubrimiento de capa 3, marque el recuadro de selección **Capa 3**. Para seleccionar todos los agentes requeridos para un descubrimiento de capa 2 y 3, marque el recuadro de selección **Descubrimiento completo de capa 2 y 3**.

5. Haga clic en **Guardar**  .

   Si ha seleccionado un combinación no válida de agentes o una combinación que pueda resultar en un descubrimiento poco eficaz, aparecerá un aviso.

6. Si corresponde, siga los pasos que aparecen en el aviso:

   - Si ha seleccionado un agente que ejecutar en conjunto con otro y otros agentes, el aviso indicará que se seleccionarán los agentes según corresponda. Haga clic en **Aceptar** para seleccionar los agentes o haga clic en **Cancelar**.
   - Si ha seleccionado un agente que no puede ejecutarse junto con otro u otros agentes, el aviso le indicará que dichos agentes redundantes serán deseleccionados automáticamente. Haga clic en **Aceptar** para deseleccionar el agente recomendado o haga clic en **Cancelar**.

Configuración de filtros de descubrimiento

Puede utilizar filtros para filtrar dispositivos antes o después del descubrimiento. Puede filtrar dispositivos basándose en una variedad de criterios, lo que incluye ubicación, tecnología y fabricante. Los filtros proporcionan restricciones adicionales a las definidas en las zonas de ámbito.

Acerca de esta tarea

Un filtro se compone de una o más condiciones de filtrado. Las condiciones de filtrado se definen en OQL (lenguaje de consulta de objetos). Puede agregar los siguientes tipos de filtrado:

Filtros de predescubrimiento
Los filtros de predescubrimiento impiden que se sondeen dispositivos descubiertos en busca de información de conectividad.

Nota: Utilice filtros de predescubrimiento para configurar el ámbito de dispositivos no IP en la red, como se muestra en los ejemplos que figuran más abajo.

Filtros de postdescubrimiento
Los filtros de postdescubrimiento impiden que los dispositivos descubiertos se pasen a MODEL.

Nota: Para asegurarse de que no se generen alertas para las interfaces excluidas por el filtro postdescubrimiento, debe establecer la variable `RaiseAlertsForUnknownInterfaces`. Para ello, lleve a cabo los siguientes pasos:

1. Edite el archivo de configuración `$NCHOME/etc/precision/NcPollerSchema.cfg`.
2. Añada la siguiente línea al archivo:

```
update config.properties set RaiseAlertsForUnknownInterfaces = 0;
```

Los pasos para agregar, editar y suprimir filtros son idénticos para ambos tipos.

Para establecer los filtros de descubrimiento:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en **Filtros**.
4. Para utilizar un filtro en el descubrimiento, seleccione un filtro en la lista **Filtros disponibles** y haga clic en **Seleccionar filtro**.

   El filtro se agrega al campo **Filtro de predescubrimiento seleccionado** o el campo **Filtro de postdescubrimiento seleccionado**, dependiendo del tipo de filtro.
5. Para eliminar un filtro, seleccione el filtro en la lista **Filtros de predescubrimiento seleccionados** o la lista **Filtros de postdescubrimiento seleccionados** y haga clic en **Deseleccionar filtro**.
6. Para agregar un nuevo filtro o editar uno existente, haga clic en **Biblioteca de filtros**.

   Aparecerá la página **Biblioteca de filtros**.
7. Agregue o edite un filtro tal como se especifica a continuación:

Acción	Instrucciones
Agregar un nuevo filtro	Haga clic en **Agregar** y escriba el nombre requerido en el campo **Nombre**.
Edite un filtro existente	Seleccione el filtro requerido en la lista.

8. En el separador **Básico**, construya las condiciones de filtrado tal como se muestra a continuación:
   a) Seleccione el valor y comparador requerido.
   b) Escriba el valor de comparación con el campo seleccionado.

      Consulte el apartado "Configuración de filtros de descubrimiento" en la página 170 para obtener un ejemplo.
   c) Haga clic en **Agregar nueva fila**  o **Suprimir esta fila** para agregar o eliminar filas.
   d) Seleccione **Todas** para combinar varias condiciones en una relación AND o **Cualquiera** para combinar las condiciones en una relación OR.
   e) Haga clic en **Guardar**.
9. Opcional: En el separador **Avanzado**, escriba las cláusulas de SQL WHERE requeridas. Para varias condiciones, utilice una relación AND u OR según corresponda. Haga clic en **Guardar**.

   Nota: El filtro se basa en realidad en formateo OQL, aunque la GUI hace referencia a la cláusula SQL .
10. Haga clic en **Cerrar** para cerrar la **Biblioteca de filtros** y, a continuación, haga clic en **Guardar** para guardar la configuración de los filtros.

Configuración de filtros de descubrimiento

Puede utilizar un filtro de predescubrimiento para ajustar el ámbito. El filtro de predescubrimiento se aplica a chasis e interfaces, siempre que el filtro de postdescubrimiento se aplique a todas las entidades. Tenga cuidado al definir los filtros de postdescubrimiento para no dejar fuera del filtro objetos como VPN, tarjetas o subredes.

Pasar solo dispositivos no IP al descubrimiento

El siguiente filtro de ejemplo se suministra de forma predeterminada. Garantiza que solo los dispositivos no IP pasarán al descubrimiento y se les interrogará posteriormente. Este filtro excluiría todos los dispositivos basados en IP:

```
m_Protocol = 4
```

Pasar al descubrimiento solo dispositivos no IP y excluir dispositivos no IP con una clave exclusiva especificada

La siguiente inserción garantiza que solo se pasan al descubrimiento los dispositivos no IP y que los que se pasan no pueden incluir la cadena especificada en su clave de Sistema de gestión de elementos (EMS).

```
( m_Protocol = 4 )
    AND
( m_UniqueAddress NOT LIKE 'LONDON' )
```

Excluir dispositivos con un ID de objeto especificado.

El siguiente ejemplo muestra una condición de un filtro de predescubrimiento que excluye dispositivos con un ID de objeto especificado.

```
m_ObjectId not like '1\.3\.6\.1\.4\.1\.2\.3\.1\.'
```

Restricción de la instanciación de un chasis basado en el nombre de entidad

El filtro de postdescubrimiento del ejemplo siguiente restringe la creación de instancias de un chasis y su contenido.

```
BASENAME != 'jane'
```

Restricción de la instanciación de múltiples chasis

El filtro de postdescubrimiento del ejemplo siguiente restringe la creación de instancias de un chasis y su contenido.

```
snmpSystem->SYSDESCR NOT LIKE ' device'
```

Qué hacer a continuación

Para obtener más información sobre la sintaxis de OQL, consulte *Referencia de IBM Tivoli Network Manager*.

Valores de filtros disponibles

Utilice esta información de consulta para familiarizarse con los valores aceptables al configurar filtros de descubrimiento en la página **Configuración de descubrimiento de red**.

Valores de filtro de predescubrimiento

Cuando se construye un filtro de predescubrimiento, puede filtrar basándose en cualquiera de los campos en la tabla Details.returns. Estos campos son los siguientes:

m_AddressSpace

El nombre del espacio de dirección NAT al que pertenece el dispositivo. Este valor se establece en la tabla translations.NATAddressSpaceIds. Si el descubrimiento no está utilizando NAT, o si el dispositivo está en el dominio público, este valor es NULL.

m_Description

Valor de la variable MIB de `sysDescr` de la entidad.

m_ExtraInfo

Cualquier información extra.

m_HaveAccess

Distintivo que indica si hay acceso SNMP al dispositivo:

- 1: Tiene acceso
- 0: Sin acceso

m_LastRecord

Un distintivo que indica si este es el último registro para esta entidad (es decir, si la entidad se ha procesado completamente):

- 1: Verdadero

- 0: Falso

m_ManagerId

Identifica el gestor del dispositivo. Toma el valor "" si se accede directamente al dispositivo.

m_Name

Nombre exclusivo de una entidad de la red.

m_ObjectId

Representación textual de la clase de dispositivo (una dirección ASN.1).

m_Protocol

Una representación de entero del protocolo IP utilizada por la zona definida inmediatamente:

- 1: IPv4
- 2: IPv4 que ha pasado por la conversión de direcciones de red (NAT)
- 3: IPv6

m_UniqueAddress

Dirección IP de la entidad de red descubierta.

m_UpdAgent

El agente que actualizó este dispositivo.

Además, utilizando el separador **Avanzado**, puede construir filas de filtros utilizando cualquiera de los campos dentro del campo m_ExtraInfo.

Valores de filtro de postdescubrimiento

Al construir un filtro de postdescubrimiento, puede filtrar basándose en cualquiera de los campos de la base de datos ncimCache.

Configuración del sistema de nombres de dominio

Puede especificar los métodos que los ayudantes del sistema de nombres de dominio (DNS) utilizan para realizar búsquedas de nombres de dominio.

Acerca de esta tarea

Los ayudantes son aplicaciones especializadas que recuperan información de dispositivos de red para los agentes de descubrimiento.

Cada método que especifique utiliza uno de los siguientes tres métodos de dominio:

Servidor DNS
Un servidor en la red dedicado a realizar la resolución de nombres de dominio.

Archivo
El nombre de un archivo en el host de Network Manager que contiene direcciones IP y nombres de host en el formato de tabla de búsqueda.

Sistema
El sistema de DNS local en el host de Network Manager.

Consejo: Puede definir tantos métodos como sea necesario. Puede cambiar el orden en el que el ayudante de DNS recupera los métodos para que se recupere en primer lugar el método al que se accede más a menudo. También permite un uso más eficaz de los recursos durante el descubrimiento.

Para configurar DNS:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en el separador **DNS**.
4. Agregue un nuevo ayudante de DNS o edite uno ya existente tal como se muestra a continuación:

   - Para agregar un nuevo ayudante de DNS, haga clic en **Nuevo**  .
   - Para editar un ayudante existente, haga clic en el nombre del ayudante requerido.

   Aparecerá la página **Propiedades del servicio DNS**.
5. Complete los campos tal como se muestra a continuación y haga clic en **Aceptar**.

   Nombre de servicio
   Escriba el nombre del método.

   Tipo
   Seleccione una de las siguientes opciones:

   Sistema
   Elija esta opción para utilizar el sistema local de DNS en el servidor Network Manager. Esta es la opción predeterminada.

   Servidor DNS
   Escriba la dirección del servidor DNS requerido. En el campo **Tiempo de espera excedido**, especifique el número de segundos que desea esperar una respuesta del servidor DNS antes de superar el tiempo de espera.

   Archivo
   Escriba el nombre del archivo que contiene la información de búsqueda de dominio. Especifique el orden en el que aparece esta información en la tabla de búsqueda marcando uno de los siguientes botones de selección:

   - **Nombre, después IP**
   - **IP, después nombre**

   Sufijo de dominio
   Especifique el sufijo para añadir a cada nombre de dispositivo después de buscar el nombre. El sufijo de dominio especificado solo se agrega si no hay presente ningún sufijo de dominio en el nombre de dispositivo.

   Nota: Si espera que el descubrimiento devuelva algunos o todos los nombres de dispositivo con sufijos de dominio anexados, especifique una lista de sufijos de dominio esperados. El valor de sufijo de dominio especificado en el campo **Sufijo de dominio** no se anexa a ningún nombre de dispositivo devuelto por el descubrimiento con estos sufijos esperados. Para especificar una lista de sufijos de dominio esperados, debe configurar el archivo de configuración DiscoDNSHelperSchema.cfg en la línea de comandos.
6. Repita los pasos “4” en la página 173 a “5” en la página 173 para agregar o editar los métodos requeridos.
7. En la columna **Mover**, haga clic en **Subir** y **Bajar** para ordenar los métodos en orden de frecuencia de utilización, con los métodos utilizados más frecuentemente en la parte superior.
8. Haga clic en **Guardar**  .

Configuración de la conversión NAT

Para configurar la conversión NAT para descubrir entornos de NAT, correlacione el identificador de espacio de direcciones de un dominio NAT con la dirección IP del dispositivo de pasarela NAT asociado.

Acerca de esta tarea

Después de activar NAT, deberá correlacionar las zonas de ámbito del descubrimiento a los espacios de direcciones de NAT. Puede hacer esto en el separador **Ámbito**.

Si selecciona **Habilitar el soporte de NAT (conversión de direcciones de red)** en el separador **NAT** deberá configurar como mínimo una pasarela NAT.

Para configurar pasarelas NAT:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en **NAT**.
4. Agregue una nueva pasarela NAT, o edite una pasarela existente:
   - Para agregar una nueva pasarela NAT, haga clic en **Nuevo**  .
   - Para editar una pasarela NAT existente, haga clic en la dirección IP en la fila requerida.

   Aparecerá la página **Pasarela de NAT**.
5. Cumplimente los campos como se indica a continuación y haga clic en **Aceptar**:

   Dirección IP
   Escriba la dirección IP pública del dispositivo de pasarela NAT.

   Espacio de direcciones
   Escriba el identificador del espacio de direcciones que desea utilizar para el dominio NAT asociado.
6. Haga clic en **Guardar**  .
7. Para activar la conversión NAT para el descubrimiento, seleccione **Habilitar soporte de NAT (conversión de direcciones de red)**. Haga clic en **Guardar** y correlacione las zonas de ámbito de descubrimiento con los espacios de dirección NAT:
   a) Haga clic en **Ámbito**.
   b) Haga clic en una zona de ámbito para editarla.
      Aparecerá la página **Propiedades del ámbito**.
   c) En el campo **Espacio de direcciones**, especifique el espacio de direcciones de NAT y haga clic en **Aceptar**.
      Aparecerá la ventana **Espacio de direcciones** en **Propiedades del ámbito** sólo después de haber seleccionado **Habilitar soporte de conversión de direcciones de red (NAT)**.
   d) Repita los dos pasos anteriores para todas las zonas de ámbito necesarias.
   e) Haga clic en **Guardar**  .

   La vista NAT Address Spaces Dynamic Distinct se crea automáticamente si **Habilitar el soporte de NAT (conversión de direcciones de red)** está habilitado. Una vez finalizado el descubrimiento, utilice las **Vistas de red** para visualizar la vista de red Espacios de direcciones NAT.

Configuración de un descubrimiento multidifusión

Configure un descubrimiento multidifusión habilitando los agentes seleccionados y definiendo el ámbito del descubrimiento.

Habilitación de agentes multidifusión

Para descubrir grupos multidifusión, debe habilitar los agentes correspondientes y agregar las cadenas de comunidad SNMP relevantes.

Acerca de esta tarea

Para habilitar los agentes, complete los siguientes pasos.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en el separador **Agentes de descubrimiento completo**.

   Aparecerá la **Lista de agentes**, que muestra todos los agentes de descubrimiento disponibles de la opción de descubrimiento seleccionada.
4. Haga clic en **Descubrimiento completo de capa 2 y capa 3** > **Multidifusión**.
5. Marque el recuadro de selección que se encuentra junto a los agentes que desea habilitar.
   a) Habilite el agente StandardPIM para descubrir grupos multidifusión independientes del protocolo que siguen la norma RFC2934 PIM MIB.
   b) Habilite el agente StandardIPMRoute para descubrir redes de multidifusión de IP que siguen la norma RFC2932 IPMRoute MIB.
   c) Habilite el agente StandardIGMP para descubrir grupos multidifusión que ejecuten el protocolo de pertenencia a grupo de Internet (IGMP).
6. Haga clic en **Guardar**  .
7. Si desea redescubrir grupos multidifusión, habilite también los agentes correspondientes para realizar descubrimientos parciales.
8. Asegúrese de que las cadenas de comunidad SNMP están configuradas correctamente para acceder a dispositivos en los grupos multidifusión.

Ámbito de un descubrimiento multidifusión

Configure qué grupos de multidifusión y qué orígenes se van a descubrir utilizando el separador **Multidifusión**.

Acerca de esta tarea

Para configurar un descubrimiento multidifusión, complete los siguientes pasos.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en **Multidifusión**.
4. En la sección **Grupos multidifusión**, cree un nuevo grupo multidifusión o edite un grupo existente:

   - Para crear un nuevo grupo que se vaya a descubrir, haga clic en **Nuevo**  .
   - Para editar un grupo existente, haga clic en el nombre de grupo.

   Aparecerá la página **Propiedades de grupo de multidifusión**.
5. Defina las propiedades de ámbito utilizando los siguientes campos:

   Nombre de grupo
   Especifique un nombre para este grupo de multidifusión.

   Modalidad de PIM
   Selecciona si incluir o excluir datos de PIM (Protocol Independent Multicast) del descubrimiento. De manera predeterminada, se incluyen datos PIM.

   Modalidad de ruta de IPM
   Selecciona si incluir o excluir datos de grupo IPM (Internet Protocol Multicast) del descubrimiento. De manera predeterminada, se incluyen los datos de grupo IPM.

Modalidad de IGMP
Selecciona si incluir o excluir datos IGMP (Internet Group Management Protocol) del descubrimiento. De forma predeterminada, se incluyen los datos IGMP.

Protocolo
Solo IPv4 es soportada.

Especifique qué subredes de Grupo se deben agregar a los grupos de multidifusión
Utilice los siguientes campos y botones para agregar y suprimir subredes de grupos:

Subred
Escriba una subred y máscara de red de una subred de grupo para agregar a los grupos de multidifusión.

Agregar
Haga clic en **Agregar** para agregar este grupo.

Suprimir
Seleccione una subred de grupo de la lista adyacente y haga clic en **Suprimir** para suprimir el grupo seleccionado.

Nota: Las direcciones de multidifusión reservadas se excluyen del ámbito de manera predeterminada.

6. Haga clic en **Aceptar**.
7. Para suprimir uno o más grupos, seleccione los grupos que desee suprimir y haga clic en el botón **Suprimir**  . Para seleccionar deseleccionar todos los grupos, haga clic en el botón **Seleccionar todos**  o **deseleccionar todos**  .
8. En la sección **Orígenes de multidifusión**, cree un nuevo origen multidifusión o edite un origen existente.

   - Para crear un nuevo origen que se vaya a descubrir, haga clic en **Nuevo**  .
   - Para editar un origen existente, haga clic en el nombre del origen.

   Aparecerá la página **Propiedades de origen de multidifusión**.
9. Defina las propiedades de origen utilizando los siguientes campos:

Modalidad de ruta de IPM
Selecciona si incluir o excluir el grupo:

- **Desconocido: utilizar valor predeterminado**
- **Incluir origen**
- **Excluir origen**

Protocolo
Solo IPv4 es soportada.

Especifique qué subredes de Grupo se deben agregar a los orígenes de multidifusión
Utilice los siguientes campos y botones para agregar y suprimir subredes de grupos:

Subred
Escriba una subred y máscara de red de una subred de grupo para agregar a los orígenes de multidifusión.

Agregar
Haga clic en **Agregar** para agregar este grupo.

Suprimir
Seleccione una subred de grupo de la lista adyacente y haga clic en **Suprimir** para suprimir el grupo seleccionado.

Especifique qué subredes de Origen se deben agregar a los orígenes de multidifusión
Utilice los siguientes campos y botones para agregar y suprimir subredes de grupos:

Subred
Escriba una subred y máscara de red de una subred de origen para agregar a los orígenes de multidifusión.

Agregar
Haga clic en **Agregar** para agregar este grupo.

Suprimir
Seleccione una subred de origen de la lista adyacente y haga clic en **Suprimir** para suprimir el origen seleccionado.

10. Haga clic en **Aceptar**.
11. Para suprimir uno o más grupos, seleccione los grupos que desee suprimir y haga clic en el botón Suprimir  . Para seleccionar deseleccionar todos los grupos, haga clic en el botón Seleccionar todos  o deseleccionar todos  .
12. Haga clic en **Guardar**  .

Parámetros de descubrimiento avanzado

La configuración avanzada controla características del descubrimiento como procesos simultáneos y tiempos de espera. Utilice estos parámetros para aumentar la velocidad del descubrimiento pero equilibrando la velocidad con la carga en el servidor. Generalmente, un descubrimiento más rápido resulta en mayor utilización de memoria en el servidor.

Establezca los parámetros avanzados en el separador **Avanzado** de la página **Configuración del descubrimiento de red**. Después de haber establecido los parámetros avanzados, haga clic en **Guardar**  .

Atención: Modifique la configuración avanzada sólo si es un usuario experimentado de Network Manager. Si modifica los parámetros avanzados y el descubrimiento no funciona tal como se espera, haga clic en **Restablecer** para restaurar los valores predeterminados.

"Configuración avanzada del buscador" en la página 177
"Configuración avanzada del buscador de pings" en la página 177
"Configuración avanzada del ayudante Telnet" en la página 178
"Configuración avanzada del ayudante SNMP" en la página 178
"Configuración avanzada del ayudante de DNS" en la página 179
"Configuración avanzada de descubrimiento" en la página 179

Configuración avanzada del buscador

Para establecer parámetros avanzados para el Buscador de archivos, utilice el campo siguiente:

Buscadores de archivos simultáneos
Especifique el número de hebras que debe utilizar el Buscador de archivos. Cada hebra puede procesar un archivo de fuente distinto simultáneamente. Si tiene muchos archivos de fuente y recursos de reserva en el servidor de descubrimiento, que haya más hebras puede dar lugar a un descubrimiento más rápido. Si sólo tiene un archivo de fuente, el aumento del número de hebras no tiene efecto.

Configuración avanzada del buscador de pings

Para establecer los parámetros avanzados del Buscador de pings, utilice los siguientes campos:

Buscadores de pings simultáneos
Especifique el número de hebras que serán utilizadas por el Buscador de pings. Cada hebra procesa una inserción pingFinder.pingRules a la vez. El aumento del número de hebras no acelera un único gran barrido de ping, pero es posible que acelere la retroalimentación de muchas direcciones. Sin embargo, debe equilibrar la velocidad en relación con los recursos de su máquina y la capacidad del

receptor de ping para procesar las respuestas al ping en el momento oportuno. Si el número de subprocesos es demasiado alto, el receptor de ping puede quedarse atrás, lo que producirá como resultado errores de ping falsos y una pérdida del descubrimiento del dispositivo.

Los estudios han demostrado que el número predeterminado de 10 subprocesos es óptimo en la mayoría de los casos. Puede aumentar de forma gradual el número de subprocesos y supervisar el número de errores de ping y tomar nota del ahorro de tiempo. En función de los recursos disponibles, en un determinado momento las ventajas empezarán a disminuir a medida que se sobrecarguen los recursos.

Tiempo de espera predeterminado
Especifique el tiempo máximo, en milisegundos, que deberá esperarse una respuesta de la dirección a la que se ha hecho ping. Si sabe que la latencia de la red es baja, un tiempo de espera reducido puede dar lugar a un descubrimiento más rápido. Un valor que sea demasiado bajo para su red puede dar lugar a que los dispositivos no se descubran.

Número predeterminado de reintentos
Especifique el número de veces que se tiene que hacer ping en un dispositivo de nuevo siguiendo un ping inicial fallido.

Tiempo entre pings
Especifique el intervalo en milisegundos entre intentos de ping realizados en los dispositivos contenidos en una lista o subred. Si el tráfico de red resultante del descubrimiento no es un problema, este valor se puede reducir.

Permitir ping de difusión:
Para permitir los pings de difusión de direcciones, marque este recuadro de selección.

Permitir ping de multidifusión
Para permitir los pings de multidifusión de direcciones, marque este recuadro de selección.

Configuración avanzada del ayudante Telnet

Para establecer parámetros avanzados para el ayudante de Telnet, utilice los siguientes campos:

Ayudantes de Telnet simultáneos
Especifique el número de hebras que debe utilizar el ayudante de Telnet. Si tiene muchos dispositivos desde los que desee acceder a los datos con Telnet o SSH, el aumento de este valor puede dar lugar a un descubrimiento más rápido. Los ejemplos típicos de tales dispositivos son los conmutadores Catalyst, los dispositivos MPLS y las pasarelas NAT. Si modifica este valor, compruebe que el sistema está configurado para permitir al menos el número especificado de sesiones Telnet.

Tiempo de espera predeterminado
Especifique el tiempo máximo, en milisegundos, que debe esperarse para acceder a un dispositivo.

Número de reintentos
Especifique el número de veces que debe intentar conectarse al dispositivo siguiendo un intento de conexión inicial fallida.

Consejo: También puede configurar algunos otros valores avanzados en el archivo `DiscoTelnetHelperSchema.cfg`.

Configuración avanzada del ayudante SNMP

Para utilizar los parámetros avanzados del ayudante de SNMP, utilice los siguientes campos:

Ayudantes de SNMP simultáneos
Especifique el número de hebras que debe utilizar el ayudante. Si tiene muchos dispositivos con acceso SNMP y recursos de reserva en el servidor de descubrimiento, que haya más hebras puede dar lugar a un descubrimiento más rápido. Si modifica este valor, compruebe que el sistema está configurado para permitir al menos el número especificado de sesiones SNMP simultáneas. Este valor debe ser mayor que el número de hebras utilizadas por el agente de descubrimiento Detalles.

Tiempo de espera excedido
Especifique el tiempo máximo, en milisegundos, que debe esperarse para acceder a un dispositivo.

Número de reintentos
Especifique el número de intentos para recuperar una o más variables SNMP de un dispositivo después de un intento inicial fallido.

Retraso GetNext
Especifique el retraso, en milisegundos, entre cada solicitud de GetNext de SNMP. El parámetro **m_GetNextSlowDown** se aplica cuando el número de solicitudes GetNext independientes emitidas para recuperar una variable SNMP no escalar supera el valor del parámetro **m_GetNextBoundary**.

Límite GetNext
Especifique el número de solicitudes GetNext que emitir cuando se recupera una variable SNMP no escalar de un dispositivo. El parámetro **m_GetNextBoundary** se aplica antes de introducir el retraso especificado por el parámetro **m_GetNextSlowDown**.

Configuración avanzada del ayudante de DNS

Para establecer parámetros avanzados del ayudante de DNS, utilice los siguientes campos:

Ayudantes de DNS simultáneos
Especifique el número de hebras que debe utilizar el ayudante. Si modifica este valor, compruebe que el sistema está configurado para permitir al menos el número especificado de sesiones DNS.

Tiempo de espera predeterminado
Especifique el tiempo máximo, en milisegundos, que deberá esperarse una respuesta de un dispositivo.

Configuración avanzada de descubrimiento

Para especificar controles avanzados de retroalimentación, verificación de pings y más parámetros avanzados de descubrimiento, utilice los siguientes campos:

Habilitar control de retroalimentación
Especifique si debe habilitarse el control de retroalimentación. La retroalimentación quiere decir que los datos devueltos por los agentes serán utilizados por el descubrimiento para encontrar otros dispositivos. Algunos ejemplos de datos de retroalimentación incluyen las direcciones IP de vecinos remotos y las direcciones de la subred dentro de la que existe un vecino local.

Sin retroalimentación
La retroalimentación está desactivada para todos los descubrimientos y redescubrimientos. Sólo se descubrirán los dispositivos especificados en los buscadores. Esta opción quiere decir que los descubrimientos y redescubrimientos finalizarán en el tiempo más breve posible. Sin embargo, la topología de red resultante estará incompleta a menos que especifique todos los dispositivos que desee descubrir como fuentes.

Consejo: Desactive la retroalimentación si desea descubrir sólo una lista de ciertos dispositivos. Especifique los dispositivos que desee descubrir como fuentes.

Retroalimentación
La retroalimentación está activada para los descubrimientos completos, redescubrimientos completos y para los redescubrimientos parciales. Esta opción proporciona una topología completa en todas las situaciones pero tarda más tiempo que el resto.

Retroalimentación sólo para completas
Este valor está activado de forma predeterminada. La retroalimentación está activada para los descubrimientos y redescubrimientos completos pero desactivada para los redescubrimientos parciales.

Habilitar verificación de pings
Especifique si el descubrimiento comprueba la existencia de interfaces a los que se puede hacer ping. Si no puede hacerse ping a un dispositivo, el dispositivo no será sondeado en busca de alertas.

No comprobar posibilidad de hacer ping
No se comprobará si se puede hacer ping en ninguna de las interfaces descubiertas. Las interfaces se sondearán independientemente de si puede hacerse o no ping en el descubrimiento.

Comprobar posibilidad de ping
Tras el descubrimiento, cada interfaz descubierta se comprueba para ver si se puede hacer ping en ella. La comprobación se ejecuta en la tabla details.returns. Podrá hacerse ping a los interfaces con una entrada en esta tabla. No podrá hacerse ping a las interfaces sin una entrada en esta tabla. Las interfaces a las que pueda hacerse ping aparecerán marcados para ser sondeados.

Detectar mejor valor
Este valor está activado de forma predeterminada. Si se ha habilitado el control de retroalimentación, después del descubrimiento se comprueba si puede hacerse ping a todas las interfaces descubiertas. La comprobación se ejecuta en la tabla details.returns. Podrá hacerse ping a los interfaces con una entrada en esta tabla. No podrá hacerse ping a las interfaces sin una entrada en esta tabla. Las interfaces a las que pueda hacerse ping aparecerán marcados para ser sondeados.

Restricción: Esta opción solo funciona cuando ha seleccionado una de las siguientes opciones en la lista **Habilitar control de retroalimentación**: `Retroalimentación` o `Retroalimentación solo para completas`.

Habilitar 'Permitir virtual'
Especifique cómo desea que el descubrimiento gestione las direcciones IP virtuales: [1].

No permitir virtual
No descubre direcciones IP virtuales.

Permitir virtual
Descubre direcciones IP virtuales. Este valor está activado de forma predeterminada.

Permitir si está en scope.special
Descubre direcciones IP virtuales sólo si la dirección está definida la tabla scope.special. Esta tabla define las direcciones IP de gestión.

Habilitar modelado de VLAN
Habilite este valor para modelar las VLAN en este descubrimiento. Si habilita el modelado de VLAN, podrá particionar las topologías descubiertas según la pertenencia a VLAN. La inhabilitación del modelado de VLAN reduce el tiempo de descubrimiento.

Habilitar denominación SysName
Habilite este valor para denominar a dispositivos utilizando el valor de la variable SNMP sysName como origen principal de la información de denominación. La variable sysName debe establecerse y ser exclusiva en toda la red. La habilitación de este valor no tiene impacto en el tiempo de descubrimiento, dado que la variable sysName la recupera el agente Detalles de forma predeterminada.

Importante:

Si se han descubierto dispositivos previamente con la denominación SysName inhabilitada, pueden aparecer dispositivos duplicados en el siguiente descubrimiento. Por ejemplo, el mismo dispositivo puede aparecer dos veces, una con la dirección IP y otra con el nuevo nombre. Para evitar entradas de dispositivo duplicadas, establezca el valor LingerTime de todos los dispositivos en la topología en cero antes de ejecutar el siguiente descubrimiento. Inicie sesión en el proveedor de servicios OQL con el siguiente mandato:

```
ncp_oql -domain NCOMS -service Model
```

[1] Los dispositivos se descubren normalmente mediante direcciones IP recuperadas por el agente AssocAddress. Si se descubre un dispositivo utilizando una dirección IP no recuperada por el agente AssocAddress, quiere decir probablemente que es una dirección IP no estándar. Este tipo de dirección IP se denomina una *dirección IP virtual*. Algunos ejemplos de direcciones IP virtuales son direcciones HSRP y VRRP, que comparten varios dispositivos para crear tolerancia a fallos. Otros ejemplos incluyen determinadas interfaces de gestión que pueden estar en un único dispositivo pero que no aparecen en la tabla IP por motivos de seguridad. Las direcciones IP virtuales incluyen direcciones de gestión. Una dirección de gestión es una dirección IP cuya única función es gestionar el dispositivo. Las direcciones de gestión suelen encontrarse en una red independiente aislada del tráfico cliente. Estas direcciones se definen en la tabla scope.special.

Ejecute el mandato siguiente para establecer LingerTime en cero:

```
update ncimCache.lingerTime set lingerTime = {LINGERTIME=0};
go
```

Habilitar almacenamiento en caché de tablas de descubrimiento

Habilite este valor para colocar en la memoria caché los datos durante el proceso de descubrimiento para permitir la recuperación de datos en caso de que falle el motor de descubrimiento, ncp_disco. Un descubrimiento en ejecución en esta modalidad es más lento que un descubrimiento estándar debido al tiempo extra requerido para almacenar datos en el disco en todo el proceso de descubrimiento.

Un administrador puede ocultar esta opción en la página **Configuración de detección de redes** al establecer la propiedad `discoconfig.allow.table.caching` en `false` en `discoconfig.properties`. Si la opción no está presente en la GUI, un administrador puede controlar si las tablas de descubrimiento se almacenan en caché al establecer la propiedad `disco.config.m_WriteTablesToCache` en `true` en el archivo `DiscoConfig.cfg` o en la versión específica del dominio de ese archivo.

Habilitar verificación de buscador de archivos

Habilite este valor para utilizar el Buscador de pings para verificar la existencia de dispositivos especificados en los archivos utilizados por el Buscador de archivos. Si habilita este valor, compruebe que está habilitado el Buscador de pings. Habilite este valor si no está seguro de que los dispositivos sigan conectados a la red. Por ejemplo, puede que desee habilitar este valor si la red está cambiando rápidamente.

Habilitar capas de reconstrucción de redescubrimiento

Habilite este valor para reconstruir las capas de topología que siguen a un redescubrimiento parcial. Si especifica que se reconstruyen las capas de topología siguiendo un redescubrimiento parcial, el resultado es una topología precisa que muestra toda la conectividad. Sin embargo, el proceso de agregar nuevos dispositivos tarda más tiempo.

Consejo: Para configurar un redescubrimiento parcial para que se ejecute tan rápido como sea posible, inhabilite esta opción.

Habilitar redescubrimiento de dispositivos relacionados

Los vecinos remotos de un dispositivo no se vuelven a descubrir de forma predeterminada, incluso si el redescubrimiento de dicho dispositivo indica que es posible los vecinos hayan cambiado. Los vecinos remotos pueden ser redescubiertos en el siguiente redescubrimiento completo. Habilite este valor si desea cambiar este comportamiento predeterminado y redescubrir cualquier vecino remoto cambiado al redescubrir dicho dispositivo. Si se descubren nuevos dispositivos vecinos durante la fase de inactividad, se desencadena otro redescubrimiento parcial después de la fase de inactividad. Si la conectividad de la red cambia con frecuencia, por ejemplo, si va a redescubrir dispositivos con tablas de base de datos de reenvío de conmutadores, la habilitación del redescubrimiento de dispositivos relacionados puede provocar que se ejecuten varios descubrimientos uno tras otro. Es más probable que se produzcan varios descubrimientos consecutivos si el descubrimiento parcial tarda más tiempo, por ejemplo, si está habilitado el valor **Habilitar capas de reconstrucción de redescubrimiento**.

Consejo: Para configurar un redescubrimiento parcial para que se ejecute tan rápido como sea posible, inhabilite esta opción.

Habilitar denominación de interfaces ifName/ifDescr

Cambia el convenio de denominación predeterminado para interfaces descubiertos. Denomina interfaces utilizando datos de los campos ifName e ifDescr de la tabla de interfaces SNMP como sea apropiado. Por ejemplo, `Fa0/0, Gi 1.0.2:0, Gigabit Ethernet 4/1`. Si cambia el convenio de denominación predeterminado de las interfaces descubiertas, deberá alterar el agrupador BuildInterfaceName para que especifique su convenio de denominación.

Consejo: Algunos dispositivos pueden informar de nombres de interfaces y de descripciones que son demasiado largos para mostrarse adecuadamente en la visualización de la topología. Si hay dispositivos que informan de nombres y descripciones de interfaces largos o incorrectos, inhabilite este valor.

Habilitar deducción de PE utilizando datos BGP en CE

Descubre redes de proveedor participantes como objetos de "terceros" en varias redes que se ejecutan en una red de proveedores. Algunos ejemplos de este tipo de red incluye VPN empresariales en toda una red troncal MPLS de proveedor. Seleccione esta opción si desea enlazar todas las redes en una única topología y realizar análisis de causa raíz (RCA) en todas las redes.

Esta opción deduce la existencia de dispositivos PE (de proveedor) inaccesibles utilizando los datos BGP en los dispositivos CE (del lado del cliente) que apuntan a los dispositivos PE. Para descubrir estos datos BGP, deben habilitarse los agentes de descubrimiento BGP. Si desea utilizar la función de descubrimiento de dominios cruzados, deseleccione esta opción. Si se selecciona esta opción, se generarán errores durante el descubrimiento de dominios cruzados.

Opcionalmente, también puede especificar cual de los dispositivos PE deducidos son dispositivos válidos, rellenando la tabla scope.inferMPLSPEs, utilizando entradas de ámbito de formato estándar, como en la tabla scope.zones. Si se ha rellenado, esta tabla le permite definir qué direcciones IP verá en dispositivos CE que considere dispositivos PE válidos. Utilice esta opción cuando tenga dispositivos inaccesibles que estén conectados mediante BGP pero que no sean dispositivos PE.

Habilitar deducción de direccionadores CE de MPLS en subredes /30

Genera sucesos afectados por servicio en VPN de clientes. Seleccione esta opción si es un proveedor de servicio sin acceso a los direccionadores CE del cliente.

Normalmente, no es necesario habilitar la inferencia de los dispositivos CE y PE.

Iniciar un descubrimiento

Una vez haya configurado un descubrimiento, puede iniciar y, si fuese necesario, detener el descubrimiento.

Antes de empezar

Realice los cambios de configuración de descubrimiento antes de iniciar el descubrimiento.

Acerca de esta tarea

Puede iniciar los siguientes tipos de descubrimiento:

Descubrimiento

Inicie un descubrimiento completo para descubrir la red por primera vez o para actualizar la topología de red si sabe que la red ha cambiado.

Descubrimiento parcial

Ejecute un descubrimiento parcial si sabe que los cambios en la red se han limitado a un número reducido de dispositivos. Deberá configurar el ámbito y las fuentes como parte del inicio de cada descubrimiento parcial. Si la relación de los dispositivos que se encuentran en ámbito con los dispositivos colindantes ha cambiado, los dispositivos colindantes también se pueden descubrir. Si el descubrimiento parcial necesita descubrir una gran cantidad de dispositivos basándose en información de conectividad, se iniciará un descubrimiento completo.

Nota: Si detiene un descubrimiento que se está ejecutando, debe realizar un descubrimiento completo antes de que pueda llevar a cabo un descubrimiento parcial.

Para iniciar un descubrimiento, realice los siguientes pasos.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Estado del descubrimiento de red**.
2. Seleccione el dominio en el que desea ejecutar un descubrimiento desde el menú **Dominio**. Puede empezar a escribir el nombre del dominio y hacer coincidir los dominios que están enumerados bajo el campo **Dominio**.
3. Iniciar un descubrimiento completo o parcial:

- Para iniciar un descubrimiento completo, sólo haga clic en **Iniciar descubrimiento**  . Se inicia el descubrimiento.
- Para iniciar un descubrimiento parcial, haga clic en la flecha que indica hacia abajo junto al botón **Iniciar descubrimiento**  y seleccione **Iniciar descubrimiento parcial** del menú (si no se ha ejecutado ningún descubrimiento completo desde la última vez que el motor de descubrimiento, **ncp_disco**, se inició, la opción de iniciar un descubrimiento parcial aparecerá en gris). Se muestra la ventana **Descubrimiento parcial**. Especifique las direcciones IP y subredes que contienen los dispositivos que se van a descubrir:

a) En **Descubrimiento parcial**, seleccione los nodos y subredes requeridas.

b) Para agregar una nueva subred o nodo, haga clic en **Nuevo.**

c) Cumplimente los campos como se indica a continuación y haga clic en **Aceptar**:

Descubrir
Seleccione una de las siguientes opciones:

Identificador
Escriba la dirección IP requerida.

Subred
Escriba la subred requerida y especifique el número de bits de máscara de red. El campo **Máscara de red** se actualiza automáticamente.

Nombre de dispositivo de EMS
Escriba el nombre de un dispositivo que se ha descubierto mediante un Sistema de gestión de elementos (EMS). Puede escribir el ID nativo, el nombre de entidad, el nombre de sistema o el nombre de visualización.

Nota: Cuando ejecuta un descubrimiento parcial de un recopilador EMS desde la **GUI de estado de descubrimiento**, en la ventana **Nuevo nodo/subred de descubrimiento parcial**, debe especificar el valor del identificador del EMS en el campo **Nombre de dispositivo de EMS**, no en el campo **Identificador**. El campo **Identificador** sólo acepta direcciones IP.

d) Para agregar nuevas zonas de ámbito, haga clic en **Ámbito**.

e) Para agregar una nueva zona de descubrimiento, haga clic en **Nuevo**  . Para editar una zona de ámbito existente, haga clic en la entrada requerida en la lista.

f) Cumplimente los campos como se indica a continuación y haga clic en **Aceptar**:

Acción
Defina el rango de subred como una zona de inclusión o de exclusión. Si el rango de subred es una zona de inclusión en la que ejecutará ping durante el descubrimiento, haga clic en **Agregar a lista de fuentes de ping**. Al hacer clic en esta opción, se agregan automáticamente los dispositivos en la zona del ámbito como dispositivos de fuente de descubrimiento.

Restricción: La opción `Agregar a lista de fuente de ping` no está disponible para zonas de ámbito de IPv6. Esto evita los barridos de ping de subredes IPv6, que potencialmente pueden contener billones de dispositivos para hacer ping. Por lo tanto, un barrido de ping de redes IPv6 puede provocar un descubrimiento interminable.

g) Haga clic en **Aceptar** y en **Ir**.

Cuando se está ejecutando un descubrimiento completo o parcial, se desactiva el botón **Iniciar descubrimiento**  .

4. Para detener un descubrimiento, haga clic en **Detener descubrimiento**  . El descubrimiento tardará un poco en detenerse, y durante este tiempo se desactivarán los botones **Iniciar descubrimiento** y **Detener descubrimiento**. Si detiene un descubrimiento, no podrá realizar un descubrimiento parcial hasta que finalice el próximo descubrimiento completo.

Nota: Cuando detiene un descubrimiento, la memoria caché de descubrimiento se pierde. Por eso debe esperar hasta que finalice el siguiente descubrimiento completo para realizar un descubrimiento parcial. Es posible configurar el motor de descubrimiento de forma que guarde la memoria caché de descubrimiento cuando el descubrimiento está en ejecución, cosa que permitiría ejecutar un descubrimiento parcial inmediatamente después de la detención manual de un descubrimiento. Para configurar el motor de descubrimiento de forma que guarde la memoria caché de descubrimiento, haga clic en **Habilitar almacenamiento en caché de tablas de descubrimiento** en el separador **Avanzado**.

Resultados

Mientras se ejecuta el descubrimiento, podrá supervisar el progreso del mismo.

Nota: No puede detener el descubrimiento desde la GUI en la fase de correlación de conectividad. La detención del proceso de descubrimiento desde la línea de mandatos mientras se crea la topología puede dañar el descubrimiento.

Qué hacer a continuación

Una vez haya finalizado el descubrimiento, se activa el botón **Iniciar descubrimiento** y puede ejecutar otro descubrimiento completo o parcial en cualquier momento. Si está habilitado el conector Disco de pasarela de suceso, se puede desencadenar un nuevo descubrimiento de forma automática cuando se recibe un suceso de rearranque (ID de suceso de `NmosSnmpReboot` que la política de sondeo rebootDetection ha desencadenado).

Esquemas y tablas para parámetros de descubrimiento de GUI

Utilice esta información de referencia para aprender en qué esquemas y tablas se guardan los valores de los separadores de la página **Configuración de descubrimiento de red**.

La siguiente tabla describe las tablas en las que se guardan los valores de cada separador de la página **Configuración de descubrimiento de red**. En estas tablas, *DOMAIN_NAME* representa el nombre de los dominios de red en su despliegue, como por ejemplo NCOMS.

Tabla 20. Esquemas y tablas en los que se correlacionan los parámetros de descubrimiento

Separador Configuración de descubrimiento de red	**Descripción**	**Esquema o nombre de tabla**
Ámbito	Las zonas de la red (es decir, rangos de subred) que desee incluir en el descubrimiento y las zonas que desea excluir del mismo.	`DiscoScope.`*`DOMAIN_NAME`*`.cfg`
Fuente	La ubicación desde la que comenzar a descubrir dispositivos. Esta puede ser una o más direcciones IP, o direcciones de subredes. Para agregar fuentes al descubrimiento, se utilizan los siguientes *buscadores*: Buscador de pings y Buscador de archivos.	Buscador de pings `DiscoPingFinderSeeds.`*`DOMAIN_NAME`*`.cfg` Buscador de archivos `DiscoFileFinderParseRules.`*`DOMAIN_NAME`*`.cfg`

Tabla 20. Esquemas y tablas en los que se correlacionan los parámetros de descubrimiento (continuación)

Separador Configuración de descubrimiento de red	Descripción	Esquema o nombre de tabla
Agentes de descubrimiento completo y **Agentes de redescubrimiento parcial**	Los agentes de descubrimiento que se utilizarán para investigar la conectividad de los dispositivos. Se proporcionan agentes predeterminados para el tipo de descubrimiento que desee realizar, por ejemplo, un descubrimiento de capa 2 ó 3. Puede seleccionar distintos conjuntos de agentes para descubrimientos completos y para descubrimientos parciales. Los agentes varían porque la información de conectividad varía según la tecnología del hardware en la red.	`DiscoAgents.`*`DOMAIN_NAME`*`.cfg`
Acceso a dispositivos	Cadenas de comunidad SNMP y parámetros de Telnet que Network Manager utiliza para interrogar a dispositivos que utilizan SNMP y Telnet.	cadenas de comunidad SNMP `SnmpStackSecurityInfo.cfg` Acceso a Telnet: `SnmpStackSecurityInfo.cfg`
Filtros	Puede utilizar filtros para filtrar dispositivos antes o después del descubrimiento. Puede filtrar dispositivos basándose en una variedad de criterios, lo que incluye ubicación, tecnología y fabricante. Los filtros de predescubrimiento impiden que se sondeen dispositivos descubiertos en busca de información de conectividad. Los filtros de postdescubrimiento impiden que los dispositivos descubiertos se pasen a MODEL.	`DiscoSchema.`*`DOMAIN_NAME`*`.cfg`
DNS	Acceso a servicios DNS utilizado para realizar búsquedas de nombres de dominio.	`DiscoDNSHelperSchema.cfg`
NAT	Los datos que proporcionan las correlaciones de descubrimiento entre los datos de espacio de direcciones y las direcciones IP de dispositivos reales para facilitar más descubrimientos.	`DiscoSchema.`*`DOMAIN_NAME`*`.cfg`
Multidifusión	Los grupos y orígenes de multidifusión utilizados por el motor de descubrimiento para configurar ámbitos de multidifusión.	`DiscoScope.`*`DOMAIN_NAME`*`.cfg`
Avanzado	La configuración avanzada controla características del descubrimiento como procesos simultáneos y tiempos de espera excedidos. Utilice estos parámetros para aumentar la velocidad del descubrimiento pero equilibrando la velocidad con la carga en el servidor. Generalmente, un descubrimiento más rápido resulta en mayor utilización de memoria en el servidor.	`DiscoSchema.`*`DOMAIN_NAME`*`.cfg`

Descubrimiento de la red utilizando la interfaz de línea de mandatos

Como usuario experimentado, puede configurar y rastrear un descubrimiento de red utilizando archivos de configuración y consultas de bases de datos.

Archivos de configuración de descubrimiento

Los usuarios experimentados pueden configurar el descubrimiento mediante la edición de los archivos de configuración de descubrimiento.

Para configurar el descubrimiento utilizando la interfaz de línea de comandos (línea de comandos), edite los archivos de configuración de descubrimiento y cree o edite inserciones en las bases de datos de los procesos de descubrimiento.

Nota: El archivo de configuración DiscoSchema.cfg contiene los esquemas de todas las bases de datos de descubrimiento. A diferencia de los archivos mencionados a continuación, el archivo de configuración DiscoSchema.cfg no contiene instrucciones de inserción. Puede ver este archivo, pero no debe editarlo.

Cuando se ejecuta ncp_disco, examina de forma periódica los directorios de los agentes y agrupadores y carga cualquier definición de agente de descubrimiento o agrupador nueva o modificada.

Tabla 21 en la página 186 muestra qué archivos de configuración deben editarse para configurar el descubrimiento y si la configuración se puede realizar también utilizando la GUI **Configuración de descubrimiento**.

Tabla 21. Archivos de configuración de descubrimiento editables por el usuario

Tarea de configuración de descubrimiento	**Archivo de configuración**	**Separador GUI**
Definición del ámbito del descubrimiento		
Definición de zonas de inclusión y exclusión	DiscoScope.cfg	**Ámbito**
Omisión del ámbito de descubrimiento	DiscoScope.cfg	**Ámbito**
Adición de fuentes a un descubrimiento		
Utilización y configuración del buscador de pings	DiscoPingFinderSeeds.cfg	**Fuente**
Ejecución de varias instancias de un buscador		
Configuración del ping de las direcciones de difusión y multidifusión	DiscoPingFinderSeeds.cfg	**Avanzado**
Utilización y configuración del buscador de archivos	DiscoFileFinderParseRules.cfg	**Fuente**
Habilitar la verificación de dispositivos del buscador de archivos	DiscoConfig.cfg	**Avanzado**
Habilitar verificación de ping	DiscoConfig.cfg	
Utilización y configuración del buscador de base de datos	DiscoDBEntryFinderQueries.cfg	
Uso y configuración del buscador de recopiladores	DiscoCollectorFinderSeeds.cfg	

Tabla 21. Archivos de configuración de descubrimiento editables por el usuario (continuación)		
Tarea de configuración de descubrimiento	**Archivo de configuración**	**Separador GUI**
SNMP		
Configuración de cadenas de comunidad SNMP y contraseñas	SnmpStackSecurityInfo.cfg	**Contraseñas**
Configuración del ayudante SNMP	DiscoSnmpHelperSchema.cfg	**Avanzado**
Sustitución de la configuración del ayudante SNMP para dispositivos y subredes específicos		
Telnet		
Configuración del acceso telnet a los dispositivos de red	TelnetStackPasswords.cfg	**Contraseñas**
Configuración del ayudante telnet	DiscoTelnetHelperSchema.cfg	**Avanzado**
Configuración de un descubrimiento sensible al contexto	DiscoConfig.cfg	
Agentes		
Habilitación e inhabilitación de agentes de descubrimiento	DiscoAgents.cfg	**Agentes de descubrimiento completo** **Agentes de redescubrimiento parcial**
Filtrado de dispositivos enviados a los agentes	Archivos de definición del agente de descubrimiento	**Filtros**
Filtrado de los datos de topología devueltos por un agente	Archivos de definición del agente de descubrimiento	
Filtro de datos de topología devueltos por todos los agentes	DiscoAgentReturns.filter	
Cambio del número de subproceso utilizados por un agente	DiscoAgents.cfg	
Habilitación de la operación multiproceso de agentes de Perl	Archivos de definición del agente de descubrimiento	
Habilitación e inhabilitación de coincidencias parciales	Archivo de definición del agente IpForwardingTable.agnt (para dispositivos modernos que utilizan RFC2096) Archivo de definición del agente IpRoutingTable.agnt (para dispositivos antiguos que utilizan RFC1213).	
Restricciones del descubrimiento		

Tabla 21. Archivos de configuración de descubrimiento editables por el usuario (continuación)		
Tarea de configuración de descubrimiento	**Archivo de configuración**	**Separador GUI**
Restricciones de la detección de dispositivos	DiscoScope.cfg DiscoPingFinderSeeds.cfg	**Alcance** **Fuente**
Restricciones del interrogatorio de dispositivos	DiscoScope.cfg	
Restricciones de la creación de instancias de dispositivos		
Filtrado de interfaz SNMP	DiscoSnmpHelperFilters.cfg	
Configuración de los servicios del ayudante DNS	DiscoDNSHelperSchema.cfg	**DNS**
Configuración de un descubrimiento de NAT	Agente NATTextFileAgent agente NATGateway	**NAT**
Configuración avanzada		
Configuración avanzada del buscador de archivos Configuración avanzada del buscador de pings Configuración avanzada del ayudante de DNS Configuración avanzada del ayudante SNMP Configuración avanzada del ayudante Telnet	DiscoFileFinderParseRules.cfg DiscoPingFinderSeeds.cfg DiscoDNSHelperSchema.cfg DiscoSnmpHelperSchema.cfg DiscoTelnetHelperSchema.cfg **Nota:** Como experto usuario, podrá establecer los parámetros de configuración más avanzados en los archivos de configuración que están disponibles en el separador Avanzado de la GUI.	**Avanzado**

Archivos de definición del agente de descubrimiento

Los archivos de definición del agente de descubrimiento definen la operación de los agentes de descubrimiento.

Dispositivos de filtrado que utilizan los archivos de definición

Nota: Network Manager elimina a todos los agentes de descubrimiento al final de la etapa 3 de la recopilación de datos. Esto asegura que el siguiente descubrimiento reinicie los agentes y fuerza a que los agentes relean sus archivos de configuración al comienzo de un descubrimiento, con lo que se detectará cualquier cambio en los archivos de configuración.

Puede aplicar un filtro a un agente de descubrimiento editando el filtro de dispositivos soportados en la sección DiscoAgentSupportedDevices( ); del archivo de definición del agente de descubrimiento $NCHOME/precision/disco/agents/*.agnt). Todos los agentes de descubrimiento tienen un archivo de definición en este directorio, independientemente de si el agente está basado en texto o se ha compilado con anterioridad.

El filtro de dispositivos soportados es un filtro que se aplica en los atributos de la tabla agentTemplate.despatch.

La sección DiscoAgentSupportedDevices( ); acepta pruebas de comparación OQL completas mediante operadores de comparación como `like`, < , > , = , and <>. Se puede encontrar información detallada sobre pruebas de comparación en OQL en *Referencia de IBM Tivoli Network Manager*.

Consejo: La alteración de los archivos de definición de agente puede introducir errores de análisis. Para comprobar errores de análisis en su agente, ejecute el agente en modalidad de depuración y examine la salida de depuración.

Ejemplo: dispositivos de filtrado que se envían al agente CDP

El siguiente ejemplo muestra la sección DiscoAgentSupportedDevices(); del archivo de definición de agente `CDP.agnt`. El agente CDP procesa solo las entidades de red que coinciden con los ID de objeto especificado, es decir, solo los dispositivos que utilizan Cisco Discovery Protocol. El agente CDP no procesa dispositivos con el ID de objeto 1.3.6.1.4.1.9.1.226.

```
DiscoAgentSupportedDevices
(
            " (
                        ( m_ObjectId like '1\.3\.6\.1\.4\.1\.9\..*' )
                        AND
                        ( m_ObjectId <> '1.3.6.1.4.1.9.1.226' )
            ) "
);
```

Ejemplo: utilización de comodines en filtros de dispositivo

El siguiente ejemplo muestra el uso de comodines en la columna de la dirección IP. El agente solo acepta dispositivos con una dirección IP que empiece por 10.10.2.

```
DiscoAgentSupportedDevices
(
            " ( m_UniqueAddress like '10\.10\.2\..*' ) "
);
```

Ejemplo: utilización de varias condiciones de filtro de dispositivo

El siguiente ejemplo muestra la combinación de varias condiciones de filtro. El agente acepta solo dispositivos que tienen el ID de objeto 1.3.6.1.4.1.9.5.7.. que tienen una dirección IP que empieza por 10.10 y no tienen un nombre clandestino.

```
DiscoAgentSupportedDevices
(
            "(
                    ( m_ObjectId = '1.3.6.1.4.1.9.5.7' )
                    AND
                    ( m_UniqueAddress like '^10\.10\..*' )
                    AND
                    ( m_Name not like '.*[cC]landestin[eE].*' )
            )"
);
```

Habilitación de operación multihebra para agentes de descubrimiento Perl

El número de hebras que utilizan los agentes de descubrimiento está definido en el archivo de configuración `DiscoAgents.cfg`. Los agentes Perl deben tener la operación multihebra habilitada antes de que el valor en el archivo de configuración `DiscoAgents.cfg` surta efecto.

Para habilitar una operación multihebra para un agente de descubrimiento Perl, agregue la siguiente línea a su archivo de definición:

```
DiscoAgentDefaultThreads( 10 );
```

La inserción anterior especifica que el agente utiliza 10 hebras de forma predeterminada. Si define un número diferente de hebras en el archivo de configuración `DiscoAgents.cfg`, ese valor sustituye al valor en el archivo de definición del agente.

Restricción: Muchos de los módulos CPAN complementarios que se utilizan a menudo con Perl no son seguros para las hebras. Los agentes de descubrimiento de Perl que utilizan esos módulos tendrán que ser restringidos a una sola hebra.

Filtrado de datos de topología que ha devuelto un agente de descubrimiento

Para filtrar datos de topología que ha devuelto un único agente, defina un filtro en el archivo de agente relevante (.agnt).

Ejemplo: filtrado de interfaces de módem por cable de suscriptor

El archivo agente CMTS.agnt recupera datos de los módems por cable conectados a un dispositivo de servicio de terminación de módem por cable. Este ejemplo describe un filtro que se ha agregado al archivo CMTS.agnt que filtra interfaces de módem por cable de suscriptor desde datos de topología devueltos para los dispositivos CMTS. El filtro de ejemplo es el siguiente:

```
DiscoAgentReturnsFilterList
{
      DiscoReturnsFilter
      {
            "(
             m_LocalNbr->m_IfType = 229
            )"
      }
};
```

Ejemplo: definición de varios filtros de topología

El siguiente ejemplo ilustra cómo definir varios filtros de datos de topología en un agente. El primer filtro especifica que cada vez que se devuelve un registro en el que el valor ifIndex de interfaz es 4, los campos m_Name, m_HaveAccess, m_LocalNbr->m_SubnetMask, y m_RemoteNbr->m_RemoteNbrPhysAddr se deben suprimir del registro. El segundo filtro suprime los registros que se devuelven cuando el valor ifIndex de la interfaz es 5.

```
DiscoAgentReturnsFilterList
{
      DiscoReturnsFilter
      {
            "(
             m_LocalNbr->m_IfIndex = 4
            )"
            DiscoDeleteFields {
                  "m_Name",
                  "m_HaveAccess",
                  "m_LocalNbr->m_SubnetMask",
                  "m_RemoteNbr->m_RemoteNbrPhysAddr",
            }
      }
      DiscoReturnsFilter
      {
            "(
             m_LocalNbr->m_IfIndex = 5
            )"
      }
};
```

Ejemplo: Inhabilitación de la coincidencia parcial

Se podría agregar el siguiente ejemplo al archivo de definición IpForwardingTable.agnt para garantizar que si se descubre un direccionador con m_ObjectId='1.3.6.1.4.1.9.1.48' (es decir, un direccionador 7505 de Cisco), solo se intenta la coincidencia parcial cuando el direccionador ejecuta IOS versión 12.2 o posterior.

```
            DiscoRouterPartialMatchRestrictions
            (
                        "(m_ObjectId='1.3.6.1.4.1.9.1.48', m_OSVersion>='12.2',
                        m_MibVar='sysDescr')"
            );
```

Ejemplo: Inhabilitación de la coincidencia parcial mediante comodines

El siguiente ejemplo garantiza que se utiliza la coincidencia parcial en direccionadores 2600 de Cisco, en direccionadores 7505 de Cisco que ejecutan una revisión de IOS menor que 12.2 y direccionadores Redstone.

```
            DiscoRouterPartialMatchRestrictions
            (
                        "(m_ObjectId='1.3.6.1.4.1.9.1.209'),
                        (m_ObjectId='1.3.6.1.4.1.9.1.48', m_OSVersion>='12.2',
                         m_MibVar='sysDescr'),
                        (m_ObjectId like '1\.3\.6\.1\.4\.1\.2773\..*')"
            );
```

Archivo de configuración DiscoAgents.cfg

El archivo de configuración DiscoAgents.cfg define qué agentes se ejecutan durante un descubrimiento.

Tabla de base de datos utilizada

El archivo de configuración DiscoAgents.cfg se puede utilizar para configurar inserciones en la tabla de base de datos disco.agents.

Ejemplo: habilitación del agente de descubrimiento IpRoutingTable

El ejemplo siguiente activa el agente de descubrimiento IpRoutingTable.

```
insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
        'IpRoutingTable', 1, 0, 0, 2
    );
```

Ejemplo: habilitación de los agentes Details y Associated Address

Las siguientes inserciones OQL de ejemplo activan los agentes Details y Associated Address.

```
insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
        'Details', 1, 0, 0, 1
    );

insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
        'AssocAddress', 1, 0, 0, 2
    );
```

Ejemplo: habilitación del agente ARP cache

El agente ARP Cache ayuda en la resolución de direcciones MAC a IP durante el descubrimiento. Debe habilitar este agente para ejecutarlo durante un descubrimiento de capa 2. El ejemplo siguiente muestra cómo comprobar que el agente ARP Cache se ejecute durante un descubrimiento.

```
insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
)
values
(
```

```
        'ArpCache', 1, 0, 0, 2
);
```

Ejemplo: desactivar los agentes StandardSwitch y SuperStack3ComSwitch

El ejemplo siguiente desactiva los agentes de descubrimiento StandardSwitch y SuperStack3ComSwitch.

```
insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
        'StandardSwitch', 0, 1, 1, 3
    );

insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
        'SuperStack3ComSwitch', 0, 1, 1, 3
    );
```

Ejemplo: cambio del número de hebras utilizadas por el agente de descubrimiento IpRoutingTable

El siguiente ejemplo establece el número de hebras utilizadas por el agente de descubrimiento IpRoutingTable hasta 50. El aumento del número de hebras utilizadas por un agente permite al agente procesar más dispositivos de una vez, y puede acelerar el descubrimiento. Sin embargo, el aumento del número de hebras utilizadas por un agente también utiliza más memoria.

```
insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence, m_NumThreads
    )
values
(
        'IpRoutingTable', 1, 0, 0, 2, 50
    );
```

Ejemplo: cambio del número de hebras utilizadas por el agente de descubrimiento NMAPScan Perl

El siguiente ejemplo establece el número de hebras utilizadas por el agente de descubrimiento NMAPScan Perl hasta 50. Para definir el número de hebras utilizadas por un agente de descubrimiento Perl, debe habilitar en primer lugar varias hebras para dicho agente en el archivo de definición del agente de descubrimiento.

```
insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence, m_NumThreads
    )
values
(
        'NMAPScan', 1, 0, 0, 2, 50
    );
```

Archivo de configuración DiscoAgentReturns.filter

El archivo de configuración DiscoAgentReturns.filter le permite aplicar un filtro de datos de topología a datos devueltos por todos los agentes de descubrimiento.

Filtro de datos de topología devueltos por todos los agentes

El archivo de configuración $NCHOME/precision/disco/agents/DiscoAgentReturns.filter filtra los mismos datos de topología de todas las tablas de devoluciones del agente. La sintaxis utilizada en este archivo es la misma que la sintaxis utilizada en filtros de topología en los archivos de definición del agente de descubrimiento.

Ejemplo: filtrado de interfaces de módem por cable de suscriptor

El ejemplo siguiente filtra interfaces de módem por cable de suscriptor de datos de topología:

```
DiscoAgentReturnsFilterList
{
      DiscoReturnsFilter
      {
            "(
             m_LocalNbr->m_IfType = 229
            )"
      }
};
```

Archivo de configuración DiscoARPHelperSchema.cfg

El archivo de configuración DiscoARPHelperSchema.cfg realiza la resolución de la dirección IP a la dirección MAC.

Bases de datos utilizadas

El archivo de configuración DiscoARPHelperSchema.cfg define las inserciones en la tabla de la base de datos ARPHelper.configuration.

Ejemplo: Configuración del ayudante de ARP

La siguiente inserción de ejemplo configura el ayudante de ARP para utilizar una hebra.

```
insert into ARPHelper.configuration
(
       m_NumThreads
)
values
(
       1
);
```

Archivo de configuración DiscoCollectorFinderSeeds.cfg

El archivo de configuración `DiscoCollectorFinderSeeds.cfg` define cómo se adquieren datos de topología de los recopiladores del Sistema de gestión de elementos (EMS) durante el descubrimiento.

Bases de datos utilizadas

El archivo de configuración `DiscoCollectorFinderSeeds.cfg` define las inserciones en la base de datos collectorFinder.

Tenga en cuenta que existe otro archivo asociado con la base de datos collectorFinder, el archivo DiscoCollectorFinderSchema.cfg, pero no es necesario que altere este archivo.

Ejemplo: configuración de un único recopilador

El siguiente ejemplo agrega un único recopilador que se ejecuta en el servidor local. El ejemplo no especifica valores para otros campos, como m_DataSourceId y m_NumRetries y toman automáticamente los valores predeterminados de la tabla de configuración.

```
insert into collectorFinder.collectorRules
       ( m_Port)
values
       ( 8082 );
```

Archivo de configuración DiscoDBEntryFinderQueries.cfg

El archivo DiscoDBEntryFinderQueries.cfg se utiliza para especificar una consulta de base de datos que se ejecuta en una base de datos para recuperar una lista de direcciones IP de dispositivos para descubrir en la red.

Tablas de bases de datos utilizadas

Este archivo de configuración se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos:

- dbEntryFinder.configuration
- dbEntryFinder.dbQueries

Ejemplo: Configuración del buscador de base de datos para utilizar cinco hebras

La siguiente inserción de ejemplo configura el buscador de base de datos para utilizar cinco hebras.

```
insert into dbEntryFinder.configuration
   ( m_NumThreads )
values
   ( 5 );
```

Ejemplo: Configuración del buscador de base de datos para utilizar una base de datos externa de Tivoli Data Warehouse

La siguiente configuración de ejemplo indica al buscador de base de datos que recupere los datos de dispositivos de una base de datos Tivoli Data Warehouse externa.

```
insert into dbEntryFinder.dbQueries
(
            m_DbId, m_TriggerType, m_Query, m_Parameters, m_Mapping
)
values
(
            "TDW",
            1,
            "select DISTINCT MAC_Address , System_Name ,
                Network_Interface_Name , Interface_Status ,
                Device_Type , Interface_IP_Address
                from ABC_Network where Linux_OS_Config = ?",
            [ 'Redhat 6.5'  ],
            [
               {
                   FromDb = "eval(text,'&System_Name')",
                   ToFinder = 'm_Name'
               },
               {
                   FromDb = "eval(text,'&Interface_IP_Address')",
                   ToFinder = 'm_UniqueAddress'
               },
               {
                   FromDb = 23,
                   ToFinder = 'm_ExtraInfo->m_SourceId'
               },
               {
                   FromDb = "eval(text,'&Device_Type')",
                   ToFinder = 'm_ExtraInfo->m_DeviceType'
               }
            ]
);
```

La inserción anterior especifica que:

- La base de datos que aloja los detalles de dispositivos tiene el identificador de base de datos (dbId) de TDW en el archivo de configuración DbLogins.*DOMAIN*.cfg.
- El tipo de desencadenante is 1. Esto significa que esta consulta se invocará durante un descubrimiento completo.
- La consulta para ejecutar en la base de datos de TDW debe recuperar los datos siguientes para cada dispositivo:
  - Dirección MAC
  - Nombre de dispositivo
  - Nombre de interfaz de red

  - Estado de interfaz
  - Tipo de dispositivo
  - Dirección IP
- Utilizando el campo de parámetro opcional, especifique que el sistema operativo Linux es RedHat 6.5.
- Correlacione los datos de dispositivos que ha recuperado la consulta con los campos relevantes de la tabla `finders.returns`.

Archivo de configuración DiscoDNSHelperSchema.cfg

El archivo de configuración DiscoDNSHelperSchema.cfg define el acceso a DNS, lo que permite al descubrimiento realizar búsquedas de nombre de dominio, configurando el ayudante de DNS.

Tablas de bases de datos utilizadas

El archivo de configuración DiscoDNSHelperSchema.cfg se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos:

- DNSHelper.configuration
- DNShelper.methods

Ejemplo: configuración del ayudante de DNS

Las siguientes inserciones de ejemplo configuran el ayudante de DNS utilizando la información en la tabla de la base de datos de DNSHelper.configuration y en la tabla de la base de datos de DNShelper.methods. En este ejemplo, se muestran inserciones en la tabla de base de datos DNShelper.methods que corresponden a los siguientes tipos de método:

- 0 - Sistema
- 1 - DNS que utiliza `m_NameDomain` para especificar un sufijo de dominio para agregar a todos los nombres de dispositivos descubiertos.
- 1 - DNS que utiliza `m_NameDomainList` para especificar una lista de sufijos de dominio esperados.
- 2 - Archivo

```
insert into DNSHelper.configuration
(
     m_NumThreads, m_MethodList, m_TimeOut
)
values
(
     1, ['HostsFile'] , 5
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType
)
values
(
     "HostService", 0
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType, m_NameServerAddr, m_TimeOut, m_NameDomain
)
values
(
     "abcIPv6DNS", 1, "2222:15f8:106:203:250:4ff:fee8:6d75", 3,
"tivlab.raleigh.ibm.com"
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType, m_TimeOut, m_NameServerAddr, m_NameDomainList
)
values
(
     "defIPv6DNS", 1, 3, "2222:15f8:106:203:250:4ff:fee8:6d75",
```

```
     ['uk.eu.org',
     'fra.eu.org',
     'de.eu.org',
     'it.eu.org',
     'sp.eu.org']
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType, m_FileName, m_FileOrder
)
values
(
     'HostsFile', 2, 'etc/hosts', 1
);
```

Archivo de configuración DiscoFileFinderParseRules.cfg

El archivo DiscoFileFinderParseRules.cfg se puede utilizar para especificar los archivos que se van a analizar para obtener una lista de direcciones IP de dispositivos que existen en la red.

Tablas de bases de datos utilizadas

Este archivo de configuración se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos:

- fileFinder.parseRules
- fileFinder.configuration

Tenga en cuenta que existe otro archivo de configuración asociado con la base de datos fileFinder, el archivo DiscoFileFinderSchema.cfg, pero no es necesario que altere este archivo.

Ejemplo: configuración del buscador de archivos para utilizar cinco hebras

La siguiente inserción de ejemplo configura el buscador de archivos para utilizar cinco hebras.

```
insert into fileFinder.configuration
   ( m_NumThreads )
values
   ( 5 );
```

Ejemplo: configuración del buscador de archivos para analizar /var/tmp/logged_hosts

La siguiente configuración de ejemplo le indica al buscador de archivos que analice un archivo de texto de ejemplo, logged_hosts, que se ha guardado en el directorio /var/tmp. El contenido del archivo de ejemplo se muestra a continuación.

```
vi /var/tmp/logged_hosts

172.16.1.21   dharma              04:02:08
172.16.1.201  phoenix             19:07:08
172.16.1.25   lnd-sun-tivoli   15:10:00
172.16.2.33   ranger              19:07:07
~
"/var/tmp/logged_hosts" [Read only] 4 lines, 190 characters
```

Las tres columnas de este archivo de ejemplo contienen una dirección IP, el nombre del dispositivo y un valor de hora, respectivamente. Las columnas están separadas por espacios en blanco, que pueden ser varios separadores, espacios o una combinación de los dos. Puede configurar el buscador de archivos para analizar este archivo de texto de ejemplo utilizando una inserción similar a la del ejemplo.

```
insert into fileFinder.parseRules
(
            m_FileName, m_Delimiter, m_ColDefs
)
values
(
        "/var/tmp/logged_hosts",
        "[     ]+",
```

```
        [
            {
                m_VarName="m_UniqueAddress",
                m_ColNum=1
            },
            {
                m_VarName="m_Name",
                m_ColNum=2
            }
        ]
);
```

La inserción anterior especifica que:

- La vía de acceso completa y nombre del archivo es /var/tmp/logged_hosts.
- El delimitador del archivo origen es el espacio en blanco. El delimitador de columna está indicado en la inserción utilizando una expresión regular simple, [*tabulación espacio*]+ . Debe pulsar las teclas **tabulación** y **espacio** en vez de escribir \t para representar el carácter de tabulador.
- La primera columna contiene direcciones IP y se debe correlacionar con la columna m_UniqueAddress de la tabla finders.returns.
- La segunda columna contiene nombres de host y se debe correlacionar con la columna m_Name de la tabla finders.returns.

Ya que la tercera columna en el archivo de texto de ejemplo no es relevante, no se ha correlacionado con una columna de finders.returns y el buscador de archivos la ignora durante el descubrimiento.

Ejemplo: configuración del buscador de archivos para analizar el archivo /etc/hosts

La siguiente inserción indica al buscador de archivos que:

- Analice /etc/hosts.
- Considere al espacio en blanco como el separador de datos.
- Utilice las siguientes definiciones de columna:
  - m_UniqueAddress para la primera columna
  - m_Name para la segunda columna

```
insert into fileFinder.parseRules
(
            m_FileName,
            m_Delimiter,
            m_ColDefs
)
values
(
            "/etc/hosts",
            "[     ]",
            [
                {
                    m_VarName="m_UniqueAddress",
                    m_ColNum=1
                },
                {
                    m_VarName="m_Name",
                    m_ColNum=2
                }
            ]
);
```

Ejemplo: configuración del buscador de archivos para analizar /etc/defaultrouter

La siguiente inserción indica al buscador de archivos que:

- Analice /etc/defaultrouter.
- Considere una o más apariciones de espacios en blanco como separadores de datos.

- Utilice m_UniqueAddress como la definición de columna.

```
insert into fileFinder.parseRules
(
            m_FileName,
            m_Delimiter,
            m_ColDefs
)
values
(
            "/etc/defaultrouter",
            "[     ]+",
            [
                {
                    m_VarName="m_UniqueAddress",
                    m_ColNum=1
                }
            ]
);
```

Archivo de configuración DiscoHelperServerSchema.cfg

El archivo de configuración `DiscoHelperServerSchema.cfg` define el contenido de las diferentes bases de datos del ayudante.

Tablas de bases de datos utilizadas

Este archivo de configuración se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos.

Tablas de la base de datos del ayudante de ARP:

- ARPHelper.ARPHelperTable
- ARPHelper.ARPHelperConfig

Tablas de la base de datos del ayudante de DNS:

- DNSHelper.DNSHelperTable
- DNSHelper.DNSHelperConfig

Tablas de la base de datos del ayudante de Ping:

- PingHelper.PingHelperTable
- PingHelper.PingHelperConfig

Tablas de la base de datos del ayudante de SNMP:

- SnmpHelper.SnmpHelperTable
- SnmpHelper.SnmpHelperConfig

Tablas de la base de datos del ayudante de Telnet:

- TelnetHelper.TelnetHelperTable
- TelnetHelper.TelnetHelperConfig

Tablas de la base de datos del ayudante de XMLRPC:

- XmlRpcHelper.XmlRpcHelperTable
- XmlRpcHelper.XmlRpcHelperConfig

Archivo de configuración DiscoPingFinderSeeds.cfg

El archivo de configuración DiscoPingFinderSeeds.cfg se utiliza para agregar fuentes al buscador de pings y restringir la detección de dispositivos.

Tablas de bases de datos utilizadas

El archivo de configuración DiscoPingFinderSeeds.cfg se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos:

- pingFinder.pingRules
- pingFinder.scope

Tenga en cuenta que existe otro archivo de configuración asociado con la base de datos pingFinder, el archivo DiscoPingFinderSchema.cfg, pero no es necesario que altere este archivo.

Nota: Si está agregando fuentes a un descubrimiento IPv6 tenga en cuenta que, potencialmente, hay miles de millones de dispositivos en los que se puede hacer ping dentro de una única subred de IPv6. Para comprobar que el descubrimiento se completa, debe especificar una máscara de red lo suficientemente grande si especifica una subred IPv6 como una fuente de pings.

Ejemplo: agregar fuentes a un buscador de pings con un única dirección de dispositivo

La siguiente inserción de ejemplo define una única fuente con una dirección IP de 10.10.2.224. Este ejemplo no especifica valores para m_NumRetries y m_TimeOut porque toman automáticamente los valores predeterminados de la tabla de configuración.

Restricción: Network Manager no soporta el formato IPv4–mapped IPv6 y espera que todas las direcciones IPv6 estén en un formato IPv6 estándar separado por dos puntos. Por ejemplo, Network Manager no soporta una dirección IPv6 correlacionada con IPv4 como `::ffff:192.0.2.128`. En su lugar, especifique esta dirección como `::ffff:c000:280` (formato IPv6 estándar separado por dos puntos).

```
insert into pingFinder.pingRules
        ( m_Address, m_RequestType )
values
        ( "10.10.2.224", 1 );
```

Ejemplo: agregar fuentes a un buscador de pings con una dirección de subred de clase B

La siguiente inserción de ejemplo define una única subred de clase B como fuente.

```
insert into pingFinder.pingRules
        ( m_Address, m_RequestType, m_NetMask )
values
        ( "10.10.0.0", 2, "255.255.0.0" );
```

Ejemplo: agregar el buscador de pings con direcciones de subred de clase C

La siguiente inserción de ejemplo define dos subredes de clase 2 como fuentes.

```
insert into pingFinder.pingRules
        ( m_Address, m_RequestType, m_NetMask )
values
        ( "10.10.2.0", 2, "255.255.255.0" );

insert into pingFinder.pingRules
        ( m_Address, m_RequestType, m_NetMask )
values
        ( "10.10.47.0", 2, "255.255.255.0" );
```

Ejemplo: restricción de la detección de dispositivos

La siguiente inserción de ejemplo configura el buscador de pings para utilizar la tabla scope.zones y el ámbito del descubrimiento.

```
insert into pingFinder.scope
        ( m_UseScope, m_UsePingEntries )
values
        ( 1, 1 );
```

Importante: No son recomendables otras combinaciones de los filtros m_UseScope y m_UsePingEntries. Especificar valores (0,0) da como resultado un descubrimiento ilimitado, mientras que especificar valores (0,1) da como resultado dispositivos que no desea descubrir y con los que se hace ping innecesariamente.

Archivo de configuración DiscoPingHelperSchema.cfg

El archivo de configuración DiscoPingHelperSchema.cfg define cómo se tiene que hacer ping en los dispositivos.

Tabla de base de datos utilizada

El archivo de configuración DiscoPingHelperSchema.cfg se puede utilizar para configurar inserciones en la tabla de la base de datos pingHelper.configuration.

En esta configuración de ejemplo del archivo de configuración DiscoPingHelperSchema.cfg, los parámetros especifican:

- Utilizar 20 hebras de ejecución de procesos.
- Esperar un máximo de 250 ms para una respuesta de un dispositivo.
- Reintentar en los dispositivos que no responden un máximo de cinco veces.
- Esperar 50 ms entre dispositivos que hacen ping en una subred.
- No utilizar el ping de difusión o de multidifusión.

```
insert into pingHelper.configuration
(
        m_NumThreads,
        m_TimeOut,
        m_NumRetries,
        m_InterPingTime,
        m_Broadcast,
        m_Multicast
)
values
(
        20, 250, 5, 50, 0, 0
);
```

Archivo de configuración DiscoConfig.cfg

El archivo de configuración DiscoConfig.cfg se utiliza para que el buscador de pings compruebe de forma automática los dispositivos que el buscador de pings ha descubierto y para habilitar un descubrimiento sensible al contexto.

Tabla de base de datos utilizada

El archivo de configuración DiscoConfig.cfg se puede utilizar para configurar inserciones en las siguientes tablas:

- disco.config
- disco.managedProcesses
- disco.NATStatus
- translations.NATAddressSpaceIds
- disco.ipCustomTags
- disco.filterCustomTags
- translations.collectorInfo
- failover.restartPhaseAction
- failover.config
- failover.doNotCache

Los siguientes ejemplos muestran inserciones en la tabla de la base de datos disco.config.

Ejemplo: hacer ping en dispositivos del buscador de archivos

El siguiente mandato de ejemplo configura el descubrimiento para que el buscador de pings compruebe de forma automática los dispositivos que el buscador de archivos ha descubierto.

```
update disco.config set m_CheckFileFinderReturns = 1;
```

Ejemplo: habilitación de un descubrimiento sensible al contexto

Atención: La habilitación de un descubrimiento sensible al contexto habilita automáticamente todos los agentes de contexto. La inhabilitación de un descubrimiento sensible al contexto inhabilita automáticamente todos los agentes de contexto. No habilite o inhabilite manualmente agentes de contexto, utilizando los archivos de configuración o mediante la GUI Configuración de descubrimiento.

Para habilitar el descubrimiento sensible al contexto, agregue la siguiente inserción al archivo `DiscoConfig.cfg`:

```
insert into disco.config
(
      m_UseContext
)
values
(
      1
)
```

La inserción del valor `0` inhabilita el descubrimiento sensible al contexto.

Enriquecimiento de la topología mediante etiquetas personalizadas

Puede utilizar las tablas disco.ipCustomTags y disco.filterCustomTags para enriquecer la topología descubierta asociando una o varias etiquetas de pares de nombre-valor con entidades descubiertas.

Archivo de configuración DiscoScope.cfg

El archivo de configuración DiscoScope.cfg se puede utilizar para configurar el ámbito del descubrimiento.

Tablas de bases de datos utilizadas

Este archivo de configuración se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos:

- scope.zones
- scope.detectionFilter
- scope.instantiateFilter
- scope.multicastGroup
- scope.multicastSource
- scope.special

Restricción: La tabla scope.zones sólo se puede utilizar para configurar el ámbito de entidades basadas en IP. El ámbito de las entidades no IP, como los dispositivos ópticos de capa 1, debe determinarse utilizando la tabla scope.detectionFilter.

Ejemplo: definición de una zona de inclusión

La siguiente inserción de ejemplo define la subred 10.10.2.* como zona de inclusión.

Restricción: Network Manager no soporta el formato IPv4–mapped IPv6 y espera que todas las direcciones IPv6 estén en un formato IPv6 estándar separado por dos puntos. Por ejemplo, Network

Manager no soporta una dirección IPv6 correlacionada con IPv4 como ::ffff:192.0.2.128. En su lugar, especifique esta dirección como ::ffff:c000:280 (formato IPv6 estándar separado por dos puntos).

```
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        1,
        [
            {
                m_Subnet="10.10.2.*"
            }
        ]
);
```

Ejemplo: definición de varias zonas de inclusión

El siguiente ejemplo define tres zonas de inclusión de IP diferentes y cada una utiliza una sintaxis diferente para definir la máscara de subred. Se descubren los siguientes dispositivos:

- Cualquier dispositivo dentro de la subred 172.16.1.0 (con una máscara de subred de 24, es decir, 24 bits activados y 8 bits desactivados, lo que implica una máscara de red de 255.255.255.0).
- Cualquier dispositivo dentro de la subred 172.16.2.0 con una máscara de 255.255.255.0.
- Cualquier dispositivo dentro de la subred 172.16.3.0 con una máscara de 255.255.255.0.

```
insert into scope.zones
(
    m_Protocol,
    m_Action,
    m_Zones
)
values
(
        1,
        1,
        [
              {
                    m_Subnet="172.16.1.0",
                    m_NetMask=24
              },
              {
                    m_Subnet="172.16.2.*"
              },
              {
                    m_Subnet="172.16.3.0",
                    m_NetMask="255.255.255.0"
              }
        ]
);
```

Ejemplo: definición de una zona de exclusión

La siguiente inserción de ejemplo define una única zona de exclusión para el protocolo de IP y asocia la zona con una subred.

```
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        2,
        [
            {
                m_Subnet="172.16.1.0",
                m_NetMask=24
```

```
        ]
);
```

Ejemplo: definición de una zona de inclusión dentro de un dominio NAT

El siguiente ejemplo define una zona de inclusión. La zona de inclusión incluye los dispositivos con una dirección IP que empieza por 172.16.2 que también pertenece al espacio de direcciones de NAT NATDomain1. El protocolo se define en 1, es decir, la IP.

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="172.16.2.*",
            }
        ],
        "NATDomain1"
);
```

Ejemplo: restricción de interrogación de dispositivos basada en dirección IP

El siguiente ejemplo muestra cómo impedir una mayor interrogación de dispositivos que coinciden con una dirección IP determinada. Solo se interroga en mayor medida a aquellos dispositivos que no tienen la dirección IP 10.10.63.234. Dentro de la tabla scope.detectionFilter, especifique:

- Las condiciones de filtro. Solo a los dispositivos que pasen este filtro, es decir, a los que el filtro evalúa como true, se interrogan en mayor medida. Si no se especifica ningún filtro, se pasan todos los dispositivos por el filtro de detección.

```
insert into scope.detectionFilter
(
        m_Filter
)
values
(
        "( ( m_UniqueAddress <> '10.10.63.234' ) )"
);
```

Un agrupador prueba cada dispositivo que se ha descubierto contra la condición de filtro en la tabla scope.detectionFilter y el resultado de esta prueba determina si se ha descubierto el dispositivo.

Ya que el flujo de proceso del descubrimiento es completamente configurable, puede configurar este agrupador para actuar en cualquier momento durante el proceso de descubrimiento. De forma predeterminada, el agrupador realiza la prueba de condición en los detalles del dispositivo que devuelve el agente Detalles. Por lo tanto, el filtro debe estar basado en las columnas de la tabla Details.returns.

Aunque puede configurar la condición de filtro para probar cualquiera de las columnas en la tabla Details.returns, será necesario que utilicé la dirección IP como base para el filtro para restringir la detección de un dispositivo en particular. Si el dispositivo no otorga acceso SNMP al agente detalles, el agente Detalles no podrá recuperar las variables MIB, como el ID de objeto. Sin embargo, se le garantiza al menos la devolución de la dirección IP cuando se detecta el dispositivo.

Los siguientes ejemplos muestran cómo puede configurar de otra manera el filtro de detección.

Ejemplo: restricción de interrogación basada en ID de objeto

El siguiente ejemplo muestra cómo impedir una mayor interrogación de dispositivos que coinciden con un ID de objeto determinado. La cláusula `not like` de OQL indica que solo se interroga en mayor medida a los dispositivos que pasen el filtro (es decir, los dispositivos para los que el OID *no* es como 1.3.6.1.4.1.*).

Se debe utilizar la barra inclinada invertida en la inserción para evitar el `.`, que por otro lado se considera un comodín. Se puede encontrar una explicación completa de la sintaxis de OQL en *Referencia de IBM Tivoli Network Manager*.

```
insert into scope.detectionFilter
(
        m_Filter
)
values
(
        "(
                ( m_ObjectId not like '1\.3\.6\.1\.4\.1\..*' )
        )"
);
```

Ejemplo: combinación de varias restricciones de filtro

Puede combinar condiciones de filtro dentro de una única inserción de OQL. El siguiente ejemplo asegura que solo se detectan los dispositivos que no tienen el OID especificado ni la dirección IP especificada:

```
insert into scope.detectionFilter
(
        m_Filter
)
values
(
        "(
                ( m_ObjectId not like '1\.3\.6\.1\.4\.1\..*' )
                AND
                ( m_UniqueAddress <> '10.10.63.234' )
        )"
);
```

Restricción de la instanciación: limitación al filtrar interfaces

Tenga en cuenta las siguientes limitaciones al restringir la instanciación de interfaces.

Restricción: Para asegurarse de que no se generen alertas para las *interfaces* excluidas por el filtro de instanciación, debe configurar la variable `RaiseAlertsForUnknownInterfaces`. Para ello, lleve a cabo los siguientes pasos:

1. Edite el archivo de configuración `$NCHOME/etc/precision/NcPollerSchema.cfg`.
2. Añada la siguiente línea al archivo:

```
update config.properties set RaiseAlertsForUnknownInterfaces = 0;
```

Ejemplo: restricción de instanciación basada en el nombre de entidad

Para restringir los dispositivos que están instanciados, agregue una inserción de OQL en la tabla scope.instantiateFilter. La tabla instantiateFilter requiere de una prueba condicional. Solo se envían a ncp_model los dispositivos que pasen el filtro. Si no hay filtro definido, todos los dispositivos descubiertos se pasan a ncp_model.

La prueba condicional debe estar basada en el formato de datos ncimCache.

El filtro de postdescubrimiento del ejemplo siguiente restringe la creación de instancias de un chasis y su contenido.

```
insert into scope.instantiateFilter
(
    m_Filter
)
values
(
    "
    (
        BASENAME != 'jane'
```

```
    )
    "
);
```

El filtro de postdescubrimiento del ejemplo siguiente restringe la creación de instancias de un chasis y su contenido.

```
insert into scope.instantiateFilter
(
    m_Filter
)
values
(
    "
    (
        snmpSystem->SYSDESCR NOT LIKE ' device'
    )
    "
);
```

Utilización de scope.special para restringir la detección de dispositivos

Cree entradas en la tabla scope.special para las interfaces de red a las que se pueda acceder mediante varias direcciones IP. Las entradas de la tabla scope.special controlan qué direcciones IP utiliza Network Manager para supervisar los dispositivos para las políticas de sondeo SNMP y NCMP.

El ejemplo siguiente muestra una sentencia INSERT en la tabla scope.special. Define la dirección IP 192.168.1.3 como una interfaz de gestión potencial para chasis e interfaces. Proporciona información de cliente adicional que se añade a la sección ExtraInfo de la entidad en la tabla de base de datos master.entityByName del modelo si se descubre la dirección IP.

```
insert into scope.special
(
        m_Zones,
        m_Identifier,
        m_Priority,
        m_NonPingable,
        m_AdminInterface,
        m_ExtraInfo,
        m_Protocol,
        m_IsManagement,
        m_OutOfBand,
        m_IsValidVirtual
)
values
(
        [
                {
                        m_Subnet="192.168.1.3",
                        m_NetMask=32
                }
        ],
        "CustomerFacing",
        99,
        0,
        1,
        {
                m_CustomerName = 'MyCompany',
                m_CustomerType = 'Internal'
        },
        1,
        0,
        1,
        0
);
```

Para un dispositivo que tiene 2 direcciones IP, 172.20.1.1 y 192.168.1.3, la configuración implica que 172.20.1.1 no se elige como dirección IP a través de la cual se va a gestionar el dispositivo. En su lugar, se utiliza 192.168.1.3. El ejemplo siguiente muestra el aspecto de la entrada de topología final de

master.entityByName en esta instancia. Los datos de ExtraInfo que tienen como prefijo m_ScopeSpecial vienen de la entrada scope.zones coincidente con la dirección IP 192.168.1.3.

```
{
        EntityName='192.168.1.3';
        Address=['','','192.168.1.3'];
        EntityType=1;
        EntityOID='1.3.6.1.4.1.8072.3.2.10';
        IsActive=1;
        Status=1;
        ExtraInfo={
                m_SysName='SYS1';
                m_DNSName='DNS1';
                m_time=1362486845;
                m_DisplayLabel='DNS1';
                m_AssocAddress=
[{m_IfIndex = 1, m_IpAddress = '172.20.1.1', m_Protocol = 1, m_IfOperStatus = 1 },
{m_IfIndex = 2, m_IpAddress = '192.168.1.3', m_Protocol = 1, m_IfOperStatus = 1 }];
                m_ScopeSpecialIsManagement=1;
                m_ScopeSpecialPriority=99;
                m_ScopeSpecialIdentifier='CustomerFacing';
                m_ScopeSpecialExtraInfo={
                          m_CustomerName = 'MyCompany',
                    m_CustomerType = 'Internal'
                    };
                m_DefinedMgmtIP=1;
                m_IsOutOfBand=1;
                m_BaseName='192.168.1.3';
                m_AddressSpace=NULL;
                m_AccessProtocol=1;
                m_AccessAddress='192.168.1.3';
                };
        LingerTime=3;
        ActionType=0;
        CreateTime=1362486848;
        ChangeTime=1362486848;
        ClassName='NetworkDevice';
        ClassId=5;
        ObjectId=2272;
}
```

Configuración del ámbito para dispositivos no IP
Para configurar el ámbito para dispositivos no IP, configure inserciones en la tabla de base de datos scope.detectionFilter dentro del archivo de configuración DiscoScope.cfg.

Nota: El filtro de detección se ejecuta en los datos devueltos por los agentes, en las tablas `Details.returns` y `CollectorDetails.returns`, por lo que la definición del ámbito de los dispositivos de esta forma tiene un impacto mínimo en los dispositivos de destino.

Ejemplo: pasar sólo dispositivos no IP para el descubrimiento

La siguiente inserción de ejemplo garantiza que sólo se pasan al descubrimiento los dispositivos no IP, para su interrogación posterior. Este filtro excluiría todos los dispositivos basados en IP.

```
insert into scope.detectionFilter
(
        m_Filter,
 )
values
(
       "( m_Protocol = 4 )"
 );
```

Ejemplo: combinación de varias restricciones de filtro para los dispositivos no IP

La siguiente inserción garantiza que solo se pasan al descubrimiento los dispositivos no IP y que los que se pasan no pueden incluir la cadena especificada en su clave de Sistema de gestión de elementos(EMS).

```
insert into scope.detectionFilter
(
        m_Filter,
 )
```

```
values
(
       "(
            ( m_Protocol = 4 )"
             AND
            ( m_UniqueAddress NOT LIKE 'LONDON' )"
       )"
 );
```

Dispositivos con interfaces fuera del ámbito
Una red puede contener dispositivos que estén dentro del ámbito de descubrimiento pero contener interfaces que estén fuera del ámbito. Debido a que el dispositivo está dentro del ámbito, el comportamiento predeterminado de los agentes de descubrimiento de capa 3 es descargar la tabla de interfaces del dispositivo y descubrir todas las interfaces de un dispositivo, incluso si las propias interfaces están fuera del ámbito.

Si esta situación se aplica a la red y desea modificar la forma en que el proceso de descubrimiento gestionará los dispositivos que se encuentran parcialmente dentro del ámbito, existen varias formas de modificar el descubrimiento y supervisar el proceso para excluir estas interfaces del descubrimiento.

Un posible ajuste de configuración es modificar la inserción en scope.instantiateFilter para que no se creen instancias de interfaces fuera de ámbito. Esta solución significa que las interfaces fuera de ámbito se seguirán descubriendo, pero no se pasarán a MODEL para crear una instancia en una clase de objeto activo (AOC); por lo tanto, las interfaces fuera de ámbito no se representan en la topología ni se supervisan.

También puede configurar un filtro de instancia de SNMP para impedir la descarga de datos SNMP para determinadas interfaces.

También puede filtrar los datos devueltos por los agentes de descubrimiento mediante el archivo de configuración DiscoAgentReturns.filter.

Archivo de configuración DiscoSnmpHelperFilters.cfg

El archivo de configuración DiscoSnmpHelperFilters.cfg define filtros de interfaz SNMP para el ayudante de SNMP. Los filtros de interfaz SNMP definen las interfaces para las que desea que el ayudante de SNMP recupere información.

Tabla de base de datos utilizada

El archivo de configuración DiscoSnmpHelperFilters.cfg se puede utilizar para configurar inserciones en la tabla de la base de datos snmpHelper.instanceFilter.

Ejemplo de filtro de interfaz simple

El ejemplo siguiente recupera información para interfaces con un nombre similar a "Gi0" en un tipo de dispositivo concreto.

```
insert into snmpHelper.instanceFilter
(
    m_FilterName,
    m_DeviceFilter,
    m_InstanceFilter
)
values
(
    "TESTFILTER",
    "sysObjectID = '1.3.6.1.4.1.4874.1.1.1.1.3' OR sysDescr LIKE 'ERX-1440'",
    "ifName like 'Gi0'"
);
```

Archivo de configuración DiscoSnmpHelperSchema.cfg

El archivo de configuración DiscoSnmpHelperSchema.cfg define la operación del ayudante de SNMP, que especifica las reglas generales de la recuperación de información de SNMP.

Tabla de base de datos utilizada

El archivo de configuración DiscoSnmpHelperSchema.cfg se puede utilizar para configurar inserciones en la tabla de la base de datos snmpHelper.configuration.

Ejemplo: Configuración de tiempos de espera y hebras

La siguiente configuración de ejemplo hace que el ayudante de SNMP se comporte de la siguiente manera:

- Se han iniciado 120 hebras de ejecución de programa para procesar solicitudes entrantes de datos de SNMP desde el servidor de ayudantes. El ayudante de SNMP procesa un máximo de 120 solicitudes simultáneamente.
- Se especifica un tiempo de espera de tres segundos para que un dispositivo responda a una consulta de SNMP que ha emitido el ayudante de SNMP. Si el dispositivo no ha respondido después de ese intervalo de tiempo, el ayudante emite la solicitud de nuevo, una vez.

```
insert into snmpHelper.configuration
(
        m_NumThreads,
        m_TimeOut,
        m_NumRetries,
)
values
(
    120, 3000, 1
);
```

Archivo de configuración DiscoTelnetHelperSchema.cfg

El archivo de configuración DiscoTelnetHelperSchema.cfg define la operación del ayudante de Telnet, que devuelve los resultados de una operación de Telnet a un dispositivo especificado.

Tablas de bases de datos utilizadas

El archivo de configuración DiscoTelnetHelperSchema.cfg se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos:

- telnetHelper.configuration
- telnetHelper.deviceConfig

Puede configurar el Ayudante de Telnet para utilizar el programa Secure Shell (SSH). SSH habilita la autenticación y proporciona comunicaciones más seguras por la red.

Ejemplo: configuración del ayudante de Telnet

Se puede agregar la siguiente inserción al archivo de configuración DiscoTelnetHelperSchema.cfg para configurar la operación del ayudante de Telnet. La inserción configura el ayudante de Telnet para:

- Utilizar 20 hebras de ejecución de procesos
- Esperar un máximo de 5000 ms por la respuesta de un dispositivo
- Poner a prueba la respuesta hasta tres veces

```
insert into telnetHelper.configuration
(
          m_NumThreads,
          m_TimeOut,
          m_Retries
)
values
(
          20,
          5000,
          3
);
```

Configuración de valores específicos de dispositivo

El ayudante de Telnet también acepta varias inserciones en la tabla telnetHelper.deviceConfig dentro del archivo de configuración DiscoTelnetHelperSchema.cfg que define la interacción de la operación de Telnet.

Los siguientes ejemplos muestran cómo configurar valores específicos de dispositivo de Telnet. Puede configurar valores de dispositivo basados en la variable MIB sysObjectID o basados en una IP o subred. La manera más efectiva de definir estas opciones está basada en la variable de MIB sysObjectID. Esta variable identifica al proveedor del dispositivo. Las opciones de configuración específicas de dispositivo suelen variar con el proveedor del dispositivo. Puede configurar valores para todos los dispositivos de Cisco, por ejemplo, independientemente de donde se encuentren esos dispositivos en la red.

Ejemplo: configuración de los valores para dispositivos de un proveedor específico

La siguiente configuración típica muestra cómo configurar valores para todos los dispositivos de un proveedor específico. La inserción especifica:

- 1.3.6.1.4.1.9.1. como la variable MIB sysObjectID para que coincida con esta entrada de configuración. Todos los dispositivos con ID de objeto de formato 1.3.6.1.4.1.9.1.* son coincidentes. En general, estos son dispositivos IOS de Cisco, aunque hay excepciones.
- terminal length es el mandato que define la longitud de página de salida para los dispositivos de Cisco.

  Nota: Este mandato varía con dispositivos de diferentes tipos de proveedor.
- Sin transferencia de páginas
- Solicitud desde dispositivo remoto
- La respuesta que se va a enviar al dispositivo remoto para continuar con la salida paginada.

```
insert into telnetHelper.deviceConfig
(
          m_SysObjectId,
          m_PageLengthCmd,
          m_PageLength,
          m_ContinueMsg,
          m_ContinueCmd
)
values
(
          "1.3.6.1.4.1.9.1.", "terminal length", 0, ".*[Mm]ore.*", " "
);
```

El archivo de configuración DiscoTelnetHelperSchema.cfg contiene inserciones con valores de configuración específicos de dispositivo para los siguientes tipos de proveedor:

- Dispositivos IOS de Cisco
- Dispositivos Cat OS de Cisco
- Dispositivos JUNOS de Juniper
- Dispositivos ERX de Juniper
- Dispositivos Huawei
- Dispositivos Dasan

Ejemplo: configuración de valores de respuesta de dispositivo basados en dirección IP

Si la salida del mandato de telnet pasa de una página, el dispositivo envía un mensaje preguntando si mostrar la siguiente página. Configure los mensajes que se esperan y las respuestas que dará el ayudante de Telnet en el archivo de configuración DiscoTelnetHelperSchema.cfg.

Los mandatos que empiezan por m_Continue (como m_ContinueMsg) y m_PageLength (comom_PageLengthCmd) se excluyen mutuamente: debe utilizar o uno u otro. Si estos valores no están configurados correctamente para estos dispositivos, los datos se pueden perder.

El siguiente ejemplo muestra cómo configurar los valores para los dispositivos basados en dirección IP. La inserción especifica:

- 192.168.112.0 como la dirección IP
- La solicitud del dispositivo remoto es una expresión regular que contiene "wish to continue"
- La respuesta que se envía al dispositivo remoto para continuar con la salida paginada es "y"

```
insert into telnetHelper.deviceConfig
(
          m_IpOrSubNet,
          m_NetMaskBits,
          m_Protocol,
          m_ContinueMsg,
          m_ContinueCmd
)
values
(
          192.168.112.0,
          24,
          1,
          ".*wish to continue.*",
          "y"
);
```

Archivo de configuración DiscoXmlRpcHelperSchema.cfg

El archivo de configuración DiscoXmlRpcHelperSchema.cfg se puede utilizar para configurar el ayudante XML-RPC, que permite a Network Manager comunicarse con recopiladores EMS mediante la interfaz XML-RPC.

Tabla de base de datos utilizada

El archivo de configuración DiscoXmlRpcHelperSchema.cfg se puede utilizar para configurar inserciones en la tabla de la base de datos xmlRpcHelper.configuration.

Esta inserción de ejemplo configura el ayudante XML-RPC para:

- Utilizar un subproceso de ejecución del proceso.
- Permitir un tamaño máximo de 1048576 bytes para una respuesta XML-RPC.

```
insert into xmlRpcHelper.configuration
(
    m_NumThreads,
    m_MaxResponseSize
)
values
(
    1, 1048576
);
```

Nota: Es posible que el tamaño máximo predeterminado de la respuesta sea demasiado pequeño al ejecutar un descubrimiento basado en recopiladores en los recopiladores que dan como resultado respuestas largas. En estos casos, aumente el tamaño de respuesta máximo. Para aumentar el tamaño de respuesta máximo, establezca el parámetro **m_MaxResponseSize** en un nivel más alto. Asegúrese de que establece el mismo valor para **m_MaxResponseSize** en los archivos siguientes:

- NCHOME/etc/precision/DiscoCollectorFinderSchema.cfg
- NCHOME/etc/precision/DiscoXmlRpcHelperSchema.cfg

Archivo de configuración SnmpStackSecurityInfo.cfg

El archivo de configuración SnmpStackSecurityInfo.cfg define las cadenas de comunidad, el mantenimiento de versiones y otras propiedades que utilizan los procedimientos que necesitan interrogar a dispositivos utilizando SNMP, por ejemplo, el ayudante de SNMP. Se pueden configurar las cadenas de comunidad mediante dispositivo o subred, para permitir que el ayudante SNMP recupere las variables MIB de los dispositivos.

Tablas de bases de datos utilizadas

Este archivo de configuración se puede utilizar para configurar inserciones en las siguientes tablas de bases de datos:

- snmpStack.configuration
- snmpStack.verSecurityTable
- snmpStack.accessParameters

Tenga en cuenta que existe otro archivo de configuración asociado con la base de datos snmpStack, el archivo SnmpStackSchema.cfg, pero no es necesario que altere este archivo.

Ejemplo: Configuración de versiones de SNMP

Si está activado el mantenimiento de versiones automático, el siguiente ajuste de configuración especifica que se utiliza una cadena de comunidad de 'public' para dispositivos que soportan la versión 1 de SNMP y se utiliza una configuración específica para los dispositivos que soportan la versión 3 de SNMP. Ya que no se ha especificado ningún valor para m_SnmpPort, este valor se establece como predeterminado en el puerto 161 estándar de SNMP.

```
insert into snmpStack.verSecurityTable
(
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName,
)
values
(
        0,
        'public',
        2,
        {
            m_AuthPswd="authpassword",
            m_PrivPswd="privpassword"
        },
        'authPriv'
);
```

Ejemplo: Definición de cadenas de comunidad

Las siguientes inserciones definen las cadenas de comunidad public y crims0n que se utilizan para acceder a los dispositivos de SNMP.

Puede agregar tantas inserciones como contraseñas hay para el archivo de configuración SnmpStackSecurityInfo.cfg. Se prueban todas las contraseñas y configuraciones de subred hasta que se encuentra una coincidencia.

Nota: Solo una cadena de comunidad de SNMP, la cadena de comunidad public, está configurada de forma predeterminada.

```
insert into snmpStack.verSecurityTable
(
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName
)
values
(
        0,
        'public',
        2,
        {
            m_AuthPswd="authpassword",
            m_PrivPswd="privpassword"
        },
        'authPriv'
```

```
);

insert into snmpStack.verSecurityTable
(        m_IpOrSubNetVer,
        m_NetMaskBitsVer,
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName
)
values
(
        "10.10.2.0",
        24,
        0,
        'crims0n',
        2,
        {
            m_AuthPswd="authpassword",
            m_PrivPswd="privpassword"
        },
        'authPriv'
);
```

Ejemplo: Especificar un puerto SNMP

Este ejemplo configura los mismos valores SNMP que en el ejemplo anterior en todos los dispositivos dentro de la subred 192.168.64.0 y especifica el puerto SNMP como 6161 en todos los dispositivos dentro de esta subred.

```
insert into snmpStack.verSecurityTable
(
        m_IpOrSubNetVer,
        m_NetMaskBitsVer,
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName,
        m_SnmpPort,
)
values
(
        192.168.64.0,
        24,
        0,
        'public',
        2,
        {
            m_AuthPswd="authpassword",
            m_PrivPswd="privpassword"
        },
        'authPriv'
        6161
);
```

Archivo de configuración TelnetStackPasswords.cfg

El archivo de configuración TelnetStackPasswords.cfg define credenciales de acceso para el acceso de Telnet a los dispositivos.

Puede utilizar el archivo de configuración TelnetStackPasswords.cfg para especificar una conexión Secure Shell (SSH) al configurar el acceso a dispositivos de Telnet. SSH permite el cifrado de contraseña al realizar el acceso de Telnet. Las versiones 1 y 2 de SSH están soportadas (las restricciones se aplican en el modo FIPS).

Importante: SSH en Network Manager soporta actualmente autenticación basada en contraseña o no autenticación. No soporta autenticación con firma RSA.

Tabla de base de datos utilizada

El archivo de configuración TelnetStackPasswords.cfg se puede utilizar para configurar inserciones en la tabla de la base de datos telnetStack.passwords.

Tenga en cuenta que existe otro archivo de configuración asociado con la base de datos telnetStack, el archivo TelnetStackSchema.cfg, pero no es necesario que altere este archivo.

Ejemplo: Configuración de los parámetros de acceso de Telnet para una subred

La siguiente inserción de ejemplo configura los parámetros de acceso de Telnet para una subred. La inserción especifica:

- Una dirección de subred de `192.168.200.0` con un máscara de red de 25.
- La contraseña y el nombre de usuario para acceder al dispositivo.
- Contraseña, indicadores de consola e inicio de sesión que se esperan del dispositivo.
- Los dispositivos de esta subred soportan SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '192.168.200.0',
        25,
        '3v3rt0n',
        'user',
        '.*assword:.*',
        '.*ogin.*',
        '.*onsole>.*',
        1
);
```

Ejemplo: Configuración de los parámetros de acceso de Telnet para un dispositivo

La siguiente inserción de ejemplo muestra cómo puede configurar los parámetros de acceso para una única dirección IP. La inserción especifica:

- Un única dirección IP de `172.16.1.21`. La dirección se identifica como una única dirección ya que `m_NetMaskBits=32`.
- La contraseña y el nombre de usuario para acceder al dispositivo.
- Contraseña, indicadores de consola e inicio de sesión que se esperan del dispositivo.
- Este dispositivo no soporta SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '172.16.1.21',
        32,
        '',
        '',
```

```
        '.*assword.*',
        '.*sername.*',
        '.*Morr.*',
        0
);
```

Ejemplo: Configuración del acceso a dispositivos de Telnet para una subred

La siguiente inserción de ejemplo configura los parámetros de acceso de Telnet para una subred. La inserción especifica:

- Una dirección de subred de `192.168.200.0` con un máscara de red de 25.
- La contraseña y el nombre de usuario para acceder al dispositivo.
- Contraseña, indicadores de consola e inicio de sesión que se esperan del dispositivo.
- Los dispositivos de esta subred soportan SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '192.168.200.0',
        25,
        '3v3rt0n',
        'user',
        '.*assword:.*',
        '.*ogin.*',
        '.*onsole>.*',
        1
);
```

Ejemplo: Configuración del acceso a dispositivos de Telnet para una única dirección IP

La siguiente inserción de ejemplo muestra cómo puede configurar los parámetros de acceso para una única dirección IP. La inserción especifica:

- Un única dirección IP de `172.16.1.21`. La dirección se identifica como una única dirección ya que `m_NetMaskBits=32`.
- La contraseña y el nombre de usuario para acceder al dispositivo.
- Contraseña, indicadores de consola e inicio de sesión que se esperan del dispositivo.
- Este dispositivo no soporta SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '172.16.1.21',
        32,
        '',
        '',
        '.*assword.*',
        '.*sername.*',
        '.*Morr.*',
```

```
        0
);
```

Recuperación de información adicional

Puede configurar los agentes de descubrimiento para recuperar información adicional de los dispositivos y almacenar esta información en la columna ExtraInfo de la base de datos de topología.

Acerca de esta tarea

Para especificar qué información adicional se recuperará por parte de un determinado agente de descubrimiento, modifique el archivo de definición del agente ($NCHOME/precision/disco/agents/*.agnt). Todos los agentes de descubrimiento tienen un archivo de definición en el directorio de agentes, independientemente de si el agente es basado en texto o precompilado.

Los cambios que se deben realizar en la definición de agente se describen en los siguientes temas.

Cambio del tipo de agente

Puede cambiar el tipo de agente en el archivo de definición de agente.

Acerca de esta tarea

Al inicio del archivo de definición del agente de descubrimiento, se identifica uno de los siguientes tipos de agente:

Procedimiento

- `DiscoCompiledAgent{}`: Denota un agente de descubrimiento compilado (con una biblioteca compartida correspondiente en el directorio `$NCHOME/precision/lib`).
- `DiscoDefinedAgent{}`: Denota un agente de descubrimiento basado en texto (sin ninguna biblioteca compartida correspondiente).
- `DiscoCombinedAgent{}`: Denota un agente de descubrimiento que es una combinación de agente basado en texto y precompilado, donde el proceso adicional (como la recuperación de información extra de dispositivos) se define en el archivo de definición del agente de descubrimiento.

Resultados

Para recuperar información adicional de los dispositivos, el tipo de agente debe ser `DiscoDefinedAgent{}` o `DiscoCombinedAgent{}`. Por lo tanto, si va a modificar un agente compilado existente para recuperar información adicional, el primer paso es cambiar el tipo de agente de `DiscoCompiledAgent{}` a `DiscoCombinedAgent{}`.

Capas de mediación y de proceso

La recuperación de información adicional de los dispositivos y la adición de la información a los registros de entidad se lleva a cabo en dos capas: de mediación y de procesamiento. En la capa de mediación, se llevan a cabo las peticiones SNMP para recuperar las variables. En la capa de procesamiento, las variables recuperadas se añaden a los registros de entidad correctos. También existe un filtro opcional en la capa de mediación.

El siguiente segmento de código es una descripción general de la estructura de las secciones de mediación y procesamiento del archivo de definición del agente de descubrimiento.

```
DiscoAgentMediationFilter
            {
                    // Optional section containing filters for the mediation layer.
            }

DiscoAgentMediationLayer
            {
                    // Contains the SNMP Get and GetNext requests to be performed.
                    // In addition, an ICMP trace can be performed and SNMP access
                    // parameters can be retrieved in the mediation layer.
```

```
            }

DiscoAgentProcessingLayer
            {
                    // Adds the retrieved variables to the appropriate entity
                    // record(s).
            }
```

La capa de mediación

La capa de la mediación es donde las solicitudes de SNMP e ICMP se llevan a cabo.

En el siguiente código, la regla `DiscoSnmpGetResponse();` realiza una solicitud Get de SNMP, y la regla `DiscoSnmpGetNextResponse();` ejecuta una solicitud Get Next de SNMP. Puede incluir tantos tipos de solicitud como necesite.

También puede incluir la regla `DiscoSnmpGetAccessParameters();`, que recupera los detalles de acceso de SNMP al dispositivo y la regla `DiscoICMPGetTrace();`, que recupera todas las direcciones IP en la ruta al dispositivo.

```
DiscoAgentMediationLayer
  {
        DiscoSnmpRequests
                {
                        DiscoSnmpGetResponse( ARGUMENT, VARIABLE );
                        DiscoSnmpGetNextResponse( ARGUMENT, VARIABLE, );
                        DiscoSnmpGetAccessParameters( VARIABLE );
                }
        DiscoICMPRequests
                {
                        DiscoICMPGetTrace( VARIABLE );
                }
  }
```

DiscoSnmpGetResponse();
DiscoSnmpGetResponse (); ejecuta una solicitud Get de SNMP. El formato simple de esta regla toma dos argumentos, separados por una coma. El primer argumento es la clave para asignar a la respuesta. Esta clave se utiliza en la capa de proceso. El segundo argumento es el OID (ID de objeto) para recuperar desde el dispositivo.

El siguiente ejemplo recupera sysUpTime, y asigna la clave m_SysUpTime al valor que se devuelve.

```
DiscoSnmpGetResponse( "m_SysUpTime", sysUpTime );
```

Un formato más complejo de DiscoSnmpGetResponse(); toma un tercer argumento, el índice OID. El siguiente ejemplo recupera ifDescr, asigna la clave m_IfDescr al valor devuelto y utiliza el índice OID 1.

```
DiscoSnmpGetResponse( "m_IfDescr", ifDescr, "1" );
```

DiscoSnmpGetNextResponse();
DiscoSnmpGetNextResponse (); ejecuta una solicitud GetNext de SNMP. Esta regla toma los mismos argumentos que DiscoSnmpGetResponse();.

El ejemplo siguiente recupera ipRouteIfIndex y asigna la clave m_IpRouteIfIndex al valor devuelto.

```
DiscoSnmpGetNextResponse( "m_IpRouteIfIndex", ipRouteIfIndex );
```

DiscoSnmpGetAccessParameters();
`DiscoSnmpGetAccessParameters ();` recupera los parámetros de acceso SNMP del dispositivo.

Si configura el agente de descubrimiento para recuperar los parámetros de acceso en la capa de mediación, debe también configurar el agente para añadir la información al registro de base de datos de la capa de proceso.

```
DiscoSnmpGetAccessParameters( "m_AccessParam" );
```

DiscoICMPGetTrace();
`DiscoICMPGetTrace ();` recupera las direcciones IP de la ruta de acceso al dispositivo.

Si configura el agente de descubrimiento para recuperar la vía de acceso al dispositivo en la capa de mediación, debe también configurar el agente para añadir la información al registro de base de datos de la capa de proceso.

```
DiscoICMPGetTrace( "m_Trace" );
```

Filtro de la capa de mediación

El filtro de la capa de la mediación es un filtro opcional que restringe las peticiones SNMP para obtener información adicional de dispositivos específicos. Puede incluir una condición en la sección DiscoMediationSnmpGetFilter{} dentro de DiscoAgentMediationFilter{} para que solo los dispositivos que pasen el filtro sean procesado por el agente.

El siguiente ejemplo garantiza que solo se procesarán los dispositivos con un valor ipForwarding de 1.

```
DiscoAgentMediationFilter
            {
                    DiscoMediationSnmpGetFilter
                    {
                            "ipForwarding" = 1 ;
                    }
            }
```

La capa de procesamiento

La capa de procesamiento es donde la información recuperada se añade a los registros de entidad. Tanto la sección DiscoAgentProcLayerAddTags{} como DiscoAgentProcLayerAddLocalTags{} son opcionales. Sin embargo, si se omiten las dos secciones, no se almacenará información extra en los registros de base de datos.

A continuación, se muestra la estructura de la capa de procesamiento.

```
DiscoAgentProcessingLayer
  {
       DiscoAgentProcLayerAddTags
               {
                    DiscoAddTagSnmpGet( KEY );
                    DiscoAddTagSnmpGetNext( KEY );
                    DiscoAddTagSnmpGetAccessParameters( "m_AccessParam" );
                    DiscoAddTagTrace( "m_Trace" );
               }
       DiscoAgentProcLayerAddLocalTags
               {
                    DiscoAddTagSnmpGet(
                                  TAG FROM KEY WHERE CONDITION );
                    DiscoAddTagSnmpGetNext(
                                  TAG FROM KEY WHERE CONDITION );
               }
  }
```

DiscoAgentProcLayerAddTags{}
Dentro de la sección `DiscoAgentProcLayerAddTags{}`, puede incluir tantas reglas `DiscoAddTagSnmpGet();` o `DiscoAddTagSnmpGetNext();` como resulte necesario. Estas reglas añaden la variable recuperada al registro de base de datos de la entidad descubierta.

Cada regla de la sección `DiscoAgentProcLayerAddTags{}` toma un solo argumento, que es la clave asignada a la variable recuperada en la capa de mediación. En el ejemplo siguiente, se añade el valor `m_SysUpTime`, recuperado en la capa de mediación, al registro de entidad.

```
DiscoAddTagSnmpGet( "m_SysUpTime" );
```

Si ha configurado el agente de descubrimiento para recuperar los parámetros de acceso SNMP o la ruta al dispositivo durante la capa de mediación, debe incluir la regla `DiscoAddTagSnmpGetAccessParameters();` o `DiscoAddTagTrace();` en la sección

DiscoAgentProcLayerAddTags{} para asegurarse de que la información recuperada se añade a la base de datos MODEL.

DiscoAgentProcLayerAddLocalTags{}
Dentro de la sección DiscoAgentProcLayerAddLocalTags{}, puede incluir tantas reglas DiscoAddTagSnmpGet(); o DiscoAddTagSnmpGetNext(); como resulte necesario. Estas reglas añaden la variable recuperada al registro de base de datos de un vecino local.

La estructura de las reglas es:

```
DiscoAddTagSnmpGet( TAG FROM KEY WHERE CONDITION );
DiscoAddTagSnmpGetNext( TAG FROM KEY WHERE CONDITION );
```

Los argumentos que determinan el vecino local al que se añade la etiqueta son:

- *TAG* especifica el nombre de campo de la etiqueta para añadir.
- *KEY* indica la clave asignada al valor devuelto en la capa de mediación.
- *CONDITION* indica una condición que determina si se añadirá o no la etiqueta.

El siguiente ejemplo añade un campo denominado m_IfDescr al objeto de vecino local (utilizando el valor devuelto en la capa de mediación a la que se asignó la clave m_IfDescr) donde m_IfIndex=1.

```
DiscoAddTagSnmpGet( "m_IfDescr" FROM "m_IfDescr"
                                    WHERE ( "m_IfIndex" = "1" )
                             );
```

El siguiente ejemplo añade un campo denominado m_IfType al objeto del vecino local utilizando la lista de valores devueltos por la solicitud GetNext ejecutada en la capa de mediación y a la que se ha asignado la clave m_IfType. La cláusula WHERE indica el valor particular necesario de la lista de datos. El valor se recupera buscando la entrada donde el valor del campo m_IfIndex del objeto del vecino local equivale a SNMPINDEX(0), es decir, el primer valor de la entrada de tabla SNMP.

```
DiscoAddTagSnmpGetNext( "m_IfType" FROM "m_IfType"
                                    WHERE ( "m_IfIndex" = SNMPINDEX(0) )
                                );
```

Configuración del reenvío de condiciones de excepción

El multiplexor de interrupciones SNMP, el proceso **ncp_trapmux**, escucha en un único puerto y reenvía las interrupciones que recibe a un conjunto de pares de host/socket.

Restricción: El multiplexor de la condición de excepción SNMP no redireccione mensajes SNMPv3 Inform.

Acerca de la gestión de las condiciones de excepción

La gestión de condiciones de excepción le permite asegurarse de que las condiciones de excepción recibidas de los dispositivos de red se reenvían a los puertos, donde pueden ser gestionadas por Network Manager y otros sistemas de gestión de red.

En la mayoría de las redes, las condiciones de excepción llegan a un único puerto predeterminado (por lo general, el puerto 162). Esto puede causar problemas si tiene Network Manager y otro sistema de gestión de red instalados en el mismo servidor. Es posible que estos dos sistemas necesiten escuchar condiciones de excepción; sin embargo, solo se puede enlazar un proceso a un puerto simultáneamente.

El multiplexor de condiciones de excepción de SNMP es un proceso de Network Manager que resuelve este problema: escucha un puerto único y reenvía todas las condiciones de excepción que recibe a un conjunto de pares de host/socket.

El multiplexor de condiciones de excepción de SNMP escucha, de forma predeterminada, condiciones de excepción en el puerto 162, pero puede cambiarlo insertando un número de puerto alternativo en la tabla de base de datos trapMux.config.

El proceso ncp_trapmux también puede almacenar sucesos de condiciones de excepción en un archivo en formato binario (incluye la condición de excepción y datos de temporización) que se puede utilizar para volver a crear los sucesos de condición de excepción en el orden en que se produjeron en una fecha posterior. Esto resulta útil sobre todo a efectos de depuración.

Inicio del multiplexor de condiciones de excepción de SNMP

Aunque resulta una buena práctica asegurarse de que se ha configurado el proceso **ncp_ctrl** para iniciar el multiplexor de condiciones de excepción de SNMP, puede también iniciarlo de forma manual.

Acerca de esta tarea

Para iniciar el proceso **ncp_trapmux**, utilice el siguiente mandato:

```
ncp_trapmux -domain DOMAIN_NAME
```

Reenvío de condiciones de excepción

Con el multiplexor de condiciones de excepción de SNMP, puede reenviar condiciones de excepción a uno o varios servidores.

Acerca de esta tarea

Para configurar el multiplexor de condiciones de excepción de SNMP para que reenvíe condiciones de excepción a los sistemas de gestión de red que se ejecutan en host1 y host2:

Procedimiento

1. Edite el archivo de esquema, `$NCHOME/etc/precision/TrapMuxSchema.cfg`, para que contenga un conjunto de pares host/socket. Por ejemplo, añada las siguientes líneas al archivo:

   ```
   insert into trapMux.sinkHosts (host, port) values ("host1", 5999);
   insert into trapMux.sinkHosts (host, port) values ("host2", 5999);
   ```

2. Inicie el multiplexor de condiciones de excepción de SNMP con los siguientes mandatos:

   ```
   ncp_trapmux -domain DOMAIN1
   ncp_trapmux -domain DOMAIN2
   ```

Resultados

En el ejemplo anterior, cuando se envía una condición de excepción que se está ejecutando en el proceso **ncp_trapmux**, se reenvía a `test-host1`, puerto 5999 y a `test-host2`, puerto 5999.

Inicio de capturas de condiciones de excepción

Puede iniciar la captura de condiciones de excepción insertando mandatos en la base de datos del multiplexor de condiciones de excepción de SNMP.

Acerca de esta tarea

Para ordenar al multiplexor de condiciones de excepción de SNMP que inicie la captura de condiciones de excepción:

Procedimiento

1. Inicie sesión en el servicio `TrapMux` utilizando el proveedor de servicios OQL o la página Acceso a la base de datos de gestión.
2. Emita los siguientes mandatos:

```
insert into trapMux.command
(command) values( "capture_start" );
go
```

Detención de capturas de condiciones de excepción
Puede detener la captura de condiciones de excepción insertando mandatos en la base de datos del multiplexor de condiciones de excepción de SNMP.

Acerca de esta tarea

Para ordenar al multiplexor de condiciones de excepción de SNMP que detenga la captura de condiciones de excepción:

Procedimiento

1. Inicie sesión en el servicio TrapMux utilizando el proveedor de servicios OQL o la página Acceso a la base de datos de gestión.
2. Emita los siguientes mandatos:

```
insert into trapMux.command
(command) values( "capture_stop" );
go
```

Impresión de condiciones de excepción en un archivo
Puede imprimir condiciones de excepción en un archivo insertando mandatos en la base de datos del multiplexor de condiciones de excepción de SNMP.

Acerca de esta tarea

Para indicar a **ncp_trapmux** que imprima condiciones de excepción:

Procedimiento

1. Inicie sesión en el servicio TrapMux utilizando el proveedor de servicios OQL o la página Acceso a la base de datos de gestión.
2. Emita los siguientes mandatos:

```
insert into trapMux.command
(command, fileName) values( "print", FILENAME );
go
```

Resultados

Donde *FILENAME* especifica el archivo en el que se escribe la salida. Si no se especifica el archivo, se utiliza $NCHOME/etc/precision/trapmux.out.

Reproducción de las condiciones de excepción de un archivo
Si ha creado un archivo de texto legible para las condiciones de excepción, puede utilizar el proceso **ncp_trapmux** para recrear los sucesos de condiciones de excepción en el orden especificado en este archivo.

Acerca de esta tarea

El proceso **ncp_trapmux** puede reproducir condiciones de excepción utilizando un archivo binario o un archivo legible para humanos; sin embargo, el proceso **ncp_trapmux** solo puede generar archivos binarios.

Para indicar a **ncp_trapmux** que reproduzca condiciones de excepción:

Procedimiento

1. Inicie sesión en el servicio TrapMux utilizando el proveedor de servicios OQL o la página Acceso a la base de datos de gestión.
2. Emita los siguientes mandatos:

```
insert into trapMux.command
(command, fileName) values( "replay", "trapmux.out" );
go
```

Mandatos del multiplexor de condiciones de excepción de SNMP

Puede emitir mandatos al multiplexor de condiciones de excepción de SNMP, el proceso ncp_trapmux, para controlar su funcionamiento.

Los mandatos utilizados para controlar los procesos ncp_trapmux se describen en la siguiente tabla:

Tabla 22. Mandatos utilizados para controlar el proceso ncp_trapmux

Mandato	Función y nombre de archivo predeterminado
`capture_start`	Comenzar a registrar condiciones de excepción en la memoria. El nombre de archivo predeterminado es NULL (no necesario).
`capture_stop`	Dejar de registrar condiciones de excepción en la memoria. El nombre de archivo predeterminado es NULL (no necesario).
`capture_continue`	Continuar registrando condiciones de excepción en la memoria. El nombre de archivo predeterminado es NULL (no necesario).
`capture_empty`	Borrar de la memoria todas las condiciones de excepción registradas actualmente. El nombre de archivo predeterminado es NULL (no necesario).
`rehash`	Finalizar el proceso ncp_trapmux y borra toda la memoria. El daemon vuelve a leer el archivo de configuración y se inicia nuevo. El nombre de archivo predeterminado es NULL (no necesario).
`restart`	Establecer el daemon en la modalidad normal. El nombre de archivo predeterminado es NULL (no necesario).
`replay`	Leer las condiciones de excepción en la memoria o la información de paquetes TRAP sin procesar en el archivo especificado y volver a reproducir las condiciones de excepción con un pequeño retraso entre ellas. El nombre de archivo predeterminado es NULL (reproducir desde memoria).
`replay timed`	Leer las condiciones de excepción en la memoria o la información de paquetes TRAP sin procesar en el archivo especificado y volver a reproducir las condiciones de excepción en el orden en que se recibieron con los mismos retrasos entre las condiciones de excepción. El nombre de archivo predeterminado es NULL (reproducir desde memoria).
`imprimir`	Imprimir las condiciones de excepción actuales de la memoria en un formato no legible en el archivo especificado. La información temporal se codifica con la condición de excepción. El nombre de archivo predeterminado es `$NCHOME/etc/precision/trapmux.out`.

Tipos de condiciones de excepción

Las condiciones de excepción son mensajes administrativos enviados desde dispositivos de red, como direccionadores, que indican que el dispositivo o sus conexiones se han iniciado o detenido.

Acerca de esta tarea

El buscador de condiciones de excepción descubre dispositivos al escuchar las condiciones de excepción SNMP y al extraer direcciones IP de ellas. Los distintos tipos de condiciones de excepción están descritos en Tabla 23 en la página 222.

Tabla 23. Tipos de condiciones de excepción

Number	Nombre	Descripción
0	Condición de excepción coldStart	Una condición de excepción coldStart significa que la entidad de protocolo de envío se reinicializa de tal manera que la configuración del agente o la implementación de la entidad de protocolo pueden alterarse.
1	Condición de excepción warmStart	Una condición de excepción warmStart significa que la entidad de protocolo se reinicializa de tal manera que no se puedan alterar la configuración del agente ni la implementación de la entidad de protocolo.
2	Condición de excepción linkDown	Una condición de excepción linkDown se genera por el fallo de un enlace de comunicación reconocido.
3	Condición de excepción linkUp	Una condición de excepción linkUp se genera cuando reaparece un enlace de comunicación que estaba inhabilitado.
4	Condición de excepción authenticationFailure	Una condición de excepción authenticationFailure se genera por un mensaje de protocolo que el receptor no autenticó. Por ejemplo, una contraseña incorrecta.
5	Condición de excepción egpNeighborloss	Una condición de excepción egpNeighborLoss significa que un vecino del Protocolo de pasarela exterior (EGP), que era un par de EGP para la entidad del protocolo de envío, se marcó y la relación de par ya no es válida.
6	Condición de excepción específica de la empresa	Una condición de excepción específica de la empresa significa que la entidad de protocolo de envío reconoce que se produjo un suceso específico de la empresa.

Filtrado de información SNMP de dispositivos

Puede filtrar la información SNMP cuando el ayudante de SNMP consulta los dispositivos mediante la configuración de inserciones en la base de datos del ayudante de SNMP.

Filtrado de interfaz SNMP

Puede filtrar los datos SNMP recuperados de los dispositivos por el proceso de descubrimiento mediante la configuración de filtros de interfaz SNMP. Sólo puede configurar filtros de interfaz SNMP desde la línea de mandatos.

Por qué utilizar el filtrado de interfaz SNMP

En ocasiones, un dispositivo o una clase de dispositivos devuelve demasiados datos de MIB. Por ejemplo, si los dispositivos virtuales tienen un gran número de interfaces, descubrirlas puede tardar bastante tiempo. Para acelerar el descubrimiento de estos dispositivos, puede utilizar filtros de interfaz SNMP para reducir el número de interfaces recuperadas por el ayudante de SNMP.

Cómo funciona el filtrado de interfaz SNMP

Cuando los agentes de descubrimiento, scripts de Perl o el **Navegador de MIB de SNMP** solicitan información SNMP, el ayudante de SNMP recupera la información de los dispositivos de red. Los filtros de interfaz SNMP definen filas en las tablas de MIB que recupera el ayudante de SNMP. El ayudante de SNMP

recupera un subconjunto de la información que se habría devuelto sin filtro y la envía al proceso que ha solicitado la información SNMP. Los filtros de interfaz SNMP también pueden definir tablas completas que no deben ser recuperadas por el ayudante de SNMP.

Los filtros de interfaz SNMP sólo se aplican a solicitudes de recorridos completos de tablas de MIB. Las solicitudes Get o GetNext de SNMP de interfaces específicas dentro de una tabla de MIB no se filtran.

Los dispositivos que deberían tener el filtro aplicado se definen en el *filtro de dispositivos*. Si hay un filtro de dispositivos definido, las solicitudes de información SNMP para un dispositivo se comprueban primero en el filtro de dispositivos. Únicamente los dispositivos que pasen el filtro se comprueban a continuación para el filtrado de interfaz.

El filtro puede filtrar varias filas de una tabla. La primera vez que se accede a una tabla filtrada, se recorren una o más columnas de la tabla. Todas las solicitudes posteriores de recorridos SNMP de dicha tabla devuelven sólo las interfaces que coinciden con el filtro.

Inclusión de varias tablas con filtros dependientes

También puede definir *filtros dependientes*. Si se define un filtro de interfaz SNMP *Filtro 1* en la Tabla A, puede definirse un segundo filtro dependiente *Filtro 2* en la Tabla B. La información SNMP en la Tabla B que esté relacionada con la misma interfaz también se recupera.

Para definir un filtro dependiente, además de definir un filtro en la Tabla A, deben ser ciertas una o más de las condiciones siguientes:

- Tabla A y Tabla B tienen índices equivalentes.
- El índice de Tabla A es un valor de Tabla B.

Si Tabla A y Tabla B tienen exactamente el mismo índice, no es necesario definir un filtro dependiente. La información de Tabla B se recupera automáticamente en función del filtro definido en Tabla A.

Cuándo puede utilizar el filtrado de interfaz SNMP

Puede utilizar el filtrado de interfaz SNMP en cualquier tabla de MIB SNMP que tenga una clave en ifIndex. Por ejemplo, al filtrar en ifTable o ifXTable se permite el filtrado en valores como ifType e ifDescr.

Restricción: No se admite el filtrado sobre cualquier variable de MIB SNMP distinta de las interfaces. Sin embargo, puede acceder en bloque a cualquier tabla utilizando la opción m_InstanceFilterTable.

El fragmento de ejemplo siguiente muestra la definición para la ipAddrTable del archivo `NCHOME/precision/mibs/RFC1213.mib`:

```
          -- the IP address table

          -- The IP address table contains this entity's IP addressing
          -- information.

          ipAddrTable OBJECT-TYPE
              SYNTAX  SEQUENCE OF IpAddrEntry
              ACCESS  not-accessible
              STATUS  mandatory
              DESCRIPTION
                      "The table of addressing information relevant to
                      this entity's IP addresses."
              ::= { ip 20 }
```

La sintaxis "SEQUENCE OF" define esto como una tabla. Puede averiguar qué tablas están definidas en el MIB buscando esta cadena. El ejemplo siguiente muestra la salida de la ejecución de una búsqueda en UNIX:

```
% grep 'SEQUENCE OF'  RFC1213.mib
              SYNTAX  SEQUENCE OF IfEntry
              SYNTAX  SEQUENCE OF AtEntry
              SYNTAX  SEQUENCE OF IpAddrEntry
              SYNTAX  SEQUENCE OF IpRouteEntry
              SYNTAX  SEQUENCE OF IpNetToMediaEntry
              SYNTAX  SEQUENCE OF TcpConnEntry
```

```
            SYNTAX  SEQUENCE OF UdpEntry
            SYNTAX  SEQUENCE OF EgpNeighEntry
```

Configuración de filtros de interfaz SNMP

Puede configurar uno o más filtros de interfaz por tipo de dispositivo.

Acerca de esta tarea

Para configurar uno o más filtros de interfaz, realice los pasos siguientes:

Procedimiento

1. Asegúrese de que el agente Entity está habilitado. Puede habilitar el agente Entity en la **GUI de configuración del descubrimiento**.
2. Realice una copia de seguridad del archivo siguiente y edítelo:

   NCHOME/etc/precision/DiscoSnmpHelperFilters.*NOMBRE_DOMINIO*.cfg
3. Especifique una inserción en la tabla snmpHelper.instanceFilter. Puede utilizar los ejemplos que se proporcionan más adelante en este procedimiento o copiar otra inserción de ejemplo de esta documentación.
4. Proporcione un nombre para este filtro. Localice el valor de m_FilterName y proporcione un nombre descriptivo para el filtro, delimitado por comillas dobles.
5. Configure qué dispositivos deben tener este filtro de interfaz aplicado mediante la definición de un filtro de dispositivos. Localice el valor de m_DeviceFilter y defina un filtro, delimitado por comillas dobles. Puede utilizar Identificadores de objeto (OID) para construir el filtro. Utilice la sintaxis OQL (lenguaje de consulta de objetos).

   El filtro debe tener el formato siguiente:

   ```
   mibVariableName expression values
   [ optional_Boolean_operator expression optional_Boolean_operator .. ]
   ```

   Por ejemplo, son válidos los filtros siguientes:

   ```
   // Apply the interface filter to only a specific type of device
   sysObjectID = '1.3.6.1.4.1.4874.1.1.1.1.3'


   // More complex example of the above
   sysObjectID = '1.3.6.1.4.1.4874.1.1.1.1.3' OR sysDescr LIKE 'ERX-1440'

   // Apply the interface filter only to devices in certain locations
   sysLocation in ( 'location1', 'location2' )

   //Apply the interface filter to all types of device.
   sysObjectID != ''
   ```
6. Defina la expresión de filtro de interfaz SNMP que desee aplicar a las tablas de MIB. Únicamente se recuperan las filas que coinciden con este filtro, es decir, aquellas para las que esta expresión se evalúa como verdadera. Localice el valor de m_InstanceFilter y defina un filtro, delimitado por comillas dobles. Puede utilizar Identificadores de objeto (OID) para construir el filtro. Utilice la sintaxis OQL (lenguaje de consulta de objetos). Puede definir más de un filtro de interfaz por cada filtro especificado.

   El filtro debe tener el formato siguiente:

   ```
   mibVariableName expression values
   [ optional_Boolean_operator expression optional_Boolean_operator .. ]
   ```

   Por ejemplo, son válidos los filtros siguientes:

   ```
   // Only interfaces with names like this are returned
   ifName like 'Gi0'

   // This filter is against 2 distinct tables (ifTable and ifXTable)
   ```

```
with the requirement that these share a common index (ifIndex)
ifName like 'Gi0' or ifDescr like 'FastEthernet'

// Filter out interfaces of these types
ifType not in ( 1, 53, 166 )
```

7. Opcional: Si desea filtrar información relacionada con la misma interfaz en las tablas de MIB relacionadas que no están definidas explícitamente con el mismo índice, especifique qué tablas desea incluir utilizando un *filtro dependiente*. Copie y edite una inserción predeterminada en la tabla `snmpFilter.dependentInstances` del archivo `NCHOME/etc/precision/DiscoSnmpHelperFilters.`*`NOMBRE_DOMINIO`*`.cfg` o copie una inserción de ejemplo de esta documentación.

   La sintaxis del filtro es

   ```
   MIB_variable_name in
   (eval(list_type,'&MIB_table.MIB_entry'))
   ```

   donde *MIB_variable_name* debe existir en *MIB_table*, y se ha definido un filtro sobre *MIB_table* en la tabla snmpHelper.instanceFilter.
8. Ejecute el mandato siguiente para indicar al ayudante de SNMP, ncp_dh_snmp, que vuelva a leer sus archivos de configuración:

   ```
   kill -HUP PID
   ```
9. Puede configurar más de un filtro de interfaz SNMP en el archivo `NCHOME/etc/precision/DiscoSnmpHelperFilters.`*`DOMAIN_NAME`*`.cfg`. Si se ha configurado más de un filtro de interfaz, se recupera una fila de tabla que coincida con cualquier filtro.
10. Si se han configurado uno o más filtros de interfaz, asegúrese de que la propiedad `RaiseAlertsForUnknownInterfaces` del archivo `NCHOME/etc/precision/NcPollerSchema.cfg` está establecida en `0`. Este valor garantiza que no se generen alertas para las interfaces que no se han descubierto, por ejemplo, debido a que se excluyeron del descubrimiento mediante los filtros de interfaz.

Ejemplo de filtro de interfaz simple

El ejemplo siguiente recupera información para interfaces con un nombre similar a "Gi0" en un tipo de dispositivo concreto.

```
insert into snmpHelper.instanceFilter
(
    m_FilterName,
    m_DeviceFilter,
    m_InstanceFilter
)
values
(
    "TESTFILTER",
    "sysObjectID = '1.3.6.1.4.1.4874.1.1.1.1.3' OR sysDescr LIKE 'ERX-1440'",
    "ifName like 'Gi0'"
);
```

Ejemplo de filtro de interfaz SNMP dependiente

Puede crear filtros dependientes que utilicen los resultados de filtros anteriores para filtrar tablas adicionales.

En el ejemplo siguiente, ipNetToMediaTable se indexa en ipNetToMediaIfIndex, que es equivalente a ifIndex. La tabla ifTable también se indexa en ifIndex. Esta relación se escribe en la definición de MIB, pero no se puede determinar mediante programación. La especificación de la relación como un filtro dependiente garantiza que se incluyan también las entradas coincidentes de ipNetToMediaTable.

```
insert into snmpHelper.dependentInstanceFilter
(
    m_InstanceFilter
)
values
```

```
(
    "ipNetToMediaIfIndex in ( eval(list type int, '&ifTable.ifEntry') )"
)
;
```

En el ejemplo siguiente, ipAddrTable se indexa en la dirección IP, pero cada fila contiene ipAdEntIfIndex, cuyo valor es equivalente a ifIndex. La tabla ifTable también se indexa en ifIndex. Esta relación se escribe en la definición de MIB, pero no se puede determinar mediante programación. La especificación de la relación como un filtro dependiente garantiza que se incluyan también las entradas coincidentes de ipAddrTable.

```
insert into snmpHelper.dependentInstanceFilter
(
    m_InstanceFilter
)
values
(
    "ipAdEntIfIndex in ( eval(list type int, '&ifTable.ifEntry') )"
)
;
```

Ambos filtros de ejemplo devuelven filas que coinciden con el filtro. Si una fila de la tabla de MIB no tiene un valor válido, no se recupera. Por ejemplo, si una fila de la tabla ipAddrTable no contiene un valor válido para ipAdEntIfIndex, el ayudante de SNMP no la recupera.

Ambos filtros de ejemplo se basan en un filtro de interfaz ya definido en ifIndex. Los resultados coincidentes de las tablas ipAddrTable e ipNetToMediaTable se almacenan en memoria caché, por lo no se vuelve a consultar el MIB.

Los dos filtros anteriores están configurados de forma predeterminada.

Configuración de copias de seguridad de la caché ncp_store

Puede realizar una copia de seguridad y restaurar la caché `ncp_store` para tener una copia de la topología.

Acerca de esta tarea

Cuando se configuran las copias de seguridad, se llama al agrupador `RunCacheCopy.stch` como parte del descubrimiento. Este agrupador ejecuta el script `RunCacheCopy.pl`, que realiza una copia de seguridad de los archivos en la caché. No es necesario modificar el agrupador o el script.

Los archivos de caché se copian de `$NCHOME/var/precision/` a `$NCHOME/var/precision/backup/StoreCacheBackup/`. Dentro de este directorio, se crea un subdirectorio llamado `Full_`*`domain_timestamp`*.

Procedimiento

1. Las copias de seguridad están desactivadas de forma predeterminada. Para habilitar y configurar las copias de seguridad, edite el archivo `EventGatewaySchema.cfg`.
   a) Realice una copia de seguridad y edite el archivo `$NCHOME/etc/precision/EventGatewaySchema.cfg`.
   b) Busque la inserción en la tabla de base de datos `config.defaults` y edite los valores.
   c) Establezca `backupDiscoveryCaches` en `1` para habilitar las copias de seguridad, o `0` para deshabilitarlas.
   d) Establezca `numberOfBackupsToKeep` al número de copias de seguridad que deben conservarse. Después de realizar este número de copias de seguridad, se eliminan las anteriores.
2. Reinicie los componentes principales con el uso de los comandos `itnm_stop ncp` y `itnm_start ncp`.
3. Para restaurar las copias de seguridad:
   a) Apague los componentes principales mediante el comando `itnm_stop ncp`.

b) Copie los archivos de caché de `$NCHOME/var/precision/backup/StoreCacheBackup/` de vuelta a `$NCHOME/var/precision/`.

c) Reinicie los componentes principales mediante el comando `itnm_start ncp`.

Configuración de descubrimientos especializados

Puede configurar el sistema para que realice descubrimientos más complejos, como de MPLS y de NAT.

Acerca de esta tarea

Los descubrimientos especializados incluyen:

descubrimientos de EMS
Recopila datos de topología de sistemas de gestión de elementos e integra estos datos en la topología descubierta.

Descubrimientos MPLS
Descubre VPN de capa 3 y VPN de capa 2 mejoradas que se ejecutan en redes principales de MPLS.

Descubrimientos de NAT
Descubre dispositivos de pasarela de NAT y, por lo tanto, le permite recuperar datos en dispositivos de espacios de direcciones privadas.

Configuración de un descubrimiento sensible al contexto

Si necesita descubrir dispositivos que soportan varios contextos, debe ejecutar un descubrimiento sensible al contexto. Por ejemplo, un dispositivo que utiliza contextos SNMP separados para proporcionar acceso a sus direccionadores virtuales. El descubrimiento sensible al contexto garantiza la correcta representación de dispositivos virtuales que pueden acceder al contexto. Compruebe siempre que el tipo de dispositivo particular está soportado para el descubrimiento.

Acerca de esta tarea

En un descubrimiento sensible al contexto, se pasa información sobre un dispositivo de la tabla `returns` del agente Detalles a la tabla `despatch` del agente de contexto relevante.

Los agentes de contexto utilizan los filtros en los archivos con una extensión de .agnt para determinar qué dispositivos procesar. Esto es verdadero para todos los agentes de descubrimiento. Si el dispositivo no es de un tipo que soporte direccionadores virtuales que pueden acceder al contexto, es decir, que no necesita procesamiento sensible al contexto, se pasa directamente al agente de dirección asociada.

Atención: La habilitación de un descubrimiento sensible al contexto habilita automáticamente todos los agentes de contexto. La inhabilitación de un descubrimiento sensible al contexto inhabilita automáticamente todos los agentes de contexto. No habilite o inhabilite manualmente agentes de contexto, utilizando los archivos de configuración o mediante la GUI Configuración de descubrimiento.

Para habilitar el descubrimiento sensible al contexto, agregue la siguiente inserción al archivo `DiscoConfig.cfg`:

```
insert into disco.config
(
      m_UseContext
)
values
(
      1
)
```

La inserción del valor `0` inhabilita el descubrimiento sensible al contexto.

Configuración de descubrimientos de EMS

Puede configurar Network Manager para recopilar datos de topología del sistema de gestión de elementos (EMS) e integrar estos datos en la topología descubierta.

Acerca de esta tarea

Los siguientes temas describen cómo configurar un descubrimiento de EMS.

Para obtener una visión general de cómo Network Manager recopila datos de topología del sistema de gestión de elementos (EMS) e integra estos datos en la topología descubierta, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*.

Acerca de la integración con EMS

La integración con EMS de Network Manager permite a Network Manager recopilar datos de topología de sistemas de gestión de elementos (EMS).

Acerca de los recopiladores

Un recopilador es un módulo de software que recupera datos de topología de un origen de datos, como un archivo EMS (sistema de gestión de elementos) o un archivo CSV (comma-separated value), y hace estos datos disponibles para el proceso de descubrimiento como un conjunto de datos XML. Network Manager puede agrupar estos datos en la topología descubierta.

Un recopilador convierte los datos de topología del formato en el que se mantienen en el EMS propietario a la estructura XML estándar que se puede procesar mediante Network Manager. Esto significa que se debe desarrollar un recopilador distinto para cada proveedor y modelo de EMS distinto. Los recopiladores predefinidos proporcionados con Network Manager se graban en Java o Perl. Sin embargo, se pueden grabar los recopiladores en cualquier lenguaje, siempre que dicho lenguaje pueda proporcionar un servidor XML-RPC que pueda consultar el proceso **ncp_disco**. Network Manager se suministra con módulos Java y Perl para admitir el desarrollo de recopiladores en esos idiomas.

Los recopiladores pueden ejecutarse en el mismo host que el Network Manager. Los recopiladores también se pueden ejecutar en un host distinto.

Toda interacción entre Network Manager y los recopiladores se lleva a cabo utilizando XML, y esta interacción se produce en una interfaz XML-RPC.

Recopiladores predefinidos

Network Manager se entrega con un conjunto de recopiladores predeterminados que recuperan datos de servicio de varios EMS, incluidos los EMS que gestionan la red de acceso mediante radio (RAN) y los dispositivos ópticos.

Acerca de esta tarea

Los scripts y un archivo de configuración de texto sin formato de cada recopilador se conservan en directorios independientes llamados como el recopilador dentro del directorio `$NCHOME/precision/collectors/`, como se indica a continuación:

- Los recopiladores escritos en Java se almacenan en el directorio `$NCHOME/precision/collectors/javaCollectors/`.
- Los recopiladores escritos en Perl se almacenan en el directorio `$NCHOME/precision/collectors/perlCollectors/`.

Por ejemplo, el recopilador CiscoLMS se almacena en el directorio `javaCollectors/CiscoLMS/`, y el recopilador AlcatelNR8PLIooIsn se almacena en el directorio `perlCollectors/AlcatelNR8PLIooIsn/`.

Cada recopilador proporcionado con Network Manager descarga datos desde un EMS utilizando un protocolo Northbound Interface (NBI) o utiliza datos descargados de EMS por el usuario. Cada EMS gestiona dispositivos que dan soporte a ciertas tecnologías.

Los recopiladores predeterminados se incluyen en las tablas siguientes:

Tabla 24. Recopiladores Java predeterminados

Recopilador	Descripción	Protocolos de NBI	Tecnologías
Alcatel5620Sam	Recopilador del EMS SAM de Alcatel 5620. Este recopilador de Java recupera la misma información que el recopilador de Perl Alcatel5620SamSoapFindToFile y, adicionalmente, recupera información de Link Aggregation Group (LAG). El recopilador recupera datos de contención LAG, que se modelan y presentan en el Navegador de estructura. El recopilador recupera la información de la interfaz VLAN. El recopilador recupera la información de dirección y subred de los elementos ENodeB, crea la información de VLAN basándose en esa información, y modela los puertos Ethernet y las placas de control. A partir de V4.2 Fixpack 1, los datos de descubrimiento relacionados con LTE para SAM 5620 EMS ya no están soportados para el descubrimiento parcial de Network Manager. Fix Pack 6 El recopilador recupera información para MMEs (extensiones multimedia) virtuales o basadas en la nube. Fix Pack 6 El recopilador recupera información para las puertas de enlace SAE de Nokia, que tienen funcionalidades LTE PPDNGateway y ServingGateway.	SOAP	Long Term Evolution (LTE), LAG, OSI Capa 2, OSI Capa 3, Interfaz, Inventario, Entidad física, VPN Capa 3 y VPN Capa 2
Cisco APIC REST	Recopilador de Cisco Application Policy Infrastructure Controller (APIC) EMS.	Protocolo JSON y XML sobre REST WebSocket	Inventario de interfaz, Entidad física
CiscoLMS	Recopilador del CiscoWorks LMS EMS. Este recopilador utiliza el esquema de base de datos abierto de Cisco y el motor de extracción de datos de Cisco para comunicarse con el EMS.	Servidores web JDBC y REST	Entidad física, Inventario de interfaz

Tabla 24. Recopiladores Java predeterminados (continuación)

Recopilador	Descripción	Protocolos de NBI	Tecnologías
csv	Recopilador genérico basado en CSV que lee archivos `.csv` para los datos de entrada. Existe un recopilador GenericCsv escrito en Java y un segundo recopilador GenericCsv escrito en Perl.	N/A	Varios
Huawei CORBA TMF 814	Recopilador para Huawei CORBA TMF 814 EMS. Este recopilador recopila información de los sistemas EMS que utilizan la interfaz CORBA TMF 814 como, por ejemplo, Huawei T2000 y U2000. El recopilador recupera datos SNC para complementar los datos CTP. No se admite la visualización de datos de SNC.	CORBA TMF814	OSI Capa 1, Inventario de interfaz, Entidad física, SONET, SDH
Huawei M2000	Recopilador de Huawei M2000 EMS. Este recopilador procesa dispositivos IMS y STP, y datos de LTE 3G, 2G, PSCore y CSCore utilizando los archivos XML de gestión de la configuración que se han generado desde un Huawei M2000 EMS. Coloque los archivos XML en un directorio local para que el recopilador pueda acceder a los mismos. Huawei M2000 EMS puede producir muchos tipos diferentes de archivos XML. Este recopilador da soporte específicamente a los siguientes archivos XML: • LNBI_XML_RT_*.xml • SRANNBIExport_ XML_LTE_RT_*.xml • CMExport_*.xml • GNBIExport_XML_RT_*.xml • UNBIExport_XML_RT_*.xml El recopilador también procesa los archivos IM*.xml, AIM_*.xml y W_OMC_*.xml disponibles para complementar los datos de los archivos XML anteriores.	N/A	eNodeB, BSC, BTS, NodeB, RNC, MGW, UGW, USN, HIR, EIR, HSS, CGNE, MSS, ATS, CCF, CSCF, MRFP, SE2900, SPG, SG7000, USCDB

Tabla 24. Recopiladores Java predeterminados (continuación)

Recopilador	Descripción	Protocolos de NBI	Tecnologías
MTOSISoap	Recopilador genérico que descubre sistemas de gestión de elemento que soporta el NBI de MTOSI Soap, por ejemplo, el Huawei U2000 iManager EMS. Tecnologías soportadas Descubrimiento de Capa 2, descubrimiento de Capa 3 y descubrimiento de inventario físico.	MTOSI SOAP	Inventario físico, Capa 2, Capa 3
NetActCMDump	Procesa datos 2G, 3G y LTE RAN utilizando el archivo XML de gestión de configuración para el recopilador EMS de NetAct. El recopilador debe conectarse al recopilador NetAct EMS para recuperar este archivo XML y lo hace mediante FTP o SFTP. Para utilizar los datos desde la interfaz XML de NetAct para el recopilador de Gestión de la configuración en un descubrimiento de red, debe configurar el archivo de propiedades del recopilador con los detalles de conexión FTP y SFTP entre el EMS de NetAct y Network Manager.	FTP o SFTP	LTE, RAN, SGSN, eNodeB, MME, PGW, BTS, RNC, SGW, BSC, NodeB, MGW, TRX, MSC, PCU
NetViewer	Recopilador de Nokia Solutions and Networks (NSN) NetViewer EMS.	CORBA TMF814	OSI Capa 1, Inventario de interfaz, Entidad física, SONET, SDH
Nokia5529Idm	Recopilador del Nokia5529Idm EMS. Este recopilador de Java recupera la misma información que el recopilador de Perl Nokia5529Idm y es compatible adicionalmente con la característica Bulk Network Export y el Java Message Service (JMS). El recopilador escucha notificaciones de JMS sobre entidades que se han añadido o eliminado de EMS. El recopilador se detiene y, a continuación, vuelve a descubrir el EMS. Durante el siguiente descubrimiento o descubrimiento, la base de datos de topología NCIM se actualiza con los datos más recientes del recopilador.	SOAP	Inventario de interfaz, Entidad física
NokiaOMS1350	Recopilador para Nokia OMS 1350 EMS. Este recopilador encuentra dispositivos de red óptica basados en el Nokia 1830 PSS.	REST	OSI Capa 1

Tabla 24. Recopiladores Java predeterminados (continuación)			
Recopilador	**Descripción**	**Protocolos de NBI**	**Tecnologías**
Tellabs INM8000	Recopilador del Tellabs INM8000 EMS.	API de Java	OSI Capa 3, OSI capa 2, Inventario de interfaz, Entidad física

Tabla 25. Recopiladores Perl predeterminados			
Recopilador	**Descripción**	**Protocolos de NBI**	**Tecnologías**
Nokia5529Idm	Recopilador del Nokia5529Idm EMS.	SOAP	Inventario de interfaz, Entidad física
Alcatel5620SamSoap	Recopilador del EMS SAM de Alcatel 5620.	SOAP	OSI Capa 2, OSI Capa 3, Inventario de interfaz, Entidad física, VPN Capa 3, VPN Capa 2
Alcatel5620SamSoap FindToFile	Recopilador del EMS SAM de Alcatel 5620. El recopilador recupera los mismos datos que el recopilador Alcatel5620SamSoap FindToFile. El recopilador almacena los datos del EMS en archivos ZML con el mismo nombre que los objetos solicitados. El recopilador transfiere los archivos ZML al Network Manager mediante FTP. Debe configurar los detalles de conexión FTP antes de ejecutar el recopilador.	SOAP, FTP	LTE, OSI Capa 2, OSI Capa 3, Inventario de interfaz, PCRF, SGW, PGW, MME, eNodeB, Entidad física, VPN Capa 3, VPN Capa 2
Alcatel5620SamCsv	Recopilador del EMS SAM de Alcatel 5620. Este recopilador recupera datos de topología de EMS de un volcado CSV el EMS SAM Alcatel 5620.	N/A	Inventario de interfaz, Entidad física
AlcatelNR8PLIooIsn	Recopilador del Alcatel Lucent 1353 NM y componentes del Alcatel Lucent 1354 RM dentro del AlcatelNR8PL EMS.	IOO (para el componente Alcatel Lucent 1353), ISN (para el componente Alcatel Lucent 1354 RM)	1353 NM, 1354 RM

Tabla 25. Recopiladores Perl predeterminados (continuación)			
Recopilador	**Descripción**	**Protocolos de NBI**	**Tecnologías**
Recopilador GenericCsv	Recopilador genérico basado en CSV que lee archivos `.csv` para los datos de entrada. Existe un recopilador GenericCsv escrito en Java y un segundo recopilador GenericCsv escrito en Perl.	N/A	Inventario
HuaweiU2000ImanagerTL1	Recopilador del HuaweiU2000Imanager EMS.	TL1	Entidad física, Inventario de interfaz
HuaweiU2000iManagerTL1DumpExport	Recopilador del HuaweiU2000Imanager EMS. Este recopilador utiliza archivos XML de EMS.	N/A	Entidad física, Inventario de interfaz
OpticalBlackboxXml	Recopilador de caja negra que permite añadir entidades pasivas de capa 1 a la topología de red descubierta.	N/A	Entidad física, Inventario de interfaz, Capa 1

Otros componentes de la integración EMS

Además de los recopiladores, la integración EMS se compone de muchos componentes que asisten en la recopilación de datos de topología.

Los componentes de la integración EMS se describen en Tabla 26 en la página 233.

Tabla 26. Componentes de la integración EMS	
Componente	**Descripción**
Buscador de recopiladores `ncp_df_collector`	El Buscador de recopiladores lee las fuentes del host del recopilador de una tabla de fuentes de la base de datos `collectorFinder`. Luego consultará a los recopiladores especificados en esta tabla para obtener una lista de dispositivos gestionados por el EMS asociado con cada recopilador.
Agentes de recopiladores	Recupera información básica y detallada acerca de los dispositivos del recopilador. Cada agente hace uso del Ayudante del recopilador para recuperar esta información.
Agente CollectorDetails	Recupera información básica acerca de los dispositivos del recopilador, incluidos sysObjectId, sysDescr y datos de denominación.

Tabla 26. Componentes de la integración EMS (continuación)	
Componente	**Descripción**
Agente CollectorInventory	Recupera el vecino local, la entidad y los datos de dirección asociada para cada uno de los dispositivos del recopilador.
Agente CollectorLayer1	Recupera información de capa 1 y de microondas para los dispositivos del recopilador.
Agente CollectorLayer2	Recupera la información de conectividad de capa 2 para los dispositivos del recopilador.
Agente CollectorLayer3	Recupera información de conectividad de capa 3 para los dispositivos del recopilador.
Agente CollectorLTE	Recupera información de entidades específicas de LTE para los dispositivos del recopilador.
Agente CollectorRan	Recupera información de red de acceso mediante radio (RAN) para los dispositivos del recopilador.
Agente CollectorVpn	Recupera los datos VPN de capa 2 y capa 3 para los dispositivos del recopilador.
Ayudante del recopilador `ncp_dh_xmlrpc`	Habilita a Network Manager para comunicarse con los recopiladores utilizando la interfaz XML-RPC.

Flujo de datos de descubrimiento EMS

Utilice esta información para entender los pasos de un descubrimiento EMS.

Flujo de datos de descubrimiento EMS estándar

Utilice esta información para entender la forma en la que Network Manager recopila los datos de topología desde un EMS como parte de un descubrimiento normal o descubrimiento parcial.

La tabla a continuación muestra los pasos incluidos en la recopilación de datos de topología desde EMS como parte de un descubrimiento normal o parcial. Una vez recopilados estos datos, Network Manager lo agrupa con la topología.

Tabla 27. Recopilación de datos de topología de EMS durante el descubrimiento	
Paso	**Flujo de datos**
1	Utilizando el buscador de recopiladores, el sistema de descubrimiento consulta al recopilador para obtener una lista de dispositivos administrados por el EMS. En el caso de un descubrimiento parcial, el descubrimiento puede consultar solo un dispositivo o subred.
2	El recopilador consulta al EMS la lista de dispositivos.
3	El EMS responde con la lista de dispositivos gestionados.
4	El recopilador responde proporcionando la lista de dispositivos.

Tabla 27. Recopilación de datos de topología de EMS durante el descubrimiento (continuación)	
Paso	**Flujo de datos**
5	Utilizando varios agentes de descubrimiento de recopilador especializados en distintos momentos durante el descubrimiento, el sistema de descubrimiento consulta al recopilador información básica y detallada sobre cada uno de los dispositivos de la lista. La información detallada solicitada incluye: • Información de inventario. • Detalles de conexión de microondas y capa 1. • Detalles de conexión de capa 2. • Detalles de conexión de capa 3. • Información de LTE. • Información de red de acceso mediante radio (RAN). • Información de VPN.
6	El recopilador responde proporcionando la información básica y detallada según se solicite.

Sincronización para varios orígenes de datos
Si ejecuta un descubrimiento que incluye un recopilador y orígenes de datos SNMP, o varios recopiladores, debe sincronizar la fase "Interrogando dispositivos" (fase 1) del descubrimiento entre todos los orígenes de datos. La fase 1 de sincronización disminuye la posibilidad de que se produzcan un número excesivo de ciclos de descubrimiento y garantiza que esté disponible la cantidad máxima datos durante la compilación de la topología. La función de sincronización la proporciona el valor de configuración `m_WaitForManagedProcs`. `m_WaitForManagedProcs` está establecido de manera predeterminada en 0 (desactivado), el cual es el valor más adecuado para los descubrimientos solo de SNMP.

Durante la fase 1 de un descubrimiento de IP, el descubrimiento espera hasta 90 segundos de forma predeterminada entre el descubrimiento de un dispositivo y el siguiente. Si no se encuentran más dispositivos tras 90 segundos, el descubrimiento pasa a la fase 2. Este tiempo de espera se controla mediante el campo `m_NothngFndPeriod` en la tabla de base de datos de descubrimiento `disco.config` y resulta ideal para los descubrimientos SNMP en los que no todas las entidades responden al mismo tiempo.

Sin embargo, el comportamiento de los recopiladores es diferente a SNMP. Los recopiladores devuelven todos sus dispositivos de una vez, potencialmente después de un retardo inicial comparativamente largo, durante el cual se consulta el EMS. Utilizando sólo `m_NothngFndPeriod` cuando se ejecutan varios recopiladores o un recopilador y descubrimientos SNMP bajo el mismo dominio, es posible que se produzcan un número de ciclos de descubrimiento no deseado. Este efecto se debe a que el retardo de la fase de interrogación entre cada recopilador puede superar por mucho los 90 segundos. Este retardo hace que el descubrimiento continúe en la fase siguiente si se ha completado la fase de ping de SNMP.

Para asegurarse de que los datos de todos los recopiladores de un descubrimiento de varios recopiladores se recopilen y agrupen juntos en el mismo ciclo de descubrimiento, debe configurar los campos siguientes en la tabla de base de datos de descubrimiento `disco.config`:

`m_WaitForManagedProcs`
Establezca este campo en 1. Este valor garantiza que el proceso de descubrimiento permanece en la fase 1 hasta que todos los recopiladores hayan terminado de procesar los datos de sus respectivos EMS.

De forma predeterminada, esta campo está establecido en 0. Este valor significa que cuando el primer recopilador completa el proceso de datos y transcurre el número de segundos definido en el campo `m_NothngFndPeriod`, el proceso de descubrimiento pasará a la fase 2 sin esperar a que los demás recopiladores comiencen el procesamiento.

m_ManagedWaitTimeOut
Aplicable cuando m_WaitForManagedProcs está establecido en 1. Este campo define el tiempo máximo de espera para que todos los recopiladores terminen de recuperar los datos de sus EMS. De hecho, este valor es un mecanismo a prueba de errores para cubrir la situación en la que uno de los recopiladores nunca completa su proceso. Establézcalo en el valor máximo en segundos que se debe esperar para que todos los recopiladores finalicen el procesamiento de datos. Una vez que se haya agotado el tiempo de espera y haya transcurrido el número de segundos definido en el campo m_NothngFndPeriod, el proceso de descubrimiento pasará a la fase 2.

De forma predeterminada, este valor está establecido en 0, lo cual implica esperar indefinidamente.

Configuración de un descubrimiento de EMS

Configure un descubrimiento de EMS para recopilar datos de topología de Sistemas de gestión de elementos e integrar estos datos en la topología descubierta.

Acerca de esta tarea

Configure un descubrimiento de EMS de la misma forma que el descubrimiento cualquier otro tipo de red. Además de las actividades de configuración de descubrimiento estándar, deberá realizar algunas actividades de configuración de descubrimiento específicas de EMS.

Para configurar un descubrimiento de EMS, realice las siguientes actividades además de las de configuración de descubrimiento estándar:

- Configure e inicie los recopiladores de EMS
- Inicie el descubrimiento de EMS iniciando el buscador de recopiladores

Nota: Los agentes de recopilador están habilitados de forma predeterminada, por lo que se ejecutarán automáticamente cuando configure el descubrimiento basado en recopilador.

Estas actividades de configuración de descubrimiento específicas de EMS se describen en los siguientes temas.

Configuración de recopiladores

La finalidad de un recopilador es recopilar datos EMS estándar basados en las solicitudes del proceso de descubrimiento de Network Manager principal, para que los consuma el proceso de descubrimiento. La configuración del recopilador rige el modo en que el recopilador interroga el EMS, o el origen de datos, para dar servicio a las solicitudes del proceso de descubrimiento de Network Manager y el modo en que el recopilador escucha las solicitudes del proceso de descubrimiento de Network Manager.

Acerca de esta tarea

La configuración del recopilador consta de tres áreas:

- Configuración del recopilador de EMS o de orígenes de datos: estos valores definen el modo en que el recopilador interroga el EMS, o el origen de datos, para dar servicio a las solicitudes del proceso de descubrimiento de Network Manager.
- Configuración del recopilador para Network Manager: Estos valores definen cómo escucha el recopilador las solicitudes del proceso de descubrimiento de Network Manager.
- Configuraciones diversas: Estos valores son opcionales e incluyen valores, tales como la modalidad de depuración.

Normalmente estos valores de configuración se conservan en un único archivo, de forma individual para cada recopilador, en el directorio del recopilador asociado.

Los scripts y los archivos de configuración de texto sin formato de cada recopilador se conservan en un directorio independiente dentro del directorio $NCHOME/precision/collectors/, como se indica a continuación:

- Los recopiladores escritos en Java se almacenan en el directorio $NCHOME/precision/collectors/javaCollectors/.

- Los recopiladores escritos en Perl se almacenan en el directorio $NCHOME/precision/collectors/perlCollectors/.

Nota: Para que los recopiladores puedan ejecutarse de forma aislada, es decir, en otra máquina en una instalación de Network Manager, el directorio de recopilador puede moverse a esa máquina y los recopiladores pueden ejecutarse en ella, siempre que se mantenga lo siguiente:

- Para el directorio de recopilador Perl, Perl debe estar instalado en la máquina de destino.
- Para el directorio de recopilador Java, debe haber disponible una máquina virtual Java adecuada en la máquina de destino.

Los usuarios expertos pueden crear recopiladores para permitir a Network Manager interactuar con otros EMS. Los archivos ejecutables y de configuración de cada recopilador nuevo deben colocarse en un directorio con un nombre adecuado dentro de uno de los directorios listados arriba, dependiendo de si el recopilador está escrito en Java o Perl. Para obtener más información, consulte la *Guía de desarrollador de recopilador EMS*.

Configuración de recopiladores Java
Puede configurar valores genéricos para todos los recopiladores Java. También puede configurar valores específicos para cada recopilador Java.

Configuración de valores genéricos para los recopiladores Java
Puede configurar valores genéricos para todos los recopiladores Java en el archivo collector.properties genérico.

Acerca de esta tarea

Puede configurar valores genéricos para todos los recopiladores Java editando el archivo collector.properties, que se encuentra en: $NCHOME/precision/collectors/javaCollectors/framework/. El archivo utiliza la notación de par de claves-valor Java estándar, es decir, clave = valor. Utilizando este archivo, puede configurar los siguientes parámetros:

- Puerto donde se ejecutan los recopiladores Java.
- Detalles de registro de los recopiladores Java.

Archivo collector.properties de ejemplo

El siguiente fragmento de código muestra valores de ejemplo de un archivo collector.properties.

```
# Port on which to run the embedded collector server
port = 8080

# Log directory relative to the bin directory
log.directory = ../log/

# Name of the collector log file
log.filename = collector.log

# Level of logging for the collector framework
log.level = INFO

# Name of the collector log file
trace.filename = collector-trace.log

# Level of logging for the collector framework
trace.level = FINEST
```

Referencia del archivo de propiedades genérico de los recopiladores Java
Utilice esta información para entender cómo se construye el archivo de propiedades genérico de los recopiladores Java.

El archivo de propiedades genérico de los recopiladores Java contiene las propiedades que se listan en la siguiente tabla.

Tabla 28. Contenidos del archivo de propiedades genérico	
Propiedad	**Descripción**
`puerto`	Puerto donde se ejecuta el recopilador.
`log.directory`	Directorio base donde deben almacenarse los archivos de registro.
`log.filename`	Nombre del archivo de registro. También puede especificar un patrón para el nombre del archivo de registro utilizando un conjunto de elementos definidos por el sistema.
`log.level`	Una de las siguientes: • NONE • FINEST • FINER • FINE • CONFIG • INFO • AVISO • SEVERE • TODOS
`log.maxsize`	Tamaño máximo del archivo de registro. Cuando se alcanza este máximo, el archivo se redenomina y se mantiene como una copia de seguridad.
`log.count`	Número de archivos de registro de copia de seguridad que se mantienen.
`log.messageprefix`	Prefijo del mensaje de registro.
`trace.filename`	Nombre del archivo de rastreo. También puede especificar un patrón para el nombre del archivo de rastreo utilizando un conjunto de elementos definidos por el sistema.
`trace.level`	Una de las siguientes: • NONE • FINEST • FINER • FINE • CONFIG • INFO • AVISO • SEVERE • TODOS
`trace.maxsize`	Tamaño máximo del archivo de rastreo. Cuando se alcanza este máximo, el archivo se redenomina y se mantiene como una copia de seguridad.
`trace.count`	Número de archivos de rastreo de copia de seguridad que se mantienen.

Configuración de recopiladores Java individuales
Puede configurar valores específicos de cada recopilador Java editando el archivo `.properties` para el recopilador.

Configuración del recopilador Java Nokia5529Idm
Este recopilador utiliza la característica de exportación masiva de red para recuperar datos del EMS Alcatel Lucent 5529 IDM. Antes de ejecutar el recopilador Java Nokia5529Idm en un descubrimiento de red, debe copiar determinados archivos necesarios y configurar los detalles de conexión entre el EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS.

Restricción: El recopilador Java Nokia5529Idm solo es compatible con el 5529 IDM EMS en ejecución en las ediciones 9.4, 9.6.07, y 9.6.08.

Para configurar el recopilador, lleve a cabo los siguientes pasos:

Procedimiento

1. Antes de ejecutar el recopilador, copie los archivos .jar necesarios desde el EMS en el servidor en el que está instalado el recopilador:
   a) Inicie sesión en la página Esquema del IDM con las credenciales de un usuario IDM NBI.
      El URL de la página Esquema de IDM es https:// *hostname* :8443/idm/schemadoc/html/index.html, donde *hostname* es el nombre o la dirección IP del servidor de IDM.
   b) Haga clic en el URL de ejemplo del cliente y descargue el archivo `idm-oss-client.tar.gz` en el servidor en el que se ha instalado el recopilador.
   c) Descomprima el archivo.
   d) Si la versión de EMS es 9.4 o anterior, copie los siguientes archivos en el directorio `$NCHOME/precision/collectors/javaCollectors/lib`:

```
axs-mobject-remote-api-9.4-268573.jar
hornetq-core-client-2.3.1.Final-ALU-1
hornetq-jms-client-2.3.1.Final-ALU-1.jar
jaxen-1.1.jar
jboss-as-security-7.2.0.Final-ALU-8.jar
jboss-client.jar
jboss-logging-3.1.2.GA-ALU-1.jar
jboss-remoting-3.2.17.GA.jar
jdom-1.1.2-ALU-2.jar
jms-1.1.jar
log4j-1.2.13.jar
netty-3.6.2.Final-ALU-1.jar
trove-2.1.1.jar
```

   e) Si la versión de EMS es 9.6.07 o 9.6.08, copie los siguientes archivos en el directorio `$NCHOME/precision/collectors/javaCollectors/lib`:

```
axs-encription-app-9.6.07-399857.jar
jboss-logging-3.3.0.Final.jar
slf4j-simple-1.7.21.jar
axs-mobject-api-9.6.07-399857.jar
log4j-1.2.14.jar
wildfly-client-all.jar
axs-mobject-remote-api-9.6.07-399857.jar
picketbox-4.9.6.Final.jar
xbean-2.6.0.jar
idm-oss-client-1_9.6.07-399857.jar
picketbox-infinispan-4.9.6.Final.jar
```

2. Cambie al directorio del recopilador:

```
cd $NCHOME/precision/collectors/javaCollectors/Alcatel5529Idm/
```

3. En este directorio, busque el archivo de configuración de ejemplo del recopilador Java Nokia5529Idm y cópielo en el archivo de configuración de trabajo utilizando un mandato similar al siguiente ejemplo:

```
cp Alcatel5529IdmCollector.properties.sample Alcatel5529IdmCollector.properties
```

4. El archivo de configuración consta de las secciones siguientes:

   Propiedades del Recopilador
   Parámetros de configuración general para el recopilador, como el número de puerto y los detalles de registro y rastreo.

   Propiedades del origen de datos
   Detalles del EMS al que se conecta el recopilador. Utiliza los datos de estos campos para Network Manager modelar el EMS.

   Propiedades de la adquisición de datos
   Parámetros que especifican los datos a recopilar desde EMS.

   Propiedades de SOAP
   Parámetros específicos de SOAP.

   Propiedades de FTP
   Parámetros específicos de FTP.

   Propiedades de JMS
   Propiedades relacionadas con Java Messaging System.

   Fix Pack 9 **Propiedades JMS HTTPS**
   Propiedades relacionadas con la configuración JMS HTTPS.

   Propiedades de CSV
   Propiedades relacionadas con archivos de formato de valores separados por comas.

5. Configure el puerto del recopilador y los parámetros de registro y rastreo:

   puerto
   Puerto donde se ejecuta el recopilador. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8080.

   log.filename
   Nombre del archivo de registro del recopilador. También puede especificar un patrón para el nombre del archivo de registro utilizando un conjunto de elementos definidos por el sistema. El valor predeterminado es Alcatel5529IdmCollector.log.

   log.level
   Tiene uno de los valores siguientes:

   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIGINFO
   - AVISO
   - SEVERE
   - TODOS

   trace.filename
   Nombre del archivo de rastreo del recopilador . También puede especificar un patrón para el nombre del archivo de rastreo utilizando un conjunto de elementos definidos por el sistema. El valor predeterminado es Alcatel5529Collector-trace.log.

   trace.level
   Tiene uno de los valores siguientes:

   - NONE
   - FINEST

- FINER
- FINE
- CONFIGINFO
- AVISO
- SEVERE
- TODOS

6. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

   DataSource.id
   Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

   DataSource.descr
   Descripción del EMS.

   DataSource.emsName
   Nombre del EMS.

   DataSource.emsPort
   Puerto del EMS.

   DataSource.emsVersion
   Versión del EMS.

   DataSource.emsIdentifier
   Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

   DataSource.emsRole
   Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

   - desconocido
   - primary
   - backup
   - otro

   DataSource.emsStatus
   Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

   - desconocido
   - up
   - down
   - otro

7. En la sección de propiedades Adquisición de datos, configure los parámetros de adquisición de datos:

   collectData
   El valor predeterminado es `true`.

   Verdadero
   Habilita el recopilador. El recopilador recopila datos del EMS.

   Falso
   Inhabilita el recopilador. El recopilador no recopila datos del EMS.

   DataAcquisition.fullDiscoTimeout
   El número de segundos que el recopilador espera a que el EMS finalice la operación de exportación masiva de red. El valor predeterminado es 30.

8. En la sección de propiedades de SOAP, configure las propiedades de SOAP:

soap.username
Nombre de usuario para el servicio SOAP.

soap.password
Contraseña para el servicio SOAP.

soap.port
Puerto para el servicio SOAP.

soap.secure
Esta propiedad puede ser `true` o `false`. El valor predeterminado es false. Si está en true, se utiliza una conexión HTTPS segura para conectarse al EMS. Si es false, el recopilador utiliza una conexión HTTP al EMS.

jsse.httpsImpl
El nombre de la clase de implementación HTTPS. El nombre de clase predeterminado es `com.ibm.net.ssl.www2.protocol`. Esta propiedad surte efecto solo cuando la propiedad `soap.secure` se establece en `true`.

jsse.trustStore
Ruta completa al archivo trust-store. Esta propiedad surte efecto solo cuando la propiedad `soap.secure` se establece en `true`.

jsse.trustPass
Contraseña del archivo trust-store. Esta propiedad surte efecto solo cuando la propiedad `soap.secure` se establece en `true`.

Fix Pack 9 **TLSVersion**
La versión de protocolo del protocolo SSL TLS. La versión predeterminada es `TLSv1.1`. Si especifica el valor `TLSv1.2`, el recopilador usa TLS v1.2 en su lugar durante el protocolo de enlace SSL.

SSLDebugInfo
Si es `true`, la información de seguimiento del protocolo de enlace SSL se registra durante el protocolo de enlace SSL. Si es `false`, la información de depuración no se imprime. El valor predeterminado es `false`.

9. En la sección de propiedades de FTP, configure las propiedades de FTP.

ftp.host
El nombre de host o la dirección IP del servidor en el que se ejecuta el recopilador.

ftp.username
Nombre de usuario de la sesión de FTP. Este usuario debe poder iniciar sesión en el servidor y tener permisos de grabación para el directorio FTP.

ftp.password
La contraseña para el nombre de usuario especificado para la sesión de FTP.

ftp.directory
La vía de acceso completa del directorio de destino para los archivos transferidos desde el EMS. Este directorio está en el servidor en el que se está ejecutando el recopilador. El directorio predeterminado es `/tmp`.

ftp.compressed
El valor predeterminado es `false`.

Verdadero
Los archivos se transfieren en un archivo comprimido.

Falso
Los archivos no se comprimen.

10. En la sección de propiedades JMS, configure las propiedades relacionadas con Java Messaging Service:

jms.username
Nombre de usuario para el servicio JMS.

jms.password
Contraseña para el servicio JMS.

jms.topic
El nombre del tema para escuchar mensajes JMS.

jms.filter
Filtro de mensajes para procesar mensajes específicos. Déjelo en blanco para no utilizar ningún filtro.

jms.durable
Establézcalo en `true` para habilitar la suscripción duradera. El valor predeterminado es `false`.

jms.unsubscribe
Configúrelo como `true` para anular la suscripción del tema cuando se habilite la suscripción duradera. El valor predeterminado es `false`.

jms.clientId
Identificador de cliente JMS que se va a establecer para suscripciones duraderas.

jndi.properties.file
Ruta completa del archivo `jndi.properties` que contiene todas las propiedades relacionadas con JNDI. Si esta propiedad no se encuentra o no está configurada, o el archivo es incorrecto, el recopilador utilizará la configuración JNDI predeterminada. Si configura esta propiedad, establezca estas propiedades en el archivo:

java.naming.factory.initial
Especifica la fábrica de contexto inicial a utilizar. El valor de la propiedad debe ser el nombre de clase completo de la clase de fábrica que creará un contexto inicial. El valor predeterminado es `org.jboss.naming.remote.client.InitialContextFactory`.

java.naming.provider.url
Especifica la ubicación del proveedor de servicios JBoss JNDI que utilizará el cliente. La clase NamingContextFactory utiliza esta información para saber a qué servidor JBossNS conectarse. El valor de la propiedad debe ser una serie URL. El formato de este valor es `remote://`*`EMS host`*`:`*`port`*. El valor predeterminado es `remote://127.0.0.1:4447`. Cambie este valor al host y puerto EMS.

java.naming.factory.url.pkgs
Especifica la lista de prefijos de paquetes que se usarán al cargar en las fábricas de contexto de URL. El valor de la propiedad debe ser una lista de prefijos de paquete separados por dos puntos para el nombre de clase de la clase de fábrica que creará una fábrica de contexto de URL. El valor predeterminado es `org.jboss.ejb.client.naming`.

java.naming.security.principal
El principal para autenticar. Esta debe ser una serie que represente el nombre de un principal. El valor predeterminado es `admin`.

java.naming.security.credentials
Las credenciales para autenticar el principal, por ejemplo, la contraseña. El valor predeterminado es `admin`.

jnp.maxRetries
Un entero que controla el número de reintentos de conexión que se realizarán en la conexión inicial al servidor de nombres. Este parámetro solo se aplica a fallas de ConnectException. Un valor menor o igual a 1 significa que solo se hará un intento. El valor predeterminado es 5..

jnp.timeout
El tiempo de espera de conexión en milisegundos. El valor predeterminado es `30000`. Si este valor se establece en `0`(cero), la conexión se bloqueará hasta que se agote el tiempo de espera de la capa VM TCP/IP.

jnp.partitionName
Esta propiedad solo es aplicable para una configuración JNDI de clúster. Si no está utilizando una configuración JNDI de clúster, elimine esta propiedad. Especifica el nombre de la partición del clúster al que se debe restringir el descubrimiento. Si está ejecutando el producto en un entorno con varios clústeres, es posible que desee restringir el

descubrimiento de nombres a un clúster particular. No hay un valor predeterminado, lo que significa que se aceptará cualquier respuesta de clúster.

jnp.discoveryGroup
Esta propiedad solo es aplicable para una configuración JNDI de clúster. Si no está utilizando una configuración JNDI de clúster, elimine esta propiedad. La dirección IP de multidifusión a la que se envía la consulta de descubrimiento. El valor predeterminado es `228.1.2.5`.

jboss.naming.client.connect.options.org.xnio.Options.SSL_STARTTLS

Nota: Esta propiedad solo es aplicable a AMS/IDM versión 9.6 o superior. Si no está utilizando AMS/IDM versión 9.6 o superior, elimine esta propiedad del archivo.

Parámetro booleano.

jboss.naming.client.connect.options.org.xnio.Options.SASL_POLICY_NOPLAINTEXT

Nota: Esta propiedad solo es aplicable a AMS/IDM versión 9.6 o superior. Si no está utilizando AMS/IDM versión 9.6 o superior, elimine esta propiedad del archivo.

Parámetro booleano.

jboss.naming.client.remote.connectionprovider.create.options.org.xnio.Options.SSL_ENABLED

Nota: Esta propiedad solo es aplicable a AMS/IDM versión 9.6 o superior. Si no está utilizando AMS/IDM versión 9.6 o superior, elimine esta propiedad del archivo.

Parámetro booleano.

jboss.naming.client.connect.options.org.xnio.Options.SSL_PROTOCOL=

Nota: Esta propiedad solo es aplicable a AMS/IDM versión 9.6 o superior. Si no está utilizando AMS/IDM versión 9.6 o superior, elimine esta propiedad del archivo.

Especifica el protocolo que se va a utilizar. Los valores permitidos son `TLSv1.2`.

11. Configure la sección Propiedades de CSV.

    Los datos del EMS se descargará como un archivo con formato de valores separados por comas (CSV). Puede configurar qué valores del EMS para NE y NE System se exportarán a un archivo CSV. Los primeros tres valores siempre se correlacionan con el nombre de NE (o el nombre de NE System), tipo de objeto gestionado e identificador de objeto. Dado que el orden exacto de los valores restantes del archivo CSV puede variar en diferentes sistemas, debe configurar la correlación de forma que los valores se correlacionen de forma correcta con el recopilador.

    Restricción: Los valores que utilice con las siguientes variables deben coincidir exactamente con los nombres de atributos exportados por el EMS.

    csv.NE.1

    Especifica la correlación de la primera variable sin correlacionar para una línea del archivo CSV y describe un NE, es decir, la cuarta variable de la línea. Por ejemplo:

    ```
    csv.NE.1=IP Address
    ```

    csv.NE.n
    Especifica la correlación de la siguiente variable sin correlacionar, donde n es un entero que se incrementa en 1 con cada variable posterior.

    csv.NE_System.1

    Especifica la correlación de la primera variable sin correlacionar para una línea del archivo CSV y describe un NE System, es decir, la cuarta variable de la línea. Por ejemplo:

    ```
    csv.NE_System.1=Contact
    ```

csv.NE_System.n
Especifica la correlación de la siguiente variable sin correlacionar, donde n es un entero que se incrementa en 1 con cada variable posterior.

En los siguientes datos de ejemplo para un NE, el nombre de NE es ISAM123, el tipo de objeto gestionado es NE y el identificador de objeto es ISAM123.

```
ISAM123,NE,ISAM123,192.168.242.175
```

El valor 192.168.242.175 es la dirección IP. Por lo tanto, debe definir la siguiente propiedad:

```
csv.NE.1=IP Address
```

En los siguientes datos de ejemplo para un NE System, el nombre de NE System es ISAM123, el tipo de objeto gestionado es NE System y el identificador de objeto es ISAM123.

```
ISAM123,NE System,ISAM123,Mike,Main UK ISAM system,R4.5.02,,00:80:C0:52:D4:8F,
"Administrators
 office"/,3FE478262BNAA_E3.2.0.9,EX1234,LEUK,
10/9/14 3:11:26 AM
```

Para correlacionar correctamente los valores restantes, defina las siguientes propiedades:

```
csv.NE_System.1=Contact
csv.NE_System.2=Description
csv.NE_System.3=Ethernet DSL
csv.NE_System.4=ETSI Version
csv.NE_System.5=HUB MAC Address
csv.NE_System.6=Location
csv.NE_System.7=MIB Version
csv.NE_System.8=System ID
csv.NE_System.9=Type
csv.NE_System.10=Up Time
```

12. En la sección de propiedades JMS HTTPS, configure las propiedades relacionadas con el Java Messaging Service seguro:

    jms.secure
    Si es `true`, se establece la conexión JMS segura HTTPS. Si es `false`, la conexión es insegura. El valor predeterminado es `true`.

    jms.keystore
    La ruta completa al archivo trust-store. Esta propiedad surte efecto solo cuando la propiedad `soap.secure` se establece en `true`.

    jms.keypass
    Contraseña del archivo trust-store. Esta propiedad surte efecto solo cuando la propiedad `soap.secure` se establece en `true`.

    jndi.isClusterSetup
    Establézcalo en `true` si el servidor JNDI se ejecuta en modo de clúster. Establézcalo en `false` si el servidor JNDI no se ejecuta en modo de clúster. Si la versión del EMS es 9.6 o superior, establezca el valor en `false`. El valor predeterminado es `true`.
13. Guarde el archivo de configuración del recopilador.

Configuración del recopilador de Java Alcatel5620Sam
Para utilizar datos del recopilador de Java Alcatel5620Sam en un descubrimiento de red, debe copiar determinados archivo de EMS al servidor donde está instalado el recopilador, y configurar los detalles de conexión entre EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador Alcatel5620Sam Java, siga estos pasos:

Procedimiento

1. Antes de ejecutar el recopilador por primera vez, copie el archivo `/opt/5620sam/server/nms/integration/samOss.jar` desde el servidor EMS al directorio `/opt/IBM/netcool/core/precision/collectors/javaCollectors/lib/`. Debe utilizar el archivo `samOss.jar` desde la misma versión y release que el sistema Aclatel 5620.
2. Instale Oracle JRE en el servidor Alcatel 5620.
3. Cree un nuevo script para ejecutar el recopilador.
   a) Cree una copia del script `/opt/IBM/tivoli/netcool/precision/collectors/javaCollectors/bin/collector.sh` en el mismo directorio.

      Este script se utiliza para iniciar sólo el recopilador SAM 5620.

      Por ejemplo, ponga nombre al script `collectorSAM5620Java.sh`
   b) Edite el nuevo script y cambie el valor para `COLL_JAVA` para que apunte al JRE recién instalado. Por ejemplo, cambie `COLL_JAVA=$JAVA` a `COLL_JAVA=/usr/local/java/jre1.7.0_72/bin/java`
4. Cambie al directorio que contiene los archivos del recopilador.

```
cd $NCHOME/precision/collectors/javaCollectors/Alcatel5620Sam/
```

5. En este directorio, busque el archivo de configuración de ejemplo del recopilador y cópielo en el archivo de configuración de trabajo.

```
cp Alcatel5620Sam.
properties.sample
Alcatel5620Sam.
properties
```

6. Edite el archivo de configuración del recopilador:

```
$NCHOME/precision/collectors/javaCollectors/Alcatel5620Sam/Alcatel5620Sam.
properties.
```

   Este archivo contiene las siguientes secciones de configuración:

   - Propiedades del recopilador. Parámetros de configuración general para el recopilador, como el número de puerto y los detalles de registro y rastreo.
   - Propiedades de conexión de EMS. Detalles del EMS al que se conecta el recopilador. Network Manager Utiliza los datos de estos campos para modelar el EMS.
   - Propiedades HTTPS. Propiedades para la configuración de comunicación HTTPS con el EMS de SAM 5620.
   - Propiedades del FTP. Define el archivo en el servidor Network Manager en el que el EMS de SAM 5620 graba la respuesta de SOAP XML generada. Debe asegurarse de que el directorio FTP tiene permisos de lectura/escritura públicos.
   - Propiedades de la adquisición de datos. Parámetros que especifican los datos a recopilar desde EMS.

   En los pasos siguientes se muestran los parámetros configurables. Las restantes propiedades en este archivo son configuraciones basadas en el sistema recopilador y no se pueden modificar.
7. Configure el puerto del recopilador y los parámetros de registro y rastreo:

   puerto
   Puerto donde se ejecuta el recopilador. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`.

   log.filename
   Nombre del archivo de registro del recopilador. También puede especificar un patrón para el nombre del archivo de registro utilizando un conjunto de elementos definidos por el sistema.

log.level
Tiene uno de los valores siguientes:

- NONE
- FINEST
- FINER
- FINE
- CONFIGINFO
- AVISO
- SEVERE
- TODOS

log.maxsize

Tamaño máximo del archivo de registro del recopilador en MB. El valor predeterminado es 50.

log.maxcount

Número máximo de archivos de registro del recopilador generados. El valor predeterminado es 100.

trace.maxsize

Tamaño máximo del archivo de rastreo del recopilador en MB. El valor predeterminado es 50.

log.maxcount

Número máximo de archivos de rastreo del recopilador generados en MB. El valor predeterminado es 100.

trace.filename
Nombre del archivo de rastreo del recopilador . También puede especificar un patrón para el nombre del archivo de rastreo utilizando un conjunto de elementos definidos por el sistema.

trace.level
Tiene uno de los valores siguientes:

- NONE
- FINEST
- FINER
- FINE
- CONFIGINFO
- AVISO
- SEVERE
- TODOS

8. En la sección Configuración de conexión EMS, configure estos parámetros:

EmsHost
Dirección IP de host SAM 5620.

EmsPort
Puerto SAM 5620 que acepta solicitudes SOAP.

Nombre de usuario
Nombre de usuario de un usuario OSS de SAM 5620 con privilegios de Gestión de OSS.

Contraseña
Contraseña de SAM 5620, en texto sin formato. Esta propiedad sólo surte efecto si no se utiliza la propiedad `md5Password`.

Md5Password
La contraseña de SAM 5620 como hash MD5. Si se especifica `Password` y`Md5Password`, se utiliza `Md5Password`.

Secure
Si se establece en `true`, se utiliza el protocolo HTTPS para comunicarse con EMS.

9. En la sección Configuraciones de FTP, configure los siguientes parámetros:

IsRemoteFTPServer
Indica si el FTP es un servidor FTP remoto. Para utilizar el servidor FTP remoto, establezca el valor en true. El valor predeterminado es false. Si este valor se establece en true, los archivos de inventario de EMS se copian primero en el servidor FTP remoto y, a continuación, se descargan en el servidor ITNM local para su procesamiento.

FtpUsername
El nombre de usuario de FTP que se utiliza para conectarse al EMS.

FtpPassword
La contraseña de FTP que se utiliza para conectarse al EMS.

FtpHost
La dirección IP del host de Network Manager.

LocalFtpDirectory
Ruta absoluta al directorio local donde se guarda el archivo.

SecureFTP
Si es true, se utiliza SFTP

RemoteFTPDirectory
Ruta absoluta en el servidor FTP remoto, al que EMS transfiere los archivos de inventario.

Nota: Válido sólo cuando el servidor FTP no es el mismo que el servidor ITNM y está configurado como servidor remoto. Por ejemplo, `IsRemoteFTPServer` se establece en `true`.

RemoteFTPTimeout
Intervalo de tiempo de espera para el proceso FTP (en segundos). Válido sólo cuando `IsRemoteFTPServer` se establece en `true`.

10. En la sección Configuraciones de HTTPS, configure los siguientes parámetros:

HTTPSSecure
Si es `true`, se utiliza HTTPS (en lugar de HTTP) para conectarse a EMS.

TrustStore
La vía de acceso completa del archivo de almacén de confianza SAM 5620.

TrustStorePassword
La contraseña de almacén de confianza.

HTTPSPort
Puerto HTTPS para SAM 5620. El valor predeterminado es 8443.

HTTPSProtocolHandler
Gestor del protocolo de una conexión HTTPS. Dado que el SAM 5620 no admite el paquete del gestor del protocolo de IBM HTTPS, el recopilador utiliza el paquete del gestor de HTTPS de Oracle de forma predeterminada.

Fix Pack 8 **TLSVersion**
La versión de protocolo del protocolo SSL TLS. La versión predeterminada es `TLSv1.1`. Si especifica el valor `TLSv1.2`, el recopilador usa TLS v1.2 en su lugar durante el protocolo de enlace SSL.

Fix Pack 8 **SSLDebugInfo**
Si es `true`, la información de depuración SSL se imprime durante el protocolo de enlace SSL. Si es `false` , la información de depuración no se imprime. El valor predeterminado es `false`.

11. En la sección de configuración Adquisición de datos, configure los siguientes parámetros:

GetEntities

1: Habilitar
Habilita la descarga de datos de entidad física del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de entidad física del EMS.

GetVplsVpns

1: Habilitar
Habilita la descarga de datos VPN de VPLS desde EMS.

0: Inhabilitar
Inhabilita la descarga de datos VPN de VPLS desde EMS.

GetVllVpns

1: Habilitar
Habilita la descarga de datos VPN de VLL desde EMS.

0: Inhabilitar
Inhabilita la descarga de datos VPN de VLL desde EMS.

GetLayer3Vpns

1: Habilitar
Habilita la descarga de datos VPN de Capa 3 desde EMS.

0: Inhabilitar
Inhabilita la descarga de datos VPN de Capa 3 desde EMS.

GetMplsInterfaces

1: Habilitar
Habilita la descarga de datos de interfaz de MPLS desde EMS.

0: Inhabilitar
Inhabilita la descarga de datos de interfaz de MPLS desde EMS.

GetLayer2Connections

1: Habilitar
Habilita la descarga de datos de conectividad de Capa 2 de EMS.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de Capa 2 de EMS.

GetLteData

1: Habilitar
Habilita la descarga de los datos LTE desde EMS.

0: Inhabilitar
Inhabilita la descarga de los datos LTE desde EMS.

Fix Pack 8 **loadFirstRun**
Si es `true`, el recopilador consulta el EMS cuando se inicia el recopilador. Si es `false`, el recopilador consulta el EMS cuando inicia el descubrimiento de la red.

Fix Pack 8 **EntityExtendedNameRequired**

Si es `true`, `ifName` y `entityDescription` para las interfaces físicas contienen información adicional, como se muestra en los siguientes ejemplos.

```
ifName: (displayedName att value or PortName) - Mode (mode att value)
 : - Speed (speed att value) : -Encap (encapType att value) : - State
(compositeEquipmentState att value)
```

```
EntityDescription : displayedName ( bit att value) ,
(compositeEquipmentState att value) , (redundantStatus att value)
```

Si es `false`, `ifName` y `entityDescription` para las interfaces físicas no contienen información adicional. El valor predeterminado es `false`.

12. Guarde el archivo de configuración del recopilador.

Qué hacer a continuación

Utilice el script para iniciar el recopilador. Por ejemplo, utilice una línea de comandos similar a la siguiente:

```
./collectorSAM5620Java.sh -Xms512m -Xmx1024m
-jar Alcatel5620Sam/Alcatel5620SamCollector.jar
-propsFile Alcatel5620Sam/Alcatel5620Sam.properties
```

Cisco APIC REST コレクターの構成

ネットワーク・ディスカバリーで Cisco APIC REST コレクターからのデータを使用するには、Cisco Application Policy Infrastructure Controller (APIC) と Network Manager の間の接続の詳細を構成する必要があります。

このタスクについて

EMS から追加情報が収集されるよう構成することもできます。Cisco APIC REST コレクターを構成するには、以下の手順を実行します。

手順

1. Cisco APIC REST コレクター・ディレクトリーに変更します。

   ```
   cd $NCHOME/precision/collectors/javaCollectors/CiscoAPICREST/
   ```

2. このディレクトリー内で、Cisco APIC REST コレクター用のサンプル構成ファイルを見つけ、作業構成ファイルにコピーします。

   ```
   cp CiscoApicRestCollector.properties.sample CiscoApicRestCollector.properties
   ```

3. 次のコレクター構成ファイルを編集します。

   `$NCHOME/precision/collectors/javaCollectors/CiscoAPICREST/CiscoApicRestCollector.properties`.

   このファイルには、以下の構成セクションが含まれています。

   - コレクター固有のプロパティー
   - データ収集プロパティー
   - データ・ソースのプロパティー
   - REST 接続のプロパティー

   以下の手順で、構成可能パラメーターをリストします。このファイル内の残りのプロパティーは、コレクター・システム・ベースの構成であり、変更してはなりません。

4. 以下のコレクター・ポート、ならびにログおよびトレース・パラメーターを構成します。

   port
   コレクターを実行するポート。このポートは、`DiscoCollectorFinderSeeds.cfg` ファイル内の `collectorFinder.collectorRules` テーブルへの insert で構成されたポートと一致する必要があります。デフォルト値は 8080 です。

   log.filename
   コレクター・ログ・ファイルのファイル名。システムで定義された一連のエレメントを使用して、ログ・ファイル名のパターンを指定することもできます。デフォルト値は、`CiscoApicRestCollector.log` です。

   log.level
   以下の値のいずれかをとります。

- NONE
- FINEST
- FINER
- FINE
- CONFIGINFO
- WARNING
- SEVERE
- ALL

trace.filename
コレクター・トレース・ファイルのファイル名。システムで定義された一連のエレメントを使用して、トレース・ファイル名のパターンを指定することもできます。デフォルト値: `CiscoApicRestCollector-trace.log`

trace.level
以下の値のいずれかをとります。

- NONE
- FINEST
- FINER
- FINE
- CONFIGINFO
- WARNING
- SEVERE
- ALL

5. コレクターの以下のデータ収集パラメーターを構成します。

collectData
以下の値のいずれかをとります。デフォルト値は `True` です。

True
コレクターを有効にします。コレクターは、データを EMS から収集します。

False
コレクターを無効にします。コレクターは、データを EMS から収集しません。

DataAcquisition.GetEntities
以下の値のいずれかをとります。デフォルト値は 1 です。

1:Enable
EMS からの物理エンティティー・データのダウンロードを有効にします。

0:Disable
EMS からの物理エンティティー・データのダウンロードを無効にします。

DataAcquisition.GetLayer1Connections
以下の値のいずれかをとります。デフォルト値は 1 です。

1:Enable
EMS からのレイヤー 1 接続データのダウンロードを有効にします。

0:Disable
EMS からのレイヤー 1 接続データのダウンロードを無効にします。

DataAcquisition.GetLayer2Connections
以下の値のいずれかをとります。デフォルト値は 1 です。

1:Enable
EMS からのレイヤー 2 接続データのダウンロードを有効にします。

0:Disable
EMS からのレイヤー 2 接続データのダウンロードを無効にします。

DataAcquisition.GetLayer3Connections
以下の値のいずれかをとります。デフォルト値は 1 です。

1:Enable
EMS からのレイヤー 3 接続データのダウンロードを有効にします。

0:Disable
EMS からのレイヤー 3 接続データのダウンロードを無効にします。

DataAcquisition.localDataDirectory
Cisco APIC から生成される出力ファイルを保管するロケーション。ディレクトリー・ロケーションの相対パスまたは絶対パスが必要です。$NCHOME は使用できません。例えば、`/opt/IBM/netcool/core/precision/collectors/javaCollectors/CiscoAPICREST/data/` です。

6. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

DataSource.id
整数の形式での、データ・ソースの固有 ID。 このフィールドは値 1 を取り、これがプライマリー・データ・ソースであることを示します。

DataSource.descr
Cisco APIC データ・ソースの説明。

DataSource.emsHost
EMS の IP アドレスまたはホスト名。

DataSource.emsPort
EMS のポート。

DataSource.emsUserName
Cisco APIC への接続に使用するユーザー名。

DataSource.emsPassword
DataSource.emsUserName プロパティーで指定したユーザーのパスワード。

DataSource.emsName
EMS の名前。

DataSource.emsVersion
EMS のバージョン。

DataSource.emsIdentifier
EMS の ID であり、Network Manager コレクターを Netcool Configuration Manager ドライバーに統合するためのキーとなります。Cisco APIC REST コレクターでは、この ID は `ciscoapicrest` に設定する必要があります。

DataSource.emsRole
EMS の役割。このパラメーターは、以下のいずれかの値をとることができます。

- unknown
- primary
- backup
- other

DataSource.emsStatus
EMS の状況。このパラメーターは、以下のいずれかの値をとることができます。

- unknown
- up
- down
- other

7. コレクターの Web サービスおよび REST 接続のプロパティーを構成します。

enableSSL
コレクターと EMS サーバーの間の SSL 接続を有効または無効にします。このプロパティーでは、次の値を指定できます: `true` または `false`。デフォルトは `false` です。

Fix Pack 6 **TLSVersion**
TLS プロトコルのバージョン。使用可能な値は以下のとおりです。SSL, SSLv2, SSLv3, TLS, TLSv1, TLSv1.1

Fix Pack 6 **MaxBufferSize**
コレクタが処理する REST 応答の最大サイズ（MB 単位）。デフォルトは 1024 です。

keyStoreFileName

SSL クライアント証明書および信頼機関証明書が含まれる鍵ストア・ファイルの名前を指定します。

鍵ストア・ファイルは、`pathToKeyStoreFile` パラメーターで指定されているディレクトリー内に配置する必要があります。

keyStorePassword

`keyStoreFileName` プロパティーで指定した証明書にアクセスするために必要なパスワードを指定します。

pathToKeyStoreFile
`keyStoreFileName` ディレクトリーの絶対パス。ディレクトリー・ロケーションの相対パスまたは絶対パスを指定する必要があります。$NCHOME は使用できません。例えば、`/opt/IBM/netcool/core/precision/collectors/javaCollectors/CiscoApicRest/` です。

setResponseTimeout

コレクターが EMS からの応答を待機する時間 (秒単位) を指定します。この時間が経過した後、タイムアウトになります。デフォルトは、300 です。

setHttpVersion

ターゲット・システムがサポートしている HTTP プロトコルのバージョンを指定します。Cisco APIC の場合、このプロパティーは `1.0` に設定する必要があります。

setRefreshInterval

コレクターが次のログイン最新表示要求を待機する間隔 (秒単位) を指定します。Cisco APIC セッションのタイムアウト期間は 300 秒 (つまり 5 分) であるため、この値は 300 未満にする必要があります。デフォルトは 180 です。

ヒント: ネットワークにパフォーマンスまたは安定性の問題がある場合、180 よりも小さいに値に設定してください。

8. コレクター構成ファイルを保存します。
9. オプション: コレクターと Network Manager の間で SSL をセットアップします。
   a) Cisco APIC サーバーの管理者から必要な SSL 証明書および信頼機関証明書を入手します。
   b) これらの証明書をローカル Java 鍵ストアに追加して、KeyStore プロパティーで参照できるようにします。
   c) サーバーからの鍵と証明書が別々のファイル内にある場合、それらのファイルを結合して、新しい鍵ストアにロードするための単一の PKCS12 フォーマットのファイルにする必要があります。サーバー証明書を PKCS12 フォーマットに変換するには、以下の OpenSSL ツールキット・コマンドを使用します。

```
openssl pkcs12 -export -inkey key_file-in cert_file-out cert_pkcs12
```

   ここに、`key_file` はサーバーから取得した鍵ファイルで、`cert_file` はサーバーから取得した証明書です。`cert_pkcs12` は、鍵ストアにロードするための PKCS12 フォーマットの結合ファイルです。
10. Keytool ユーティリティーを 使用して Java 鍵ストアを作成するには、以下の手順に従います。
    a) 次のコマンドを使用して、鍵ストアおよび自己署名証明書を生成します。

```
keytool -genkey -keyalg RSA -alias alias_name -keystore keystore_file
 -storepass keystore_password -validity 360 -keysize 2048
```

b) 次のコマンドを使用して、Cisco APIC から新しく作成した Java 鍵ストア・ファイルに SSL 証明書をインポートします。

```
keytool -import -trustcacerts -alias alias_name -file cert_file
 -keystore keystore_file
```

c) 次のコマンドを使用して、証明書が Java 鍵ストア内にあることを確認します。

```
keytool -list -v -keystore keystore_file
```

d) コレクターのプロパティー・ファイルで keyStoreFileName プロパティーおよび keyStorePassword プロパティーを設定します。

e) コレクターのプロパティー・ファイルで enableSSL プロパティーを true に設定します。

f) Fix Pack 6
必要に応じて、コレクタ・プロパティファイルで TLSVersion プロパティを設定します。

g) コレクターのプロパティー・ファイルで DataSource.emsPort プロパティーが HTTPS ポートに設定されていることを確認します。

h) 生成した鍵ストア・ファイルを、pathToKeyStoreFile プロパティーで指定されているディレクトリーにコピーします。

タスクの結果

コレクターは、取得したデータを .xml ファイルおよび .json ファイルとして $NCHOME/precision/collectors/javaCollectors/CiscoAPICREST/data/ディレクトリーに保管します。このディレクトリー内にファイルを作成するための適切な権限が必要です。

Configuración del recopilador CiscoWorks LMS

Para utilizar datos del recopilador CiscoWorks LMS en un descubrimiento de red, debe configurar los detalles de conexión entre el CiscoWorks LMS EMS y Network Manager.

Antes de empezar

Para habilitar la integración del recopilador CiscoWorks LMS de Network Manager con CiscoWorks LMS EMS, primero debe copiar el controlador JDBC. Para ello, sujeto a la comprobación de que tiene la autorización o el permiso necesario, copie manualmente la biblioteca jconn2.jar desde el servidor CiscoLMS en el directorio de la biblioteca de recopilador Network ManagerJava en $NCHOME$NCHOME/precision/collectors/javaCollectors/lib.

Nota: De forma predeterminada, la ubicación de jconn2.jar en el servidor Cisco LMS EMS es /opt/CSCOpx/lib/classpath.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador CiscoWorks LMS, siga estos pasos:

Para utilizar datos del recopilador CiscoWorks LMS en un descubrimiento de red, debe configurar los parámetros del esquema de base de datos abierto de Cisco y el motor de extracción de datos de Cisco para la comunicación entre CiscoWorks LMS EMS y Network Manager.

Procedimiento

1. Cambie al directorio del recopilador CiscoWorks LMS.

```
cd $NCHOME/precision/collectors/javaCollectors/CiscoLMS/
```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador CiscoWorks LMS y cópielo en el archivo de configuración de trabajo.

```
cp CiscoLMSCollector.properties.sampleCiscoLMSCollector.properties
```

3. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/javaCollectors/CiscoLMS/CiscoLMSCollector.properties`.
   Este archivo contiene las siguientes secciones de configuración:
   - Una sección que contiene parámetros para la interfaz del esquema de base de datos abierto de Cisco y el motor de extracción de datos de Cisco. Esta sección también contiene valores de distintivo de adquisición de datos.
   - Una sección de configuración del sistema.

   En los pasos siguientes se muestran los parámetros configurables. Las restantes propiedades en este archivo son configuraciones basadas en el sistema recopilador y no se pueden modificar.
4. Configure el puerto del recopilador y los parámetros de registro y rastreo:

   puerto
   Puerto donde se ejecuta el recopilador. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`.

   log.filename
   Nombre del archivo de registro del recopilador CiscoWorks LMS. También puede especificar un patrón para el nombre del archivo de registro utilizando un conjunto de elementos definidos por el sistema.

   log.level
   Tiene uno de los valores siguientes:
   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIGINFO
   - AVISO
   - SEVERE
   - TODOS

   trace.filename
   Nombre del archivo de rastreo del recopilador CiscoWorks LMS. También puede especificar un patrón para el nombre del archivo de rastreo utilizando un conjunto de elementos definidos por el sistema.

   trace.level
   Tiene uno de los valores siguientes:
   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIGINFO
   - AVISO
   - SEVERE
   - TODOS
5. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

DataSource.id
Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

DataSource.descr
Descripción del EMS.

DataSource.emsName
Nombre del EMS.

DataSource.emsPort
Puerto del EMS.

DataSource.emsVersion
Versión del EMS.

DataSource.emsIdentifier
Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

DataSource.emsRole
Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- primary
- backup
- otro

DataSource.emsStatus
Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- up
- down
- otro

6. Configure los parámetros para la interfaz de la base de datos de Cisco LMS:

DB.Host
La dirección IP o el nombre de host de la base de datos Cisco LMS.

DB.Port
Número de puerto de la base de datos. El valor predeterminado es 43455.

DB.DbName
Nombre del esquema de la base de datos Cisco LMS (esquema de base de datos). El valor predeterminado es rmengdb.

DB.UserName
Nombre de usuario utilizado para conectarse a la base de datos. El valor predeterminado es lmsdatafeed.

DB.Password
Contraseña utilizada para conectarse a la base de datos. El valor predeterminado es lmsdatafeed.

7. Configure los parámetros para la interfaz del motor de extracción de datos de Cisco:

webservice.host
La dirección IP o el nombre de host del motor de extracción de datos de Cisco.

webservice.port
Puerto del motor de extracción de datos de Cisco. El valor predeterminado es 1741.

webservice.servicename
Servicio web del motor de extracción de datos de Cisco. El valor predeterminado es `/campus/servlet/CMExportServlet`.

webservice.username
Nombre de usuario del motor de extracción de datos de Cisco. El valor predeterminado es admin.

webservice.password
Contraseña de usuario del motor de extracción de datos de Cisco. El valor predeterminado es admin.

8. Configure los parámetros de proceso de datos para el motor de extracción de datos de Cisco.

   A veces, el motor de extracción de datos de Cisco puede generar archivos XML de gran tamaño para la topología de capa 2. Para poder gestionar el proceso XML, el recopilador CiscoWorks LMS tiene la capacidad de leer el sobre XML del motor de extracción de datos de Cisco y procesarlo inmediatamente, o ponerlo en spool en un archivo sin formato para su proceso posterior. De forma predeterminada, el recopilador lee el sobre Cisco en el motor de extracción de datos de Cisco y lo procesa inmediatamente.

   Los parámetros del motor de extracción de datos de Cisco son los siguientes:

   L2TopologyXML.inputStreamEnable
   Tiene uno de los valores siguientes:

   1: Habilitar
   El recopilador lee la corriente de entrada y utiliza el sobre XML.

   0: Inhabilitar
   El recopilador lee la corriente de entrada, pone en spool el sobre XML en un archivo y utiliza el sobre XML.

   L2TopologyXML.outputdirectory
   El directorio de salida del sobre XML en spool si `L2TopologyXML.inputStreamEnable = 1`. El valor predeterminado es `../CiscoLMS/tmp`.

   L2TopologyXML.outputfilename
   El archivo de salida del sobre XML en spool si `L2TopologyXML.inputStreamEnable = 1`. El valor predeterminado es `output.xml`.

9. Configure los parámetros de adquisición de datos para el recopilador:

   collectData
   Tiene uno de los valores siguientes. El valor predeterminado es `True`.

   Verdadero
   Habilita el recopilador. El recopilador recopila datos del CiscoWorks LMS EMS.

   Falso
   Inhabilita el recopilador. El recopilador no recopila datos del CiscoWorks LMS EMS.

   DataAcquisition.GetEntities
   Tiene uno de los valores siguientes. El valor predeterminado es 1.

   1: Habilitar
   Habilita la descarga de datos de entidad física del CiscoWorks LMS EMS.

   0: Inhabilitar
   Inhabilita la descarga de datos de entidad física del CiscoWorks LMS EMS.

   DataAcquisition.GetLayer2Connections
   Tiene uno de los valores siguientes. El valor predeterminado es 1.

   1: Habilitar
   Habilita la descarga de datos de conectividad de capa 2 del CiscoWorks LMS EMS.

   0: Inhabilitar
   Inhabilita la descarga de datos de conectividad de capa 2 del CiscoWorks LMS EMS.

10. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Huawei M2000
Para utilizar datos procedentes del recopilador Huawei M2000 en un descubrimiento de red, debe configurar el recopilador para procesar los archivos XML.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador Huawei M2000, siga estos pasos:

Procedimiento

1. Cambie al directorio del recopilador Huawei M2000.

   ```
   cd $NCHOME/precision/collectors/javaCollectors/HuaweiM2K/
   ```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador y cópielo en el archivo de configuración de trabajo.

   ```
   cp HuaweiM2KCollector.properties.sample HuaweiM2KCollector.properties
   ```

3. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/javaCollectors/HuaweiM2K/HuaweiM2KCollector.properties`.

   El archivo incluye las secciones siguientes:

   Propiedades del Recopilador
   Parámetros de configuración general para el recopilador, como el número de puerto y los detalles de registro y rastreo.

   Propiedades del origen de datos
   Detalles del EMS al que se conecta el recopilador. Network Manager Utiliza los datos de estos campos para modelar el EMS.

   Propiedades de la adquisición de datos
   Parámetros que especifican los datos a recopilar desde EMS.

   Propiedades de proceso de archivos
   Parámetros que especifican las opciones para el proceso de archivos.

4. En la sección de propiedades del recopilador, configure las propiedades generales del recopilador:

   puerto
   Puerto donde se ejecuta el servidor del recopilador incorporado. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8080.

   log.filename
   Nombre del archivo de registro del recopilador Huawei M2000. El valor predeterminado es `HuaweiM2KCollector.log`.

   log.level
   Nivel de registro del marco del recopilador. El nivel de registro adopta uno de los siguientes valores:

   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIG
   - INFO
   - AVISO
   - SEVERE
   - TODOS

   El valor predeterminado es INFO.

trace.filename
Nombre del archivo de rastreo del recopilador Huawei M2000. El valor predeterminado es `HuaweiM2KCollector-trace.log`.

trace.level
Nivel de rastreo del marco del recopilador. El valor predeterminado es INFO.

5. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

   DataSource.id
   Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

   DataSource.descr
   Descripción del EMS.

   DataSource.emsName
   Nombre del EMS.

   DataSource.emsVersion
   Versión del EMS.

   DataSource.emsIdentifier
   Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

   DataSource.emsRole
   Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

   - desconocido
   - primary
   - backup
   - otro

   DataSource.emsStatus
   Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

   - desconocido
   - up
   - down
   - otro

6. En la sección de propiedades Adquisición de datos, configure los parámetros de adquisición de datos:

   collectData
   Establézcalo en `true` para adquirir datos o en `false` para no adquirirlos.

   DataAcquisition.GetEntities
   Tiene uno de los valores siguientes. El valor predeterminado es `0`.

   1: Habilitar
   Habilita el descubrimiento de datos de entidad física del archivo XML.

   0: Inhabilitar
   Inhabilita el descubrimiento de datos de entidad física del archivo XML.

7. En la sección de propiedades del proceso de archivos, configure parámetros de proceso de archivos:

   file.localDirectory
   El directorio local donde están ubicados los archivos que va a procesar el recopilador. Especifique la vía de acceso completa a la ubicación del directorio.

8. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Huawei CORBA TMF 814
Para utilizar datos del recopilador Huawei CORBA TMF 814 en un descubrimiento de red, debe configurar los detalles de conexión entre el Huawei CORBA TMF EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador Huawei CORBA TMF 814, lleve a cabo los siguientes pasos:

Procedimiento

1. Cambie al directorio del recopilador Huawei CORBA TMF 814.

   ```
   cd $NCHOME/precision/collectors/javaCollectors/HuaweiCorbaTMF814/
   ```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador Huawei CORBA TMF 814 y cópielo en el archivo de configuración de trabajo.

   ```
   cp HuaweiCorbaTMF814Collector.properties.sample
   HuaweiCorbaTMF814Collector.properties
   ```

3. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/javaCollectors/HuaweiCorbaTMF814/HuaweiCorbaTMF814Collector.properties`.

   El archivo se compone de las secciones siguientes:

   Propiedades del Recopilador
   Parámetros de configuración general para el recopilador, como el número de puerto y los detalles de registro y rastreo.

   Propiedades del origen de datos
   Detalles del EMS al que se conecta el recopilador. Network Manager Utiliza los datos de estos campos para modelar el EMS.

   Propiedades de la adquisición de datos
   Parámetros que especifican los datos a recopilar desde EMS.

   Propiedades de inicialización de ORB
   Parámetros específicos de ORB de CORBA.

   Propiedades de NameService
   Parámetros del servicio de nombres.

   Propiedades de EmsSessionFactory
   Parámetros que especifican la forma en la que el recopilador debe obtener la referencia del objeto EMSSessionFactory.

   Propiedades del gestor
   Parámetros que especifican los nombres de las interfaces del gestor.

   Propiedades del iterador
   Parámetros que definen el comportamiento del iterador de CORBA.

   Propiedades de filtrado
   Parámetros que definen los dispositivos que se deben excluir del procesamiento.

4. En la sección de propiedades del recopilador, configure las propiedades generales del recopilador:

   puerto
   Puerto donde se ejecuta el servidor del recopilador incorporado. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8080.

   log.filename
   Nombre del archivo de registro Huawei CORBA TMF 814del recopilador. El valor predeterminado es `HuaweiCorbaTMF814Collector.log`.

log.level
Nivel de registro del marco del recopilador. El valor predeterminado es INFO.

trace.filename
Nombre del archivo de rastreo del recopilador Huawei CORBA TMF 814. El valor predeterminado es `HuaweiCorbaTMF814Collector-trace.log`.

trace.level
Nivel de rastreo del marco del recopilador. El valor predeterminado es INFO.

5. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

DataSource.id
Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

DataSource.descr
Descripción del EMS.

DataSource.emsHost
Nombre de host del EMS.

DataSource.emsName
Nombre del EMS.

DataSource.emsPort
Puerto del EMS.

DataSource.emsVersion
Versión del EMS.

DataSource.emsIdentifier
Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

DataSource.emsRole
Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- primary
- backup
- otro

DataSource.emsStatus
Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- up
- down
- otro

DataSource.emsUserName
Nombre de usuario del EMS.

DataSource.emsPassword
Contraseña del EMS.

Nota: Los campos DataSource.emsHost y DataSource.emsPort son obligatorios si la variable `nameService.useNameService` es TRUE.

6. En la sección de propiedades Adquisición de datos, configure los parámetros de adquisición de datos:

collectData
Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
Habilita el recopilador. El recopilador recopila datos del EMS.

Falso
Inhabilita el recopilador. El recopilador no recopila datos del EMS.

DataAcquisition.GetEntities
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de datos de entidad física del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de entidad física del EMS.

Fix Pack 2 **DataAcquisition.GetEquipmentAdditionalInfo**
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de información adicional sobre los equipos desde el EMS.

0: Inhabilitar
Inhabilita la descarga de información adicional sobre los equipos desde el EMS.

DataAcquisition.GetCTPs
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de los datos ConnectionTP desde EMS.

0: Inhabilitar
Inhabilita la descarga de los datos ConnectionTP desde EMS.

DataAcquisition.GetTopoLinks
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de la conectividad de enlace topológica de capa 1 del EMS.

0: Inhabilitar
Inhabilita la descarga de la conectividad de enlace topológica de capa 1 del EMS.

DataAcquisition.GetSNCs
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita el descubrimiento de la conectividad de conexiones de subred de capa 1.

0: Inhabilitar
Inhabilita el descubrimiento de la conectividad de conexiones de subred de capa 1.

7. En la sección de propiedades de Inicialización de ORB, no modifique las siguientes propiedades de inicialización de ORB a menos que se lo indique el soporte de IBM:

orbProp.1.name=org.omg.CORBA.ORBClass
orbProp.1.value=com.ibm.CORBA.iiop.ORB
Especifica la implementación de IBM ORB que se va a activar.

orbProp.2.name=org.omg.CORBA.ORBSingletonClass
orbProp.2.value=com.ibm.rmi.corba.ORBSingleton
Especifica la implementación de IBM ORB que se va a activar.

orbProp.3.name=com.ibm.CORBA.Debug.Output
orbProp.3.value=../log/orbtrc.log
Especifica el archivo de registro donde se van a escribir los mensajes de error del ORB cuando el recopilador no puede conectarse al servicio CORBA en el EMS.

8. En la sección de propiedades NameService, configure las propiedades del servicio de denominación:

nameService.useNameService
Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
El recopilador obtiene la referencia de contexto de denominación raíz cuando accede al servicio de denominación utilizando un URL corbaloc

Falso
El recopilador obtiene la referencia de contexto de denominación raíz del archivo IOR especificado y omite el servicio de denominación.

nameService.iorFile
La vía de acceso completa del archivo IOR que contiene la referencia NameService. Da soporte a la vía de acceso local y la vía de acceso remota; por ejemplo, HTTP y FTP.

nameService.nameServiceName
Nombre de servicio del servicio de denominación.

9. En la sección de propiedades de EmsSessionFactory, configure las propiedades de EmsSessionFactory:

emsSessionFactory.useNameService
Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
El recopilador obtiene la referencia EmsSessionFactory_I utilizando el servicio de denominación y resolviendo las propiedades de contexto de denominación especificadas.

Falso
El recopilador obtiene la referencia EmsSessionFactory_I del archivo IOR especificado y omite el servicio de denominación.

emsSessionFactory.iorFile
Vía de acceso completa del archivo IOR que contiene la referencia EmsSessionFactory. Da soporte a la vía de acceso local y la vía de acceso remota; por ejemplo, HTTP y FTP.

emsSessionFactory.namingContext.*
Las propiedades de contexto de denominación representan los enlaces de contexto de denominación para resolver la referencia EmsSessionFactory del servicio de denominación. Todas las entradas deben estar en pares *.id y *.kind y especificarse en la secuencia correcta para que la referencia EmsSessionFactory pueda resolverse correctamente.

10. En la sección de propiedades de Gestor, configure las propiedades del gestor:

manager.emsMgr
Nombre de la interfaz de EMSMgr. El valor predeterminado es `EMS`.

manager.equipmentInventoryMgr
Nombre de la interfaz de EquipmentInventoryMgr. El valor predeterminado es `EquipmentInventory`.

manager.managedElementMgr
Nombre de la interfaz de ManagedElementMgr. El valor predeterminado es `ManagedElement`.

manager.multiLayerSubnetworkMgr
Nombre de la interfaz de MultiLayerSubnetworkMgr. El valor predeterminado es `MultiLayerSubnetwork`.

11. En la sección de propiedades del Iterador, configure las propiedades del iterador de CORBA:

iterator.resultSize
Especifica el número máximo de resultados devueltos para cada conjunto por el iterador CORBA. El valor predeterminado es 20. Aumente este valor si desea disminuir el número de iteraciones y aumentar el tamaño de la respuesta de datos del EMS.

iterator.destroyIterator
Establézcala en true si desea que el iterador CORBA destruya el objeto de iterador correspondiente en el lado del EMS. El valor predeterminado es `false`. Habilite esta propiedad sólo si el EMS no realiza automáticamente la recogida de basura de memoria.

12. En la sección de propiedades del filtrado, configure las propiedades de filtrado de dispositivos:

filter.enabled
Tiene uno de los valores siguientes:

- True: el filtro está habilitado; el recopilador excluirá dispositivos que tengan especificada la propiedad filter.productName.
- False: el filtro está inhabilitado. Este es el valor predeterminado.

filter.productName
Especifique aquí el modelo o tipo de dispositivo a excluir del procesamiento. Esta propiedad no tiene un valor predeterminado, y podría dejarse en blanco. Para varias entradas, separe los nombres de producto con comas. Por ejemplo;

```
filter.productName=Virtual NE,OptiX OSN 7500,OptiX DWDM OADM
```

Durante el procesamiento, los valores especificados en la propiedad filter.productName se comparan con el contenido del campo entityData.Description.

13. Guarde el archivo de configuración del recopilador.

Configuración del recopilador MTOSISoap
Para utilizar datos desde el recopilador MTOSISoap en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador MTOSISoap, lleve a cabo los siguientes pasos:

Procedimiento

1. Cambie al directorio del recopilador MTOSISoap.

```
cd $NCHOME/precision/collectors/javaCollectors/MTOSISoap/
```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador MTOSISoap y cópielo en el archivo de configuración de trabajo.

```
cp MTOSISoapCollector.properties.sample
MTOSISoapCollector.properties
```

3. Edite el archivo de configuración del recopilador:
`$NCHOME/precision/collectors/javaCollectors/MTOSISoap/MTOSISoapCollector.properties`.

   El archivo incluye las secciones siguientes:

   Propiedades del Recopilador
   Parámetros de configuración general para el recopilador, como el número de puerto y los detalles de registro y rastreo.

   Propiedades de la adquisición de datos
   Parámetros que especifican los datos a recopilar desde EMS.

   Propiedades del origen de datos
   Detalles del EMS al que se conecta el recopilador. Utiliza los datos de estos campos para Network Manager modelar el EMS.

4. En la sección de propiedades del recopilador, configure las propiedades generales del recopilador:

   puerto
   Puerto donde se ejecuta el servidor del recopilador incorporado. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8080.

log.filename
Nombre del archivo de registro MTOSISoapdel recopilador. El valor predeterminado es `MTOSISoapCollector.log`.

log.level
Nivel de registro del marco del recopilador. El nivel de registro adopta uno de los siguientes valores:

- NONE
- FINEST
- FINER
- FINE
- CONFIG
- INFO
- AVISO
- SEVERE
- TODOS

El valor predeterminado es INFO.

trace.filename
Nombre del archivo de rastreo del recopilador MTOSISoap. El valor predeterminado es `MTOSISoapCollector-trace.log`.

trace.level
Nivel de rastreo del marco del recopilador. El valor predeterminado es INFO.

5. En la sección de propiedades Adquisición de datos, configure los parámetros de adquisición de datos:

collectData
Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
Habilita el recopilador. El recopilador recopila datos del EMS.

Falso
Inhabilita el recopilador. El recopilador no recopila datos del EMS.

DataAcquisition.MSLN
El valor de la subred multicapa de EMS. El valor predeterminado es 1.

DataAcquisition.ManagementDomain
Nombre del dominio de gestión del EMS. El valor predeterminado es `Huawei/U2000`.

DataAcquisition.ManagedElementsBatchSize
Define el número máximo de objetos MTOSI que pueden incluirse en una respuesta SOAP EMS para una ManagedElementsRequest. El valor predeterminado es de 4500 objetos.

Nota: Debe establecer los parámetros `DataAcquisition.ManagedElementsBatchSize` y `DataAcquisition.TopologicalLinksBatchSize` en valores que sean menores que el número de elementos en el EMS. De lo contrario, el descubrimiento falla y verá este error en los registros de descubrimiento:

```
Register Iterator faild.The number of Active Iterators is more than allowed!
```

DataAcquisition.TopologicalLinksBatchSize
Define el número máximo de objetos MTOSI que pueden incluirse en una respuesta SOAP EMS para una TopologicalLinkRequest. El valor predeterminado es de 6000 objetos.

Nota: Debe establecer los parámetros `DataAcquisition.ManagedElementsBatchSize` y `DataAcquisition.TopologicalLinksBatchSize` en valores que sean menores que el

número de elementos en el EMS. De lo contrario, el descubrimiento falla y verá este error en los registros de descubrimiento:

```
Register Iterator faild.The number of Active Iterators is more than allowed!
```

DataAcquisition.GetEntities
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de datos de entidad física del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de entidad física del EMS.

DataAcquisition.GetLayer2Connections
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 2 del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 2 del EMS.

DataAcquisition.GetLayer3Connections
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 3 del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 3 del EMS.

Fix Pack 4 **DataAcquisition.receiveTimeout**
El tiempo máximo en segundos para esperar una respuesta del EMS. El valor predeterminado es 300 segundos.

6. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

DataSource.id
Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

DataSource.descr
Descripción del EMS.

DataSource.emsHost
Nombre de host del EMS.

DataSource.emsName
Nombre del EMS.

DataSource.emsPort
Puerto del EMS.

DataSource.emsVersion
Versión del EMS.

DataSource.emsIdentifier
Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

DataSource.emsRole
Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- primary
- backup

- otro

DataSource.emsStatus
Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- up
- down
- otro

DataSource.emsUserName
Nombre de usuario del EMS.

DataSource.emsPassword
Contraseña del EMS.

7. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Nokia Solutions and Networks NetAct XML Interface for Configuration Management
El recopilador Nokia Solutions and Networks (NSN) NetAct XML Interface for Configuration Management procesa datos 2G, 3G y LTE RAN utilizando el archivo XML de gestión de la configuración para NSN NetAct EMS. Este archivo XML contiene los datos de configuración de red de NetAct Configurator, en formato RAML/CM2.

Acerca de esta tarea

El recopilador puede recuperar el archivo XML de gestión de la configuración para el NSN NetAct EMS de una de las maneras siguientes:

- Conectándose a NSN NetAct EMS. En este caso, el recopilador utiliza FTP o SFTP. Por lo tanto, si desea utilizar este método, debe configurar el archivo de propiedades del recopilador con los detalles de conexión FTP y SFTP entre NSN NetAct EMS y Network Manager.
- Accediendo al archivo XML en un directorio local designado. Si desea utilizar este método, debe especificar el directorio local que va a contener los archivos XML recuperados del EMS.

En cualquier caso, debe configurar las propiedades de adquisición de datos relevantes dentro del archivo de configuración del recopilador, tal como se especifica en el procedimiento siguiente.

Nota: El recopilador almacena la indicación de fecha y hora del sistema operativo de cada archivo XML procesado. Si, durante un descubrimiento, el recopilador detecta que la indicación de fecha y hora de la última modificación del archivo XML actual es la misma que la indicación de fecha y hora registrada durante el último descubrimiento, el archivo no se procesa. Esto garantiza que sólo se procesan los archivos que contienen datos de dispositivos actualizados desde el último descubrimiento.

Para configurar el recopilador NetAct XML Interface for Configuration Management, realice los pasos siguientes:

Procedimiento

1. Cambie al directorio del recopilador NSN NetAct XML Interface for Configuration Management.

```
cd $NCHOME/precision/collectors/javaCollectors/NetActCMDump/
```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador y cópielo en el archivo de configuración de trabajo.

```
cp NetActCMDumpCollector.properties.sample NetActCMDumpCollector.properties
```

3. Edite el archivo de configuración del recopilador:
`$NCHOME/precision/collectors/javaCollectors/NetActCMDump/NetActCMDumpCollector.properties`.

Este archivo contiene las siguientes secciones de configuración:

- Propiedades de configuración del recopilador
- Propiedades de adquisición de datos
- Propiedades del origen de datos

Nota: En los pasos siguientes se muestran los parámetros configurables. Las restantes propiedades en este archivo son valores de configuración basados en el sistema recopilador y no se pueden modificar.

4. Configure las siguientes propiedades del recopilador:

   puerto
   Puerto donde se ejecuta el recopilador. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8080.

   log.filename
   Nombre del archivo de registro del recopilador. También puede especificar un patrón para el nombre del archivo de registro utilizando un conjunto de elementos definidos por el sistema.

   log.level
   Nivel de registro del marco del recopilador. Tiene uno de los valores siguientes:

   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIGINFO
   - AVISO
   - SEVERE
   - TODOS

   El valor predeterminado es INFO.

   trace.filename
   Nombre del archivo de rastreo del recopilador . También puede especificar un patrón para el nombre del archivo de rastreo utilizando un conjunto de elementos definidos por el sistema.

   trace.level
   Nivel de rastreo del marco del recopilador. Tiene uno de los valores siguientes:

   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIGINFO
   - AVISO
   - SEVERE
   - TODOS

   El valor predeterminado es INFO.

5. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

   DataSource.id
   Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

DataSource.descr
Descripción del EMS.

DataSource.emsHost
Nombre de host del EMS.

DataSource.emsName
Nombre del EMS.

DataSource.emsPort
Puerto del EMS.

DataSource.emsVersion
Versión del EMS.

DataSource.emsIdentifier
Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

DataSource.emsRole
Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- primary
- backup
- otro

DataSource.emsStatus
Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- up
- down
- otro

DataSource.emsUserName
Nombre de usuario del EMS.

DataSource.emsPassword
Contraseña del EMS.

6. Configure los parámetros de adquisición de datos para el recopilador:

collectData
Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
Habilita el recopilador. El recopilador recopila datos del EMS.

Falso
Inhabilita el recopilador. El recopilador no recopila datos del EMS.

DataAcquisition.GetEntities
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de datos de entidad física del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de entidad física del EMS.

DataAcquisition.getRanTopology
Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Habilita la descarga de los datos de conectividad RAN para Net Act EMS.

0: Inhabilitar
Inhabilita la descarga de los datos de conectividad RAN para Net Act EMS.

DataAcquisition.localDataDirectory
Especifica la ubicación de los archivos XML recuperados del EMS.

DataAcquisition.postProcessFlag
Define la forma en la que el recopilador gestiona el archivo de datos tras el procesamiento. El valor predeterminado es 0.

0: Suprimir
Suprime el archivo XML tras el procesamiento.

1: Mover
Mueve el archivo XML tras el procesamiento. Se utiliza junto con el parámetro DataAcquisition.moveLocation.

2: Dejar
Deja el archivo XML en el directorio de datos tras el procesamiento. Se utiliza junto con el parámetro DataAcquisition.localDataDirectory.

DataAcquisition.moveLocation
Especifica la ubicación de los archivos que se van a mover después del proceso. Este parámetro sólo es efectivo si la variable DataAcquisition.postProcessFlag tiene el valor 1.

DataAcquisition.loadFirstRun
Define si se procesan archivos XML en el directorio de datos locales XML al iniciar el recopilador, sin esperar la llamada XML-RPC desde la GUI.

0
No procesar el directorio de datos al iniciar el recopilador. Otros valores procesarán el directorio de datos inmediatamente.

1
Procesar el directorio de datos al iniciar el recopilador.

DataAcquisition.downloadFile
Define si se debe descargar el archivo XML mediante FTP o SFTP (FTP seguro) del EMS en el momento del descubrimiento.

0
No descargar.

1
Descargar.

El valor predeterminado es 1.

DataAcquisition.maskCredentials
Define si aplicar máscara a las credenciales de usuario en el registro cuando se emite un mandato de FTP o SFTP para transferir el archivo XML desde el EMS.

0
No usar máscara para las credenciales.

1
Utilizar máscara para las credenciales.

DataAcquisition.remoteFtpHost
Nombre de host o IP del EMS en la que se generan los datos XML.

DataAcquisition.remoteDir
Directorio remoto que contiene el archivo o archivos a procesar.

DataAcquisition.remoteFile
Nombre del archivo XML que contiene los datos de CM. Si se recuperan archivos mediante FTP o SFTP, establezca esta propiedad en un carácter comodín, como `*.xml` o `*.xml.gz`.

Nota: Si el directorio remoto se ha configurado utilizando la propiedad DataAcquisition.remoteDir contiene más que el archivo actual, ha establecido DataAcquisition.remoteFile como carácter

comodín, todos los archivos que coincidan con el carácter comodín se transferirán desde el directorio remoto y se procesarán. Para impedir que el recopilador recupere todos los archivos procesados con anterioridad, el directorio remoto sólo debe tener el archivo o archivos XML más recientes a procesar.

DataAcquisition.remoteFtpUser
Nombre de usuario a utilizar para la conexión FTP o SFTP.

DataAcquisition.remoteFtpPassword
Contraseña a utilizar para la conexión FTP o SFTP.

DataAcquisition.remoteFtpPort
Puerto a utilizar para la conexión FTP o SFTP.

DataAcquisition.secureConnection
Indica si se debe utilizar una conexión segura (SFTP) al recuperar los archivos cmdump.

1
Utilizar SFTP para conectar al EMS.

0
Utilizar FTP para conectar al EMS.

El valor predeterminado es 0.

DataAcquisition.ftpTimeout
El intervalo de tiempo de espera para el proceso FTP.

DataAcquisition.technologyType
Tecnología móvil que gestionará el recopilador. Las opciones disponibles son las siguientes:

- 2G3G
- LTE
- TODOS

El valor predeterminado 2G3G.

7. Guarde el archivo de configuración del recopilador.

Fix Pack 6 *Configuración del recopilador de Java NokiaOMS1350*

Este recopilador recupera datos de EMS de Nokia OMS 1350. Antes de ejecutar el recopilador en un descubrimiento de red, es necesario copiar algunos archivos requeridos y configurar los detalles de conexión entre EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS.

Para configurar el recopilador, lleve a cabo los siguientes pasos:

Procedimiento

1. Cambie al directorio del recopilador:

```
cd $NCHOME/precision/collectors/javaCollectors/NokiaOMS1350/
```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador y cópielo en el archivo de configuración de trabajo utilizando un mandato similar al siguiente ejemplo:

```
cp NokiaOMS1350RestCollector.properties.sample NokiaOMS1350RestCollector.properties
```

3. El archivo de configuración consta de las secciones siguientes:

Propiedades del Recopilador
Parámetros de configuración general para el recopilador, como el número de puerto y los detalles de registro y rastreo.

Propiedades de la adquisición de datos
Parámetros que especifican los datos a recopilar desde EMS.

Propiedades del origen de datos
Detalles del EMS al que se conecta el recopilador. Network Manager Utiliza los datos de estos campos para modelar el EMS.

Propiedades de conexión de REST
Propiedades relacionadas con la conexión REST al EMS.

Propiedades de depuración
Propiedades para llevar a cabo la depuración.

4. Configure el puerto del recopilador y los parámetros de registro y rastreo:

puerto
Puerto donde se ejecuta el recopilador. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8443.

log.filename
Nombre del archivo de registro del recopilador. También puede especificar un patrón para el nombre del archivo de registro utilizando un conjunto de elementos definidos por el sistema.

log.level
Tiene uno de los valores siguientes:

- NONE
- FINEST
- FINER
- FINE
- CONFIGINFO
- AVISO
- SEVERE
- TODOS

trace.filename
Nombre del archivo de rastreo del recopilador . También puede especificar un patrón para el nombre del archivo de rastreo utilizando un conjunto de elementos definidos por el sistema.

trace.level
Tiene uno de los valores siguientes:

- NONE
- FINEST
- FINER
- FINE
- CONFIGINFO
- AVISO
- SEVERE
- TODOS

5. En la sección de propiedades Adquisición de datos, configure los parámetros de adquisición de datos:

collectData
El valor predeterminado es `true`.

Verdadero
Habilita el recopilador. El recopilador recopila datos del EMS.

Falso
Inhabilita el recopilador. El recopilador no recopila datos del EMS.

DataAcquisition.GetEntities
Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Habilita la descarga de datos de entidad física.

0: Inhabilitar
Desactiva la descarga de datos de la entidad física.

DataAcquisition.GetLayer1Connections
Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Permite la descarga de datos de conectividad de capa 1.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 1.

DataAcquisition.GetLayer2Connections
Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 2.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 2.

DataAcquisition.GetLayer3Connections
Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 3.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 3.

DataAcquisition.localDataDirectory
Especifica la ubicación de los archivos de salida generados desde el EMS. Utilice una ruta relativa o absoluta hacia la ubicación del directorio. No utilice variables de directorio como $NCHOME.

6. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

DataSource.id
Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

DataSource.descr
Descripción del EMS.

DataSource.emsHost
El nombre de host de EMS.

DataSource.emsPort
Puerto del EMS.

DataSource.emsUserName
El nombre de usuario que se usará al iniciar sesión en EMS.

DataSource.emsPassword
La contraseña que se usará al iniciar sesión en EMS.

DataSource.emsServiceName
El nombre del servicio EMS.

DataSource.emsPresHost
El nombre de host del servidor de presentación.

DataSource.emsPresUsername
El nombre de usuario para iniciar sesión en el servidor de presentación.

DataSource.emsPresPassWord
La contraseña para iniciar sesión en el servidor de presentación.

DataSource.emsName
Nombre del EMS.

DataSource.emsVersion
Versión del EMS.

DataSource.emsIdentifier
Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

DataSource.emsRole
Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- primary
- backup
- otro

DataSource.emsStatus
Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- up
- down
- otro

DataSource.emsNumNEElements
El número de elementos de red que se procesarán en el DataStore.

7. Configure las propiedades de conexión REST para el recopilador.

enableSSL
Habilite o inhabilite la conectividad SSL entre el recopilador y el servidor de EMS. Esta propiedad toma los valores siguientes: `true` o `false`. El valor predeterminado es `false`.

pathToKeyStoreFile
La ruta completa al directorio `keyStoreFileName`. Debe especificar la ruta relativa o completa hacia la ubicación del directorio. No puede utilizar $NCHOME. Por ejemplo, `/opt/IBM/netcool/core/precision/collectors/javaCollectors/CiscoApicRest/`.

keyStoreFileName

Especifique el nombre del archivo de claves que contenga el certificado de cliente SSL y el certificado de autoridad de confianza.

El archivo de almacén de claves debe estar ubicados en el directorio especificado en el parámetro `pathToKeyStoreFile`.

keyStorePassword

Especifique la contraseña necesaria para acceder al certificado especificado por la propiedad `keyStoreFileName`.

setResponseTimeout

Especifique cuánto tiempo (en segundos) el recopilador esperará una respuesta del EMS antes de agotar el tiempo de espera. El valor predeterminado es 300.

setHttpVersion

Especifique la versión del protocolo HTTP que admite el sistema de destino. El valor predeterminado es 1.1.

setRefreshInterval

Especifique el intervalo (en segundos) que el recopilador espera entre las diferentes solicitudes de inicio de sesión sucesivas de renovación. El valor predeterminado es 600.

TLSVersion
La versión del protocolo TLS. Los valores permitidos son: SSL, SSLv2, SSLv3, TLS, TLSv1, TLSv1.1

8. En la sección Propiedades de depuración, configure las siguientes propiedades.

```
#   emsSelectElements    - Debug the Selected EMS Items
#   emsNENode.1    - Select NE Node name 1 for debug
#   emsNENode.2    - Select NE Node name 2 for debug
#   enable_manual_service_ticket    - Enable or Disable the Manual service Ticket
#   service_ticket- Set the Service Ticket Value for Override and validating with manual
way.
#---------------------------------------

=ST-1083-Gz5plCWlPlq9gBkrLfj4-cas01.example.org
```

Debug.emsSelectElements
Ajuste en `verdadero` para habilitar la depuración de los elementos de EMS especificados. Ajuste en `falso` para desactivar la depuración.

Debug.emsNENode.1
El nombre del primer nodo que quiere depurar.

Debug.emsNENode.2
El nombre del segundo nodo que quiere depurar.

Debug.enable_manual_service_ticket
Ajuste en `verdadero` para activar el boleto de servicio manual. Ajuste en `falso` para desactivar el boleto de servicio manual.

Debug.service_ticket
El valor del boleto de servicio que desea anular y validar manualmente.

9. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Nokia Solutions and Networks NetViewer
Para utilizar datos del recopilador Nokia Solutions and Networks (NSN) NetViewer en un descubrimiento de red, debe configurar los detalles de conexión entre el NSN NetViewer EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador NSN NetViewer, siga estos pasos:

Procedimiento

1. Cambie al directorio del recopilador NSN NetViewer.

```
cd $NCHOME/precision/collectors/javaCollectors/NetViewer/
```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador NSN NetViewer y cópielo en el archivo de configuración de trabajo.

```
cp NetViewerCollector.properties.sampleNetViewerCollector.properties
```

3. Edite el archivo de configuración del recopilador:
`$NCHOME/precision/collectors/javaCollectors/NetViewer/NetViewerCollector.properties`.
4. Configure las siguientes propiedades del recopilador:

puerto
Puerto donde se ejecuta el servidor del recopilador incorporado. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8080.

log.filename
Nombre del archivo de registro del recopilador NSN NetViewer. El valor predeterminado es `NetViewerCollector.log`.

log.level
Nivel de registro del marco del recopilador. El valor predeterminado es INFO.

trace.filename
Nombre del archivo de rastreo del recopilador NSN NetViewer. El valor predeterminado es `NetViewerCollector-trace.log`.

trace.level
Nivel de rastreo del marco del recopilador. El valor predeterminado es INFO.

5. Configure los parámetros de adquisición de datos para el recopilador:

collectData
Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
Habilita el recopilador. El recopilador recopila datos del EMS.

Falso
Inhabilita el recopilador. El recopilador no recopila datos del EMS.

DataAcquisition.GetEntities
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de datos de entidad física del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de entidad física del EMS.

DataAcquisition.GetLayer2Connections
Tiene uno de los valores siguientes. El valor predeterminado es `0`.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 2 del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 2 del EMS.

6. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

DataSource.id
Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

DataSource.descr
Descripción del EMS.

DataSource.emsHost
Nombre de host del EMS.

DataSource.emsName
Nombre del EMS.

DataSource.emsPort
Puerto del EMS.

DataSource.emsVersion
Versión del EMS.

DataSource.emsIdentifier
Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

DataSource.emsRole
Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- primary
- backup
- otro

DataSource.emsStatus
Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- up
- down
- otro

DataSource.emsUserName
Nombre de usuario del EMS.

DataSource.emsPassword
Contraseña del EMS.

7. No modifique las siguientes propiedades de inicialización de ORB a menos que se lo indique el soporte de IBM:

   Estas propiedades están codificadas como parámetros de pares nombre-valor.

   orbProp.1.name=org.omg.CORBA.ORBClass
   orbProp.1.value=com.ibm.CORBA.iiop.ORB
   Especifica la implementación de IBM ORB que se va a activar.

   orbProp.2.name=org.omg.CORBA.ORBSingletonClass
   orbProp.2.value=com.ibm.rmi.corba.ORBSingleton
   Especifica la implementación de IBM ORB que se va a activar.

   orbProp.3.name=com.ibm.CORBA.Debug.Output
   orbProp.3.value=../log/orbtrc.log
   Especifica el archivo de registro donde se van a escribir los mensajes de error del ORB cuando el recopilador no puede conectarse al servicio CORBA en el EMS.

   orbProp.4.name=com.ibm.CORBA.ORBWCharDefault
   orbProp.4.value=UTF16
   Indica que se utilizará el conjunto de codificación de caracteres UTF-16 para la integración con NSN NetViewer EMS.

   orbProp.5.name=com.ibm.CORBA.ListenerPort
   orbProp.5.value=10005
   La integración con NSN NetViewer EMS utiliza un archivo Corba Interoperable Object Reference (IOR). La interactuación por medio de un archivo IOR precisa de comunicación bidireccional. Para facilitarlo, el parámetro ListenerPort se establece en el puerto 10005, y este es el puerto a utilizar para la comunicación desde NSN NetViewer EMS al recopilador. La configuración de este parámetro es especialmente importante si quiere integrar el recopilador con NSN NetViewer EMS en un entorno de cortafuegos o NAT.

8. Configure las propiedades del servicio de denominación:

   nameService.useNameService
   Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
El recopilador obtiene la referencia de contexto de denominación raíz cuando accede al servicio de denominación utilizando un URL corbaloc

Falso
El recopilador obtiene la referencia de contexto de denominación raíz del archivo IOR especificado y omite el servicio de denominación.

nameService.iorFile
La vía de acceso completa del archivo IOR que contiene la referencia NameService. Da soporte a la vía de acceso local y la vía de acceso remota; por ejemplo, HTTP y FTP.

nameService.nameServiceName
Nombre de servicio del servicio de denominación.

9. Configure las propiedades de EmsSessionFactory:

emsSessionFactory.useNameService
Tiene uno de los valores siguientes. El valor predeterminado es `True`.

Verdadero
El recopilador obtiene la referencia EmsSessionFactory_I utilizando el servicio de denominación y resolviendo las propiedades de contexto de denominación especificadas.

Falso
El recopilador obtiene la referencia EmsSessionFactory_I del archivo IOR especificado y omite el servicio de denominación.

emsSessionFactory.iorFile
Vía de acceso completa del archivo IOR que contiene la referencia EmsSessionFactory. Da soporte a la vía de acceso local y la vía de acceso remota; por ejemplo, HTTP y FTP.

10. Configure las propiedades del gestor:

manager.emsMgr
Nombre de la interfaz de EMSMgr. El valor predeterminado es `EMS`.

manager.equipmentInventoryMgr
Nombre de la interfaz de EquipmentInventoryMgr. El valor predeterminado es `EquipmentInventory`.

manager.managedElementMgr
Nombre de la interfaz de ManagedElementMgr. El valor predeterminado es `ManagedElement`.

manager.multiLayerSubnetworkMgr
Nombre de la interfaz de MultiLayerSubnetworkMgr. El valor predeterminado es `MultiLayerSubnetwork`.

11. En la sección de propiedades del Iterador, configure las propiedades del iterador de CORBA:

iterator.resultSize
Especifica el número máximo de resultados devueltos para cada conjunto por el iterador CORBA. El valor predeterminado es `20`. Aumente este valor si desea disminuir el número de iteraciones y aumentar el tamaño de la respuesta de datos del EMS.

iterator.destroyIterator
Establézcala en true si desea que el iterador CORBA destruya el objeto de iterador correspondiente en el lado del EMS. El valor predeterminado es `false`. Habilite esta propiedad sólo si el EMS no realiza automáticamente la recogida de basura de memoria.

12. Configure las propiedades de las correlaciones extraInfo:

Estas propiedades correlacionan los valores de los campos proporcionados con las tablas correspondientes en la base de datos NCIM. Pueden especificarse varios valores, pero deben diferenciarse mediante un número en las propiedades; por ejemplo, chassisData.2.extraInfo, shelfData.3.extraInfo, etc.

- chassisData.1.extraInfo
- shelfData.1.extraInfo

- slotData.1.extraInfo
- moduleData.1.extraInfo
- ptpData.1.extraInfo
- ctpData.1.extraInfo
- topologyData.1.extraInfo

13. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Tellabs INM8000
Para utilizar datos del recopilador Tellabs INM8000 en un descubrimiento de red, debe configurar los detalles de conexión entre el Tellabs INM8000 EMS y Network Manager.

Antes de empezar

Para habilitar la integración del recopilador Tellabs INM8000 de Network Manager con Tellabs INM8000 EMS, primero debe copiar los dos archivos siguientes en el recopilador Tellabs INM8000 de Network Manager:

- Archivo de biblioteca `tol.jar`
- Archivo de búsqueda `NbifAttributeValues.ini`

Para ello, realice las siguientes operaciones de copia manuales, sujeto a la comprobación de que tiene la autorización o el permiso necesario:

- Copie el archivo de biblioteca `tol.jar` del servidor Tellabs INM8000 en el directorio de biblioteca del recopilador Network Manager Java en `$NCHOME/precision/collectors/javaCollectors/lib`.
- Copie el archivo de búsqueda `NbifAttributeValues.ini` del servidor Tellabs INM8000 en el directorio dat del recopilador Tellabs INM8000 Network Manager Java en `$NCHOME/precision/collectors/javaCollectors/TellabsINM8000/dat`.

Nota: Puede obtener el archivo de biblioteca `tol.jar` y el archivo de búsqueda `NbifAttributeValues.ini` del servidor Tellabs INM8000 EMS, preferiblemente de un servidor que ejecute la versión INM SR5.0-SP2. Estos archivos también están disponibles en el CD-ROM que se suministra con la instalación de Tellabs INM8000 etiquetado como: `Tellabs 8000 Intelligent Network Manager SRxx-SPxx Inventory and PePerformance adapter, JavaAPI and NBITestClient for Northbound Interface`.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador Tellabs INM8000, siga estos pasos:

Procedimiento

1. Cambie al directorio del recopilador Tellabs INM8000.

   ```
   cd $NCHOME/precision/collectors/javaCollectors/TellabsINM8000/
   ```

2. En este directorio, busque el archivo de configuración de ejemplo del recopilador Tellabs INM8000 y cópielo en el archivo de configuración de trabajo.

   ```
   cp TellabsINM8000Collector.properties.sampleTellabsINM8000Collector.properties
   ```

3. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/javaCollectors/TellabsINM8000/TellabsINM8000Collector.properties`.

   Este archivo contiene las siguientes secciones de configuración:

   - Propiedades de configuración del recopilador
   - Propiedades de adquisición de datos

- Propiedades del origen de datos
- Propiedades de correlación

En los pasos siguientes se muestran los parámetros configurables. Las restantes propiedades en este archivo son configuraciones basadas en el sistema recopilador y no se pueden modificar.

4. Configure el puerto del recopilador y los parámetros de registro y rastreo:

   puerto
   Puerto donde se ejecuta el recopilador. El puerto debe coincidir con el puerto configurado en la inserción en la tabla `collectorFinder.collectorRules` en el archivo `DiscoCollectorFinderSeeds.cfg`. El valor predeterminado es 8080.

   log.filename
   Nombre del archivo de registro del recopilador. También puede especificar un patrón para el nombre del archivo de registro utilizando un conjunto de elementos definidos por el sistema. El valor predeterminado es `TellabsINM8000Collector.log`.

   log.level
   Tiene uno de los valores siguientes:

   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIGINFO
   - AVISO
   - SEVERE
   - TODOS

   trace.filename
   Nombre del archivo de rastreo del recopilador . También puede especificar un patrón para el nombre del archivo de rastreo utilizando un conjunto de elementos definidos por el sistema. El valor predeterminado es `TellabsINM8000Collector-trace.log`.

   trace.level
   Tiene uno de los valores siguientes:

   - NONE
   - FINEST
   - FINER
   - FINE
   - CONFIGINFO
   - AVISO
   - SEVERE
   - TODOS

5. Configure los parámetros del identificador de región específico de Tellabs.

   regionId.enable
   Si Tellabs INM8000 EMS da soporte a los identificadores de región, el usuario podrá recopilar datos basándose en el identificador de región configurado en el EMS. Este parámetro adopta uno de los siguientes valores:

   - Verdadero
   - Falso

   El valor predeterminado es True.

regionId.set
Define el número de identificador de región (regid) por el que se va a filtrar. Este parámetro puede tomar la forma de un identificador de región individual o una combinación de varios identificadores de región. Por ejemplo:

- Identificador de región individual: `regionId.set=5`
- Varios identificadores de región: `regionId.set=5,10,11`

6. Configure los parámetros del proceso por lotes específico de Tellabs.

   Si utiliza el proceso por lotes, Network Manager puede descubrir todos los nodos del EMS. Si el parámetro `regionId.enable` se establece en False, se aplica la serie de valores batch.*entity*.size, donde entity puede ser cualquiera de los siguientes valores:

   - subrack
   - unit
   - module
   - interface
   - trunk

   Defina el tamaño de lote de cada una de las entidades:

   - batch.subrack.size
   - batch.unit.size
   - batch.module.size
   - batch.interface.size
   - batch.trunk.size

   Por ejemplo, defina cada uno de estos parámetros para el uso de la API `getFilteredAllData`. El tamaño de lote hace referencia al número de nodos (nid) que Network Manager va a consultar y procesar en cualquier momento. Cada valor de tamaño de lote debe ser mayor que 1. Consulte las entidades soportadas en el modelo de información de Tellabs NBI. Algunos valores típicos son los siguientes:

   - batch.subrack.size=100
   - batch.unit.size=50
   - batch.module.size=50
   - batch.interface.size=20
   - batch.trunk.size=20

7. Configure los parámetros de adquisición de datos para el recopilador:

   collectData
   Tiene uno de los valores siguientes. El valor predeterminado es `True`.

   Verdadero
   Habilita el recopilador. El recopilador recopila datos del EMS.

   Falso
   Inhabilita el recopilador. El recopilador no recopila datos del EMS.

   DataAcquisition.GetEntities
   Tiene uno de los valores siguientes. El valor predeterminado es 1.

   1: Habilitar
   Habilita la descarga de datos de entidad física del EMS.

   0: Inhabilitar
   Inhabilita la descarga de datos de entidad física del EMS.

   DataAcquisition.GetLayer1Connections
   Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 1 del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 1 del EMS.

DataAcquisition.GetLayer2Connections
Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 2 del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 2 del EMS.

DataAcquisition.GetLayer3Connections
Tiene uno de los valores siguientes. El valor predeterminado es 1.

1: Habilitar
Habilita la descarga de datos de conectividad de capa 3 del EMS.

0: Inhabilitar
Inhabilita la descarga de datos de conectividad de capa 3 del EMS.

8. De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen en la sección de propiedades de Origen de datos, configurando los siguientes campos genéricos. Network Manager Utiliza los datos de estos campos para modelar el EMS.

DataSource.id
Identificador exclusivo para el origen de datos, en forma de un entero. Este campo tiene el valor 1, lo que indica que es el origen de datos primario.

DataSource.descr
Descripción del EMS.

DataSource.emsHost
Nombre de host del EMS.

DataSource.emsName
Nombre del EMS.

DataSource.emsPort
Puerto del EMS.

DataSource.emsVersion
Versión del EMS.

DataSource.emsIdentifier
Identificador del EMS y clave para integrar el recopilador de Network Manager con el controlador de Netcool Configuration Manager.

DataSource.emsRole
Rol del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- primary
- backup
- otro

DataSource.emsStatus
Estado del EMS. Este parámetro puede tener uno de los valores siguientes:

- desconocido
- up
- down
- otro

DataSource.emsUserName
Nombre de usuario del EMS.

DataSource.emsPassword
Contraseña del EMS.

Nota: El puerto predeterminado de Tellabs NIMA es 2462. El identificador del EMS para Tellabs INM8000 debe establecerse en `tellabsinm8000`. El nombre de usuario de EMS predeterminado es `nbif` y la contraseña de EMS predeterminada es `tellabs8000`.

9. Configure las propiedades de correlación para que reflejen el verdadero estado de la interfaz de Tellabs.

   Los siguientes parámetros representan la correlación del objeto de variableNetwork Manager SNMP `ifOperStatus` con el atributo de la interfaz de Tellabs `ifState`.

   - map.ifoperstatus.undefined
   - map.ifoperstatus.planned
   - map.ifoperstatus.installed
   - map.ifoperstatus.inuse

   A continuación, se muestra una descripción de los valores de atributo para la interfaz de entidad de Tellabs, Interface.ifstate:

   - 0: Sin definir
   - 1: Planificado
   - 2: Instalado
   - 3: En uso

   La correlación para ifOperStatus es la siguiente:

   - 1: up
   - 2: down
   - 3: testing
   - 4: unknown
   - 5: dormant
   - 6: notPresent
   - 7: lowerLayerDown

   Los valores predeterminados para la correlación son los siguientes:

   - map.ifoperstatus.undefined=6
   - map.ifoperstatus.planned=3
   - map.ifoperstatus.installed=5
   - map.ifoperstatus.inuse=1

10. Fix Pack 2
    Configure otros valores.

    use.name.alias
    Establezca `true` si desea utilizar el nombre de alias en lugar de la descripción del tipo de hardware. De forma predeterminada, esta propiedad se establece en `false`.

    use.interface.ifmsg
    Establezca true si desea utilizar el atributo `IFMSG` de la interfaz en lugar del atributo `IFHWTYPE`. De forma predeterminada, esta propiedad se establece en `false`.

    use.filter.node.discovery
    Establezca true si desea filtrar los nodos descubiertos por nodeId. Puede que desee utilizar esta opción para probar si se descubren dos nodos y la conexión entre ellos. Si establece esta

propiedad en `true`, debe establecer dos propiedades `node.id`. De forma predeterminada, esta propiedad se establece en `false`.

node.id.n

Si establece `use.filter.node.discovery` como true, debe definir dos propiedades `node.id.n` . Sólo se descubren los nodos con un ID coincidente con una estas propiedades.

Por ejemplo, el extracto de código siguiente define dos nodeIds para descubrir:

```
use.filter.node.discovery=true
node.id.1=874
node.id.2=8856
```

11. Guarde el archivo de configuración del recopilador.

Referencia de archivo de propiedades del recopilador CSV Java
Utilice esta información para entender cómo se construye el archivo de propiedades del recopilador CSV Java.

La ubicación del archivo de propiedades del recopilador CSV Java en `$NCHOME/precision/collectors/javaCollectors/` se muestra en la Tabla 29 en la página 284. Utilizando este archivo `.properties`, puede correlacionar los datos de red con uno o varios archivos.

Nota: Las propiedades especificadas en el archivo de propiedades específico del recopilador alteran temporalmente las propiedades relacionadas especificadas en el archivo de propiedades del recopilador Java genérico, `$NCHOME/precision/collectors/javaCollectors/framework/collector.properties`.

Tabla 29. Archivo de propiedades del recopilador CSV Java

Recopilador	**Ubicación del archivo de propiedades en él**
Recopilador CSV de Java	`csv/csvcollector.properties`

Archivo .properties de ejemplo del recopilador CSV Java

El siguiente fragmento de código muestra los valores de ejemplo de un archivo `.properties` del recopilador CSV Java. Este fragmento de código define el directorio donde están ubicados los archivos de datos CSV y, a continuación, continúa con la definición del formato de los datos CSV en uno de estos archivos, el archivo `devices.csv`, que define los datos de entidad principal.

```
# Directory containing CSV data
CSVDir = ../csv/exampleCsvData/

# Main entity data (device data) is in devices.csv
MainEntityData.file = devices.csv

# The delimiter for the file is a |
MainEntityData.delimiter = \\|

# There are 6 columns of data in the file
MainEntityData.numCols = 6

# Only read lines that start with 10.1.1.
MainEntityData.lineMatch = 10\\.1\\.1\\..+

# Map the first data column to the device management IP address (<ip>)
MainEntityData.1.name = ManagementIpAddress
MainEntityData.1.mapsTo = DEVICE_MANAGEMENT_IP_ADDRESS

# Arbitrary mapping of extra information
# Map column 6 to <extraInfo><systemInfo>…</systemInfo></extraInfo>
MainEntityData.6.name = AdditionalSystemInfo
MainEntityData.6.mapsTo = EXTRA_INFO.systemInfo
```

Propiedades y correlaciones

El archivo de propiedades del recopilador CSV Java incluye las siguientes propiedades:

Directorio base
Para el recopilador CSV Java, el directorio base se define en la propiedad `CSVDir`.

Propiedades del archivo de datos
Para el recopilador CSV Java, se define un conjunto de propiedades para los distintos archivos de datos CSV que se utilizan como entrada.

La tabla siguiente muestra las propiedades contenidas en los archivos de datos CSV. Para cada propiedad, *data_type* es uno de los tipos de datos soportados, como se muestra en la Tabla 32 en la página 285.

Tabla 30. Propiedades del archivo de datos

Propiedad	Descripciones
data_type.file	Nombre de archivo que contiene los datos CSV.
data_type.delimiter	Delimitador de los datos en el archivo CSV. El delimitador predeterminado es una coma `,`.
data_type.lineMatch	Patrón de sintaxis de expresión regular. Indica al recopilador que sólo debe leer las líneas que empiecen por el patrón.
data_type.numCols	Número de columnas de datos en el archivo.
data_type.useCols	Si no se necesitan todas las columnas, esta expresión utiliza una lista separada por comas, por ejemplo, `1,3`, para indicar qué columnas de datos deben utilizarse del archivo.

La tabla siguiente muestra cómo se correlacionan los datos en los archivos de datos CSV con los atributos.

Tabla 31. Correlaciones de datos

Propiedad	Descripciones
data_type.column_number.name	Nombre legible por las personas de los datos de columna.
data_type.column_number.description	Descripción legible por las personas de los datos de columna.
data_type.column_number.mapsTo	Correlación con un atributo soportado para el tipo de datos.

Tipos de datos

La tabla siguiente muestra los tipos de datos soportados.

Tabla 32. Tipos de datos

Propiedad	Descripciones
MainEntityData	Datos de entidad (dispositivo) principal.
InterfaceData	Datos de interfaz.
EntityData	Datos de entidad con formato ENTITY-MIB.
GenericEntityData	Datos de entidad con formato no ENTITY-MIB.

Tabla 32. Tipos de datos (continuación)	
Propiedad	**Descripciones**
L1ConnectivityData	Datos de conectividad de capa 1.
L2ConnectivityData	Datos de conectividad de capa 2.
L3ConnectivityData	Datos de conectividad de capa 3.
L2VpnData	Datos de VPN de capa 2.
L3VpnData	Datos de VPN de capa 3.
L3VpnInterfaceData	Datos de interfaz de VPN de capa 3.
L3VpnRTData	Datos de destino de ruta de VPN de capa 3.
LabelSwitchPathData	Datos de vía de acceso de conmutador de etiqueta.
MplsInterfaceData	Datos de interfaz de MPLS.

Configuración de origen de datos

De manera opcional, puede configurar detalles sobre el sistema de gestión de elementos (EMS) de origen configurando los campos que se muestran en la tabla siguiente. Si configura esta información de EMS, Network Manager utilizará los datos procedentes de estos campos para modelar el EMS.

Tabla 33. Configuración de origen de datos	
Propiedad	**Descripciones**
DataSource.id	Este campo tiene el valor 1, lo que indica que es el origen de datos primario.
DataSource.descr	Descripción del EMS.
DataSource.emsHost	Nombre de host del EMS.
DataSource.emsName	Nombre del EMS.
DataSource.emsVersion	Versión del EMS.
DataSource.emsIdentifier	Identificador del EMS.
DataSource.emsRole	Rol del EMS. Tiene uno de los valores siguientes: • desconocido • primary • backup • otro
DataSource.emsStatus	Rol del EMS. Tiene uno de los valores siguientes: • desconocido • up • down • otro

Configuración de recopiladores Perl
Utilice esta información para configurar los valores de los recopiladores grabados en Perl.

Configuración del recopilador Nokia5529Idm
Para utilizar datos del recopilador Nokia5529Idm en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Procedimiento

1. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/perlCollectors/Alcatel5529IdmSoap/Alcatel5529IdmSoap Collector.cfg`
2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en `1` para activar la depuración. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es `8081`. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

   Tiempo de espera excedido
   Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

   El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15
},
```

3. Edite la sección `DataSource` del archivo de configuración. Configure las propiedades siguientes:

   Host
   El nombre de host del EMS.

   Puerto
   El puerto al que conectar el EMS.

   Nombre de usuario
   El nombre de usuario al que conectar el EMS.

   Contraseña
   La contraseña a utilizar para conectar al EMS.

   Tiempo de espera excedido
   El tiempo de espera para la comunicación SOAP entre el recopilador y el EMS.

   Dominio
   El dominio del sistema AMS en el que Inventory Data Manager se ejecuta.

   GetEntities
   Distintivo para el descubrimiento de entidades físicas, como bastidores, tarjetas y puertos. Establecer en 1 para descubrir entidades físicas. Si este distintivo se establece en 0, sólo se descubre información del chasis. El valor predeterminado es 1.

   GetOnt
   Distintivo para configurar si el recopilador recupera información de Optical Network Terminal (ONT). Establecer en 1 para habilitar la recuperación de datos del módulo ONT. La recuperación de

información de ONT se basa en la información de la entidad física. Asegúrese de que GetEntities está establecido en 1 si quiere establecer GetOnt en 1.

El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
DataSource =>
{
        Host => 192.168.1.2,
        Port => 8080

        Username => 'oss',
        Password => 'myPa55w0rd'

        Timeout => 30

             Domain => 'AMS'

            GetEntities => 1

             GetOnt => 0
,
```

4. Asegúrese de que el parámetro `Batchsize` se establezca en 500, a menos que el soporte de IBM indique lo contrario. Este parámetro controla el tamaño de cada respuesta SOAP/XML.
5. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Alcatel5620Csv
Para utilizar datos del recopilador Alcatel5620Csv en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Acerca de esta tarea

Procedimiento

1. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/perlCollectors/Alcatel5620SamCsv/Alcatel5620SamCsv Collector.cfg`
2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en 1 para activar la depuración. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es `8081`. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

   Tiempo de espera excedido
   Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

   El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15
},
```

3. Edite la sección `DataSource` del archivo de configuración y especifique el nombre del archivo de configuración del módulo del cargador de CSV, como se muestra en el siguiente ejemplo.

   El archivo de configuración del módulo del cargador de CSV a su vez especifica los archivos CSV y los archivos del controlador `.drv` que detallan cómo se analizará cada archivo CSV

```
DataSource =>
{
        CsvCfg => 'exampleCsv.cfg',
…
…
…
},
```

4. Opcionalmente, puede configurar detalles sobre el EMS originador añadiendo una subsección `SourceInfo` a la sección `DataSource` del archivo de configuración. Si configura esta información de EMS, Network Manager utilizará los datos procedentes de estos campos para modelar el EMS.

   Para configurar detalles acerca del EMS, establezca valores para los campos que se muestran en el siguiente fragmento de código:

```
        SourceInfo =>
        {
            Id => 1,
            Descr => 'Primary Data Source',
            # EmsHost => '',
            # EmsName => '',
            # EmsVersion => '',
            # EmsIdentifier => '',
            # EmsRole => '',
            # EmsStatus => '',
        },
```

5. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Alcatel5620SamSoap
Para utilizar datos del recopilador Alcatel5620SamSoap en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador Alcatel5620SamSoap, lleve a cabo los siguientes pasos:

Procedimiento

1. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/Alcatel5620SamSoap Collector.cfg`
2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en `1` para activar la depuración. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es `8081`. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

Tiempo de espera excedido
Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15
},
```

3. Edite la sección `DataSource` del archivo de configuración. Configure las propiedades siguientes:

Host
El nombre de host del EMS.

Puerto
El puerto al que conectar el EMS.

Nombre de usuario
El nombre de usuario al que conectar el EMS.

Contraseña
La contraseña a utilizar para conectar al EMS.

Tiempo de espera excedido
El tiempo de espera para la comunicación SOAP entre el recopilador y el EMS.

El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
DataSource =>
{
        Host => 192.168.1.2,
        Port => 8080

        Username => 'oss',
        Password => 'myPa55w0rd',

        Timeout => 30,
…
…
…
},
```

4. Edite la sección `DataAcquisition` del archivo de configuración y configure las propiedades siguientes:

GetEntities
Distintivo para el descubrimiento de entidades físicas, como bastidores, tarjetas y puertos. Establecer en 1 para descubrir entidades físicas. Si este distintivo se establece en 0, sólo se descubre la información siguiente: chasis, entidades lógicas y datos para otros distintivos habilitados en la sección `DataAcquisition`. El valor predeterminado es 1.

GetVplsVpns
Distintivo para el descubrimiento de los datos de VPN capa 2 basada en VPLS. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetVllVpns
Un distintivo para el descubrimiento de datos de VPN capa 2 basada en VPLS sólo para epipes. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetLayer3Vpns
Distintivo para el descubrimiento de los datos de VPN capa 3. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetMplsInterfaces
Distintivo para el descubrimiento de los datos de interfaz MPLS. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetLayer2Connections
Distintivo para el descubrimiento de los datos del enlace físico. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
DataAcquisition =>
{
        GetEntities => 1
        GetVplsVpns => 1,
        GetVllVpns => 1,
        GetLayer3Vpns => 1,
        GetMplsInterfaces => 1,
        GetLayer2Connections => 1
},
```

5. 5. Edite la sección `DataProcessing` del archivo de configuración. Configure la propiedad ContainmentMethod.

   La propiedad ContainmentMethod controla la forma en la que se procesan los datos de entidad en los casos en los que la contención sea ambigua debido a que falten (o haya duplicados) datos de índice, lo que puede suceder con los datos de la ranura/módulo (tarjeta).

   Los valores posibles de la propiedad ContainmentMethod son:

   0
   Ignorar los índices duplicados y dar prioridad a las ranuras. Se almacenan las entidades de ranura pero las entidades de módulo (tarjeta) se podrían perder si comparten los mismos datos que la ranura.

   1
   Ignorar los índices duplicados y dar prioridad a las tarjetas. Se almacenan las entidades de módulo pero las entidades de ranura se podrían perder si comparten los mismos datos que el módulo.

   2
   Mantener entidades de tarjeta y ranura. Genera un índice falso si se detectan duplicados.

   El valor predeterminado es 2.
6. Opcional: Si desea recuperar datos personalizados del EMS además de los datos recuperados de forma predeterminada, lleve a cabo los siguientes pasos:
   a) Cree un archivo de configuración nuevo en el directorio del recopilador o edite el archivo `$NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/extraInfo.cfg` del recopilador.
   b) Especifique los datos que se recuperarán, como en el siguiente ejemplo:

```
            Device =>
            {
                extraFields => [ { srcField => 'version', destField =>
 'm_Version', typeField => 'string' }]
            },
```

   Donde `srcField` es el nombre del atributo del objeto SAM, `destField` es el nombre del campo con el que se correlacionarán los datos dentro del campo extraInfo, y typeField es un descriptor de tipos opcional.

   El atributo que desea recuperar debe pertenecer a uno de los objetos ya recuperados por el recopilador. Los objetos consultados por el recopilador son:

   - netw.NetworkElement
   - equipment.PhysicalPort
   - lag.Interface
   - equipment.MediaAdaptor
   - equipment.PhysicalPort
   - equipment.DaughterCard

- equipment.Equipment
- equipment.Shelf
- vpls.L2AccessInterface
- vll.L2AccessInterface
- l3fwd.ServiceSite
- vprn.L3AccessInterface
- netw.PhysicalLink
- lldp.RemotePeer.

Los tipos válidos son `int` y `string`.

c) Guarde y cierre el archivo de configuración.

d) Edite la sección `CustomData` del archivo de configuración del recopilador `$NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/Alcatel5620SamSoapCollector.cfg`. Especifique el nombre y la ubicación del archivo de configuración que define la información adicional que se recuperará, como en el siguiente ejemplo:

```
CustomData =>
    {
    ExtraInfoCfg => 'extraInfo.cfg'
},
```

7. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Alcatel5620SamSoapFindToFile
Para utilizar los datos del recopilador Alcatel5620SamSoapFindToFile en un descubrimiento de red, debe configurar los detalles de conexión entre EMS y Network Manager, y los detalles de FTP con los que pueden enviarse los archivos XML al servidor Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador Alcatel5620SamSoapFindToFile, lleve a cabo los siguientes pasos:

Procedimiento

1. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoapFindToFile/Alcatel5620SamSoapFindToFileCollector.cfg`
2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en `1` para activar la depuración. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es `8081`. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

   Tiempo de espera excedido
   Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15
},
```

3. Edite la sección `DataSource` del archivo de configuración.
   a) Especifique el nombre de host y el puerto del EMS, el nombre de usuario y contraseña para conectarse al EMS, como se muestra en el siguiente ejemplo:

```
DataSource =>
{
        Host => 192.168.1.2,
        Port => 8080

        Username => 'oss',
        Password => 'myPa55w0rd',
        Timeout => 30,
…
…
…
},
```

   b) Configure los siguientes parámetros FTP:

   UseSFTP
   Distintivo booleano para determinar si utilizar SSH FTP (SFTP) para la transferencia de archivos XML.

   - UseSFTP = 1: indica al sistema que utilice SFTP.
   - UseSFTP = 0: indica al sistema que utilice FTP.

   FtpUsername
   El nombre de usuario FTP en el servidor Network Manager.

   FtpPassword
   La contraseña FTP en el servidor Network Manager.

   FtpHost
   La dirección IP del servidor Network Manager.

   FtpDefaultDirectory
   El directorio predeterminado del servicio FTP en el servidor Network Manager.

   FtpDirectory
   Un directorio definido por el usuario para el servicio FTP en el servidor Network Manager. Si no se utiliza, deje este valor en blanco.

   Consejo: Tras un descubrimiento correcto, copie los archivos XML generados en el directorio FTP especificado a otra ubicación antes de realizar un descubrimiento nuevo, para que dichos archivos XML no se sobrescriban.

4. Edite la sección `DataAcquisition` del archivo de configuración y configure las propiedades siguientes:

   GetEntities
   Distintivo para el descubrimiento de entidades físicas, como bastidores, tarjetas y puertos. Establecer en 1 para descubrir entidades físicas. Si este distintivo se establece en 0, sólo se descubre la información siguiente: chasis, entidades lógicas y datos para otros distintivos habilitados en la sección `DataAcquisition`. El valor predeterminado es 1.

   GetVplsVpns
   Distintivo para el descubrimiento de los datos de VPN capa 2 basada en VPLS. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetVllVpns
Un distintivo para el descubrimiento de datos de VPN capa 2 basada en VPLS sólo para epipes. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetLayer3Vpns
Distintivo para el descubrimiento de los datos de VPN capa 3. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetMplsInterfaces
Distintivo para el descubrimiento de los datos de interfaz MPLS. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetLayer2Connections
Distintivo para el descubrimiento de los datos del enlace físico. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

GetLteData
Distintivo para el descubrimiento de los datos LTE. Establecer en 1 para habilitar el descubrimiento de estos datos. El valor predeterminado es 1.

El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
DataAcquisition =>
{
        GetEntities => 1
        GetVplsVpns => 1,
        GetVllVpns => 1,
        GetLayer3Vpns => 1,
        GetMplsInterfaces => 1,
        GetLayer2Connections => 1,
        GetLteData => 1
}
```

5. Opcional: Si desea recuperar datos personalizados del EMS además de los datos recuperados de forma predeterminada, lleve a cabo los siguientes pasos:

   a) Cree un archivo de configuración en el directorio del recopilador o edite el archivo $NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/extraInfo.cfg del recopilador.

   b) Edite el archivo y especifique los datos que se recuperarán, como en el siguiente ejemplo:

```
            Device =>
            {
                extraFields => [ { srcField => 'version', destField =>
 'm_Version', typeField => 'string' }]
            },
```

   Donde srcField es el nombre del atributo del objeto SAM, destField es el nombre del campo con el que se correlacionarán los datos dentro del campo extraInfo, y typeField es un descriptor de tipos opcional.

   El atributo que desea recuperar debe pertenecer a uno de los objetos ya recuperados por el recopilador. Los objetos consultados por el recopilador son:

   - netw.NetworkElement
   - equipment.PhysicalPort
   - lag.Interface
   - equipment.MediaAdaptor
   - equipment.PhysicalPort
   - equipment.DaughterCard
   - equipment.Equipment
   - equipment.Shelf
   - vpls.L2AccessInterface
   - vll.L2AccessInterface

- l3fwd.ServiceSite
- vprn.L3AccessInterface
- netw.PhysicalLink
- lldp.RemotePeer.

Los tipos válidos son `int` y `string`.

c) Guarde y cierre el archivo de configuración.

d) Edite la sección `CustomData` del archivo de configuración del recopilador `$NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/Alcatel5620SamSoapCollector.cfg`. Especifique el nombre y la ubicación del archivo de configuración que define la información adicional que se recuperará, como en el siguiente ejemplo:

```
        CustomData =>
            {
            ExtraInfoCfg => 'extraInfo.cfg'
        },
```

6. Guarde el archivo de configuración del recopilador.

Configuración del recopilador AlcatelNR8PLIOOISN
Para utilizar datos del recopilador AlcatelNR8PLIOOISN en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Acerca de esta tarea

También puede configurar la información adicional que se recuperará del EMS. Para configurar el recopilador AlcatelNR8PLIOOISN, lleve a cabo los siguientes pasos:

Procedimiento

1. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/perlCollectors/AlcatelNR8PLIooIsn/AlcatelNR8PLIooIsnCollector.cfg`
2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en 1 para activar la depuración. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es `8081`. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

   Tiempo de espera excedido
   Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

   El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15
},
```

3. Edite la sección DataSource del archivo de configuración. El siguiente código predeterminado en la sección permite a Network Manager comunicarse con el ISN y los agentes IOO que se ejecutan en Alcatel NR8 PL EMS:

```
DataSource =>
{

    Timeout => 30,

    IOONBI =>
    {
        Host => '192.168.1.2',
        IOOAgentPort => 5001,
        Timeout => 10,
        IOOPassword => 'alcatel',
        IOOInputStream => 4096
    }

    ISNNBI =>
    {
        Host => '192.168.1.2',
        ISNAgentPort => 5002,
        ISNUserName => 'ISNTest1',
        ISNReportUnprocessedDirectory => './ISNReport',
        ISNReportProcessedDirectory => './ISNReportProcessed',
        FtpUsername => 'ftpuser',
        FtpPassword => 'ftpuserpassword',
        FtpSourceDirectory => '/tmp/report',
        GunzipPath => '/usr/bin/gunzip',
    }

    DataAcquisition =>
    {
        GetEntities => 1,
        GetLayer1Connections => 1
    }
}
```

   Establezca GetEntities en 1 si desea recopilar información de entidades del recopilador.

   Establezca GetLayer1Connections en 1 si desea recuperar datos de la capa 1 del recopilador.

4. Opcionalmente, puede configurar detalles sobre el EMS originador añadiendo una subsección SourceInfo a la sección DataSource del archivo de configuración. Si configura esta información de EMS, Network Manager utilizará los datos procedentes de estos campos para modelar el EMS.

   Para configurar detalles acerca del EMS, establezca valores para los campos que se muestran en el siguiente fragmento de código:

```
    SourceInfo =>
    {
        Id => 1,
        Descr => 'Primary Data Source',
        # EmsHost => '',
        # EmsName => '',
        # EmsVersion => '',
        # EmsIdentifier => '',
        # EmsRole => '',
        # EmsStatus => '',
    },
```

5. Guarde el archivo de configuración del recopilador.

Configuración del recopilador GenericCsv

Para utilizar datos del recopilador GenericCsv en un descubrimiento de red, debe configurar los detalles de acceso desde el recopilador al origen de datos y configurar el recopilador para el puerto de escucha de Network Manager. La configuración de los detalles de acceso del recopilador al origen de datos implica especificar cómo cargará e interpretará el recopilador los archivos CSV.

Procedimiento

1. Edite el archivo de configuración del recopilador:
   $NCHOME/precision/collectors/perlCollectors/GenericCsv/GenericCsv

`Collector.cfg`

2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en `1` para activar la depuración. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es `8081`. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

   Tiempo de espera excedido
   Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

   El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15
},
```

3. Edite la sección `DataSource` del archivo de configuración y especifique el nombre del archivo de configuración del módulo del cargador de CSV, como se muestra en el siguiente ejemplo.

   El archivo de configuración del módulo del cargador de CSV a su vez especifica los archivos CSV y los archivos del controlador `.drv` que detallan cómo se analizará cada archivo CSV

```
DataSource =>
{
        CsvCfg => 'exampleCsv.cfg',
…
…
…
},
```

4. Guarde el archivo de configuración del recopilador.

Configuración del recopilador HuaweiU2000Imanager
Para utilizar datos del recopilador HuaweiU2000Imanager en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Procedimiento

1. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/perlCollectors/HuaweiU2000iManagerTL1/HuaweiU2000iManagerTL1`
   `Collector.cfg`
2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en `1` para activar la depuración. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es 8081. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

Tiempo de espera excedido
Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15
},
```

3. Edite la sección `DataSource` del archivo de configuración. Especifique el nombre de host y el puerto del EMS, el nombre de usuario y contraseña para conectarse al EMS, como se muestra en el siguiente ejemplo:

```
DataSource =>
{
        Host => 192.168.1.2,
        Port => 8080

        Username => 'oss',
        Password => 'myPa55w0rd'

        GetEntities => 1

           DataAcquisition =>
           {
               StoreONTs => 1,
           }
…
…
,
```

Establezca GetEntities en 1 si desea recopilar información de entidades del recopilador.

Establezca StoreONTs en 1 si desea recuperar los datos de terminación de red óptica (ONT).

4. Opcionalmente, puede configurar detalles sobre el EMS originador añadiendo una subsección `SourceInfo` a la sección `DataSource` del archivo de configuración. Si configura esta información de EMS, Network Manager utilizará los datos procedentes de estos campos para modelar el EMS.

   Para configurar detalles acerca del EMS, establezca valores para los campos que se muestran en el siguiente fragmento de código:

```
        SourceInfo =>
        {
            Id => 1,
            Descr => 'Primary Data Source',
            # EmsHost => '',
            # EmsName => '',
            # EmsVersion => '',
            # EmsIdentifier => '',
            # EmsRole => '',
            # EmsStatus => '',
        },
```

5. Guarde el archivo de configuración del recopilador.

Configuración del recopilador HuaweiU2000iManagerTL1DumpExport
Para utilizar datos del recopilador HuaweiU2000iManagerTL1DumpExport en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Acerca de esta tarea

El recopilador HuaweiU2000iManagerTL1DumpExport procesa datos de dispositivos de acceso Huawei mediante el Huawei U2000 EMS.

Para obtener datos para el recopilador, realice los siguientes pasos:

1. Exporte el archivo XML desde el Huawei U2000 EMS mediante el mandato `DMP-INVENTORY`. Asegúrese de que el nombre del parámetro de EMS de `NBI_INVENTORY_DUMP_VERSION` se ha establecido en 3.
2. Compruebe que el archivo XML tiene el formato correcto. El recopilador admite archivos XML con datos de objeto ME, SHELF, CARD, PORT, SERVICEPORT y PORTOFVLAN, en formato DATAPACKET. Como referencia, se ofrece un ejemplo de archivo XML utilizado por el recopilador en la siguiente ubicación:`$NCHOME/precision/collectors/perlCollectors/HuaweiU2000iManagerTL1DumpExport/data/sample.xml`.
3. Copie el archivo XML desde el EMS al servidor donde se ha instalado el recopilador. Copie el archivo en la ubicación especificada en el parámetro `FtpDestinationDirectory` del archivo de configuración del recopilador, como se describe a continuación. El directorio predeterminado es `/opt/IBM/netcool/core/precision/collectors/perlCollectors/HuaweiU2000iManagerTL1DumpExport/data`.

Para configurar el recopilador, lleve a cabo los siguientes pasos.

Procedimiento

1. Edite el archivo de configuración del recopilador:
   `$NCHOME/precision/collectors/perlCollectors/HuaweiU2000iManagerTL1DumpExport/HuaweiU2000iManagerTL1DumpExportCollector.cfg`
2. Edite la sección `General` del archivo de configuración. Configure las propiedades siguientes:

   Debug
   La modalidad de depuración del recopilador. Establezca la propiedad en `0` para desactivar la depuración. Establezca la propiedad en 4 para activar la depuración. El establecimiento de esta propiedad en 1, 2 o 3 es equivalente a establecerla en `0`. El recopilador imprime la depuración en la pantalla (stdout).

   Listen

   El puerto en el que escucha el recopilador para solicitudes XML-RPC desde Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es `8081`. El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.

   Tiempo de espera excedido
   Tiempo de espera para la comunicación desde el recopilador a Network Manager. El tiempo de espera se mide en segundos. El valor predeterminado es 15 segundos.

   QueueSize
   El tamaño de la cola que contiene las solicitudes XML-RPC recibidas por el recopilador que todavía no se ha procesado. Si la cola está llena, es decir, si el recopilador recibe las solicitudes más rápido de lo que puede procesarlas, es posible que algunas solicitudes se descarten. Esto origina mensajes de error en el registro del ayudante XML-RPC. El valor predeterminado es 40.

   El ejemplo siguiente muestra los valores predeterminados de estas propiedades:

```
General =>
{
        Debug => 0,
        Listen => 8081,
        Timeout => 15,
```

```
        QueueSize => 40
},
```

3. Edite la sección DataSource del archivo de configuración. Especifique el nombre de host y el puerto del EMS, el nombre de usuario y la contraseña para conectarse al EMS y los detalles del archivo XML como se muestra en el siguiente ejemplo:

```
DataSource =>
{
        Host => 192.168.1.2,
        Port => 8080

        Username => 'oss',
        Password => 'myPa55w0rd'


        FtpDestinationDirectory =>
        '/opt/IBM/netcool/core/precision/collectors/perlCollectors/
HuaweiU2000iManagerTL1DumpExport/data',
        XMLDumpFileName =>
        'MA5610S.xml,MA5606T.xml',
        Timeout => 30,

           DataAcquisition =>
           {
               GetEntities => 1,
           }
…
…
,
```

Establezca GetEntities en 1 si desea recopilar información de entidades del recopilador.

Establezca FtpDestinationDirectory en la ruta de directorio completa para los archivos XML que transfiera desde el EMS. El directorio predeterminado es /opt/IBM/netcool/core/precision/collectors/perlCollectors/HuaweiU2000iManagerTL1DumpExport/data.

Establezca XMLDumpFileName en el nombre de archivo de todos los archivos XML procedentes del EMS. Si hay varios archivos XML, utilice comas para separar los nombres de archivo. Por ejemplo, fileName1.xml,fileName2.xml. Para los nombres de archivos XML únicos, la notación es fileName1.xml. El valor predeterminado es con varios nombres de archivo XML: MA5606TN2000.xml,MA5606T.xml.

Establezca el valor Timeout para el tiempo de espera de la comunicación desde el recopilador a EMS. El tiempo de espera se mide en segundos. El valor predeterminado es de 30 segundos.

4. Opcionalmente, puede configurar detalles sobre el EMS originador añadiendo una subsección SourceInfo a la sección DataSource del archivo de configuración. Si configura esta información de EMS, Network Manager utilizará los datos procedentes de estos campos para modelar el EMS.

   Para configurar detalles acerca del EMS, establezca valores para los campos que se muestran en el siguiente fragmento de código:

```
        SourceInfo =>
        {
            Id => 1,
            Descr => 'Primary Data Source',
            # EmsHost => '',
            # EmsName => '',
            # EmsVersion => '',
            # EmsIdentifier => '',
            # EmsRole => '',
            # EmsStatus => '',
        },
```

5. Guarde el archivo de configuración del recopilador.

Configuración del recopilador Optical Blackbox

Para utilizar datos del recopilador Optical Blackbox en un descubrimiento de red, debe configurar los detalles de conexión entre el EMS y Network Manager.

Procedimiento

1. Edite el archivo de configuración del recopilador:

   `$NCHOME/precision/collectors/perlCollectors/OpticalBlackboxXml/OpticalBlackboxXml Collector.cfg`.
2. Especifique el puerto en el que el recopilador debe escuchar las solicitudes XML-RPC de Network Manager.

   También es el puerto que el recopilador utiliza para proporcionar respuestas XML-RPC a Network Manager. De forma predeterminada, el puerto es 8081. También se configura un tiempo de espera predeterminado de 15 segundos. Busque y edite la sección `General` del archivo de configuración, como se muestra en el siguiente ejemplo:

   ```
   General =>
   {
           Debug => 0,
           Listen => 8081
           Timeout => 15
   },
   ```

   El puerto debe coincidir con el puerto que haya configurado en la inserción en la tabla collectorFinder.collectorRules del archivo `DiscoCollectorFinderSeeds.cfg` al iniciar el recopilador para un primer descubrimiento.
3. Edite la sección `DataSource` del archivo de configuración y especifique el nombre de archivo del archivo XML, como se muestra en el siguiente ejemplo:

   ```
   DataSource =>
   {
               BlackboxXml => './exampleXmlData/blackbox.xml',

               DataAcquisition =>
               {
                   GetEntities => 1,
                   GetLayer1Connections => 1
               }
   }
   ```
4. Opcionalmente, puede configurar detalles sobre el EMS originador añadiendo una subsección `SourceInfo` a la sección `DataSource` del archivo de configuración. Si configura esta información de EMS, Network Manager utilizará los datos procedentes de estos campos para modelar el EMS.

   Para configurar detalles acerca del EMS, establezca valores para los campos que se muestran en el siguiente fragmento de código:

   ```
           SourceInfo =>
           {
               Id => 1,
               Descr => 'Primary Data Source',
               # EmsHost => '',
               # EmsName => '',
               # EmsVersion => '',
               # EmsIdentifier => '',
               # EmsRole => '',
               # EmsStatus => '',
           },
   ```
5. Guarde el archivo de configuración del recopilador.

Inicio de recopiladores

Antes de que se inicie el descubrimiento, se tienen que estar ejecutando todos los recopiladores. Debe iniciar los recopiladores o asegurarse de que se estén ejecutando antes de iniciar un descubrimiento que incluya recopiladores.

Inicio de recopiladores Java

Utilice esta información para iniciar los recopiladores grabados en Java.

Acerca de esta tarea

Para iniciar un recopilador Java, vaya al directorio bin del recopilador Java en $NCHOME/precision/collectors/javaCollectors/bin y emita un mandato de interfaz de línea de mandatos. Emita el siguiente mandato para iniciar un recopilador Java (tenga en cuenta que el mandato debe introducirse en una sola línea; las opciones se explican en la Tabla 34 en la página 302):

```
collector.sh -jar [ -Xmsminimum_memory-sizem ] [ -Xmxmaximum_memory-sizem ]
jar_file -propsFile file_name -port port_number [ -bg ]
```

Tabla 34. Explicación de las opciones de línea de mandatos

Opción	Explicación
-jar *archivo_jar*	Necesaria: vía de acceso del archivo JAR del recopilador que se va a ejecutar respecto al directorio del recopilador Java raíz; por ejemplo, csv/csvcollector.jar.
-propsFile *nombre_archivo*	Opcional: vía de acceso del archivo de propiedades del recopilador. El valor predeterminado está especificado por el recopilador; por ejemplo, para el recopilador de CSV, el valor predeterminado es ../csvcollector.properties.
-port *número_puerto*	Opcional: puerto donde se ejecuta el recopilador. El valor predeterminado es 8080. **Nota:** Este valor también se puede especificar en un archivo de propiedades del recopilador.
-bg	Opcional y sólo en UNIX. Utilice este parámetro para ejecutar el recopilador en segundo plano. **Nota:** No utilice el parámetro & de UNIX para ejecutar un recopilador en segundo plano. Utilice sólo la opción -bg.
[-Xms*tamaño_memoria_mínimo*m]	Opcional: el tamaño de almacenamiento dinámico mínimo para el recopilador. Aumente los valores de tamaño de almacenamiento dinámico si recibe errores relacionados con la falta de memoria en el proceso de recopilador. El tamaño de almacenamiento dinámico mínimo predeterminado es 256M.
[-Xmx*tamaño_memoria_máximo*m]	Opcional: el tamaño de almacenamiento dinámico máximo para el recopilador. Aumente los valores de tamaño de almacenamiento dinámico si recibe errores relacionados con la falta de memoria en el proceso de recopilador. El tamaño de almacenamiento dinámico máximo predeterminado es 768M.

Ejemplo: inicio del recopilador CSV Java

Para iniciar el recopilador CSV Java, siga estos pasos:

1. Vaya al siguiente directorio:

   ```
   $NCHOME/precision/collectors/javaCollectors/bin
   ```

2. Ejecute el siguiente mandato para iniciar el recopilador CSV Java con el archivo .jar predeterminado y los archivos de propiedades, en el puerto 8089, con un tamaño de almacenamiento dinámico mínimo de 512M y un tamaño de almacenamiento dinámico máximo de 1024M:

```
./collector.sh -Xms512m   -Xmx1024m  -jar csv/csvcollector.jar -propsFile
csv/csvcollector.properties  -port 8089 -bg
```

Detención de recopiladores Java
Utilice esta información para detener los recopiladores grabados en Java.

Acerca de esta tarea

Para detener un recopilador Java, vaya al directorio bin del recopilador Java en `$NCHOME/precision/collectors/javaCollectors/bin` y emita un mandato de interfaz de línea de mandatos. Un recopilador Java puede detenerse en una máquina local o en una máquina remota emitiendo este mandato. Emita el siguiente mandato para detener un recopilador Java (tenga en cuenta que el mandato debe introducirse en una sola línea; las opciones se explican en la Tabla 35 en la página 303):

```
shutdown_collector.sh -port port_number -host host_name
```

Tabla 35. Explicación de las opciones de línea de mandatos

Opción	**Explicación**
`-port` *número_puerto*	Necesaria: puerto donde se ejecuta el recopilador que se va a concluir.
`-host` *nombre_host*	Opcional: nombre de host donde se ejecuta el recopilador que se va a concluir. El valor predeterminado es `localhost`.

Ejemplo: detención de un recopilador Java que se ejecuta en el servidor local en el puerto 8080

Para detener un recopilador Java que se ejecuta en el servidor local en el puerto 8080, siga estos pasos:

1. Vaya al siguiente directorio:

```
$NCHOME/precision/collectors/javaCollectors/bin
```

2. Ejecute el siguiente mandato:

```
shutdown_collector.sh –port 8080
```

Inicio de recopiladores Perl
Utilice esta información para iniciar los recopiladores grabados en Perl.

Acerca de esta tarea

Para iniciar un recopilador, vaya al directorio de recopiladores correspondiente y emita un mandato de interfaz de línea de mandatos. Emita el siguiente mandato para iniciar un recopilador (tenga en cuenta que el mandato debe introducirse en una sola línea; las opciones se explican en la tabla que figura a continuación):

```
ncp_perl collector_script -cfg  COLLECTOR_CONFIG_FILE
[ -csvcfg CSV_COLLECTOR_CONFIG_FILE ] [ -listen PRECISION_PORT ]
[ -debug DEBUG ] [ -logdir ] [ -nologdir DIRNAME ]
[ -help ] [ -version ]
```

Tabla 36. Explicación de las opciones de línea de mandatos	
Opción	**Explicación**
collector_script	El nombre del script de Perl que implementa el recopilador; por ejemplo, `main.pl`.
`-cfg` *COLLECTOR_CONFIG_FILE*	Especifica el archivo de configuración del recopilador.
`-csvcfg` *CSV_COLLECTOR_CONFIG_FILE*	Utilice este parámetro opcional para especificar el nombre de un archivo CSV para utilizar como origen de datos. Especifique también este parámetro en el archivo de configuración del recopilador. **Restricción:** Este parámetro es válido sólo cuando el origen de datos es un archivo CSV.
`-listen` *PRECISION_PORT*	Método alternativo para especificar el puerto en el que el recopilador debe escuchar peticiones de Network Manager. Únicamente especifique un valor aquí si no se ha especificado ningún valor de puerto en el archivo de configuración del recopilador basado en SOAP o en el archivo de configuración del recopilador basado en CSV.
`-debug` *DEBUG*	El nivel de salida de depuración (1-4, donde 4 representa la salida más detallada).
`-logdir` *DIRNAME*	Direcciona los mensajes de registro iniciados por CTRL a `NCHOME/log/precision`.
`-nologdir` *DIRNAME*	Direcciona los mensajes de registro de cada proceso iniciado por CTRL a un archivo aparte del directorio especificado.
`-help`	Todos los componentes de Network Manager tienen una opción especial `-help` que muestra las opciones de línea de mandatos. El componente no se inicia aunque se utilice `–help` junto con otros argumentos.
`-version`	Todos los componentes de Network Manager tienen una opción `-version` especial que muestra el número de versión del componente. El componente no se inicia aunque se utilice `–version` junto con otros argumentos.

Inicio de un descubrimiento de EMS

Inicie el descubrimiento de EMS iniciando el buscador de recopiladores. Por lo general es una tarea de configuración única, necesaria cuando se añade un nuevo recopilador a la instalación.

Acerca de esta tarea

Para habilitar Network Manager para localizar los recopiladores, debe iniciar el buscador de recopiladores. El inicio del buscador de recopiladores implica la especificación de cada recopilador:

- El nombre de host del dispositivo en el que se ejecuta el recopilador.

  Nota: El nombre de host no es necesario si el recopilador se está ejecutando en el mismo servidor que el descubrimiento de Network Manager.
- El puerto del dispositivo en el que escucha el recopilador.

Si se está ejecutando un recopilador en el mismo host que Network Manager, únicamente necesita especificar el puerto.

Nota: Si va a redescubrir un dispositivo utilizando el buscador de recopiladores, especifique la dirección IP del dispositivo o la subred para redescubrir mediante la GUI de configuración de descubrimiento.

Puede iniciar el buscador de recopiladores para realizar un descubrimiento o un redescubrimiento parcial de un solo dispositivo o subred. Si inicia el buscador de recopiladores para realizar un redescubrimiento parcial, también puede especificar un solo dispositivo o subred recuperado por el recopilador.

Debe iniciar el buscador de recopiladores con el nombre de host del dispositivo en el que se está ejecutando el recopilador y el puerto de ese dispositivo en el que escucha el recopilador. Si el recopilador se está ejecutando en el mismo host que Network Manager, solo necesita especificar el puerto.

Inicio del recopilador para un primer descubrimiento

Inicie el buscador de recopiladores para un primer descubrimiento añadiendo una inserción a la tabla collectorFinder.collectorRules del archivo de configuración DiscoCollectorFinderSeeds.cfg. La siguiente inserción inicia el buscador de recopiladores con el nombre de host 172.16.25.1 y el puerto 8082. Esta inserción significa que el recopilador se está ejecutando en un host con la dirección IP 172.16.25.0, que es diferente al host en el que se está ejecutando Network Manager. El número de intentos de sustitución de este colector es de 5.

```
insert into collectorFinder.collectorRules
(
        m_Host,
        m_Port,
        m_NumRetries
)
values
(
        "172.16.25.1",
        8082,
        5
);
```

Descubrimiento de enlaces agregados

Como parte de un descubrimiento de EMS, puede recuperar información sobre algunos enlaces que se están agregando lógicamente.

Acerca de esta tarea

Network Manager puede descubrir y modelar información de agregación de enlaces desde dispositivos que ejecutan Alcatel 5620 SAM EMS.

Para descubrir la información del enlace agregado, complete las siguientes tareas:

Procedimiento

1. Configure el recopilador de Java Alcatel 5620Sam.
2. Inicie un descubrimiento.
3. Abra el Navegador de estructura y examine un dispositivo que contiene enlaces agregados.
   Los enlaces agregados se muestran dentro de la contención de dispositivo.

Resultados

Se genera un suceso afectado por servicio (SAE) si alguno de los puertos que participan en un enlace agregado tiene una alerta de gravedad 5 o superior.

Desactivación de supresión aislada para RCA

Para asegurarse de que el RCA funciona correctamente para descubrimientos de EMS, debe desactivar la supresión aislada.

Acerca de esta tarea

Network Manager aplica un modelo de RCA para la red que supone una sola ubicación desde la que el sondeo se lleva a cabo. En descubrimientos de EMS, hay, de forma efectiva, varias ubicaciones de sondeo. Para que RCA funcione correctamente, necesita desactivar la regla de RCA conocida como supresión aislada.

Para desactivar la supresión aislada, realice las siguientes tareas:

Procedimiento

1. Edite el siguiente archivo: `$NCHOME/precision/eventGateway/stitchers/RCA/ProcessProblemEvent.stch`
2. Comente la siguiente línea:
   numberOfSuppressedEvents = ExecuteStitcher('IsolatedEntitySuppression');
3. Guarde y cierre el archivo.
4. Reinicie la pasarela de sucesos, ncp_g_event.

Adición de entidades pasivas a la red

Puede utilizar el servicio de *caja negra* para definir las entidades pasivas de capa 1 en la red, para que estas entidades no gestionadas se representen en la red. Las entidades pasivas son entidades definidas por el usuario. Son las entidades adicionales que desea ver en la topología para tener una imagen completa del entorno de red.

Acerca de esta tarea

Restricción: Sólo puede añadir entidades de capa 1 a la red utilizando el servicio de caja negra.

Acerca de las entidades pasivas

Las entidades de capa 1 pasivas son entidades definidas por el usuario. Son las entidades adicionales que desea ver en la topología para tener una imagen completa del entorno de red de capa 1. Son pasivas porque no puede utilizar Network Manager para descubrirlas o gestionarlas, pero sí puede verlas representadas en mapas de topología.

Puede utilizar las entidades pasivas de varias formas. Por ejemplo:

- Para mostrar nodos no gestionados en la red.
- Para mostrar dispositivos que no están gestionados por Network Manager. Por ejemplo, un proveedor de cable utiliza los filtros entre el equipo de red para aumentar o modificar las señales. En muchos casos, estos filtros no pueden gestionarse, pero pueden añadirse al servicio de caja negra para mostrar una mayor granularidad de la red.

Configuración del recopilador Blackbox

Debe realizar tareas de configuración puntuales para poder utilizar el recopilador Blackbox para añadir las entidades pasivas a la red.

Acerca de esta tarea

Tabla 37. Configuración del recopilador Blackbox

Tarea de configuración	Información adicional
Configure el recopilador Blackbox. Para ello, debe editar el archivo de configuración del recopilador Blackbox, que se encuentra en: `$NCHOME/precision/collectors/perlCollectors/OpticalBlackboxXml/`	“Configuración de recopiladores Perl” en la página 286

Tabla 37. Configuración del recopilador Blackbox (continuación)	
Tarea de configuración	**Información adicional**
Inicialice el descubrimiento del recopilador Blackbox configurando el archivo `$NCHOME/etc/precision/DiscoCollectorFinderSeeds.cfg` para que el dominio utilice el mismo puerto que se indica en el archivo de configuración del recopilador Blackbox `OpticalBlackboxXmlCollector.cfg`.	“Inicio de un descubrimiento de EMS” en la página 304

Adición de entidades pasivas

Importe datos sobre dispositivos pasivos y otras entidades editando y cargando el archivo `blackbox.xml`.

Edición del archivo blackbox.xml

Defina dispositivos pasivos y otras entidades editando el archivo `blackbox.xml`.

Acerca de esta tarea

Procedimiento

1. Vaya al directorio `$NCHOME/precision/collectors/perlCollectors/OpticalBlackboxXml/exampleXmlData`.
2. Edite el archivo `blackbox.xml` y proporcione los datos que desea importar dentro del elemento `<blackbox>`. Utilice las etiquetas adecuadas dentro del elemento `<blackbox>`para la información de entidad que desea importar.

   Cuando edite el archivo `blackbox.xml`, tenga en cuenta las siguientes reglas:
3. Guarde y cierre el archivo.

Estructura de blackbox.xml

El archivo `blackbox.xml` se utiliza para cargar entidades pasivas (no gestionables) en la red, para que pueda verlas en una correlación de topología.

Utilice este ejemplo de un archivo `blackbox.xml` para conocer la sintaxis de las sentencias permitidas en el archivo.

```
1]    <blackbox>
2]
3]     <ne name="Passive_NE1" ip="10.20.1.2" type="Passive">
4]           <properties>
5]                   <property name="company" value="IBM"/>
6]           </properties>
7]           <entities>
8]               <entity tom_id="rack" type="FLEX_Bay" position="1" />
9]               <entity tom_id="shelf" type="FLEX_shelf" position="1-1" />
10]              <entity tom_id="shelf" type="FLEX_shelf" position="1-2" />
11]              <entity tom_id="card" type="OC12Card" position="1-2-1" />
12]              <entity tom_id="card" type="TRMTR_Slot_HS" position="1-9-1" />
13]              <entity tom_id="ptp" type="OC12_LS_PTP_V" position="1-2-1-1" />
14]              <entity tom_id="ptp" type="OC48_LINE_PTP_TRMTR_HS" position=
"1-9-1-1" />
15]              <entity tom_id="ctp" type="STS3_OC48_TRMTR_HS" position=
"1-9-1-1-25" />
16]          </entities>
17]     </ne>
18]
19]     <ne name="Passive_NE2" ip="10.11.1.30" type="ECI">
20]          <properties>
21]                  <property name="Vendor" value="ECI"/>
22]                  <property name="NeType" value="XDM100"/>
23]                  <property name="LocationName" value="MELAKA"/>
24]                  <property name="Address" value="THIRD FLOOR , COLLEGE ,
```

```
MELAKA , , Malaysia"/>
25]                   <property name="City" value="MELAKA"/>
26]                   <property name="State" value="ALOR GAJAH"/>
27]           </properties>
28]           <entities>
29]                   <entity type="FLEXPort" tom_id="ptp" label="PORT" position=
"1-1-3021-1" />
30]                   <entity type="FLEXPort" tom_id="ptp" label="PORT" position=
"1-1-3022-1" />
31]           </entities>
32]     </ne>
33]
34]     <ne name="Passive_NE3" ip="10.11.1.29" type="ECI">
35]           <properties>
36]                   <property name="Vendor" value="ECI"/>
37]                   <property name="NeType" value="XDM100"/>
38]                   <property name="LocationName" value="ARAU KANGAR"/>
39]                   <property name="Address" value="3 Ground , Sate Road ,
Arau, Kangar "/>
40]                   <property name="City" value="KANGAR"/>
41]                   <property name="State" value="PERLIS"/>
42]           </properties>
43]           <entities>
44]                   <entity type="FLEXPort" tom_id="ptp" label="PORT" position=
"1-1-3036-2" />
45]                   <entity type="FLEXPort" tom_id="ptp" label="PORT" position=
"1-1-3033-1" />
46]           </entities>
47]     </ne>
48]
49]     <tc>
50]           <aend ne="Passive_NE2" tp="1-1-3021-1"/>
51]           <zend ne="Passive_NE1" tp="1-9-1-1-25"/>
52]     </tc>
53]
54]     <tc>
55]           <aend ne="Passive_NE3" tp="1-1-3036-2"/>
56]           <zend ne="Passive_NE2" tp="1-1-3022-1"/>
57]     </tc>
58]
59]   </blackbox>
```

La tabla que aparece a continuación describe esta consulta.

Tabla 38. Ejemplo de un archivo `blackbox.xml`

Números de línea	Elemento	Descripción y atributos
1-59	<blackbox>	Caja negra. No utiliza atributos.
3-17 19-32 34-47	<ne>	Elemento de red. Utiliza los siguientes atributos: **name** (Necesario) El nombre del elemento de red. Ejemplo: name="Passive_NE1". **type** (Necesario) Un valor de tipo ="Passive" indica una entidad pasiva. **ip** (Opcional) Dirección IP de la entidad pasiva.
4-6 20-27 35-42	<properties>	Las propiedades de la entidad a la que se aplica el elemento.

Tabla 38. Ejemplo de un archivo `blackbox.xml` (continuación)

Números de línea	Elemento	Descripción y atributos
5 21-26 36-41	`<property>`	Una propiedad de la entidad. La entidad puede ser un elemento de red o una conexión topológica. **name** (Necesario) El nombre de la propiedad. Ejemplo: `name="company"`. **value** (Necesario) El valor de la propiedad. Ejemplo: `value="IBM"`.
7-16 28-31 43-46	`<entities>`	Las entidades en un elemento de red.
8-15 29-30 44-45	`<entity>`	Una entidad en un elemento de red. **label** (Opcional) Etiqueta de esta entidad. **position** (Necesario) La ubicación relativa de la entidad en el elemento de red. Ejemplo: position="1-2-1-1" significa primer bastidor - segunda estantería - primera tarjeta - primer PTP. Como práctica recomendada, liste las sentencias de entidad en orden jerárquico descendente. **tom_id** (Necesario) El ID de modelo de objetos de Telecom. Ejemplo: `tom_id="rack"`. Los valores válidos son: • bastidor • estantería • tarjeta • ptp (punto de terminación física) • ctp (punto de terminación de conexión) **type** (Opcional) El tipo de entidad. Ejemplo: `type="FLEX_Bay"`.
49-52 54-57	`<tc>`	Una conexión topológica.

Tabla 38. Ejemplo de un archivo `blackbox.xml` (continuación)		
Números de línea	**Elemento**	**Descripción y atributos**
50 55	<aend>	El inicio hipotético de una conexión topológica. **dominio** (Opcional) El nombre del dominio al que pertenece el punto final (el nombre de dominio del PTP y el elemento de red al que pertenece el PTP). Puede utilizar este atributo para especificar que uno de los puntos finales reside en otro dominio de red. Si el elemento de red remota ya existe en la base de datos, se crea una conexión topológica. Si no existe en la base de datos, no se crea ninguna conexión topológica. **ne** (Necesario) El nombre del elemento de red. **tp** (Necesario) La ubicación relativa del punto de terminación del punto final en la conexión topológica. Ejemplo: tp="1-1-3021-1" significa primer bastidor- primera estantería-tarjeta 3021 - primer punto de terminación.
51 56	<zend>	El final hipotético de una conexión topológica. **dominio** (Opcional) El nombre del dominio al que pertenece el punto final (el nombre de dominio del PTP y el elemento de red al que pertenece el PTP). Puede utilizar este atributo para especificar que uno de los puntos finales reside en otro dominio de red. Si el elemento de red remota ya existe en la base de datos, se crea una conexión topológica. Si no existe en la base de datos, no se crea ninguna conexión topológica. **ne** (Necesario) El nombre del elemento de red. **tp** (Necesario) La ubicación relativa del punto de terminación del punto final en la conexión topológica. Ejemplo: tp="1-1-3036-2" significa primer bastidor- primera estantería-tarjeta 3036 - segundo punto de terminación.

Carga del archivo blackbox.xml
Inicie el recopilador OpticalBlackboxXml para cargar el archivo the blackbox.xml e importar las entidades pasivas en la topología.

Antes de empezar
Asegúrese de que no haya ningún descubrimiento en ejecución actualmente. No obstante, el motor de descubrimiento de `ncp_disco` puede estar ejecutándose.

Acerca de esta tarea
Inicie el recopilador OpticalBlackboxXml en segundo plano emitiendo el siguiente mandato:

```
ncp_perl main.pl -cfg OpticalBlackboxXmlCollector.cfg &
```

Guía del desarrollador de recopiladores

Los usuarios avanzados pueden utilizar la Guía del desarrollador de recopiladores para crear recopiladores de descubrimiento personalizados.

La Guía del desarrollador de recopiladores proporciona información de referencia que le servirá de ayuda a la hora de crear y resolver problemas con su propio recopilador de descubrimiento.

Acceda a al Guía del desarrollador de recopiladores y a la documentación sobre infraestructura de recopiladores Perl y Java en esta URL: https://www.ibm.com/support/pages/announcing-nm-v42-collector-developer-guide-v17

Configuración de descubrimientos de MPLS

Configure un descubrimiento de MPLS para descubrir redes principales de MPLS y las VPN que utilizan estas redes. La configuración de descubrimiento de MPLS avanzado proporciona funciones de personalización extra.

Acerca del descubrimiento de MPLS

Los administradores dentro de los proveedores de servicios que ofrecen servicios VPN Multiprotocol Label Switching (MPLS) pueden descubrir redes principales MPLS y VPN MPLS para habilitar NOC en el proveedor de servicios para supervisar el estado de las VPN del cliente.

Network Manager admite el descubrimiento de las siguientes VPN que se ejecutan en redes principales MPLS:

- VPN de capa 3
- VPN de capa 2 mejoradas

Para las VPN de capa 2 mejoradas, Network Manager descubre pseudoconexiones punto a punto que enlazan dos direcciones de proveedor (PE).

En las secciones siguientes se especifican la terminología y las convenciones de visualización de la topología utilizadas en Network Manager para referirse a las redes MPLS.

Nota: Los gráficos que se muestran en esta sección son solo representaciones conceptuales de una red MPLS. No podrá ver estas vistas conceptuales en la interfaz gráfica de usuario (GUI) de Vistas de red.

VPN de MPLS de capa 3

Network Manager puede visualizar topologías de VPN de MPLS de capa 3 en una vista central o una vista perimetral.

La vista central y perimetral difieren en lo siguiente:

- La vista central muestra los direccionadores de proveedor (PE) y permite ver los direccionadores de clase core de proveedor (P) y datos de vía de acceso conmutada por etiqueta (LSP) dentro del núcleo de MPLS para cada una de las VPN que se ejecutan en el núcleo MPLS.
- La vista perimetral muestra únicamente los direccionadores PE y la nube MPLS. No permite ver los dispositivos del núcleo.

VPN de MPLS de capa 2 mejoradas

Para VPN de capa 2 mejoradas, Network Manager proporciona solo una vista perimetral de la red principal de MPLS.

Network Manager muestra una VPN de capa 2 mejorada como una recopilación de pseudoconexiones de punto a punto. Esto significa que si una VPN de capa 2 mejorada contiene más de dos direccionadores de proveedor (PE), Network Manager mostrará la VPN en varias vistas, cada una de ellas consistente en un PE único para una conexión punto a punto PE.

Tabla 39 en la página 312 muestra ejemplos de VPN de capa 2 mejoradas con dos o más PE. La tabla proporciona también el número de pseudoconexiones y, por lo tanto, el número de vistas que muestra Network Manager para cada VPN.

Tabla 39. Número de pseudoconexiones de una VPN de capa 2 mejorada		
Número de PEs en una VPN de capa 2 mejorada	**Número de pseudoconexiones punto a punto**	**Número de vistas que Network Manager muestra para esta VPN**
2	1	1
3	3	3
4	6	6

Configuración de descubrimiento de MPLS estándar y avanzado

Configure un descubrimiento de MPLS estándar para descubrir todas las redes MPLS y usos de la convención de nomenclatura predeterminada para las VPN descubiertas. La configuración de descubrimiento de MPLS estándar también habilita la visualización de sucesos afectados por el servicio (SAE) en el **Visor de sucesos**. La configuración de descubrimiento de MPLS avanzado proporciona funciones de personalización extra.

Las actividades de configuración de una red MPLS incluyen el inicio, el ámbito y otras actividades de descubrimiento estándar.

Configuración de descubrimiento de MPLS estándar y avanzado difieren en lo siguiente:

- Descubrimiento de MPLS estándar: descubre todas las redes MPLS y usos de la convención de nomenclatura predeterminada para las VPN descubiertas
- Descubrimiento de MPLS avanzado: con las opciones de configuración avanzadas podrá:
  - Restrinja el ámbito del descubrimiento a una VPN o VRF concreta
  - Configure sus propias convenciones de nombres de VPN
  - Añada datos de etiquetas para descubrimientos MPLS

Después de haber configurado y ejecuta un descubrimiento de MPLS, los operadores puede supervisar VPN de cliente de las siguientes formas:

- Vea mapas de topología de las VPN seleccionadas, que muestran el estado de alerta de las VPN y otros dispositivos de las VPN.
- Identifique sucesos afectados por servicio (SAE) en **Visor de sucesos**. Un SAE es una alerta que advierte a los operadores de que un servicio al cliente esencial, por ejemplo, una VPN de cliente, se ha visto afectada por uno o varios sucesos de red. Los sucesos de red subyacentes se encuentran en una interfaz de un direccionador PE o CE.

Acerca de sucesos afectados por servicios

Un suceso afectado por servicio (SAE) es una alerta que avisa a los operadores que un suceso de cliente grave se ha visto afectado por uno o más sucesos de red.

Un SAE se produce cuando uno o varios sucesos se producen en una interfaz de proveedor (PE) o de cliente (CE) en una red privada virtual (VPN) o un servicio de LAN privada virtual (VPLS). Los sucesos de red subyacentes se encuentran en una interfaz de un direccionador PE o CE, o en el enlace entre ellos. Debe configurar el descubrimiento MPLS para inferir la existencia de direccionadores CE para que se generen todos los SAE posibles para las VPN de cliente.

La siguiente lista proporciona dos ejemplos de sucesos SAE generados en dos VPN de cliente distintas:

- Un SAE generado en una VPN de cliente-1 debido a una interrupción `Mpls VRF Down` en una interfaz del direccionador de proveedor (PE)
- Un SAE generado en una VPM de cliente-3 debido a una interrupción `LinkDown` en una interfaz de direccionador CE

Cada SAE aparece como una alerta en **Visor de sucesos**. La aparición de la SAE advierte a los operadores de que una VPN de cliente se ha visto afectada, posiblemente de manera muy grave, por uno o más

sucesos de la red. Los operadores pueden hacer clic con el botón derecho del ratón en el SAE y emitir un mandato para ver los sucesos subyacentes que causaron el SAE.

Para obtener más información sobre el **Visor de sucesos**, consulte la *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*.

Configuración del descubrimiento MPLS estándar

Configure un descubrimiento de MPLS para descubrir redes principales de MPLS y las VPN que utilizan estas redes.

Acerca de esta tarea

Además de las actividades de configuración de descubrimiento estándar, deberá realizar algunas actividades de configuración de descubrimiento específicas de MPLS.

- Configure agentes de MPLS
- Opcional: establezca las VPN para que sean los destinos de ruta los que les asignen nombres, en lugar de los VRF
- Configure SNP y Telnet para garantizar que los agentes puedan acceder a los dispositivos de red
- Configure Network Manager para inferir la existencia de direccionadores CE. Este paso es necesario para habilitar operadores para ver los sucesos afectados por el servicio en **Visor de sucesos**.

Estas actividades de configuración de descubrimiento específicas de EMS se describen en los siguientes temas.

Configuración de agentes MPLS

Como parte de la configuración del descubrimiento de MPLS debe habilitar uno o más agentes MPLS. También puede resolver el problema de direcciones IP duplicadas en redes privadas virtuales (VPN) diferentes configurando el agente AsAgent.

Acerca de esta tarea

Se proporcionan los siguientes agentes MPLS y los archivos de definición de agente (.agnt) correspondientes:

Procedimiento

- Agente Juniper Telnet (JuniperMPLSTelnet.agnt)
- Agente de direccionador Juniper ERX (UnisphereMPLSTelnet.agnt)
- Agente Cisco MPLS Telnet (CiscoMPLSTelnet.agnt)
- Agente Cisco MPLS SNMP (CiscoMPLSSnmp.agnt)
- Agente Laurel MPLS Telnet (LaurelMPLSTelnet.agnt)

  Nota: El agente Laurel MPLS Telnet está diseñado únicamente para descubrimientos basados en RT- (RouteTarget).

Resultados

Esto agentes pueden descubrir datos VPN de MPLS y del servicio privado virtual del LAN desde dispositivos de la red.

Consejo: Los agentes que recuperan información de VPLS pueden recuperar grandes cantidades de datos. La habilitación de estos agentes puede agregar un tiempo de proceso significativo al proceso de descubrimiento. Si no es necesario redescubrir información de VPLS, inhabilite estos agentes para obtener un descubrimiento más rápido.

Nota: Si tiene una red MPLS que soporta las VPN Layer 3 y Layer 2 mejorada, los mismos agentes MPLS descubren ambos tipos de VPN. Las vistas de red también pueden particionar las VPN Layer 3 y Layer 2 mejorada simultáneamente en la misma red MPLS principal.

Si la red de MPLS contiene material de Cisco, habilite los agentes Cisco MPLS Telnet y Cisco MPLS SNMP. Estos dos agentes se complementan entre sí, de la siguiente manera:

- El agente Cisco MPLS SNMP se centra solo en dispositivos con un sistema operativo de interconexión de redes (IOS) que soportan por completo un descubrimiento de MPLS basado en SNMP
- El agente CiscoMPLSTelnet se centra solo en dispositivos que ejecutan un IOS que no soporta por completo un descubrimiento basado en SNMP

Atención: Tenga cuidado al alterar el archivo CiscMPLSSnmp.agnt. Algunos dispositivos de red pueden contener versiones de IOS que tengan una brecha que afecte al dispositivo cuando se solicitan determinados datos SNMP de MPLS. Estas versiones de IOS se han filtrado de manera predeterminada en el archivo CiscMPLSSnmp.agnt.

Además de estas actividades de configuración de descubrimiento estándar, también puede cambiar el ámbito del descubrimiento de MPLS restringiendo el ámbito a VPN o VRF específicos.

Configuración de agentes Telnet de MPLS
Los agentes CiscoMPLSTelnet, JuniperMPLSTelnet, LaurelMPLSTelnet y UnisphereMPLSTelnet obtienen datos de dispositivos principalmente a través de Telnet. Debe habilitar estos agentes y configurar el acceso Telnet para asegurarse de que los agentes Telnet de MPLS pueden acceder a los dispositivos y pueden entender la salida de los mismos.

Acerca de esta tarea

Realice los siguientes pasos para configurar el acceso a Telnet para los agentes Telnet de MPLS:

Procedimiento

1. Llene el archivo de configuración de Telnet `TelnetStackPasswords.cfg` para que los agentes puedan acceder a los dispositivos de destino.
2. Configure el ayudante de Telnet para que los agentes puedan entender la salida de los dispositivos.

Configuración de agentes SNMP de MPLS
El agente de CiscoMPLSSnmp obtiene datos de dispositivos utilizando SNMP. Debe habilitar este agente y configurar el acceso SNMP para asegurarse de que este agente puede acceder a los dispositivos y puede entender la salida de los mismos.

Acerca de esta tarea

Para configurar el acceso de SNMP para agentes SNMP de MPLS:

Nota: CiscoMPLSSnmp.agnt intenta recuperar las VPN de L2 utilizando los mandatos de "muestra" de telnet si el agente no puede recuperar los datos a través de SNMP.

Procedimiento

1. Configurar el acceso de SNMP a los dispositivos.
2. Configure el ayudante de SNMP para que los agentes puedan entender la salida de los dispositivos.

Configuración del agente AsAgent
Para resolver el problema de las direcciones IP duplicadas en diferentes VPN, active el agente AsAgent y proporcione a Network Manager un archivo de correlaciones, `ASMap.txt`, que contiene una lista completa de dispositivos en cada VPN, junto con una etiqueta `AddressSpace`, que define la VPN a la que pertenece el dispositivo.

Acerca de esta tarea

Durante un descubrimiento de MPLS, es posible que Network Manager descubra dispositivos en diferentes VPN con idénticas direcciones IP. En este caso, Network Manager no podrá diferenciar estos dispositivos y es posible que resuelva la conectividad de los dispositivos de forma incorrecta. Los

dispositivos en cuestión pueden ser los direccionadores CE en el extremo de las VPN o dispositivos dentro de las VPN.

En el archivo de correlaciones ASMap.txt, proporcione una lista completa de dispositivos en cada VPN, junto con una etiqueta AddressSpace, que define la VPN a la que pertenece el dispositivo.

Tabla 40 en la página 315 proporciona una descripción del agente AsAgent que es necesario activar para resolver el problema de las direcciones IP duplicadas.

Tabla 40. Agente AsAgent

Nombre del agente	Función
AsAgent	Permite a Network Manager identificar de manera exclusiva dispositivos en distintas VPN con idénticas direcciones IP y, por lo tanto, resolver de forma correcta la conectividad de los dispositivos. Este agente funciona en conjunción con el agrupador ASRetprocessing.stch y con el archivo ASMap.txt en NCHOME/precision/etc.

Tabla 41 en la página 315 proporciona formato al archivo ASMap.txt mostrando un ejemplo del contenido de este archivo. Los campos de este archivo de texto deben estar separados por tabuladores.

Tabla 41. Formato del archivo ASMap.txt

Dirección IP exclusiva	Espacio de direcciones	Dirección IP
192.168.0.1	CUSTOMER-1	192.168.2.1
192.168.0.2	CUSTOMER-1	192.168.2.21
192.168.0.3	CUSTOMER-1	192.168.2.22
192.168.0.4	CUSTOMER-2	192.168.2.1
192.168.0.5	CUSTOMER-2	192.168.2.31
192.168.0.6	CUSTOMER-2	192.168.2.32

Uso de valores de RT en lugar de nombres VRF

De forma predeterminada, las VPN se denominan basándose en los nombres VRF familiares. Puede elegir utilizar destinos de ruta (RT) en lugar de denominar VPN.

Antes de empezar

Importante:

Si se han descubierto dispositivos previamente con la denominación VRF, pueden aparecer entidades VPN duplicadas en el siguiente descubrimiento. Por ejemplo, la misma entidad VPN puede aparecer dos veces, una vez con el nombre VRF y otra con el valor RT. Para evitar entradas de dispositivo duplicadas, establezca el valor LingerTime de todos los dispositivos en la topología en cero antes de ejecutar el siguiente descubrimiento. Para hacerlo, siga estos pasos:

1. Inicie sesión en el proveedor de servicios OQL con el siguiente mandato:

```
ncp_oql -domain NCOMS -service Model
```

2. Ejecute el mandato siguiente para establecer LingerTime en cero:

```
update ncimCache.lingerTime set lingerTime = {LINGERTIME=0};
go
```

Acerca de esta tarea

En redes MPLS, Network Manager utiliza el descubrimiento basado en destino de ruta (RT), utilizando la información de RT y VRF para determinar qué direccionadores de proveedor están implicados en una VPN. La vista principal consta de todos los dispositivos habilitados para MPLS y las VPN se resuelven basándose en la información de RT.

Para utilizar valores de RT en lugar de nombres VRF:

Procedimiento

1. Salga de todas las instancias de la GUI **Configuración de descubrimiento**.
2. Vaya al directorio `NCHOME/etc/precision`.
3. Edite el archivo `DiscoConfig.`*`NombreDominio`*`.cfg` y establezca el campo **`m_RTVPNResolution`** en 1 en la tabla disco.config. El valor predeterminado es 2 (utilizar VRF).
4. Reinicie los procesos ncp para volver a leer los archivos de configuración:

   ```
   itnm_stop ncp
   itnm_start ncp
   ```

   También puede reiniciar el proceso ncp_config.

Qué hacer a continuación

Nota: Los descubrimientos basados en RT no necesitan datos de etiqueta. No obstante, puede recuperar los datos de etiqueta tal como se describe en "Datos de etiqueta de ajuste preciso" en la página 321.

Cómo deducir la existencia de direccionadores CE

Puede deducir la existencia de los direccionadores CE de sus clientes realizando especificaciones en las opciones de configuración de descubrimiento avanzado dentro de la GUI de configuración de descubrimiento.

Acerca de esta tarea

Si el host en el que Network Manager está instalado no tiene acceso a los direccionadores CE de sus clientes, Network Manager no podrá descubrir estos direccionadores directamente. Esta situación se produce normalmente cuando la empresa que proporciona los servicios de MPLS es propietaria de los direccionadores PE pero no tiene acceso a los direccionadores CE, de los cuales los clientes que ejecutan VPN son propietarios.

Nota: Esta situación no se produce si la empresa que proporciona los servicios MPLS es propietaria y gestiona tanto direccionadores PE como CE y, por lo tanto, tiene acceso a ambos conjuntos de dispositivos.

Para deducir la existencia de los direccionadores CE de sus clientes, especifique lo siguiente en las opciones de configuración de descubrimiento avanzado dentro de la GUI de configuración de descubrimiento.

Nota: Solo debe realizar esto en donde la interfaz de PE se encuentre en una subred /30. En este caso, el otro dispositivo en la subred debe ser el direccionador CE y la dirección IP del CE será la otra dirección en la subred /30.

Limitations on inferring CE routers:

- Evite deducir la existencia de direccionadores CE si los direccionadores PE están conectados a los direccionadores CE mediante enlaces de serie y si sabe que existe un duplicado de la dirección IP entre los direccionadores y dispositivos dentro de la red principal MPLS. Network Manager eliminará de la topología los direccionadores principales MPLS descubiertos que tienen la misma dirección IP como una dirección IP CE deducida.
- Si los direccionadores PE están conectados a los direccionadores CE mediante Ethernet, puede deducir la existencia de direccionadores CE sin necesidad de realizar otro tipo de comprobaciones. En este

caso, Network Manager puede determinar la dirección MAC del direccionador CE. Si Network Manager ha descubierto otro dispositivo con la misma dirección MAC, debe ser el direccionador CE. En este caso, Network Manager utiliza los datos del dispositivo descubierto y no deduce la existencia del CE.

Configuración del descubrimiento MPLS avanzado

Configure un descubrimiento de MPLS avanzado para las funciones de personalización adicionales no incluidas en el descubrimiento de MPLS estándar.

Acerca de esta tarea

Cuando configure un descubrimiento de MPLS avanzado, debe llevar a cabo las siguientes actividades además de las necesarias para un descubrimiento de MPLS estándar.

- Definir el ámbito del descubrimiento de MPLS: permite restringir el ámbito del descubrimiento a una VPN o VRF determinada.
- Especificar un nombre de VPN: le permite configurar su propia convención de nomenclatura de VPN
- Ajustar el descubrimiento de datos de etiqueta: le permite recuperar manualmente datos de etiqueta para descubrimientos MPLS

Configuración del descubrimiento de túneles de ingeniería de tráfico MPLS

Para descubrir los túneles de ingeniería de tráfico MPLS, habilite el agente StandardMPLSTE, configure la información recuperada y configure el ámbito de la búsqueda.

Modalidades de descubrimiento de túnel de ingeniería de tráfico MPLS
Configure la modalidad de descubrimiento según cuánto detalle desee recuperar.

Se proporciona una conmutación de modalidad en el archivo de configuración del agente de descubrimiento que configura instancias de túneles específicas, al que se le pueden agregar comodines, para recuperar distintas cantidades de datos de túnel. Puede seleccionar cualquiera de las siguientes modalidades.

HeadEndHops (valor predeterminado)

En la modalidad HeadEndHops, el agente recuperará la cabecera y la cola del túnel, y los LSR de tránsito y las interfaces de próximo salto están identificados al consultar al LSR de cabecera datos de salto de ruta reales y calculados. Los datos de ruta reales y calculados se recuperan de las tablas MIB mplsTunnelARHopTable y mplsTunnelCHopTable, respectivamente. Este modo de descubrimiento no almacena instancias de túnel de transición y de extremo alejado en relación con LSR de transición y de extremo alejado. Se creará una conexión en la topología TE MPLS entre las interfaces LSR de extremo cercano y extremo alejado mediante saltos de dispositivo de transición (si están presentes), asociados con el objeto del túnel LSR de extremo alejado para la interfaz de túnel correspondiente.

Los señaladores MPLS de conexiones cruzadas que se descubren y se resuelven al principio del túnel se resolverán en el ID de LSP adecuado cuando resulte posible.

Puede utilizar esta información para determinar si la vía de acceso real tomada por un túnel es distinta a la vía de acceso calculada por los cálculos de CSPF (Compute Shortest Path First). Verá la vía de acceso calculada y la real, aunque no hay forma de determinar que un LSR esté actuando en una capacidad de tránsito o de cola sin mirar a los datos de túnel LSR de cabecera.

Nota: Los datos de ruta reales sólo están disponibles si se ha especificado RRO (Record Route Option) para la instancia del túnel.

En el esquema de la tabla scope.mplsTe, la modalidad HeadEndHops correlaciona al valor 1 de m_Mode.

HeadTailEnd

En la modalidad HeadTailEnd, sólo se resuelven los puntos de cabecera y de cola de túnel MPLS TE, consultando el LSR (Label Switching Router) de cabecera. Esta modalidad proporciona la mínima cantidad de información acerca de los túneles MPLS TE. Se creará una conexión en la topología MPLS

TE entre las interfaces LSR de cabecera y de cola. Se asociará una instancia de recurso de túnel con la entidad LSR de túnel de cabecera.

En esta modalidad, no puede identificar los LSR de tránsito, y los datos de ruta reales y calculados no se recuperan.

Los señaladores MPLS de conexiones cruzadas que se descubren y se resuelven al principio del túnel se resolverán en el ID de LSP adecuado cuando resulte posible.

En el esquema de la tabla scope.mplsTe, la modalidad HeadTailEnd correlaciona hasta el valor 2 de m_Mode.

AllLSRTunnelsAndHops

En la modalidad AllLSRTunnelsAndHops, el agente recupera la cabecera y la cola del túnel e identifica los LSR de tránsito y las interfaces de próximo salto al consultar al LSR de cabecera datos de salto de ruta reales y calculados. Los datos de ruta reales y calculados se recuperan de las tablas MIB mplsTunnelARHopTable y mplsTunnelCHopTable, respectivamente. Este modo de descubrimiento almacena instancias de túnel de transición y de extremo alejado en relación con LSR de transición y de extremo alejado. La modalidad crea una conexión en la topología MPLS TE entre las interfaces LSR de cabecera y de cola que están asociadas con los objetos de túnel LSR de cabecera (para la interfaz de túnel) y de tránsito y de cola. Las conexiones de ruta reales y calculadas están asociadas con tipos de entidad de conexión real y calculada, que están agregadas en secuencia desde la entidad de túnel LSR de cabecera. Se asociará una instancia de recurso de túnel con la entidad LSR de túnel de cabecera.

Puede utilizar esta información para determinar si la vía de acceso real tomada por un túnel es distinta a la vía de acceso calculada por los cálculos de CSPF. Consulte la vía de acceso real y calculada y determine el rol de tránsito o de cola de un LSR sin mirar a la instancia de túnel LSR de cabecera.

Nota: Los datos de ruta reales sólo están disponibles si se ha especificado RRO (Record Route Option) para la instancia del túnel.

Los señaladores MPLS de conexiones cruzadas que se descubren y se resuelven al principio del túnel se resolverán en el ID de LSP adecuado cuando resulte posible.

En el esquema de la tabla scope.mplsTe, la modalidad AllLSRTunnelsAndHops correlaciona hasta el valor 3 de m_Mode.

Tareas relacionadas

Habilitación del agente StandardMPLSTE
Para descubrir túneles TE de MPLS, habilite el agente StandardMPLSTE y añada las cadenas de comunidad de SNMP pertinentes.

Configuración del agente StandardMPLSTE
Configure los túneles que se van a descubrir y qué detalles se van a recuperar.

Habilitación del agente StandardMPLSTE
Para descubrir túneles TE de MPLS, habilite el agente StandardMPLSTE y añada las cadenas de comunidad de SNMP pertinentes.

Acerca de esta tarea

Para habilitar el agente StandardMPLSTE, realice los siguientes pasos.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Configuración del descubrimiento de red**.
2. En la lista **Dominio**, seleccione el dominio requerido.
3. Haga clic en el separador **Agentes de descubrimiento completo**.

   Aparecerá la **Lista de agentes**, que muestra todos los agentes de descubrimiento disponibles de la opción de descubrimiento seleccionada.

4. Marque el recuadro de selección, situado junto al agente StandardMPLSTE.
5. Haga clic en **Guardar**  .
6. Si desea volver a descubrir túneles TE de MPLS, habilite el agente StandardMPLSTE para redescubrimientos parciales.
   a) Haga clic en el separador **Agentes de descubrimiento parcial**.
   b) Marque el recuadro de selección, situado junto al agente StandardMPLSTE.
   c) Haga clic en **Guardar**  .
7. Asegúrese de que se han configurado correctamente las cadenas de comunidad para acceder a los dispositivos en los túneles TE de MPLS.

Conceptos relacionados

Modalidades de descubrimiento de túnel de ingeniería de tráfico MPLS
Configure la modalidad de descubrimiento según cuánto detalle desee recuperar.

Tareas relacionadas

Configuración del agente StandardMPLSTE
Configure los túneles que se van a descubrir y qué detalles se van a recuperar.

Configuración del agente StandardMPLSTE
Configure los túneles que se van a descubrir y qué detalles se van a recuperar.

Acerca de esta tarea

Para configurar el agente StandardMPLSTE, realice los siguientes pasos.

Procedimiento

1. Haga una copia de seguridad y edite el archivo `NCHOME/etc/precision/DiscoScope.cfg`.
2. Ubique y edite la inserción en la tabla scope.mplsTe o cree una nueva inserción. Cree o edite una inserción similar a la siguiente:

```
insert into scope.mplsTe
(
      m_Protocol,
   m_Zones,
   m_Mode,
   m_TunnelFilter
)
values
(
   1,
   [{m_Subnet = '192.168.1.0', m_NetMask = 24 }],
   2,
   1
);
```

   Esta inserción configura el agente para se comporte de la siguiente manera:

   - Utiliza IPv4.
   - Incluye (`m_Tunnelfilter=1`) la subred 192.168.1.* en el descubrimiento de cabeceras de túnel.
   - Recupera datos para la cabecera y la cola del túnel pero no para los direccionadores de tránsito.
3. Guarde y cierre el archivo.
4. Detenga y reinicie el motor de descubrimiento, el proceso **`ncp_disco`**, para que se apliquen los cambios en su configuración.

Conceptos relacionados

Modalidades de descubrimiento de túnel de ingeniería de tráfico MPLS
Configure la modalidad de descubrimiento según cuánto detalle desee recuperar.

Tareas relacionadas

Habilitación del agente StandardMPLSTE
Para descubrir túneles TE de MPLS, habilite el agente StandardMPLSTE y añada las cadenas de comunidad de SNMP pertinentes.

Definición del ámbito de un descubrimiento MPLS/VPN

Cuando se configure el descubrimiento de una o más redes privadas virtuales (VPN) que se ejecutan en una principal de MPLS, puede restringir el ámbito de este descubrimiento a un nombre de VPN particular o a un nombre de tabla de direccionamiento VPN y reenvío (VRF).

Acerca de esta tarea

Puede restringir el ámbito configurando la sección opcional DiscoAgentDiscoveryScoping en el archivo *.agnt. Las opciones configurables están descritas en Tabla 42 en la página 320.

Tabla 42. Definición de los requisitos del ámbito MPLS

Opción	**Función**
IncludeVRF	Permite el descubrimiento del VRF especificado
IncludeVPN	Permite el descubrimiento de la VPN especificada
ExcludeVPN	No descubre los VRF dentro de la VPN especificada
ExcludeVRF	No descubre el VRF especificado

El orden de precedencia para `Exclude` y `Include` dentro de la sección DiscoAgentDiscoveryScoping es:

1. Excluir
2. Incluir

El orden de precedencia para el VRF y la VPN dentro de DiscoAgentDiscoveryScoping es:

1. VRF
2. VPN

Por ejemplo, si incluye una VPN, pero otro filtro excluye un VRF en su VPN, se excluirá el VRF. Si se excluye una VPN, pero otro filtro incluye un VRF dentro de esa VPN, se incluirá el VRF.

Los nombres de VRF son sensibles a mayúsculas y minúsculas y un asterisco (*) representa un comodín para cualquier nombre de VRF o VPN cuando se utilizan en la parte de nombre de la configuración. El comodín se puede utilizar con cualquiera de las opciones anteriores.

El ámbito por nombre de VPN solo funciona cuando los nombres de VRF configurados en los dispositivos que descubren los agentes MPLS están en el formato VRF recomendado por Cisco. Un VRF se nombra basándose en la VPN o las VPN con servicio y en el tipo de topología. El formato para los nombres VRF es:

```
V [number assigned to make the VRF name unique]: [VPN_name]
```

Por ejemplo, en una VPN denominada `precision`, un VRF para un direccionador de límite de concentrador sería:

```
V1:precision
```

Un VRF para un direccionador de límite de radio en la VPN `precision` sería:

```
V1:precision-s
```

Un VRF para una topología de VPN de extranet en la VPN `precision` sería:

```
V1:precision-etc
```

El siguiente ejemplo define un ámbito para un descubrimiento en un sistema en el que hay cuatro VRF: `V65:Precision-etc`, `V65:Precision-s`, `V65:Precision`, y `V44:AcmeSheds`.

```
//2 VRFs are to be included
//
DiscoAgentDiscoveryScoping
{
    IncludeVRF = “V65:Precision-etc”;
    IncludeVRF = “V44:AcmeSheds”;
}
//All 4 VRFs are to be included
//
DiscoAgentDiscoveryScoping
{
    IncludeVPN = “Precision”;
    IncludeVRF = “V44:AcmeSheds”;
}
```

Datos de etiqueta de ajuste preciso

Los agentes MPLS utilizados para descubrir redes MPLS no recuperan datos de etiqueta de forma predeterminada. No obstante, puede configurar los agentes para recuperar manualmente datos de etiqueta.

Resultados

Puede recuperar manualmente datos de etiqueta con la inserción siguiente en la sección DiscoAgentDiscoveryScoping del archivo `.agnt` del agente MPLS adecuado:

```
DiscoAgentDiscoveryScoping
{
    GetMPLSLabelData = 1;
}
```

Nota: No todos los agentes MPLS admiten esta opción. Compruebe la descripción del agente para obtener información sobre si el agente concreto admite esta opción. Si se admite, el agente recupera datos de etiqueta, además de los datos utilizados para el descubrimiento MPLS. No obstante, los datos de etiqueta adicionales no los utiliza ningún agrupador predeterminado y no se almacenan en NCIM. El uso de esta opción para recuperar datos de etiqueta requiere la configuración de la recopilación de datos personalizada con agrupadores personalizados para consumir los datos de etiqueta. Para obtener más información, consulte Capítulo 17, “Descubrimiento y uso de datos personalizados”, en la página 407. Para obtener ayuda sobre cómo escribir agrupadores personalizados, póngase en contacto con el soporte de IBM.

Fix Pack 2 *Configuración del descubrimiento de VPN de Huawei*

Para visualizar la información sobre VPN de dispositivos Huawei, es necesario configurar el descubrimiento.

Acerca de esta tarea

Network Manager puede descubrir y visualizar dispositivos de límite de proveedor orientado al usuario (UPE) y límite de proveedor de red (NPE) con interfaces de pseudocable que formen parte de una VPN de Huawei. También puede crear instancias de interfaz de conmutador virtual (VSI) para los NPE.

Para configurar el descubrimiento de las VPN de Huawei, lleve a cabo los siguientes pasos.

Procedimiento

1. Asegúrese de que la salida de los dispositivos UPE y NPE está definida como `display vsi verbose`.

2. Asegúrese de que `m_RTBasedVPNs`, en la tabla de base de datos `disco.config`, está definido como 1.
3. Asegúrese de que el agente de descubrimiento HuaweiMPLSTelnet está habilitado.
4. Haga una copia de seguridad y edite estos agrupadores: `BuildMPLSContainers.stch`, `ResolveVPLSConnections.stch`, y `MPLSProcessing.stch`.
5. Establezca el valor de `modelHuaweiVPN` en 1 en cada agrupador.
6. Inicie un descubrimiento.

Qué hacer a continuación

Cuando el descubrimiento haya finalizado, vea los dispositivo de una red filtrando por VPLS VPN.

Configuración de descubrimientos de NAT

Configure un descubrimiento de conversión de direcciones de red (NAT) para descubrir entornos de NAT, correlacionando el identificador de espacio de direcciones de un dominio de NAT con la dirección IP del dispositivo de pasarela de NAT asociado.

Acerca de la conversión de direcciones de red

El número de direcciones IP disponibles en el actual formato de 32 bits no es suficiente para satisfacer el crecimiento de la demanda de acceso a Internet. La conversión de direcciones de red (NAT) se concibió como una solución a corto plazo a este problema proporcionando un método para conectar varios ordenadores a una red IP utilizando una dirección IP pública única o un número pequeño de direcciones IP públicas únicas.

NAT se utiliza por lo general en empresas en las que un direccionador NAT se sitúa en el extremo de la red privada (a la que se hace referencia en este contexto como dominio *stub*) y traduce las direcciones IP anexadas a los paquetes que entran y abandonan el dominio interno. El direccionador NAT que actúa realmente como un agentes entre Internet y la red local, mantiene una lista de las correlaciones entre direcciones públicas y privadas.

Nota: Un dominio interno es una red local que utiliza direcciones IP internas. La red puede utilizar direcciones IP sin registrar y privadas en las comunicaciones internas (estas direcciones deben convertirse en direcciones IP públicas y exclusivas en las comunicaciones fuera de la red. Las direcciones utilizadas internamente por un dominio interno pueden utilizarlas otro también internamente.

Por ejemplo, cuando un equipo dentro de la red privada solicita información de la red pública, el direccionador NAT convierte automáticamente la dirección privada de ese equipo a la dirección pública del dominio, que es la única dirección que se transmite a la red pública. Cuando se devuelve la información solicitada, el direccionador NAT consulta su lista interna de correlaciones de direcciones públicas con privadas para reenviar la información al equipo que corresponda.

Existen varias formas de configurar un entorno NAT. Las siguientes descripciones detallan los tipos de entorno NAT más frecuentes.

Entornos NAT estáticos

En un entorno NAT estático, el direccionador NAT correlaciona las direcciones privadas y públicas una por una, es decir, que la dirección privada de un determinado dispositivo se correlaciona siempre con la misma dirección pública. Este tipo de entorno NAT se utiliza con frecuencia con dispositivos a los que necesita acceder la red pública.

Entornos NAT dinámicos

En un entorno NAT dinámico, el direccionador NAT asigna dinámicamente direcciones IP públicas, procedentes de un grupo de direcciones, a los dispositivos de la red privada que deseen comunicarse con la red pública. Una variación en la NAT dinámica, *overloading* o PAT (Port Address Translation), correlaciona varias direcciones privadas a la misma dirección pública utilizando distintos puertos.

Rangos de direcciones privadas

El organismo Internet Assigned Numbers Authority (IANA) ha asignado varios rangos de direcciones para utilizar con las redes privadas.

Los rangos de direcciones para utilizar con redes privadas son:

- Clase A: `10.0.0.0` a `10.255.255.255`
- Clase B: `172.16.0.0` a `172.31.255.255`
- Clase C: `192.168.0.0` a `192.168.255.255`

Una dirección IP dentro de estos rangos se considera, por lo tanto, no direccionable, debido a que no es exclusiva. Cualquier red privada que necesite utilizar direcciones IP de forma interna puede utilizar cualquier dirección dentro de estos rangos sin tener que coordinarse con el IANA o un registro de Internet. Las direcciones dentro de este espacio de direcciones son solo exclusivas dentro de una determinada red privada.

Todas las direcciones fuera de estos rangos se consideran públicas.

Acerca del descubrimiento de NAT

Puede utilizar Network Manager para gestionar entornos de NAT, aunque existen algunas restricciones en cuanto a los tipos de entornos de NAT admitidos actualmente.

Network Manager puede interrogar a pasarelas NAT conocidas y admitidas para obtener una lista de correlaciones de direcciones IP públicas con privadas en dominios NAT. También, estas correlaciones se pueden proporcionar de forma manual. Network Manager puede descubrir estos dispositivos detrás de las pasarelas NAT que tienen una dirección IP pública.

Cada dominio NAT tiene un identificador de espacio de direcciones exclusivo. Cada dispositivo de un dominio NAT tiene el identificador de espacio de direcciones adecuado anexado a su registro. Esto permite gestionar los dispositivos (por ejemplo, sondearlos).

Restricciones relativas al descubrimiento de NAT

Existen varias restricciones sobre la gestión de entornos de NAT mediante Network Manager.

La gestión de entornos de NAT mediante Network Manager está restringida por las siguientes condiciones:

- Network Manager puede descubrir uno o varios entornos de NAT; pero todos deben usar la correlación de direcciones NAT estáticas.
- Network Manager puede descubrir dispositivos en varios dominios NAT; independientemente de si las direcciones IP privadas de los dispositivos están duplicadas en otros dominios NAT o no. Sin embargo, la dirección IP pública de cada dispositivo de cada dominio debe ser exclusiva.
- Los dispositivos con un dominio NAT que tengan solo direcciones IP privadas no podrán ser descubiertos ni gestionados mediante Network Manager.
- El proceso de descubrimiento debe descubrir el entorno NAT desde el exterior, es decir, desde la red pública.
- Las direcciones IP virtuales, como las direcciones Hot Standby Routing Protocol (HSRP), no se pueden correlacionar. Debe utilizarse la dirección física real
- Para que el descubrimiento pueda ejecutarse, es necesario proporcionar lo siguiente:
  - Las direcciones de todas las pasarelas NAT compatibles.
  - Es necesario descubrir las conversiones de pasarelas NAT, bien de forma automática o suministrando al agente de descubrimiento NATTextFileAgent un archivo sin formato de correlaciones de direcciones IP públicas con privadas.

Diferencias en un flujo de proceso de descubrimiento de NAT

El flujo de proceso de un descubrimiento de NAT difiere del flujo de proceso de un descubrimiento normal.

Descarga de información sobre conversiones
Los agentes NAT descargan información sobre la conversión NAT en la tabla de base de datos translations.NATTemp para que los buscadores puedan procesar otras entidades.

El resto de dispositivos descubiertos se insertan en la tabla finders.pending en tanto que el agrupador BuildNATTranslation.stch crea una tabla de conversión global y la almacena en la tabla de base de datos translations.NAT.

Los buscadores, ayudantes y otros componentes que necesiten acceder a los dispositivos pueden utilizar esta tabla para buscar la dirección de cualquier dispositivo detrás de una pasarela de NAT.

Creación de topología
Cuando se crea la topología, el agrupador `AddBaseNATTags.stch` añade información NAT al registro de topología de cada dispositivo en un dominio NAT.

Tabla 43 en la página 324 muestra la información que se añade al registro de topología para cada dispositivo.

Tabla 43. Información NAT añadida a un registro de dispositivo

Columna	**Descripción**
`ExtraInfo->m_AddressSpace`	El nombre del espacio de dirección NAT al que pertenece el dispositivo. Este valor se establece en la tabla `translations.NATAddressSpaceIds`. Si el descubrimiento no está utilizando NAT, o si el dispositivo está en el dominio público, este valor es NULL.
`ExtraInfo->m_NATTranslated`	Un entero booleano que indica si el dispositivo se encuentra detrás de una pasarela de NAT.
`ExtraInfo->m_InsideLocalAddress`	Dirección privada del dispositivo.
`ExtraInfo->m_OutsideGlobalAddress`	Dirección pública del dispositivo.

Configuración de un descubrimiento NAT

Configure un descubrimiento NAT para descubrir entornos de NAT y habilitar Network Manager para gestionar entornos de NAT.

Acerca de esta tarea

Establezca la mayoría de ajustes del descubrimiento NAT en la GUI de configuración de descubrimiento, salvo las siguientes tareas:

- Configure el agente NATTextFileAgent para proporcionar compatibilidad con cualquier dispositivo de pasarela NAT no admitido.
- Configure el agente NATGateway para solucionar el potencial problema de una conectividad incorrecta cuando la pasarela NAT no se encuentra en el espacio de direcciones público.

Referencia rápida para la configuración de descubrimiento NAT

Utilice esta información como una guía paso a paso para configurar un descubrimiento NAT.

Los pasos están descritos en la tabla siguiente.

Tabla 44. Referencia rápida para la configuración de descubrimiento NAT		
Acción	**Utilización de la GUI**	**Uso de la línea de mandatos**
1. Configure el descubrimiento para utilizar la conversión de direcciones de red. Puede hacer esto utilizando la GUI Configuración del descubrimiento, o utilizando la línea de mandatos.	"Configuración de la conversión NAT" en la página 173	"Habilitación de la conversión NAT" en la página 327
2. Defina cada dispositivo de pasarela NAT y su correspondiente espacio de dirección. Puede hacer esto utilizando la GUI Configuración del descubrimiento, o utilizando la línea de mandatos.		"Definición de espacios de dirección para pasarelas NAT" en la página 327
3. Agregue fuentes al buscador de pings con la dirección IP de cada dispositivo de pasarela NAT.	"Adición de fuentes a un descubrimiento" en la página 162	Guía para agregar fuentes a un descubrimiento "Archivo de configuración DiscoPingFinderSeeds.cfg " en la página 198 Guía para agregar fuentes a un descubrimiento NAT "Adición de fuentes a un descubrimiento con direcciones de pasarela NAT" en la página 328

Tabla 44. Referencia rápida para la configuración de descubrimiento NAT (continuación)

Acción	Utilización de la GUI	Uso de la línea de mandatos
4. Defina una zona de ámbito para cada dispositivo de pasarela NAT. **Nota:** No es necesario que defina una zona de ámbito para los dispositivos de pasarela NAT cuya dirección IP ya se encuentra dentro de otras zonas de ámbito definidas por el descubrimiento. **Nota:** No defina un espacio de dirección para los dispositivos de pasarela NAT o para ámbitos de subred públicos. El espacio de dirección solo se puede definir para subredes privadas.	"Definición del ámbito del descubrimiento" en la página 161	Guía para definir el ámbito de un descubrimiento "Archivo de configuración DiscoScope.cfg" en la página 201 Ejemplo: cómo definir una zona de ámbito para una subred NAT privada "Definición de una zona de ámbito dentro de un dominio NAT" en la página 328
5. Defina zonas de ámbito para las subredes públicas asociadas con cada espacio de dirección NAT. **Nota:** No defina un espacio de dirección para los dispositivos de pasarela NAT o para ámbitos de subred públicos. El espacio de dirección solo se puede definir para subredes privadas.		
6. Cuando sea posible, defina zonas de ámbito para la subred privada asociada con cada espacio de dirección NAT. **Restricción:** Solo puede definir una zona de ámbito para un espacio de dirección NAT privado en el que la combinación de subred y máscara de red de la subred privada es exclusiva en la configuración del descubrimiento. Realice las siguientes configuraciones al definir este ámbito: 1. Desmarque la opción **Agregar a lista de fuentes de ping**. Debe hacer esto porque no se puede hacer ping en las subredes privadas. 2. Defina un espacio de dirección para esta subred privada. Las ventajas de agregar una zona de ámbito para cada espacio de dirección NAT privado son las siguientes: • Asegura que sólo se retroalimenten las direcciones en dicho espacio privado durante el descubrimiento. • Si el dispositivo de pasarela NAT y los dispositivos del espacio de dirección NAT asociado son direccionadores, agregar una zona de ámbito para dicho espacio de dirección NAT privado limita la descarga de datos de direccionamiento innecesarios.		

Tabla 44. Referencia rápida para la configuración de descubrimiento NAT (continuación)		
Acción	**Utilización de la GUI**	**Uso de la línea de mandatos**
7. Habilite los agentes NAT de esta manera: • Para dispositivos de pasarela NAT soportados, habilite el agente CiscoNATTelnet o NATNetScreen. • Para dispositivos de pasarela NAT no soportados, cree un archivo de correlación NAT y habilite el agente NATTextFileAgent	"Activación de agentes" en la página 168	"Habilitación de agentes para dispositivos de pasarela NAT soportados" en la página 329 "Habilitación de agentes para dispositivos de pasarela NAT no soportados" en la página 329

Habilitación de la conversión NAT

Puede definir el sistema de descubrimiento para utilizar la conversión NAT editando $NCHOME/etc/precision/DiscoConfig.cfg para crear o corregir una inserción en disco.NATStatus para definir m_UsingNAT en 1 y m_NATStatus en 0.

Acerca de esta tarea

La inserción completada se debe parecer a lo siguiente:

```
insert into disco.NATStatus
(
        m_UsingNAT,
        m_NATStatus
)
values
(
        1,
        0
);
```

Definición de espacios de dirección para pasarelas NAT

Para especificar la dirección IP de las pasarelas NAT y el identificador de espacio de dirección que desea utilizar para cada dominio NAT asociado, edite `DiscoConfig.cfg` para crear o corregir una inserción en `translations.NATAddressSpaceIds`.

Acerca de esta tarea

Siga estas pautas al definir espacios de dirección para pasarelas NAT:

Procedimiento

- La dirección IP debe ser la dirección pública que es accesible desde el servidor de gestión.
- El campo de espacio de dirección puede ser cualquier cadena descriptiva, pero evite caracteres especiales como las comillas. Utilice las reglas estándar para nombres DNS para el espacio de dirección porque el espacio de dirección puede formar parte del nombre de estos dispositivos.

Resultados

La siguiente inserción de ejemplo configura el sistema de descubrimiento para dos pasarelas NAT.

```
insert into translations.NATAddressSpaceIds
(
        m_NATGatewayIP,
        m_AddressSpaceId
)
values
(
```

```
         '172.16.1.112',
        'NATDomain1'
);

insert into translations.NATAddressSpaceIds
(
        m_NATGatewayIP,
        m_AddressSpaceId
)
values
(
         '172.16.1.104',
        'NATDomain2'
);
```

Definición de una zona de ámbito dentro de un dominio NAT

Puede personalizar zonas de inclusión y exclusión para dominios NAT individuales, utilizando la columna `m_AddressSpace` de la tabla `scope.zones`.

Acerca de esta tarea

La siguiente inserción de ejemplo define una zona de inclusión para una subred privada asociada con un dominio NAT.

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="172.16.2.*",
            }
        ],
        "NATDomain1"
);
```

El ejemplo anterior define una zona de inclusión. Network Manager Descubre todos los dispositivos con una dirección IP que comience con `"172.16.2"`, es decir, en la subred privada `172.16.2.0` con un máscara de `255.255.255.0` y que también pertenezcan al espacio de dirección NAT `NATDomain1`. El protocolo se define en `1`, es decir, la IP.

Nota: No defina un espacio de dirección para los dispositivos de pasarela NAT o para ámbitos de subred públicos. El espacio de dirección solo se puede definir para subredes privadas.

Adición de fuentes a un descubrimiento con direcciones de pasarela NAT

Agregue un descubrimiento NAT insertando las direcciones IP en el buscador de pings de los direccionadores principales dentro del sistema. Agregue fuentes también al descubrimiento con las direcciones IP de las IP de pasarela NAT.

Acerca de esta tarea

En un descubrimiento basado en NAT, el descubrimiento debe descubrir las pasarelas NAT antes de descubrir el resto de la red, para que las pasarelas NAT se encuentren primero con un buscador.

Network Manager está configurado para desencadenar la adición de fuentes de todas las pasarelas NAT si se ha habilitado una conversión de NAT. Sin embargo, el desencadenamiento depende de si está activo el buscador de pings. Si se ha realizado una adición de fuentes, por ejemplo, utilizando solo el buscador de archivos, en las pasarelas NAT no se hace ping incluso si se ha habilitado una conversión de NAT. Es una buena idea, por lo tanto, agregar fuentes al descubrimiento con todas las pasarelas NAT. Puede hacer esto utilizando el buscador de archivos, el buscador de pings o cualquier otro método.

También puede agregar fuentes al descubrimiento con pasarelas NAT utilizando la GUI de configuración de descubrimiento.

Habilitación de agentes de NAT

Si va a ejecutar un cortafuegos NetScreen® o un direccionador Cisco® como una pasarela de NAT, debe utilizar los agentes CiscoNATTelnet o NATNetScreen.

Acerca de esta tarea

Asegúrese de que habilita los agentes de conversión de NAT correctos. Estos agentes se deben ejecutar para descubrir las pasarelas de NAT. Si no se ejecutan, el descubrimiento no se puede completar porque no puede descubrir de forma correcta la red sin descubrir primer las pasarelas de NAT.

Los agentes de NAT son actualmente: CiscoNATTelnet, NATNetScreen y NATTextFileAgent. El agente CiscoNATTelnet funciona en direccionador de E/S de Cisco, proporciona conversión de NAT y no tiene certificación para cortafuegos PIX. El agente NATNetScreen es para cortafuegos NetScreen.

Si va a utilizar una pasarela de NAT que no sea un cortafuegos de NetScreen o un direccionador de Cisco, utilice el agente de Perl NATTextFileAgent.pl, como se describe en "Habilitación de agentes para dispositivos de pasarela NAT no soportados" en la página 329.

Habilitación de agentes para dispositivos de pasarela NAT soportados

Los agentes CiscoNATTelnet y NATNetScreen se conectan directamente a las pasarelas NAT para descargar las correlaciones entre direcciones. Puede configurar estos agentes.

Antes de empezar

Antes de ejecutar estos agentes, debe realizar las siguientes tareas:

- Habilitar la conversión NAT
- Configurar manejo de interrupción

Acerca de esta tarea

Para configurar y ejecutar los agentes:

Procedimiento

1. Habilite los agentes. Hay una inserción en la tabla disco.agents en el archivo de configuración DiscoAgents.cfg para cada agente de descubrimiento instalado. Para activar un agente, debe alterar la inserción para que la columna m_Valid para ese agente se defina en 1. Para desactivar un agente, asegúrese de que m_Valid=0.

   La siguiente inserción de ejemplo activa el agente CiscoNATTelnet.

   ```
   insert into disco.agents
   (
           m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence,
           m_DebugLevel, m_LogFile
   )
   values
   (
           'CiscoNATTelnet', 1, 8, 0, 2, 4,
           "$NCHOME/log/precision/CiscoNatTelnet.log"
   );
   ```

2. Inicie un descubrimiento.

Habilitación de agentes para dispositivos de pasarela NAT no soportados

Se proporciona NATTextFileAgent como copia de seguridad si el dispositivo de conversión NAT no es soportado. Puede configurar este agente.

Antes de empezar

Antes de ejecutar el agente NATTextFileAgent, debe realizar las siguientes tareas:

- Habilitar la conversión NAT
- Configurar manejo de interrupción

Acerca de esta tarea

NATTextFileAgent lee un archivo sin formato denominado NATTranslations.txt que contiene las conversiones NAT presentes en una pasarela NAT particular. Este permite al descubrimiento utilizar un método para soportar una red que contiene actualmente una pasarela NAT no soportada. Este agente no descarga su información desde las pasarelas NAT, pero lee una lista de correlaciones entre direcciones IP privadas y públicas desde un archivo sin formato.

Para configurar y ejecutar el agente:

Procedimiento

1. Instale la API de Perl. Todos los agentes de Perl requieren la API para ejecutarse. La API está instalada de manera predeterminada en Network Manager.

   Para comprobar si la API está instalada, verifique que existe el siguiente archivo:

   ```
   $NCHOME/precision/bin/ncp_perl
   ```

   Si se ha enumerado el archivo, la API de Perl está instalada.
2. Cree un archivo de correlación NAT para que lo lea el agente que contiene las correlaciones entre direcciones privadas y públicas. Su archivo de correlación NAT debe estar en un formato que pueda leer el agente, es decir, los valores deben ser direcciones IP especificadas en columnas separadas por separadores.

   De forma predeterminada, el agente utiliza el archivo $NCHOME/etc/precision/NATTranslations.txt. Si desea crear sus propias correlaciones, debe realizar una copia de seguridad y editar este archivo predeterminado. Para que el agente utilice el archivo de correlación NAT no predeterminado, edite la siguiente línea en $NCHOME/precision/disco/agents/Perlagents/NATTextFileAgent.pl:

   ```
   my $natFileName  = "$ENV{$NCHOME}/etc/precision/NATTranslations.txt";
   ```
3. El archivo de correlación NAT contiene las siguientes columnas:
   - La dirección IP de la pasarela NAT del dominio NAT al que pertenece el dispositivo. Debe especificar correlaciones para todas las pasarelas NAT en el mismo archivo.
   - La dirección global externa del dispositivo, es decir, la dirección pública del dispositivo.
   - La dirección local interna del dispositivo, es decir, la dirección privada del dispositivo.

   El siguiente ejemplo muestra un archivo de correlación NAT para dos enlaces que tienen direcciones IP de 1.2.3.4 y 1.2.3.9 respectivamente.

   ```
   // NATGatewayIP              PublicIP                PrivateIP
   1.2.3.4                      2.3.4.5                 10.10.1.1
   1.2.3.4                      2.3.4.6                 10.10.1.2
   1.2.3.9                      2.3.6.1                 10.10.1.1
   1.2.3.9                      2.3.6.2                 10.10.1.2
   ```

   Nota: Desde la perspectiva de la estación de gestión, la dirección IP pública de una conversión de pasarela particular no es necesariamente la misma que la dirección pública que ven las estaciones de gestión. La dirección pública es la dirección IP que la pasarela recupera de un puerto y después convierte y sitúa en otro puerto. Esta diferencia es importante para tener en cuenta cuando ha encadenado pasarelas, en las que una dirección IP se puede convertir varias veces. La IP pública es, efectivamente, la dirección IP que está más próxima al dominio de gestión.
4. Habilite el agente. Hay una inserción en la tabla disco.agents en el archivo de configuración DiscoAgents.cfg para cada agente de descubrimiento instalado. Para activar un agente, debe alterar la inserción para que la columna m_Valid para ese agente se defina en 1. Para desactivar un agente, asegúrese de que m_Valid=0.

La siguiente inserción de ejemplo activa el agente NATTextFileAgent.

```
insert into disco.agents
(
        m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence, m_IsPerl
)
values
(
        'NATTextFileAgent', 1, 8, 0, 2, 1
);
```

5. Asegúrese de que el agrupador NATTimer.stch se ha configurado para desencadenar un redescubrimiento en las pasarelas NAT. De forma predeterminada, el agrupador NATTimer.stch se ejecuta cada hora. Puede alterar este intervalo ubicando la siguiente línea en el archivo del agrupador y cambiando el valor entero:

```
        ActOnTimedTrigger( ( m_Interval ) values ( 1 ) ; ) ;
```

6. Inicie un descubrimiento.

Habilitar el agente de dispositivos de pasarela NAT en un espacio de direcciones privado
Si la pasarela de NAT no está en un espacio de direcciones público, active el agente NATGateway para corregir el problema potencial de una conectividad incorrecta.

Acerca de esta tarea

El descubrimiento asumen que la interfaz de gestión de la pasarela de NAT se encuentra en un espacio de direcciones público. Si este no es el caso, Network Manager no podrá identificar el espacio de direcciones de interfaces en el dispositivo de pasarela NAT, lo que podría dar como resultado una conectividad incorrecta. Por ejemplo, cuando se utiliza una VPN para acceder a la interfaz de gestión la interfaz de gestión de pasarelas de NAT no está en un espacio de direcciones público.

El agente NATGateway habilita Network Manager para determinar si una determinada interfaz de un dispositivo de pasarela de NAT se encuentre en la parte privada o pública de la pasarela de NAT y, por lo tanto, resolver de forma correcta la conectividad de los dispositivos.

Para solucionar este problema, active el agente NATGateway y proporcione a Network Manager un archivo de correlaciones, NATGateways.txt. En este archivo, proporcione una lista de todos los dispositivos de pasarela de NAT, junto con las interfaces de cada dispositivo y un campo para indicar si la interfaz está en la parte pública o privada de la pasarela de NAT.

Este agente funciona en conjunción con el agrupador NATGatewayRetProcessing.stch y con el archivo NATGateways.txt en NCHOME/precision/etc

Tabla 45 en la página 331 proporciona formato al archivo NATGateways.txt mostrando un ejemplo del contenido de este archivo. Los campos de este archivo de texto deben estar separados por tabuladores.

Tabla 45. Formato del archivo NATGateways.txt

Nombre base	**Interior o exterior**	**Dirección de IP de la interfaz**
1.1.1.4	exterior	172.16.4.10
1.1.1.4	interior	10.52.2.10
sca_T1ukP_16	exterior	192.168.36.93
sca_T1ukP_16	exterior	192.168.36.98

Ejemplo: Configuración de un descubrimiento NAT

Este ejemplo ilustra cómo definir espacios de dirección utilizando el agente NATTextFileAgent y cómo configurar ámbitos de descubrimiento asociados.

Antes de empezar

Realice las siguientes tareas antes de ejecutar los pasos en este ejemplo:

- Configure el descubrimiento para utilizar la conversión de direcciones de red.
- Agregue fuentes al buscador de pings con la dirección IP de cada dispositivo de pasarela NAT.

Acerca de esta tarea

En este ejemplo los dispositivos de pasarela NAT no son soportados. Esto significa que se debe utilizar el agente NATTextFileAgent en este descubrimiento de NAT.

El agente NATTextFileAgent utiliza un archivo de correlación de NAT, con el siguiente contenido. Existen tres dispositivos de pasarela NAT con correlaciones para cada uno de los dispositivos en los espacios de dirección asociados.

```
//First NAT gateway and mappings
//NATGateway              PublicIP                  Private IP
201.201.201.201         61.61.61.1              192.168.1.1
201.201.201.201         61.61.61.2              192.168.1.2
201.201.201.201         61.61.61.3              192.168.1.3
201.201.201.201         61.61.61.4              192.168.1.4
201.201.201.201         61.61.61.5              192.168.1.5
201.201.201.201         61.61.61.6              192.168.1.6

//Second NAT gateway and mappings
//NATGateway              PublicIP                  Private IP
202.202.202.202         62.62.62.1              192.168.1.1
202.202.202.202         62.62.62.2              192.168.1.2
202.202.202.202         62.62.62.3              192.168.1.3
202.202.202.202         62.62.62.4              192.168.1.4
202.202.202.202         62.62.62.5              192.168.1.5
202.202.202.202         62.62.62.6              192.168.1.6

//Third NAT gateway and mappings
//NATGateway              PublicIP                  Private IP
203.203.203.203         63.63.63.1              192.168.3.1
203.203.203.203         63.63.63.2              192.168.3.2
203.203.203.203         63.63.63.3              192.168.3.3
203.203.203.203         63.63.63.4              192.168.3.4
203.203.203.203         63.63.63.5              192.168.3.5
203.203.203.203         63.63.63.6              192.168.3.6
```

Para el primer y el segundo espacio de dirección el espacio de dirección IP privada no es exclusivo. Para ambos espacios de dirección, una combinación de subred y máscara de red de 192.168.1.0/29 definen el espacio de dirección IP privada.

Basándose en este dispositivo de pasarela NAT y en datos de espacio de dirección, defina los ámbitos de descubrimiento de la siguiente manera.

Procedimiento

1. Defina cada dispositivo de pasarela NAT y su correspondiente espacio de dirección.
   En este ejemplo, los nombres de los tres espacios de dirección NAT son RTP1, RTP2 y RTP3. Por ejemplo, para el tercer dispositivo de pasarela NAT, la siguiente inserción define el dispositivo NAT y su espacio de dirección asociado, RTP3:

   ```
   insert into translations.NATAddressSpaceIds
   (
       m_NATGatewayIP, m_AddressSpaceId
   )
   values
   (
   "203.203.203.203", "RTP3"
   );
   ```

2. Defina una zona de ámbito para cada dispositivo de pasarela NAT.

   Nota: No es necesario que defina una zona de ámbito para los dispositivos de pasarela NAT cuya dirección IP ya se encuentra dentro de otras zonas de ámbito definidas por el descubrimiento.

Por ejemplo, para el primer dispositivo de pasarela NAT, la siguiente inserción define la zona de ámbito:

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="201.201.201.201",
                m_NetMask=32
            }
        ],
        ""
);
```

3. Defina zonas de ámbito para las subredes públicas asociadas con cada espacio de dirección NAT. Por ejemplo, para la tercera subred pública, la siguiente inserción define la zona de ámbito:

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="63.63.63.0",
                m_NetMask=29
            }
        ],
        ""
);
```

4. Defina una zona de ámbito para la subred privada asociada solo con el tercer espacio de dirección NAT.

   Restricción: Solo puede definir una zona de ámbito para un espacio de dirección NAT privado en el que la combinación de subred y máscara de red de la subred privada es exclusiva en la configuración del descubrimiento. Esto excluye la primera y la segunda subred privada.

   Para la tercera subred privada, la siguiente inserción define la zona de ámbito:

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="192.168.3.0",
                m_NetMask=29
            }
        ],
        "RTP3"
);
```

5. Habilite el agente NATTextFileAgent.

Qué hacer a continuación

Ahora puede iniciar el descubrimiento de NAT.

Tareas de postconfiguración de NAT

Después de configurar los descubrimientos de NAT, puede completar varias tareas de postconfiguración.

Seguimiento del progreso de un descubrimiento de NAT

Durante el descubrimiento de los dispositivo de conversión NAT, puede realizar un seguimiento del estado de descubrimiento de los valores de disco.NATStatus.

Acerca de esta tarea

Durante el descubrimiento, verá inicialmente solo los dispositivos de conversión NAT en las tablas de devoluciones y despatch de agente. Todos los demás datos devueltos por los buscadores se almacenan en la tabla de base de datos finders.pending mientras el descubrimiento de los dispositivos de conversión NAT tiene lugar.

Emita la siguiente sentencia select de OQL para ver el estado del descubrimiento:

```
select * from disco.NATStatus;
```

Esta sentencia muestra un valor de 0 a 4. El significado del valor es:

Procedimiento

- 0: Descubrimiento de NAT en estado inicial. Los dispositivos de NAT no se han procesado.
- 1: Descubrimiento de NAT iniciado. Las direcciones IP de la pasarela de NAT se han enviado al buscador de pings para comprobar su existencia
- 2: El descubrimiento de NAT se está ejecutando.
- 3: Proceso de descubrimiento de NAT. Se han procesado todas las pasarelas de NAT y el descubrimiento está generando la tabla `translations.NAT`. Esta tabla garantiza el descubrimiento correcto del resto de la red.
- 4: Descubrimiento de NAT finalizado. Se han movido las entradas de la tabla finders.pending a la tabla finders.processing, y el descubrimiento continúa como normal.

Resultados

Utilice los resultados de esta consulta para depurar un descubrimiento de NAT problemático. El valor indica si los problemas de descubrimiento han sido causados por NAT o por la parte estándar (distinta de NAT) del proceso de descubrimiento.

Depuración de un descubrimiento de NAT

Para analizar un descubrimiento de NAT, utilice ncp_oql para seguir los datos a través del sistema desde el inicio (buscadores) hasta el final, hasta que determine dónde hay datos incorrectos. Los datos incorrectos indican si el problema tiene que ver con un agente, un dispositivo o un agrupador.

Acerca de esta tarea

Hay varias preguntas que son útiles cuando se depura un descubrimiento, tanto basado en NAT como no basado en NAT.

La siguiente consulta OQL indica qué agentes están comenzando a iniciarse en ese momento (`m_State=1`), iniciándose (`m_State=2`) o en ejecución (`m_State=3`):

```
select * from agents.status where m_State <> 0 AND m_State <> 4;
```

Esta consulta indica qué agentes de la fase actual están esperando a completarse. El descubrimiento está esperando a los agentes que deben finalizarse en la fase actual y tienen el estado 1, 2 o 3.

```
select * from <agentName>.despatch
where m_UniqueAddress NOT IN
      ((
      select m_UniqueAddress from <agentName>.returns where m_LastRecord = 1
      ));
```

Con la primera consulta, podrá ver qué agentes están ejecutándose todavía en una determinada fase.

Con la siguiente consulta, podrá determinar qué entidad está procesando ese agente concreto. Esto puede resultar útil a la hora de determinar un dispositivo con problemas en la red:

```
select * from translations.ipToBaseName where m_IpAddress = '<ip>';
```

Esa segunda consulta muestra dirección base y el nombre base que se están utilizando para una IP determinada, así como si se considera esta dirección IP dentro del ámbito.

Activación del modelo de contención para su uso con NAT

El agrupador `NATAddressSpaceContainers.stch` crea objetos virtuales para cada espacio de direcciones que contiene las entidades dentro de ese espacio de direcciones. Puede activar este agrupador anulando los comentarios de la línea, // ExecuteStitcher("NATAddressSpaceContainers");, en el archivo `$NCHOME/precision/disco/stitchers/BuildContainment.stch`.

Visualización de entornos de NAT mediante las vistas de red de Topoviz

Con las vistas de red de Topoviz, puede crear vistas de red en función de los valores de cualquier columna del registro de topología de una entidad. Si ha activado el descubrimiento de NAT como parte de la configuración de descubrimiento, se creará de forma automática una vista NAT Address Spaces Dynamic Distinct.

Acerca de esta tarea

Como ejemplo de visualización de entornos de NAT, puede crear una vista de red filtrada o una vista Dynamic Distinct en el siguiente campo de la base de datos de topología de NCIM:

- Tabla ipEndPoint
- Campo addressSpace

Nota: Si se activa **Habilitar soporte de NAT (conversión de direcciones de red)** como parte de la configuración de descubrimiento, se creará de forma automática una vista NAT Address Spaces Dynamic Distinct.

Configuración de descubrimientos de dominios cruzados

Para habilitar enlaces entre dispositivos en diferentes dominios para mostrar en las vistas de red y de topología, debe configurar y ejecutar descubrimientos de dominios cruzados en los distintos dominios.

Acerca de esta tarea

La configuración de un descubrimiento de dominios cruzados es un procedimiento avanzado que requiere conocer el flujo de datos de descubrimiento, el lenguaje de consulta OQL, la estructura de la base de datos y los detalles de la conectividad y la composición de la red.

Referencia relacionada

Consideraciones de RCA en una red de dominios cruzados
En un entorno de dominios cruzados, el proceso **ncp_g_event** de cada dominio de descubrimiento ejecuta RCA en los dispositivos en el mismo dominio de descubrimiento. En cada dominio, RCA opera de la misma forma que cuando sólo hay un único dominio. También puede analizarse la causa raíz en varios dominios cuando se visualizan conjuntamente utilizando un descubrimiento de dominios cruzados.

Acerca del descubrimiento de dominios cruzados

El descubrimiento de dominios cruzados puede configurarse para unir dos o más dominios descubiertos.

A efectos operativos o de rendimiento, las redes se descubren a menudo en secciones, conocidas como *dominios de descubrimiento*. Por ejemplo, si la red es tan grande que descubrirla en un solo descubrimiento tarda un tiempo excesivo, puede optar por dividir el descubrimiento de red en diferentes dominios.

El descubrimiento de la red en dominios puede ser más conveniente y rápido. También puede optar por tener distintas opciones de configuración para los distintos dominios. Por ejemplo, cada dominio tiene sus propias políticas de sondeo. No obstante, existen desventajas en el descubrimiento por partes de la red. Si un dispositivo en el dominio A está conectado a un dispositivo en el dominio B, esta conexión no se representa en la base de datos de topología ni en la GUI. Los dominios deben verse por separado.

Si desea visualizar varios dominios enlazados en una vista de red, debe habilitar, configurar y ejecutar descubrimientos de dominios cruzados. Las conexiones entre dispositivos de dominios diferentes se encuentran y se añaden a la topología.

Cuando todos los dominios descubiertos se han agregado, las **Vistas de red** pueden estar formadas por dispositivos de todos los dominios. En la **Vista de saltos de red**, las búsquedas de dispositivos pueden abarcar varios dominios.

Nota: No es posible sondear las vistas de red de dominios cruzados; sólo se pueden sondear las vistas de red de dominios individuales.

Consideraciones para la división de la red en dominios

Los enlaces entre dispositivos de distintos dominios no son tan fáciles de descubrir como los enlaces entre dispositivos que están dentro de un dominio.

Es importante establecer el alcance de los dominios del descubrimiento para garantizar el número mínimo de enlaces entre dominios. Por ejemplo, normalmente no dividiría la red de manera que los conmutadores que tengan muchas conexiones entre sí estén en distintos dominios. Con frecuencia, las divisiones naturales para los dominios se realizan a lo largo de las líneas geográficas.

Restricción:

No obstante, al dividir su red, debe asegurarse de que un dispositivo determinado aparezca en un solo dominio. Es decir, los dominios del descubrimiento no deben solaparse si desea unirlos utilizando un descubrimiento de dominios cruzados.

Referencia relacionada

Consideraciones de RCA en una red de dominios cruzados
En un entorno de dominios cruzados, el proceso **ncp_g_event** de cada dominio de descubrimiento ejecuta RCA en los dispositivos en el mismo dominio de descubrimiento. En cada dominio, RCA opera de la misma forma que cuando sólo hay un único dominio. También puede analizarse la causa raíz en varios dominios cuando se visualizan conjuntamente utilizando un descubrimiento de dominios cruzados.

Habilitación de enlaces de dominios cruzados

El primer paso para la configuración de enlaces de dominios cruzados es habilitar los enlaces entre dominios en el archivo de configuración `DiscoConfig.cfg`. De forma predeterminada, los enlaces de dominios cruzados están inhabilitados.

Procedimiento

1. Realice copia de seguridad y edite el archivo `$NCHOME/etc/precision/DiscoConfig.domain.cfg`.
2. Realice las siguientes configuraciones:
   - Establezca **`m_EnableCrossDomainProcessing`** en `1`.
   - Establezca **`m_InferPEsUsingBGP`** en `0` para inhabilitar la inferencia de los dispositivos Provider Edge (PE). La inferencia de los dispositivos PE es incompatible con los descubrimientos de dominios cruzados. Esta configuración también puede realizarse en el separador **Avanzado** de la GUI de **Configuración de descubrimiento de red** borrando la selección de **Habilitar inferencia de PE utilizando datos BGP en CE**.
3. Repita estos pasos en el archivo `DiscoConfig.domain.cfg` de cada dominio que desee enlazar.
4. En el archivo de agrupador `LinkDomainsPopulateDomainAdjacencies.stch`, defina las adyacencias entre dominios en la tabla tmpDomainAdj.adjacencies.

Utilice las sentencias INSERT para definir las adyacencias. En el archivo se proporcionan sentencias INSERT de ejemplo. Cada sentencia INSERT define únicamente una adyacencia. Puede poner las sentencias INSERT en el orden que desee.

Por ejemplo, para definir las adyacencias entre dos dominios denominados NORTH y SOUTH, utilice la siguiente sentencia INSERT:

```
insert into tmpDomainAdj.adjacencies values ('NORTH', 'SOUTH');
```

El ejemplo siguiente muestra las sentencias INSERT que se utilizan cuando tiene tres dominios: EUROPE, ASIA, y AMERICA. EUROPE es adyacente a ASIA y AMERICA.

```
insert into tmpDomainAdj.adjacencies values (EUROPE, ASIA);
insert into tmpDomainAdj.adjacencies values (EUROPE, AMERICA);
```

Para definir una adyacencia adicional entre ASIA y AMERICA, utilice otra sentencia INSERT:

```
insert into tmpDomainAdj.adjacencies values (ASIA, AMERICA);
```

Configuración de enlaces de dominios cruzados

Para configurar enlaces de dominios cruzados, debe decidir qué método de enlace es el más adecuado para la red y configurar los agrupadores correspondientes.

Acerca de esta tarea

Configuración de enlaces de dominios cruzados entre dispositivos de capa 1.

Puede habilitar enlaces de dominios cruzados entre dispositivos de capa 1. Puede habilitar o inhabilitar la creación de enlaces entre dispositivos en distintos dominios que utilizan protocolos de capa 1. También puede configurar la forma en que se crean los enlaces.

Procedimiento

1. Haga una copia de seguridad y edite el archivo del agrupador `NCHOME/precision/disco/stitchers/LinkDomains.stch`.
2. Localice la línea que empieza por `int linkViaLayer1NameInterface`.
3. Defina el valor como 1 para habilitar las conexiones entre dispositivos de capa 1 en distintos dominios para crear como enlaces en la topología.
4. Configure los siguientes parámetros avanzados, que se aplican a los enlaces creados mediante todas las tecnologías y métodos habilitados:

   previewChanges
   Defínalo como 1 si desea que los enlaces no se creen, sino que únicamente se guarden en un archivo de registro. Para obtener una vista previa de los enlaces, configure el proceso **ncp_disco** como `-messagelevel debug` para poder iniciar el descubrimiento. Los mensajes sobre las conexiones que se habrían creado se registran en el archivo `NCHOME/log/precision/ncp_disco.DOMAIN.log`. Defínalo como `0` si desea que se creen los enlaces.

   lowLayerResolutionMode
   Si existen varios tipos de conexión entre dos puertos, puede elegir a qué nivel se creará la conexión. A menudo, resulta más práctico utilizar la conexión más específica del nivel más bajo.

   - Defínalo como `0` para crear solo la conexión que han encontrado los agrupadores de dominios cruzados.
   - Defínalo como 1 para crear la conexión **solo** entre los puertos que están apilados en el nivel más bajo, en una interfaz. Por ejemplo, cuando una interfaz POS se apila sobre un puerto SONET, esta opción crea la conexión solo entre los puertos SONET. Si habilita esta opción, la agrupación tarda más tiempo.
   - Defínalo como 2 para crear la conexión entre las interfaces **y** sus puertos apilados más bajos. Por ejemplo, en los casos en que se apila una interfaz POS sobre un puerto SONET, esta opción crea

una conexión entre los puertos SONET y una conexión entre las interfaces POS. Si habilita esta opción, la agrupación tarda más tiempo.

Configuración de enlaces de dominios cruzados entre otras tecnologías de dispositivo

Puede crear enlaces de dominios cruzados entre dispositivos utilizando tecnologías comp /30 y pseudoconexión. También puede configurar la forma en que se crean los enlaces.

Procedimiento

1. Haga una copia de seguridad y edite el archivo del agrupador `NCHOME/precision/disco/stitchers/LinkDomains.stch`.
2. Opcional: Para permitir conexiones /30 entre dispositivos en diferentes dominios para crear como enlaces en la topología, localice la línea que empieza por `int linkViaSlash30Subnet` y defina el valor como 1.
   a) Configure los siguientes parámetros:

   preventLinkPropagation
   Establézcalo en `0` para añadir la conexión /30 aunque exista una conexión de capa 2 entre las dos entidades de red. Establézcalo en 1 para evitar que se añada una conexión /30 si ya existe una conexión de capa 2 de la entidad.

   linkSlash30InLayer2
   Establézcalo en `0` para evitar que se añadan enlaces /30 como enlaces de capa 2. Configúrelo como 1 para añadir enlaces /30 como enlaces de capa 2. La configuración de esta propiedad y de `linkSlash30InLayer3` como `0` evita que se creen conexiones /30 aunque se descubran, lo que puede hacer que el descubrimiento lleve más tiempo. Puede configurar ambas propiedades como 1 para añadir enlaces /30 como enlaces de capa 2 y de capa 3.

   linkSlash30InLayer3
   Establézcalo en `0` para evitar que se añadan enlaces /30 como enlaces de capa 3. Configúrelo como 1 para añadir enlaces /30 como enlaces de capa 3. La configuración de esta propiedad y de `linkSlash30InLayer2` como `0` evita que se creen conexiones /30 aunque se descubran, lo que puede hacer que el descubrimiento lleve más tiempo. Puede configurar ambas propiedades como 1 para añadir enlaces /30 como enlaces de capa 2 y de capa 3.
3. Opcional: Para permitir conexiones /30 entre dispositivos en diferentes dominios para crear como enlaces en la topología, localice la línea que empieza por `int linkViaPseudoWires` y defina el valor como 1.
   a) Configure los siguientes parámetros:

   resolvePWViaFarEndIP
   Establézcalo en `0` para inhabilitar la creación de enlaces utilizando direcciones IP de pseudoconexión de extremo. Establézcalo en 1 para crear enlaces utilizando direcciones IP de pseudoconexión de extremo.

   resolvePWViaLabels
   Establézcalo en `0` para inhabilitar la creación de enlaces utilizando la búsqueda de direcciones inversas de pseudoconexión. Establézcalo en 1 para crear enlaces utilizando la búsqueda de direcciones inversas de pseudoconexión.

   resolvePWViaVPLSInterface
   Establézcalo en `0` para inhabilitar la creación de enlaces con VPLS (Virtual Private Label Switching) duplicados. Establézcalo en 1 para crear enlaces con VPLS (Virtual Private Label Switching) duplicados.
4. Opcional: Para habilitar conexiones de sesión de BGP entre dispositivos en diferentes dominios utilizando la información de sesión de BGP descargada por los agentes bgp, localice la línea que comienza por `int linkViaBGPSessions` y establezca el valor en 1.
   a) Configure los siguientes parámetros:

linkBGPInLayer2
Establézcalo en 1 para colocar el enlace en la topología L2 si el procesamiento de dominio cruzado de BGP encuentra un enlace de BGP entre dominios.

Establézcalo en 0 para inhabilitarlo.

linkBGPInLayer3
Establézcalo en 1 para colocar el enlace en la topología L3 si el procesamiento de dominio cruzado de BGP encuentra un enlace de BGP entre dominios.

Establézcalo en 0 para inhabilitarlo.

linkEstalbishedSessionsOnly
Establézcalo en 1 para conectar las dos interfaces de BGP si se ha encontrado una sesión de BGP de dominio cruzado para la que no está establecido el estado.

Establézcalo en 0 para conectar las dos interfaces de BGP si se ha encontrado una sesión de BGP de dominio cruzado solo si se ha establecido el estado.

linkBGPSessionsStrictly
Establézcalo en 1 para habilitar el enlace a través de coincidencias de IP generales, si falla una coincidencia de sesión de BGP estricta.

Establézcalo en 0 para inhabilitarlo.

5. Opcional: Para habilitar conexiones CDP entre dispositivos de diferentes dominios creados utilizando los datos de retorno del agente CDP, ubique la línea que comienza por `int linkViaCDP` y establezca el valor en 1.
   a) Configure los siguientes parámetros:

linkViaCDPAtLowestInterface
Establézcalo en 0 para conectar las interfaces encontradas.

Establézcalo en 1 para intentar que sea recursivo para conectarlo a la interfaz/puerto de nivel más bajo.

linkViaCDPAtLayer2
Establézcalo en 1 para colocar el enlace en la topología L2 si se encuentra el enlace CDP entre dominios.

Establézcalo en 0 para inhabilitarlo.

linkViaCDPAtLayer3
Establézcalo en 1 para colocar el enlace en la topología L3 si se encuentra el enlace CDP entre dominios.

Establézcalo en 0 para inhabilitarlo.

6. Opcional: Para utilizar datos de vecinos de agentes TE de MPLS para resolver conexiones entre dispositivos de dominios separados, ubique la línea que comienza por `int linkViaMPLSTE` y establezca el valor en 1.
   a) Configure los siguientes parámetros:

linkViaMPLSTEAtLayer2
Establézcalo en 1 para colocar el enlace en la topología L2 si se encuentra el enlace TE de MPLS entre dominios.

Establézcalo en 0 para inhabilitarlo.

linkViaMPLSTEAtLayer3
Establézcalo en 1 para colocar el enlace en la topología L3 si se encuentra el enlace TE de MPLS entre dominios.

Establézcalo en 0 para inhabilitarlo.

linkViaMPLSTEAtMPLSTE
Establézcalo en 1 para habilitar la creación de una conexión TE de MPLS si se puede identificar el enlace TE de MPLS.

Establézcalo en 0 para inhabilitarlo.

7. Opcional: Para utilizar datos de vecinos de agentes OSPF para resolver conexiones entre dispositivos de dominios separados, ubique la línea que comienza por `int linkViaOSPF` y establezca el valor en 1.
   a) Configure los siguientes parámetros:

   linkViaOSPFAtLayer2
   Establézcalo en 1 para colocar el enlace en la topología L2 si se encuentra el enlace OSPF entre dominios.

   Establézcalo en 0 para inhabilitarlo.

   linkViaOSPFAtLayer3
   Establézcalo en 1 para colocar el enlace en la topología L3 si se encuentra el enlace OSPF entre dominios.

   Establézcalo en 0 para inhabilitarlo.

   linkViaOSPFAtOSPF
   Establézcalo en 1 para habilitar la creación de una conexión OSPF si se puede identificar el enlace OSPF.

   Establézcalo en 0 para inhabilitarlo.
8. Opcional: Para utilizar datos de vecinos de agentes PIM para resolver conexiones entre dispositivos de dominios separados, ubique la línea que comienza por `int linkViaPIM` y establezca el valor en 1.
   a) Configure los siguientes parámetros:

   linkViaPIMAtLayer2
   Establézcalo en 1 para colocar el enlace en la topología L2 si se encuentra el enlace PIM entre dominios.

   Establézcalo en 0 para inhabilitarlo.

   linkViaPIMAtLayer3
   Establézcalo en 1 para colocar el enlace en la topología L3 si se encuentra el enlace PIM entre dominios.

   Establézcalo en 0 para inhabilitarlo.

   linkViaPIMAtPIM
   Establézcalo en 1 para habilitar la creación de una conexión PIM si se puede identificar el enlace PIM.

   Establézcalo en 0 para inhabilitarlo.
9. Configure los siguientes parámetros avanzados, que se aplican a los enlaces creados mediante todas las tecnologías y métodos habilitados:

   previewChanges
   Defínalo como 1 si desea que los enlaces no se creen, sino que únicamente se guarden en un archivo de registro. Para obtener una vista previa de los enlaces, configure el proceso **ncp_disco** como `-messagelevel debug` para poder iniciar el descubrimiento. Los mensajes sobre las conexiones que se habrían creado se registran en el archivo `NCHOME/log/precision/ncp_disco.`*`DOMAIN`*`.log`. Defínalo como 0 si desea que se creen los enlaces.

   lowLayerResolutionMode
   Si existen varios tipos de conexión entre dos puertos, puede elegir a qué nivel se creará la conexión. A menudo, resulta más práctico utilizar la conexión más específica del nivel más bajo.

   - Defínalo como 0 para crear solo la conexión que han encontrado los agrupadores de dominios cruzados.
   - Defínalo como 1 para crear la conexión **solo** entre los puertos que están apilados en el nivel más bajo, en una interfaz. Por ejemplo, cuando una interfaz POS se apila sobre un puerto SONET, esta opción crea la conexión solo entre los puertos SONET. Si habilita esta opción, la agrupación tarda más tiempo.
   - Defínalo como 2 para crear la conexión entre las interfaces **y** sus puertos apilados más bajos. Por ejemplo, en los casos en que se apila una interfaz POS sobre un puerto SONET, esta opción crea

una conexión entre los puertos SONET y una conexión entre las interfaces POS. Si habilita esta opción, la agrupación tarda más tiempo.

Adición y edición manual de enlaces de dominios cruzados

Si no puede ver enlaces entre dispositivos de distintos dominios, puede crearlos o configurarlos manualmente.

Acerca de esta tarea

Para añadir o editar enlaces de dominios cruzados, realice los pasos siguientes:

Procedimiento

1. Haga una copia de seguridad y edite el archivo del agrupador `NCHOME/precision/disco/stitchers/LinkDomainsLoadPresetConnections.stch`.
2. Elimine los comentarios de la sentencia de inserción de OQL.
3. Copie una sentencia de inserción OQL para cada conexión que desee establecer.
4. Edite la sentencia de inserción OQL y añada los detalles de la conexión que desea crear; utilice para ello los siguientes parámetros:

   entryNo
   Un ID numérico exclusivo para esta fila. Empiece por 1 e incremente en n.

   action
   Establézcalo como ADD para añadir una conexión.

   aEndDiscoDomainName
   El dominio en el que se descubrió el dispositivo al comienzo de la conexión. Esta conexión se crea solo cuando se ejecuta un descubrimiento en este dominio.

   aEndDiscoEntityName
   El entityName del dispositivo al comienzo de la conexión.

   zEndNCIMDomainName
   El dominio en el que se encuentra ubicado el dispositivo al final de la conexión. Si un descubrimiento se ejecuta únicamente en este dominio, la conexión no se crea.

   zEndNCIMEntityName
   El entityName del dispositivo al final de la conexión.

   topologyEntityType
   El entityType de la topología NCIM de la conexión.

Configuración de enlaces de dominios cruzados mediante descripciones de interfaz

Puede crear conexiones entre todas las interfaces que coincidan con una búsqueda de descripciones de interfaz.

Acerca de esta tarea

Para buscar interfaces y crear conexiones entre ellas, lleve a cabo los siguientes pasos:

Procedimiento

1. Haga una copia de seguridad y edite el archivo del agrupador `NCHOME/precision/disco/stitchers/LinkDomainsLoadInterfaceDescriptionMatches.stch`.
2. Copie una sentencia de inserción OQL para cada conexión que desee establecer.
3. Edite la sentencia de inserción OQL y añada los detalles de la conexión que desea crear; utilice para ello los siguientes parámetros:

   entryNo
   Un ID numérico exclusivo para esta fila. Empiece por 1 e incremente en n.

action
Establézcalo como ADD para añadir una conexión.

onlyAdminUp
Establézcalo en 1 para restringir la búsqueda a las interfaces cuyo estado administrativo es Activo. Establézcalo en 0 para incluir todas las interfaces, sin importar si su estado administrativo es activo o no.

El estado administrativo es el estado deseado de la interfaz. Un administrador de red puede establecer el estado administrativo de una interfaz en Activo, Inactivo o En prueba.

aEndDiscoMatchType
Establézcalo en EXACT para realizar una búsqueda de texto exacta o en REGEX para ejecutar una búsqueda de expresiones regulares de interfaces de origen en las bases de datos de **ncp_disco**.

aEndDiscoDomainName
El dominio en el que se descubrió el dispositivo al comienzo de la conexión. Esta conexión se crea solo cuando se ejecuta un descubrimiento en este dominio.

aEndDiscoSearchTerm
El término de búsqueda con el que debe coincidir una interfaz en el dominio aEndDiscoDomainName en las bases de datos de **ncp_disco**.

zEndNCIMMatchType
Establézcalo en EXACT para realizar una búsqueda de texto exacta o en REGEX para ejecutar una búsqueda de expresiones regulares de interfaces de destino en la base de datos de NCIM.

zEndNCIMDomainName
El dominio de NCIM en el que se realizará la búsqueda de interfaces de destino en la base de datos de NCIM.

topologyEntityType
El entityType de la topología de NCIM de la conexión en la base de datos de NCIM.

Resultados

Todas las interfaces que coincidan con la búsqueda se conectarán entre sí.

Ejemplo

En el siguiente ejemplo se muestra una inserción que conecta todas las interfaces del dominio de NCOMS cuyas descripciones contienen la cadena `connection to vmhost_network` con todas las interfaces del dominio de NCOMSADJ cuyas descripciones también contienen la cadena `connection to vmhost_network`:

```
INSERT INTO linkDomains.interfaceDescriptionMatch
(
    entryNo,
    action,
    onlyAdminUp,
    aEndDiscoMatchType,
    aEndDiscoDomainName,
    aEndDiscoSearchTerm,
    zEndNCIMMatchType,
    zEndNCIMDomainName,
    zEndNCIMSearchTerm,
    topologyEntityType
)
VALUES
(
    1,                              // entryNo
    'ADD',                          // action
    1,                              // onlyAdminUp - must be up
    'EXACT',                        // aEndDiscoMatchType
    'NCOMS',                        // aEndDiscoDomainName
    'connection to vmhost_network', // aEndDiscoSearchTerm
    'EXACT',                        // zEndNCIMMatchType
    'NCOMSADJ',                     // zEndNCIMDomainName
    'connection to vmhost_network', // zEndNCIMSearchTerm
    72                              // topologyEntityType
);
```

En el siguiente ejemplo se muestra una inserción que conecta todas las interfaces del dominio de NCOMS cuyas descripciones coinciden con la expresión regular `ELON(GW|WR|AR)` con todas las interfaces del dominio de NCOMSADJ cuyas descripciones contienen la cadena `connection to PE2_ASBR_AS2`:

```
INSERT INTO linkDomains.interfaceDescriptionMatch
(
    entryNo,
    action,
    onlyAdminUp,
    aEndDiscoMatchType,
    aEndDiscoDomainName,
    aEndDiscoSearchTerm,
    zEndNCIMMatchType,
    zEndNCIMDomainName,
    zEndNCIMSearchTerm,
    topologyEntityType
)
VALUES
(
    2,                              // entryNo
    'ADD',                          // action
    1,                              // onlyAdminUp - must be up
    'REGEX',                        // aEndDiscoMatchType
    'NCOMS',                        // aEndDiscoDomainName
    'ELON(GW|WR|AR)',               // aEndDiscoSearchTerm
    'EXACT',                        // zEndNCIMMatchType
    'NCOMSADJ',                     // zEndNCIMDomainName
    'connection to PE2_ASBR_AS2',   // zEndNCIMSearchTerm
    72                              // topologyEntityType
);
```

Ejecución de descubrimientos de dominios cruzados

Antes de crear sus vistas de red entre dominios, ejecute el descubrimiento entre dominios cruzados.

Antes de empezar

Antes de ejecutar descubrimiento entre dominios cruzados, configure la forma en que se construyen dichos dominios cruzados.

Acerca de esta tarea

Para ejecutar sus descubrimientos entre dominios cruzados, realice los pasos siguientes:

Procedimiento

1. Ejecute un descubrimiento completo en su primer dominio.
2. Ejecute un descubrimiento completo en su segundo dominio.
3. Ejecute un descubrimiento completo en el resto de dominios.

   Tras descubrir todos los dominios una vez, algunas conexiones podrían estar duplicadas, y sus enlaces entre dominios podrían no ser los esperados.
4. Ejecute un segundo descubrimiento completo en cada dominio.

   Las conexiones inferidas se sustituyen por las conexiones descubiertas.

Resultados

Los enlaces entre cada dominio se añaden mediante agrupaciones entre dominios. El dominio AGGREGATION se crea mediante el agrupador de agregación, que se ejecuta al final del descubrimiento (y siempre que se actualiza la topología).

Qué hacer a continuación

Cree el número de vistas de red que desee utilizando el dominio AGGREGATION.

Creación de vistas de red de dominios cruzados

Después de ejecutar descubrimientos de dominios cruzado, cree vistas de red de dominios cruzados para visualizar la red. Puede crear vistas de red estándar o dinámicas.

Antes de empezar

Antes de crear una vista de red dominios cruzados, debe configurar y ejecutar descubrimientos de dominios cruzados para cada dominio que desee agregar.

Acerca de esta tarea

Para crear vistas de red entre dominios, lleve a cabo los siguientes pasos:

Procedimiento

1. Pulse el icono **Incidencia** y seleccione **Disponibilidad de red** > **Vistas de red**.
2. En **Vistas de red**, en la pestaña **Bibliotecas**, pulse **Nueva vista**  .
3. Cumplimente el separador **General** tal como se muestra a continuación:

   Nombre
   Escriba un nombre para la vista de red, vista dinámica o contenedor de vista de red.

   Importante: Es recomendable usar los nombres de vista de red que contengan caracteres latinos. Los nombres de vistas de red que contienen caracteres no latinos (por ejemplo, cirílicos) no están admitidos porque no se pueden importar ni exportar cuando se migran a una nueva versión de Network Manager.

   Padre
   Seleccione el nodo en el que aparece la vista en la jerarquía en el **Árbol de navegación**. Para mostrar la vista en el nivel superior, seleccione `Ninguno`.

   Tipo
   Seleccione un tipo de vista de red. Dado que la vista de red resultante contendrá todos los dispositivos de todas las redes descubierta, tenga en cuenta el tamaño de las vistas de red para no crear una carga innecesaria en el servidor.

   Complete los otros campos según corresponda para este tipo de vista de red.
4. Haga clic en el separador **Filtro**. Cumplimente el separador tal como se muestra a continuación:

   Dominio
   Seleccione el dominio **AGGREGATION**.

   Complete los otros campos según corresponda para este tipo de vista de red.
5. Haga clic en **Aceptar**.

   Se agregará la nueva vista al árbol de navegación en el **Panel de navegación**. Si ha agregado la vista a un contenedor, amplíe el nodo de contenedor para ver la nueva vista en el árbol.

Resultados

La vista de red muestra dispositivos de todos los dominios descubiertos.

Ejemplo: Red pequeña o Prueba de concepto (POC)

Si desea comprobar si se han descubierto dos o más dominios o se han unido de la forma que esperaba, podría volver a crear todas las vistas de red que normalmente se crean de forma automática una vez finalizado un descubrimiento. Hágalo únicamente si está seguro de que el total de vistas de red resultantes no tendrá un impacto negativo en el rendimiento. Por ejemplo, puede que desee realizar esto al probar un descubrimiento de dominios cruzados en un sistema que no sea de producción. Lleve a cabo los siguientes pasos para crear todas las vistas de red habituales:

1. Cree una vista de red de tipo **Vistas dinámicas - Plantilla**.

2. Seleccione el dominio **AGGREGATION**.
3. Seleccione la plantilla **IP predeterminada**.

Comprobación de enlaces de dominios cruzados

Después de crear las vistas de red de dominios cruzados, compruebe que puede ver los enlaces entre dominios que se esperaba.

Antes de empezar

Antes de comprobar los enlaces entre dominios, asegúrese de haber ejecutado un descubrimiento habilitado por dominio cruzado dos veces en cada dominio.

Acerca de esta tarea

Si no puede ver los enlaces entre dominios que se esperaba, realice los pasos siguientes:

Procedimiento

1. Asegúrese de que están habilitados los agentes adecuados para las tecnologías y dispositivos de los límites de los dominios.
2. Asegúrese de que todas las tecnologías adecuadas están habilitadas para la agrupación de dominios cruzados.
3. Compruebe que el límite entre dominios es adecuado.

   Es importante establecer el alcance de los dominios del descubrimiento para garantizar el número mínimo de enlaces entre dominios. Por ejemplo, normalmente no dividiría la red de manera que los conmutadores que tengan muchas conexiones entre sí estén en distintos dominios. Con frecuencia, las divisiones naturales para los dominios se realizan a lo largo de las líneas geográficas.

   Restricción:

   No obstante, al dividir su red, debe asegurarse de que un dispositivo determinado aparezca en un solo dominio. Es decir, los dominios del descubrimiento no deben solaparse si desea unirlos utilizando un descubrimiento de dominios cruzados.
4. Si sabe que hay enlaces entre dispositivos presentes en distintos dominios, pero no se muestran en las vistas de red, puede añadir o editar los enlaces manualmente.

Fix Pack 2 Configuración de los descubrimientos geográficos

Para poder ver dispositivos en su contexto geográfico, antes debe configurar un descubrimiento geográfico. Elija un método para enriquecer los dispositivos con información geográfica.

Fix Pack 4 Configurar una capa de base de correspondencia

Para ver la topología de red superpuesta en un mapa contextual, configure la capa de mapeo base que desea usar.

Acerca de esta tarea

La capa base brinda la base geográfica sobre la cual se superponen los dispositivos. Los dispositivos y estados de sucesos están contenidos dentro de la capa de topología y la capa de estado, que se calculan automáticamente y siempre están visibles.

Fix Pack 4 Puede definir una o más capas de base por capa proveedor de correspondencia. De forma predeterminada, hay una capa de base definida. Los usuarios pueden seleccionar diversas capas de base para su sesión en las vistas geográficas.

Para añadir o cambiar una capa personalizada, ver “Añadir capas de mapas personalizadas” en la página 351.

Para añadir o cambiar una capa de base, complete los pasos siguientes:

Procedimiento

1. Asegúrese de que tiene la licencia correcta para el proveedor de mapas que desee utilizar.

   No se incluye ninguna licencia de proveedor de mapas con Network Manager. La capa de base de correspondencia predeterminada es OpenStreetMap, que no requiere una licencia.
2. Realice una copia de seguridad y edite el siguiente archivo: `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json`
3. Edite la sección `mapProvider`.

   Los siguientes extractos de código muestran una sección de ejemplo del archivo `config.json`.

```
"mapProvider": {
        "baseMapLayerName": "IBM Network Management",
        "baseLayer": "OpenStreetMap",
        "baseLayersDefn": [
            {
                "baseLayerName": "OpenStreetMap",
                "baseLayerType": "osm"
            },
            {
                "baseLayerName": "Microsoft Bing",
                "baseLayerType": "bing",
                "imagerySet": "Road",
                "key": "INSERT_YOUR_MICROSOFT_KEY"
            },
            {
                "baseLayerName": "OpenLayer XYZ Format",
                "baseLayerType": "xyz",
                "urls": ["https://api.mapbox.com/styles/v1/mapbox/
streets-v9/tiles/256/{z}/{x}/{y}?access_token=INSERT_YOUR_KEY"]
            },
            {
                "baseLayerName": "My Custom GeoServer WMS Layer",
                "baseLayerType": "wms",
                "url": "https://localhost:8443/geoserver/wms",
                "params": {
                }
            },
            {
                "baseLayerName": "My Custom GeoServer WMTS Layer",
                "baseLayerType": "wmts",
                "capabilities": {
                }
            }
        ],
```

4. Configurar una nueva capa base o una existente. Edite la sección existente para un proveedor de mapas compatible o cópiela y edítela. Puede incluir varias capas base para un proveedor de mapas. Por ejemplo, puede definir varias capas base que utilizan el proveedor de OpenStreetMap, mediante la edición del valor `baseLayer`.

   Importante: No suprima ninguna sección vacía del archivo `config.json`. Si faltan secciones, podrían originarse errores.

   a) Ingrese un nombre descriptivo exclusivo para `baseLayerName`.

      En el ejemplo anterior, el valor `baseLayerName` se establece en `OpenStreetMap` en la línea 3.

   b) Especifique el proveedor de mapeo para esta capa base en el parámetro `baseLayerType`.

      Solo puede especificar una de las siguientes palabras clave definidas para el valor `baseLayerType`:

      - `bing` para Bing Maps
      - `osm` para Open Streetmap
      - `wms` para Web Map Service
      - `wmts` para Web Mapping Tile Service

- `xyz` para el formato OpenLayer XYZ

5. Configure los parámetros específicos del proveedor de mapeo necesarios.

   Los proveedores de mapas pueden admitir parámetros adicionales, sin embargo, solo aquellos parámetros que se enumeren en la configuración predeterminada son compatibles con Network Manager. Consulte la documentación del proveedor de mapas para obtener información sobre qué valores son aceptables para estos parámetros.
6. Asegúrese de que el parámetro `baseLayer` coincida exactamente con uno de los valores de `baseMapLayerName`.

   El parámetro `baseLayer` define la capa base predeterminada. Solo puede especificar un parámetro `baseLayer`.
7. Guarde y cierre el archivo.

   Las vistas geográficas deben ser cerradas y reabiertas antes de que un usuario pueda ver cambios a las capas inferiores.

Fix Pack 3 Enriquecimiento del descubrimiento con datos geográficos

Para mostrar mapas geográficos, debe enriquecer la topología de red con datos geográficos.

Acerca de esta tarea

El enriquecimiento de la topología de red con datos geográficos requiere varios pasos:

- Recuperar los datos geográficos de una base de datos o sistema externo.
- Añadir los datos geográficos a la topología.
- Crear una colección en Network Manager que recopile dispositivos en una ubicación geográfica.
- Opcionalmente, puede crear colecciones para representar jerarquías de regiones geográficas.

Nota: La personalización del descubrimiento es un procedimiento avanzado. Debe estar familiarizado con el flujo de datos de descubrimiento, la administración de datos generales, y el lenguaje de agrupador.

Para recuperar los datos geográficos, dos opciones son añadirlos al campo `SysLocation` en el registro del dispositivo mediante un script o exportarlos desde una base de datos a un archivo `.csv`. Otras opciones son posibles dependiendo de cómo se almacenen los datos.

Para crear colecciones y añadir datos geográficos a la topología, debe utilizar el idioma del agrupador. Se proporcionan dos métodos de ejemplo con el producto: los agrupadores `GeoBySysLocation` y `GeoByLookup`.

- El agrupador `GeoBySysLocation` llama a un agrupador PostLayerProcessing `AddGeoLocationData`. El agrupador `AddGeoLocationData` extrae la descripción, la longitud y la latitud de la ubicación del campo `SysLocation` durante un descubrimiento de red. Los datos de ubicación rellenan el campo `m_ExtraInfo->geographicLocation` en la tabla de base de datos `workingEntities.finalEntity` para crear la recopilación de ubicaciones geográficas.
- El agrupador `GeoByLookup` llama a un agrupador DNCIM InferDNCIMObjects `PopulateDNCIM_CustomGeography`. El agrupador `GeoByLookup` crea una jerarquía de regiones geográficas-> ubicaciones geográficas-> dispositivos, y resuelve los datos geográficos a partir de una base de datos externa. El agrupador `GeoByLookup` se puede llamar con un agrupador personalizado, como el agrupador de ejemplo `ACMEDeviceLocationEnrich`. El agrupador de ejemplo `ACMEDeviceLocationEnrich` resuelve las direcciones IP en ubicaciones geográficas para crear una jerarquía de Dirección -> Ciudad -> Estado -> País.

Restricción:

Asegúrese de que cada nivel de una jerarquía sea único. Los siguientes ejemplos son incorrectos porque los valores de ciudad y estado son los mismos:

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
192.168.0.1,"113620 Redwood Gulch Rd, Cupertino, CA 95014,
 USA",PLAL,PLAL,US,37.15458,-122.05561
192.168.0.2,"113620 Redwood Gulch Rd, Cupertino, CA 95014,
```

```
 USA",CA,CA,US,37.15458,-122.05561
```

El ejemplo siguiente es incorrecto porque los valores de ciudad y país son los mismos.

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
Redwood Gulch Rd, Cupertino, CA 95014,
USA",US,CA,US,37.15458,-122.05561
```

El ejemplo siguiente es incorrecto porque el valor PLAL fue usado previamente como una ciudad, y aquí se usa como un estado. CA se usó como un estado, y aquí se usa como un país.

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
192.168.0.3,"113620 Redwood Gulch Rd, Cupertino,
CA 95014, USA",Redwood,PLAL,CA,37.15458,-122.05561
```

El ejemplo siguiente es correcto porque la jerarquía geográfica está ordenada y contenida de manera adecuada.

```
IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
192.168.0.1,"113620 Redwood Gulch Rd, Cupertino,
CA 95014, USA",PLAL,CA,US,37.15458,-122.05561
```

Las jerarquías incorrectas no se incluyen en las vistas geográficas. El agrupador `PopulateDNCIM_CustomGeography` elimina jerarquías incorrectas de la topología y registra cada ocurrencia en los registros `ncp_disco` con un error similar al siguiente:

```
Se detectó una recopilación cíclica: Entidad con entityId
123 no debe recopilarse con collectingEntityId 8912
```

Fix Pack 3 *Ejemplo: Configuración del descubrimiento geográfico mediante el uso de datos de ubicación procedentes de entradas de dispositivo*

Una manera de enriquecer los dispositivos con datos geográficos es usando datos de ubicación procedentes de los registros de dispositivo.

Acerca de esta tarea

El agrupador `AddGeoLocationData` se proporciona como una demostración de un método para añadir información geográfica procedente de los registros del dispositivo. El agrupador asume que los datos geográficos válidos se han añadido al registro de dispositivo en el campo `SysLocation` con el siguiente formato: *`location address;longitude;latitude`*. El administrador de red puede establecer el campo `SysLocation` en los dispositivos de forma manual o mediante un script. Para utilizar un campo distinto, modifique el agrupador.

Para configurar el descubrimiento para usar datos geográficos procedentes de `SysLocation`, realice estos pasos.

Procedimiento

1. Haga una copia de seguridad y edite el agrupador siguiente: `$NCHOME/precision/disco/stitchers/PostLayerProcessing.stch`.
2. Agregue la siguiente línea en el lugar adecuado del archivo para su flujo de datos de descubrimiento; por ejemplo, al final:

   ```
   ExecuteStitcher('AddGeoLocationData');
   ```

3. Inicie un descubrimiento.

   El agrupador `AddGeoLocationData` añade datos geográficos a los campos adecuados dentro del campo `m_ExtraInfo`.

Fix Pack 2 *Ejemplo: Configuración del descubrimiento geográfico mediante el uso de datos de ubicación procedentes de un archivo*

Una manera de enriquecer los dispositivos con datos geográficos es importando datos de ubicación desde un archivo de valores separados por comas (`.csv`) en la base de datos de topología NCIM.

Acerca de esta tarea

Para enriquecer los dispositivos con datos geográficos mediante un archivo `.csv` , adapte los siguientes pasos de ejemplo a sus necesidades.

Procedimiento

1. Cree un archivo `.csv` que contenga información de ubicación para los dispositivos que desee ver en las vistas geográficas. Por ejemplo, puede exportar los datos desde una base de datos a un archivo.

   La información de ubicación debe tener el formato siguiente:

   ```
   ip,dirección,ciudad,región,país,latitud,longitud
   ```

   El siguiente ejemplo muestra las dos primeras líneas de un archivo `.csv`.

   ```
   IP, ADDRESS, CITY, STATE, COUNTRY, LATITUDE, LONGITUDE
   192.168.0.1,"113620 Redwood Gulch Rd, Cupertino, CA 95014, USA",
   PLAL,CA,US,37.15458,-122.05561
   ```

   El agrupador de ejemplo `ACMEDeviceLocationEnrich.stch` espera que el archivo `.csv` tenga este formato. Si desea utilizar un formato distinto, debe modificar el agrupador.
2. Cree una tabla de base de datos en la base de datos de topología NCIM para almacenar los datos geográficos.

   El agrupador de ejemplo `ACMEDeviceLocationEnrich.stch` espera que esta tabla se llame `ACMEGeoLocation`. Si desea utilizar un nombre de tabla distinto, debe modificar el agrupador.

   En Dbs, la tabla de base de datos debe contener campos con los siguientes tipos y especificaciones:

   ```
   IP VARCHAR(255) NOT NULL,
   ADDRESS VARCHAR(255),
   CITY VARCHAR(255),
   STATE VARCHAR(255),
   COUNTRY VARCHAR(255),
   LATITUDE DECIMAL(10 , 8) NOT NULL DEFAULT 0,
   LONGITUDE DECIMAL(11 , 8) NOT NULL DEFAULT 0
   ```

   En Oracle, la tabla de base de datos debe contener campos con los siguientes tipos y especificaciones:

   ```
   IP VARCHAR(255) NOT NULL,
   ADDRESS VARCHAR(255),
   CITY VARCHAR(255),
   STATE VARCHAR(255),
   COUNTRY VARCHAR(255),
   LATITUDE NUMBER(15,8) DEFAULT 0  NOT NULL,
   LONGITUDE  NUMBER(15,8) DEFAULT 0  NOT NULL
   ```
3. Importe los datos geográficos desde el archivo `.csv` a la tabla de base de datos que haya creado con herramienta de base de datos que haya elegido.

   Por ejemplo, para cargar un archivo `core_lat_long_all.csv` en una tabla `ACMELOOKUPGEOLOCATION` en una base de datos NCIM en Oracle o usando el cargador de Oracle V12.1, ejecute el siguiente mandato en el directorio de Oracle.

   ```
   sqlldr SYSTEM/PASSWORD@mySchema control=/opt/oracle/load.ctl
   ```

Donde el archivo `load.ctl` contiene el siguiente código.

```
LOAD DATA
    infile 'core_lat_long_all.csv'
    REPLACE
    INTO TABLE NCIM.ACMELOOKUPGEOLOCATION
    fields terminated by ',' optionally enclosed by '"'
    (
 IP,
 ADDRESS,
 CITY,
 STATE,
 COUNTRY,
 LATITUDE,
 LONGITUDE
    )
```

Los mandatos para otras versiones u otras herramientas son diferentes.

4. Haga una copia de seguridad y edite el agrupador siguiente: `$NCHOME/precision/disco/stitchers/DNCIM/InferDNCIMObjects.stch`.
5. Elimine el comentario de la línea siguiente:

```
ExecuteStitcher('ACMEDeviceLocationEnrich', domainId,
isRediscovery, dynamicDiscoNode );
```

6. Inicie un descubrimiento.

Resultados

El agrupador `PopulateDNCIM_CustomGeography.stch` agrega dispositivos a las recopilaciones geográficas correctas en base a sus datos de ubicación.

El agrupador `ACMEDeviceLocationEnrich.stch` rellena las tablas geográficas de la base de datos de descubrimiento DNCIM con datos procedentes de la tabla de base de datos NCIM que haya creado.

Fix Pack 3 Integración de Web Map Service en línea y fuera de línea

Puede configurar una integración de WMS (Web Map Service) para mostrar mapas geográficos. Algunas integraciones WMS pueden mostrar mapas sin acceso a Internet.

Acerca de esta tarea

Para integrar un WMS, siga estos pasos:

Procedimiento

1. Instale un proveedor de mapas que implemente el estándar WMS. Consulte la documentación de la versión del proveedor que instale.
2. Configure el proveedor de mapas para que use SSL.
3. Ejecute el proveedor de mapas y compruebe que funciona correctamente.

   Es posible que desee almacenar un WMS publico para probar.
4. Configure una capa de mapeo base para usar un proveedor de mapeo WMS.
   a) Realice una copia de seguridad y edite el siguiente archivo: `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json`
   b) Configure una nueva sección dentro de la sección `baseLayersDefn` y especifique los parámetros correctos.

      Los parámetros aceptados por WMS OpenLayers están listados en http://openlayers.org/en/latest/apidoc/ol.source.TileWMS.html. Los parámetros que debe utilizar están definidos en la especificación de solicitudes WMS del servidor WMS.

Utilice la sintaxis siguiente para los parámetros: `"PARAM_NAME":"PARAM_VALUE"`. Para evitar errores, utilice una herramienta de validación para validar el JSON.

c) Para configurar la nueva capa base como predeterminada, establezca el valor `baseLayer` como el `baseLayerName` de la nueva capa base.

El ejemplo siguiente configura parámetros para una integración con GeoServer.

```
"baseMapLayerName": "IBM Network Management",
    "baseLayer": "My Custom GeoServer WMS Layer",
    "baseLayersDefn": [
        {
            "baseLayerName": "My Custom GeoServer WMS Layer",
         "baseLayerType": "wms",
            "url": "https://offline:443/geoserver/wms",
            "params": {
                "REQUEST": "GetMap",
                "FORMAT": "image/png",
                "SRS": "EPSG:4326",
                "BBOX": "-104.2822265625,33.5302734375,-87.4072265625,40.78125",
                "VERSION": "1.1.1",
                "STYLES": "",
                "SERVICE": "WMS",
                "WIDTH": "768 ",
                "HEIGHT": "330",
                "TRANSPARENT": "true",
                "LAYERS": "topp:states"
            }
        .....
        }
```

Si no especifica ningún parámetro en la sección `"params": {}`, deje la sección vacía.

Importante: No suprima ninguna sección vacía del archivo `config.json`. Si faltan secciones, podrían originarse errores.

Para la integración con mapas fuera de línea, el valor `baseLayerType` debe ser `wms`.

Ingrese un nombre descriptivo exclusivo para `baseLayerName`.

Añadir capas de mapas personalizadas

Puede añadir capas personalizadas a los mapas geográficos. Por ejemplo, puede añadir información geográfica, disponible a través de un servidor público.

Antes de empezar

Configure un proveedor de correlaciones fuera de línea si desea que la capa personalizada esté disponible fuera de línea. Consulte “Integración de Web Map Service en línea y fuera de línea” en la página 350 para obtener más información.

Acerca de esta tarea

Fix Pack 4 Puede definir una o más capas personalizadas y una capa de base. Los usuarios pueden seleccionar diversas capas personalizadas para su sesión en las vistas geográficas.

Se admiten los siguientes tipos de proveedor de correlaciones:

- ArcGISRest
- Web Map Service (WMS)
- Web Mapping Tile Service (WMTS)

Para añadir una capa de mapa personalizada, siga estos pasos:

Procedimiento

1. Realice una copia de seguridad y edite el siguiente archivo: `$JazzSM_HOME/profile/installedApps/JazzSMNode01Cell/isc.ear/ncp_gis.war/resources/config.json`

2. Cree una nueva sección `customLayers` o descomente una de las secciones predeterminadas, y especifique los parámetros correctos.

   Los parámetros aceptados por WMS OpenLayers están listados en http://openlayers.org/en/latest/apidoc/ol.source.TileWMS.html. Los parámetros que debe utilizar están definidos en la especificación de solicitudes WMS del servidor WMS. Utilice la sintaxis siguiente para los parámetros: `"PARAM_NAME":"PARAM_VALUE"`. Para evitar errores, utilice una herramienta de validación para validar el JSON.

   Los parámetros aceptados por ArcGISRest están listados en https://openlayers.org/en/latest/apidoc/module-ol_source_TileArcGISRest-TileArcGISRest.html.

   Los parámetros WMTS aceptados por OpenLayers están listados en https://openlayers.org/en/latest/apidoc/module-ol_source_WMTS.html.

   El siguiente ejemplo configura parámetros de una capa personalizada de WMS, una capa personalizada de ArcGISRest, y una capa personalizada de WMTS.

```
"customLayers": [
   {
       "layerName": "Drainage Divisions",
       "layerType": "wms",
       "url": "http://geoserver.nationalmap.nicta.com.au/
admin_bnds_abs/ows",
       "params": {
          "LAYERS": "admin_bnds:ADD_2011_AUST"
       }
    "selected":"true"
   }, {
       "layerName": "Prohibited Areas",
       "layerType": "arcGISRest",
       "url": "http://services.ga.gov.au/gis/rest/services/
NM_Reserves/MapServer",
       "params": {}

    "selected":"false"
    }
       {
       "layerName": "New Zealand Earthquakes",
       "layerType": "wmts",
       "capabilities": {
             "url": "https://openlayers.org/en/v4.3.4/examples
/data/WMTSCapabilities.xml",
             "layer": "layer-7328",
             "matrixSet": "EPSG:3857"
             }
    "selected":"false"
       }
]
```

   Si no va a proporcionar ningún parámetro `arcGISRest`, incluya la línea, pero déjela vacía: `"params": {}`. Eliminar u omitir secciones del archivos origina errores.

   El parámetro `layerName` se puede establecer en cualquier valor descriptivo único.

   En el caso de las capas de mapas personalizados, el valor `layerType` debe ser uno de estos valores compatibles:

   - `arcGISRest`
   - `wms`
   - `wmts`

   Las capas personalizadas que tienen el parámetro `selected` establecido en `true` se muestran de forma predeterminada en las vistas geográficas. El usuario puede mostrar u ocultar cualquier capa personalizada.
3. Defina varias capas si lo desea. El índice-z de las capas está definido por su posición en el archivo. Para mostrar una capa personalizada encima de otra, defínala en una posición más alta del archivo. La capa de topología se muestra en la parte superior de las otras capas, y la capa base se muestra debajo de las otras capas.

Fix Pack 2 Verificación de los descubrimientos geográficos

Tras ejecutar un descubrimiento geográfico, verifique que se ha ejecutado correctamente.

Acerca de esta tarea

Para comprobar que la ejecución del descubrimiento geográfico ha sido correcta, complete los siguientes pasos:

Procedimiento

1. Consulte los registros del proceso **ncp_disco** en el directorio `$NCHOME/log/precision` para averiguar si los agrupadores geográficos que ha configurado funcionan.
2. Consulte las tablas de ubicación en la base de datos de topología NCIM para descubrir si se han rellenado con datos geográficos.

   Por ejemplo, utilice el siguiente mandato:

   select * from NCIM.geographicLocation
3. Inicie sesión en Dashboard Application Services Hub. Abra el siguiente URL:

   ```
   https://server:port/ibm/console/nm_rest/topology/devices/geo/all
   ```

   Si el descubrimiento geográfico se ha completado correctamente, se muestran los resultados de JSON para los dispositivos enriquecidos geográficamente.
4. Abra una vista geográfica y compruebe que aparecen los dispositivos esperados.

Fix Pack 4 Configuración de descubrimientos IP SLA

Para poder supervisar acuerdos IP SLA, debe configurar y ejecutar un descubrimiento IP SLA.

Acerca de esta tarea

Un descubrimiento IP SLA asocia sucesos IP SLA compatibles con dispositivos y enlaces en la topología Network Manager. Puede usar vistas de red para ver análisis configurados para supervisar los tiempos de respuesta de IP SLA y sus dispositivos de origen y destino.

Procedimiento

1. Instale Netcool/OMNIbus Knowledge Library versión 4.8.1 o versiones posteriores.
2. Configure Netcool/OMNIbus Knowledge Library para usarlo con Sonda SNMP.

   Este paso permite asociar estados de suceso con análisis IP SLA en la topología de red.
3. Habilite el agente IP SLA que corresponda.

   Este paso permite descubrir análisis IP SLA. Para obtener más información sobre los agentes IP SLA disponibles, consulte *Agentes de Acuerdo de nivel de servicio* en *Referencia de IBM Tivoli Network Manager*.
4. Inicie un descubrimiento.

Qué hacer a continuación

Ahora podrá supervisar los tiempos de respuesta IP SLA usando las vistas de red, **Vista de saltos de red** y **Navegador de estructura**. Consulte *Supervisión de las configuraciones de Acuerdo de nivel de servicio IP (IP SLA)* en *Guía del usuario de IBM Tivoli Network Manager*.

Capítulo 13. Supervisión de descubrimientos de red

Puede supervisar el estado y el progreso de sus descubrimientos de red. Además, puede supervisar el descubrimiento completo y el descubrimiento parcial ejecutando consultas OQL desde la línea de mandatos.

Supervisión del descubrimiento de red desde la GUI

Desde la página **Estado del descubrimiento activo**, puede supervisar el estado y el progreso del descubrimiento completo o parcial actuales, investigar el trabajo de los agentes de descubrimiento y visualizar detalles del último descubrimiento.

Acerca de esta tarea

Desde la página **Estado del descubrimiento activo**, también puede iniciar y detener descubrimientos completos y parciales.

Supervisión de descubrimientos completos y parciales

Puede supervisar el estado y el progreso del descubrimiento completo o parcial mediante la GUI.

Supervisión del progreso del descubrimiento completo y parcial

Utilice el separador **Supervisión** para supervisar el progreso del descubrimiento completo o parcial actual a lo largo de cada una de las fases del descubrimiento.

Acerca de esta tarea

Realice los pasos siguientes para supervisar el progreso del descubrimiento completo o parcial actual.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Estado del descubrimiento de red**.
2. Seleccione un dominio.
3. Haga clic en el separador **Supervisión**.
4. Inicie un descubrimiento parcial o completo seleccionando la opción del botón Iniciar descubrimiento  .

Resultados

Las siguientes fases aparecen en la tabla.

Interrogando dispositivos
Durante esta fase, los dispositivos los descubren en primer lugar los buscadores y, a continuación, la información la recuperan los agentes desde los dispositivos. Esta fase también se conoce como fase 1.

Resolviendo direcciones
Durante esta fase, los agentes resuelven conversiones de direcciones IP a MAC. Esta fase también se conoce como fase 2.

Descargando conexiones
Durante esta fase, los agentes de conmutador descargan las tablas de reenvío desde los conmutadores de la red. Esta fase también se conoce como fase 3.

Correlacionando conexiones
Durante esta fase, se calcula la conectividad entre los dispositivos, se crea el modelo de contención y se construye la topología de red. Esta fase también se conoce como fase -1.

Puede visualizar en qué fase se encuentra el descubrimiento actual mirando la columna **Estado** de la tabla. Si no se ha iniciado la fase, la columna está vacía. Si una fase está en curso, esta columna muestra el icono de una rueda girando. Si una fase se ha finalizado satisfactoriamente, esta columna muestra el icono de una marca de referencia verde.

Estado
Muestra el estado de una fase concreta. La columna muestra los siguientes tipos de estados.

Tabla 46. Estado de fase de descubrimiento

Estado	Icono	Descripción
Completado		Si una fase se ha finalizado satisfactoriamente, esta columna muestra el icono de una marca de referencia verde.
En curso		Si una fase está en curso, esta columna muestra el icono de una rueda girando.
No iniciada		Si no se ha iniciado la fase, la columna está vacía.

Puede visualizar cuánto tiempo tarda cada fase en la columna **Tiempo transcurrido** en la tabla. Cada fase tarde una cantidad de tiempo diferente dependiendo del ámbito del descubrimiento, la complejidad de la red y la cantidad de detalles que se recuperan desde los dispositivos. Si el tiempo transcurrido sigue aumentando y el trabajo finalizado no aumenta, el descubrimiento puede encontrar problemas.

Recuerde: En la primera fase, el recuento de direcciones IP descubiertas deja de aumentar en parte durante la fase. Esto forma parte de la operación normal del descubrimiento. El recuento de direcciones IP descubiertas solo aumenta durante la primera parte de la fase, mientras los buscadores descubren nuevos dispositivos. En la última parte de la fase, los agentes de descubrimiento recuperan información de estos dispositivos y no se descubren nuevas direcciones IP.

La sección **Agentes de descubrimiento** muestra el progreso de los agentes de descubrimiento. Si cree que una fase tarda demasiado tiempo en completarse, haga clic en el separador **Agentes de descubrimiento** para visualizar qué están haciendo los agentes de descubrimiento.

Puede visualizar el progreso dentro de una fase en la columna **Trabajo finalizado** en la tabla. Para la primera fase, esta columna muestra el número de direcciones IP que se han encontrado hasta el momento. Para las otras fases, esta columna muestra el porcentaje de trabajo finalizado en la fase.

Comparación de descubrimientos completos

Puede utilizar el separador **Supervisión** para comparar el descubrimiento actual con el descubrimiento completo anterior.

Acerca de esta tarea

No puede comparar descubrimientos parciales. En la tabla, los datos de las columnas **Anteriores** son para el último descubrimiento completo. Realice los pasos siguientes para comparar los descubrimientos completos.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Estado del descubrimiento de red**.
2. En **Estado del descubrimiento de red**, pulse la barra **Supervisión**.

Resultados

Puede visualizar el tiempo que ha tardado en completarse cada fase del descubrimiento anterior en la subcolumna **Anterior** de la columna **Tiempo transcurrido**.

Nota: Para mostrar los tiempos de descubrimiento de todos los descubrimientos anteriores, ejecute el script **disco_profiling_data.pl** desde la línea de mandatos. Para obtener más información acerca del script **disco_profiling_data.pl**, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

El tiempo que tarda cada fase depende del ámbito del descubrimiento, de la complejidad de la red y de la cantidad de detalles que se recuperan de los dispositivos. Si la red no ha sufrido cambios importantes, y el ámbito y los valores de descubrimiento no se han modificado de forma significativa, pero el tiempo transcurrido de una fase del descubrimiento actual es significativamente superior al tiempo que ha tardado la misma fase en el descubrimiento anterior, es posible que el descubrimiento tenga problemas.

Puede visualizar cuántas direcciones IP se encuentran en el descubrimiento actual y cuántas se han encontrado en el descubrimiento anterior en la columna **Trabajo finalizado** de la tabla. Si se han encontrado menos direcciones IP en el descubrimiento actual, es posible que exista un problema en el ámbito del descubrimiento o en el acceso de SNMP a los dispositivos.

Supervisión del progreso del buscador de pings

Puede utilizar la tabla **Estado del buscador de pings** para supervisar el progreso del buscador de pings durante un descubrimiento completo.

Acerca de esta tarea

Para abrir **Estado de buscador de pings**, complete los pasos siguientes.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Estado del descubrimiento de red**.
2. En **Estado del descubrimiento de red**, pulse la ficha **Estado de buscador de pings**.

Resultados

Puede utilizar la tabla **Estado del buscador de pings** para visualizar las direcciones IP y las subredes que se han descubierto hasta este momento. Si el buscador de pings está procesando una subred, también puede visualizar a qué dirección IP se le ha hecho ping por última vez.

La tabla **Estado del buscador de pings** contiene la siguiente información:

Dirección
Una lista de IP y subredes descubiertas hasta este punto.

Máscara de red
Para cada subred, esta columna indica el valor de máscara de red.

Último ping
La última dirección IP en la que se ha ejecutado ping.

Estado
Indica si el Buscador de pings está aún haciendo ping a este dispositivo o subred o si ha terminado de hacer ping.

Tabla 47. Estado del buscador de pings

Estado	Icono	Descripción
Completado	✅	El buscador de pings ha completado la ejecución de ping de esta subred o dirección IP.

Tabla 47. Estado del buscador de pings (continuación)		
Estado	**Icono**	**Descripción**
Iniciado		El buscador de pings está actualmente haciendo ping en esta subred o dirección IP.
Detenido		El buscador de pings no ha comenzado a hacer ping en esta subred o dirección IP.
Esperando estado		El sistema está esperando el Estado del buscador de pings para esta subred o dirección IP.

Supervisión del progreso del agente de descubrimiento

Puede utilizar la sección **Estado de las agentes** para supervisar el progreso de los agentes de descubrimiento durante un descubrimiento completo o parcial.

Acerca de esta tarea

Los agentes de descubrimiento reúnen datos de los dispositivos descubiertos. Estos datos se utilizan durante la fase de correlación de conectividad del descubrimiento (fase -1) para crear la contención y la conectividad de la red.

Puede utilizar el **Estado de los agentes** para responder a estas y a otras preguntas mientras se ejecuta el descubrimiento:

- ¿Se están ejecutando bien todos los agentes?
- ¿Ha fallado algún agente?
- ¿Está dando error algún agente para completarse?
- ¿En qué dispositivo está trabajando actualmente un agente en concreto?

Complete los siguientes pasos para abrir el **Estado de los agentes** y supervisar el progreso de los agentes de descubrimiento.

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Estado del descubrimiento de red**.
2. Haga clic en el separador **Estado de agentes**.

   La sección **Estado de agentes** contiene dos tablas, la tabla de **Estado de agentes** en la parte superior y la tabla **Estado de entidad** de abajo. La barra de herramientas de la tabla **Estado de agentes**contiene los siguientes controles.

   Filtrar agentes por fase
   Utilice la lista desplegable de fases para seleccionar una fase de descubrimiento. La tabla de agentes muestra los siguientes agentes:

   - *Descubrimiento completo o parcial*: todos los agentes de descubrimiento que han comenzado durante el descubrimiento actual y que están planificados para finalizar en la fase de descubrimiento que ha seleccionado.

   Renovar 
   Actualiza los datos en las tablas Estado de los agentes y Estado de la entidad. El icono cambia al icono **Renovando**  mientras que los datos de la tabla se están renovando. No puede renovar las tablas de nuevo hasta que la renovación se complete.

   La tabla **Estado de los agentes** lista todos los agentes que han comenzado hasta ahora durante este descubrimiento y contiene la información siguiente. Esta información se actualiza cada 20 segundos. Cuando abra por primera vez esta tabla, se ordenará en orden descendente de **Estado**.

Agente
Agentes de descubrimiento que han comenzado durante el descubrimiento actual y que están planificados para finalizar en la fase de descubrimiento que ha seleccionado.

Completados en fase
La fase en la que se completa el agente de descubrimiento.

Estado
Estado actual del agente de descubrimiento. Los estados posibles, en el orden descendente predeterminado, están listados en la tabla siguiente.

Tabla 48. Estados del agente

Estado	Valor	Icono	Descripción
Concluido	5		El agente ha finalizado de forma inesperada. Este es un problema de descubrimiento potencial.
Finalizado	4		El agente se sigue ejecutando pero ha terminado el proceso de todas las entidades de la cola. El agente sigue estando disponible para procesar cualquier otro agente colocado en la cola.
En ejecución	3		El agente está procesando entidades actualmente.
Iniciando	2		El agente se está iniciando.
No ejecución	1		El agente no se está ejecutando.

Número total de entidades
El número total de entidades que este agente debe procesar. Este número varía, según se indica a continuación:

- *Descubrimiento completo o parcial*: el número total de entidades que necesita procesar este agente aumenta a medida que progresa el descubrimiento y que los buscadores descubren más dispositivos que tiene que procesar el agente.

Entidades pendientes
El número de entidades que esperan a ser procesadas por este agente. Este número puede aumentar y disminuir durante el descubrimiento. El número aumenta inicialmente a medida que el descubrimiento progresa y los buscadores descubren más dispositivos que tiene que procesar el agente. A medida que el agente completa el proceso de las entidades, este número se reducirá hasta que alcance cero.

Nota: Si este valor no llega a cero durante el descubrimiento, significará que el agente no pudo completar el proceso en una o varias entidades y que hay un problema de descubrimiento potencial.

3. Haga clic en un agente en la tabla **Estado de los agentes**.

La tabla **Estado de entidad** lista las entidades que ha procesado o que está procesando actualmente este agente. La tabla **Estado de entidad** responde a los cambios de la tabla **Estado de los agentes**. La tabla se actualiza en las siguientes situaciones: cuando se selecciona un nuevo agente en la tabla **Estado de los agentes**; cuando se cambia el filtro de la tabla **Estado de entidad** por **Todo** o **Cola**; y cuando se pulsa el botón **Renovar** de la tabla **Estado de los agentes**. Cuando abra por primera vez esta tabla, se ordenará en orden descendente de **Estado**.

Nombre_agente

Utilice este botón de selección para especificar si se mostrarán todas las entidades (Todos) o sólo las entidades puestas en cola para su proceso (Cola). El valor predeterminado es Cola.

Todo

Configure la tabla **Detalles** para mostrar todas las entidades para este agente. Esto incluye las entidades que se han puesto en cola para que las procese el agente, las entidades que está procesando el agente actualmente y entidades que ya ha procesado el agente.

Cola

Configure la tabla **Detalles** para mostrar sólo las entidades que se han puesto en cola para que las procese este agente.

Identificador

Identificador de las entidades procesadas por este agente. Si se selecciona **Todos**, esta columna mostrará entidades procesadas, en proceso o puestas en cola para que las procese este agente. Si se selecciona **Cola**, esta columna mostrará entidades en cola para que procese este agente.

Estado

Estado actual de la entidad. Los estados posibles, en el orden descendente predeterminado, están listados en la tabla siguiente:

Tabla 49. Estados de entidad

Estado	Valor	Icono	Descripción
Concluido	5		El proceso de la entidad ha finalizado de forma inesperada. El agente se ha detenido manualmente o se ha producido un problema con el descubrimiento.
Finalizado	4		Un agente ha completado el proceso de esta entidad.
En ejecución	3		Un agente está procesando actualmente esta entidad.
Iniciando	2		Un agente está comenzando a procesar esta entidad.
No ejecución	1		Esta entidad no está procesándose actualmente.

Tiempo transcurrido

El tiempo que se toma el agente para procesar esta entidad, expresado en el formato HH:MM:SS. Este valor sólo se muestra para aquellas entidades que han completado el proceso.

Hora de asignación

La fecha y la hora en la que el agente comenzó a procesar esta entidad. Este valor sólo se muestra para aquellas entidades para las que el proceso ha comenzado o se ha completado.

Hora de retorno

La fecha y la hora en la que el agente ha recuperado datos para esta entidad. Este valor sólo se muestra para aquellas entidades que han completado el proceso.

Acceso SNMP

Indica si el agente pudo acceder a esta entidad con SNMP.

Monitorización del progreso del descubrimiento desde la línea de mandatos

Cuando se está ejecutando el proceso **ncp_disco**, puede supervisar el progreso del descubrimiento utilizando el proveedor de servicios de OQL, el proceso **ncp_oql**, para consultar las bases de datos y determinar que es lo que está pasando en cada momento.

Supervisión de descubrimientos completos y parciales

Puede supervisar el estado y el progreso del descubrimiento completo o parcial mediante la línea de mandatos.

Acerca de esta tarea

Las consultas presentadas en los siguientes temas se han generalizado para todas las situaciones de descubrimiento y no están limitadas al descubrimiento de capa 3.

Los ejemplos se proporcionan solo para demostrar la cantidad de flexibilidad que posee cuando se recupera información de las bases de datos utilizando OQL. Utilizando las definiciones esquemáticas de todas las bases de datos y el conocimiento de la sintaxis OQL, puede construir consultas que respondan a sus preguntas con respecto al estado actual del proceso de descubrimiento.

Puede emitir consultas simples para averiguar, por ejemplo, qué está realizando actualmente el proceso **ncp_disco**, qué agentes de descubrimiento tienen dispositivos descubiertos o cuántos dispositivos se han descubierto hasta el momento. También puede emitir consultas complejas para averiguar, por ejemplo, qué dispositivos ha descubierto un agente de descubrimiento específico o qué agentes de descubrimiento han interrogado un dispositivo específico.

Para obtener información sobre cómo iniciar el proveedor de servicios de OQL, incluidos los prerrequisitos, consulte *Referencia de IBM Tivoli Network Manager*.

Ejemplo de consultas de estado de descubrimiento

Puede utilizar consultas similares a estos ejemplos para encontrar el estado de distintas partes del descubrimiento.

Ejemplo: Determinar en qué dirección está haciendo ping el Buscador de pings

La consulta siguiente devuelve la dirección actual donde ha hecho ping el Buscador de pings:

```
select m_CurrentAddress from pingFinder.status;
go
.
{
                m_CurrentAddress=192.168.0.1;
}
```

Ejemplo: Identificación de la fase actual del descubrimiento

El ejemplo siguiente muestra cómo identificar la fase actual del descubrimiento. Los resultados de la consulta anterior muestran que el proceso de descubrimiento sigue en recopilación de datos fase 1.

```
select * from disco.status;
go
.
{
                m_DiscoveryMode=0;
                m_Phase=1;
                m_BlackoutState=0;
                m_CycleCount=0;
                m_ProcessingNeeded=0;
                m_FullDiscovery=0;
}
```

Ejemplo: Identificación del estado de un descubrimiento NAT

Este ejemplo muestra cómo identificar el estado del descubrimiento NAT.

```
select m_NATStatus from disco.NATStatus;
go
.
{
                m_NATStatus=3;
}
```

Ejemplo: Identificación de qué agentes están habilitados

Este ejemplo muestra cómo identificar si ha habilitado los agentes de descubrimiento apropiados.

```
select m_AgentName, m_Valid from disco.agents
where m_Valid = 1;
go
...
{
                m_AgentName='Details';
                m_Valid=1;
}
{
                m_AgentName='AssocAddress';
                m_Valid=1;
}
{
                m_AgentName='IpRoutingTable';
                m_Valid=1;
}
{
                m_AgentName='IpForwardingTable';
                m_Valid=1;
}
```

Ejemplo: identificación del estado de los agrupadores de descubrimiento

El ejemplo siguiente muestra cómo identificar el estado de los agrupadores consultando la tabla stitchers.status.

```
select * from stitchers.status
where m_State > 0 ;
go
.........
{
                m_Name='AgentRetToInstrumentationSubnet';
                m_State=3;
}
{
                m_Name='DetailsRetProcessing';
                m_State=3;
}
.....
.....
{
                m_Name='DetectionFilter';
                m_State=3;
}
{
                m_Name='FnderProcToDetailsDesp';
                m_State=3;
}
{
                m_Name='FnderRetProcessing';
                m_State=3;
}
```

Los resultados de la consulta muestran el estado actual de todos los agrupadores que ha llamado el proceso de descubrimiento hasta ahora. Tenga en cuenta que los resultados mostrados anteriormente se han abreviado.

Ejemplo: identificación de los agentes que están activos

El ejemplo siguiente muestra cómo consultar el estado de los agentes en la base de datos agents.

```
select * from agents.status
where m_State > 0 ;
go
..
{
                m_Name='Details';
                m_State=3;
                m_NumConnects=1;
}
{
                m_Name='IpRoutingTable';
                m_State=3;
                m_NumConnects=1;
}
```

Los resultados de la consulta anterior muestran que únicamente están activos los agentes Details e IpRoutingTable (es decir, tienen un estado mayor que cero).

Ejemplo de consultas de dispositivo

Puede utilizar consultas similares a estos ejemplos para identificar los dispositivos que cumplen con ciertos criterios; por ejemplo, los dispositivos que han encontrado los buscadores.

Ejemplo: Identificación de los dispositivos que han sido encontrados por los buscadores

El ejemplo siguiente muestra cómo identificar los dispositivos que han sido encontrados por los buscadores.

```
select * from finders.processing;
go
....
{
                m_UniqueAddress='172.20.12.253';
                m_Protocol=1;
                m_Creator='IpRoutingTable';
}
{
                m_UniqueAddress='172.20.22.61';
                m_Protocol=1;
                m_Creator='IpRoutingTable';
}
{
                m_UniqueAddress='172.20.0.221';
                m_Protocol=1;
                m_Creator='IpRoutingTable';
}
{
                m_UniqueAddress='10.10.35.17';
                m_Creator='PingFinder';
}
```

La consulta anterior muestra los dispositivos detectados por el buscador de pings, así como los dispositivos notificados como resultado de las conexiones descubiertas por el agente de descubrimiento `IpRoutingTable`.

Ejemplo: Identificación de los dispositivos que se han enviado al agente de detalles

El ejemplo siguiente muestra cómo identificar los dispositivos que se han enviado al agente de detalles.

```
select * from Details.despatch;
go
.............................................................
.............................
{
                m_UniqueAddress='10.10.38.82';
}
{
                m_UniqueAddress='10.10.38.83';
```

```
}
.....
.....
{
                m_UniqueAddress='10.10.38.84';
}
{
                m_UniqueAddress='10.10.38.87';
}
{
                m_UniqueAddress='10.10.38.88';
}
{
                m_UniqueAddress='10.10.38.89';
}
{
                m_UniqueAddress='10.10.38.90';
}
```

Ejemplo: Identificación de los dispositivos que han sido descubiertos por el agente de detalles

Para identificar los dispositivos que ha devuelto el agente de detalles, consulte la tabla `returns` del agente de detalles, como se muestra a continuación.

```
select * from Details.returns;
go
.............................................................
.............................
{
                m_UniqueAddress='10.10.8.255';
                m_UpdAgent='Details';
                m_HaveAccess=1;
                m_Description='Ascend Max-HP T1/PRI S/N;
                m_ObjectId='1.3.6.1.4.1.529.1.2.6';
                m_LastRecord=1;
}
{
                m_UniqueAddress='10.10.9.1';
                m_UpdAgent='Details';
                m_Name='minotaur.Kazeem.San.COM';
                m_HaveAccess=0;
                m_LastRecord=1;
}
.....
.....
{
                m_UniqueAddress='10.10.9.2';
                m_UpdAgent='Details';
                m_Name='cyclops.Kazeem.San.COM';
                m_HaveAccess=0;
                m_LastRecord=1;
}
{
                m_UniqueAddress='10.10.9.3';
                m_UpdAgent='Details';
                m_Name='centaur.Kazeem.San.COM';
                m_HaveAccess=0;
                m_LastRecord=1;
}
```

Ejemplo: Identificación de todos los dispositivos descubiertos hasta ahora

El siguiente ejemplo muestra cómo identificar todas las entidades de red conocidas.

```
select m_Name, m_ObjectId, m_UniqueAddress
from workingEntities.finalEntity;
go
..............................
{
                m_Name='10.10.8.255';
                m_ObjectId='1.3.6.1.4.1.529.1.2.6';
                m_UniqueAddress='10.10.8.255';
}
{
                m_Name='minotaur.Kazeem.San.COM';
                m_UniqueAddress='10.10.9.1';
```

```
}
.....
.....
{
                m_Name='cyclops.Kazeem.San.COM';
                m_UniqueAddress='10.10.9.2';
}
```

Ejemplo: Identificación de los agentes que han descubierto dispositivos

El ejemplo siguiente muestra cómo identificar los agentes que han descubierto dispositivos.

```
select m_Name, m_Creator
from workingEntities.finalEntity;
go
..............................
{
                m_Name='b11-m1-2611.Kazeem.San.COM[ 0 [ 2 ] ]';
                m_Creator='IpRoutingTable';
}
{
                m_Name='b-ayo.Kazeem.San.COM';
                m_Creator='Details';
}
{
                m_Name='b11-m1-2611.Kazeem.San.COM[ 0 [ 1 ] ]';
                m_Creator='IpRoutingTable';
}
.....
.....
{
                m_Name='b11-m1-2611.Kazeem.San.COM';
```

Ejemplo: Determinación de los distintos tipos de interfaces descubiertas

El ejemplo siguiente muestra cómo identificar los tipos de interfaces en cada dispositivo descubierto. Utilice la palabra clave `select DISTINCT` para optimizar el almacenamiento de las múltiples entradas de tipo de interfaz que se almacenan para cada dispositivo en la tabla `workingEntities.finalEntity`.

```
select DISTINCT m_LocalNbr->m_IfType, m_ObjectId
from workingEntities.finalEntity
where m_EntityType = 2;
go
..............................
{
        m_IfType=166;
        m_ObjectId='1.3.6.1.4.1.9.1.222';
}
{
        m_IfType=6;
        m_ObjectId='1.3.6.1.4.1.9.1.222';
}
{
        m_IfType=1;
        m_ObjectId='1.3.6.1.4.1.9.1.222';
}
{
        m_IfType=6;
        m_ObjectId='1.3.6.1.4.1.9.1.310';
}
{
        m_IfType=22;
        m_ObjectId='1.3.6.1.4.1.9.1.310';
}
..............................
```

Ejemplo: Supervisión de agentes en la fase actual

Utilice la siguiente consulta de ejemplo para identificar qué agentes espera la fase actual para poder completarse. La siguiente consulta de ejemplo lista los nombres de todos los agentes que finalizan en la fase actual y que cumplen los criterios siguientes:

- El agente es válido. (`m_State <> 0`)
- El agente está actualmente en uso. (`m_State <> 1`)
- El estado del agente no está todavía completo. (`m_State <> 4`)

```
select m_Name from agents.status
where
m_State <> 0 AND
m_State <> 1 AND
m_State <> 4 AND
m_CompletionPhase IN (( select m_Phase from disco.status )) ;
```

Una vez ha identificado qué agentes deben completarse en la fase actual, utilice la siguiente consulta para determinar en qué dispositivos están trabajando los agentes.

```
select
    m_Name,
    m_UniqueAddress,
    m_ObjectId,
    m_Description
from
    <agentName>.despatch
where
    m_UniqueAddress NOT IN
    (( select m_UniqueAddress from <agentName>.returns where m_LastRecord = 1 )) ;
```

Ejemplos de consultas de entidades de red

Puede utilizar consultas a la base de datos de instrumentación para determinar si se han descubierto entidades de red, como subredes y VLAN. Las tablas de base de datos de instrumentación almacenan un registro de cada dispositivo descubierto.

Ejemplo: Identificación del número de subredes descubiertas

El siguiente ejemplo devuelve detalles de las subredes descubiertas.

```
select * from instrumentation.subNet;
go
.....................................
{
                m_SubNet='172.20.67.0';
                m_NetMask='255.255.255.0';
}
.....
.....
{
                m_SubNet='172.20.70.0';
                m_NetMask='255.255.254.0';
}
{
                m_SubNet='172.20.95.0';
                m_NetMask='255.255.255.0';
}
( 81 record(s) : Transaction complete )
```

Ejemplo: Identificación de las VLAN descubiertas

El siguiente ejemplo de consulta devuelve detalles de los ID de VLAN descubiertos.

```
select * from instrumentation.vlan;
go
.....................................
{
                m_Vlan=23;
}
{
                m_Vlan=65;
}
.....
.....
{
```

```
                m_Vlan=677;
}

( 4826 record(s) : Transaction complete )
```

Ejemplo de consultas de descubrimiento complejo

Puede utilizar consultas similares a estos ejemplos para identificar los dispositivos que cumplen con ciertos criterios; por ejemplo, los dispositivos que determinados agentes de descubrimiento han encontrado.

Identificación de los dispositivos que se han enviado a un agente específico

La siguiente consulta de ejemplo identifica los dispositivos que se han enviado al agente IpRoutingTable.

```
select m_Name, m_ObjectId, m_Description
from IpRoutingTable.despatch;
go
.............................
{
       m_Name='10.10.63.193';
       m_ObjectId='1.3.6.1.4.1.9.1.108';
       m_Description='Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by Cisco Systems, Inc.
Compiled Thu 29-Apr-99 06:27 by kpma';
}
.....
.....
{
       m_Name='10.10.71.248';
       m_ObjectId='1.3.6.1.4.1.9.1.258';
       m_Description='Cisco Internetwork Operating System Software
IOS (tm) MSFC Software (C6MSFC-IS-M), Version 12.0(7)XE1, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
TAC:Home:SW:IOS:Specials b-ayo k-az-eem for info
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Fri 04-Feb-00 00:';
}
```

Identificación de los dispositivos devueltos por un determinado agente

La siguiente consulta de ejemplo identifica los dispositivos devueltos por el agente de descubrimiento ipRoutingTable.

```
select m_Name from IpRoutingTable.returns;
go
.............................
{
                m_Name='10.10.71.248';
}
.....
.....
{
                m_Name='10.10.71.248';
}
{
                m_Name='10.10.71.248';
}
```

Identificación de los dispositivos adicionales descubiertos por un determinado agente

Un agente puede descubrir dispositivos adicionales al interrogar a un dispositivo. En este caso, el dispositivo adicional estarían en la tabla `returns` de ese agente, pero no en la tabla `despatch`. Puede identificar qué dispositivo se encuentran presentes en la tabla `IpRoutingTable.returns`, pero no en la tabla `IpRoutingTable.despatch` si une las tablas `IpRoutingTable.despatch` e `IpRoutingTable.returns`, como en el siguiente ejemplo.

```
select IpRoutingTable.returns.m_Name from
IpRoutingTable.returns, IpRoutingTable.despatch
```

```
where
IpRoutingTable.returns.m_Name <>
IpRoutingTable.despatch.m_Name;
go
.....................................
{
                m_Name='10.10.71.237';
}
.....
.....
{
                m_Name='10.10.71.55';
}
{
                m_Name='10.10.71.51';
}
```

Identificación de los dispositivos que un agente ha puesto en cola

El ejemplo siguiente devuelve aquellos dispositivos de la tabla despatch que no se han devuelto todavía.

```
select * from <agent>.despatch
where
(
    m_UniqueAddress NOT IN
        (( select m_UniqueAddress from <agent>.returns where m_LastRecord = 1 ))
);
```

Consultas de ejemplo para localizar un dispositivo específico

Para comprobar si se ha descubierto un determinado dispositivo, utilice consultas similares a estos ejemplos para realizar búsquedas en la totalidad del flujo de datos de descubrimiento.

Ejemplo: Identificación de si un dispositivo está presente en la base de datos workingEntities

El siguiente ejemplo de consulta determina si el dispositivo está presente en la base de datos workingEntities.

```
select * from workingEntities.finalEntity
where m_UniqueAddress ='10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Ejemplo: Identificación de si el agente AssocAddress ha devuelto un dispositivo

Si el dispositivo no está presente en la base de datos workingEntities, utilice la siguiente consulta de ejemplo para determinar si el agente AssocAddress ha devuelto el dispositivo.

```
select * from AssocAddress.returns
where m_UniqueAddress = '10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Ejemplo: Identificación de si el agente de detalles ha devuelto un dispositivo

Si el agente AssocAddress no ha devuelto el dispositivo, utilice la siguiente consulta de ejemplo para determinar si el agente de detalles ha devuelto el dispositivo.

```
select * from Details.returns
where m_UniqueAddress = '10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Ejemplo: Identificación de si un dispositivo se ha enviado al agente de detalles

Si el agente de detalles no ha devuelto el dispositivo, puede comprobar si el dispositivo se ha enviado al agente de detalles realizando una consulta a la tabla `Details.despatch`, como se muestra a continuación. Este resultado indica que el dispositivo se ha enviado al agente de detalles, pero no se ha procesado todavía.

```
select * from Details.despatch
where m_UniqueAddress='10.10.63.239';
go
.
{
                m_UniqueAddress='10.10.63.239';
}
( 1 record(s) : Transaction complete )
```

Ejemplo: Identificación de si los buscadores han descubierto un dispositivo

Si el dispositivo no está en la tabla `Details.despatch`, puede realizar una consulta a la base de datos `finders`, como se muestra a continuación. Este resultado muestra que el dispositivo ha sido descubierto por los buscadores.

```
select * from finders.processing
where m_UniqueAddress='10.10.63.239';
go
.
{
                m_UniqueAddress='10.10.63.239';
}
( 1 record(s) : Transaction complete )

select * from finders.returns
where m_UniqueAddress='10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Ejemplo de consultas de descubrimiento de recopilador

Puede utilizar consultas similares a estos ejemplos para supervisar los dispositivos descubiertos utilizando los recopiladores.

Ejemplo: Determinación de la direccionalidad de las conexiones entre los dispositivos de capa 1 descubiertos por los recopiladores

El ejemplo siguiente muestra cómo comprobar que el recopilador ha recuperado la direccionalidad de las conexiones entre los dispositivos. Los valores permitidos para la direccionalidad de las conexiones son los siguientes:

- 0 para bidireccional (enlace de dos direcciones)
- 1 para unidireccional (enlace de una dirección)

```
select * from CollectorLayer1.returns;
go
....
{
                m_UniqueAddress='10.1.1.18';
                m_Name='OpticalNE1';
                m_ManagerId='localhost:8081_1';
                m_HaveAccess=1;
                m_Protocol=1;
                m_UpdAgent='CollectorLayer1';
                m_LocalNbr={
                        m_InterfaceId='STS 1';
                        m_LocalNbrName='OpticalNE1';
                };
                m_RemoteNbr={
                        m_RemoteNbrName='OpticalNE2';
                        m_InterfaceId='PTP 1';
                        m_Unidirectional=1;
```

```
                };
        }

        {
                m_UniqueAddress='10.1.1.20';
                m_Name='OpticalNE3';
                m_ManagerId='localhost:8081_1';
                m_HaveAccess=1;
                m_Protocol=1;
                m_UpdAgent='CollectorLayer1';
                m_LocalNbr={
                        m_InterfaceId='STS 2';
                        m_LocalNbrName='OpticalNE3';
                };
                m_RemoteNbr={
                        m_RemoteNbrName='OpticalNE1';
                        m_Unidirectional=1;
                };
        }
```

Este fragmento de resultado muestra dos dispositivos.

Dispositivo 10.1.1.18

Este dispositivo tiene un vecino local denominado OpticalNE1 y un vecino remoto denominado OpticalNE2.

El dispositivo 10.1.1.18 tiene un enlace unidireccional a su vecino remoto OpticalNE2; es decir, un enlace unidireccional en la dirección 10.1.1.18 –> OpticalNE2.

Dispositivo 10.1.1.20

Este dispositivo tiene un vecino local denominado OpticalNE3 y un vecino remoto denominado OpticalNE1.

El dispositivo 10.1.1.20 tiene un enlace unidireccional a su vecino remoto OpticalNE1; es decir, un enlace unidireccional en la dirección 10.1.1.20 –> OpticalNE1.

Capítulo 14. Clasificación de dispositivos de red

Al finalizar el descubrimiento, Network Manager clasificará automáticamente todos los dispositivos de red descubiertos según una jerarquía de clases de dispositivos predefinida. Puede cambiar la forma en que los dispositivos de red se clasifican.

Cambio de la jerarquía de clases de dispositivo

Modifique la jerarquía de clase de dispositivo para cambiar la forma en que se clasifican los dispositivos de red. Una situación común que requiere un cambio en la jerarquía de clases es cuando el proceso de descubrimiento identifica un dispositivo sin clasificar, es decir, un dispositivo que no está definido en la jerarquía de clases.

Acerca de esta tarea

Después de un descubrimiento, puede comprobar si hay dispositivos sin clasificar ejecutando los siguientes informes:

- Dispositivos con informes de ID de objeto SNMP sin clasificar
- Dispositivos con informes de ID de objeto SNMP desconocido

Lista de las clases de dispositivo existentes

Antes de modificar las definiciones de AOC y volver a instanciar la topología, haga una lista de las clases de dispositivos que están actualmente en uso.

Acerca de esta tarea

Haga una lista de las clases de dispositivo existente consultando a las bases de datos de ncp_model. La consulta devuelve los nombres de las clases en las que se han instanciado dispositivos en la topología actual. Incluya su nombre de dominio y nombre de usuario donde se especifique NCOMS y admin.

Procedimiento

1. Inicie sesión en el proveedor de servicios OQL con el siguiente mandato:

   ```
   ncp_oql -domain NCOMS -username admin -service ncim
   ```

   También puede emitir esta consulta utilizando la página de acceso a la base de datos de gestión.
2. Especifique la contraseña pertinente cuando se le solicite.
3. Escriba la siguiente consulta:

   ```
   select * from entityClass;

   go
   ```

   La siguiente tabla muestra un ejemplo de la salida de esta consulta:

Tabla 50. Resultados de la consulta

Identificador de clase	Nombre de clase	Identificador de superclase	Tipo de clase	Nombre de gestor
1	Núcleo		Núcleo	PrecisionIP
2	EndNode	1	EndNode	PrecisionIP
1815493792	Brother	2	PhysicalHost	PrecisionIP
1899974822	BrotherPrinter	1815493792	Printer	PrecisionIP

Tabla 50. Resultados de la consulta (continuación)

Identificador de clase	Nombre de clase	Identificador de superclase	Tipo de clase	Nombre de gestor
1367768986	HPOfficePro85xx	2	Printer	PrecisionIP
200	PhysicalHost	2	EndNode	PrecisionIP
163	AIX	200	Direccionador	PrecisionIP
3	HPPrinter	200	EndNode	PrecisionIP
202	HypervisorHost	200	HypervisorHost	PrecisionIP
209	PowerHyperHost	202	HypervisorHost	PrecisionIP
210	VMWareHyperHost	202	HypervisorHost	PrecisionIP
4	Linux	200	EndNode	PrecisionIP
117	NoSNMPAccess	200	EndNode	PrecisionIP
211	PowerVMControl	200	EndNode	PrecisionIP
129	Dom	200	EndNode	PrecisionIP
134	Windows	200	EndNode	PrecisionIP
161	zOS	200	EndNode	PrecisionIP
201	VirtualHost	2	VirtualMachine	PrecisionIP
207	VirtualAIXHost	201	VirtualMachine	PrecisionIP
206	VirtualLinuxHost	201	VirtualMachine	PrecisionIP
205	VirtualSolarisHost	201	VirtualMachine	PrecisionIP
204	VirtualWindowsHost	201	VirtualMachine	PrecisionIP
138	InferredDevice	1	NetworkDevice	PrecisionIP
85	InferredCE	138	Direccionador	PrecisionIP
86	InferredHub	138	Conmutador	PrecisionIP

Creación y edición de archivos de AOC

Cree y edite archivos de AOC para clasificar dispositivos no clasificados o para cambiar la jerarquía de clases de la topología.

Acerca de esta tarea

Si el proceso de descubrimiento ha identificado un dispositivo sin clasificar, puede clasificar el dispositivo mediante la creación de un nuevo archivo de AOC que sea específico de la clase de dispositivo a la que pertenece el dispositivo.

Puede editar los archivos de AOC de dos maneras; actualice las bases de datos **ncp_class** o modifique las definiciones de archivos de AOC:

- Si desea editar las definiciones de AOC actuales actualizando la base de datos **ncp_class** directamente, utilice **Acceso a la base de datos de gestión** o el proveedor de servicios OQL.
- Si desea modificar las definiciones de archivos de AOC, siga estos pasos.

Procedimiento

1. Vaya al directorio NCHOME/precision/aoc.
2. Realice una copia de seguridad de los archivos que desea editar.
3. Cree un archivo de texto o edite un archivo de AOC existente con un editor de texto.

   Restricción: Solo se pueden utilizar caracteres alfanuméricos y el carácter de guión bajo (_) para nombres de archivo AOC. Todos los demás caracteres, como el guión (-), están prohibidos.
4. Consulte la sintaxis AOC y la estructura de los archivos de clase de objeto *activo* en la *Referencia de IBM Tivoli Network Manager* para construir o editar el archivo AOC. Considere la posibilidad de adaptar un archivo AOC existente para un tipo de dispositivo similar.
5. Para aplicar el AOC a un tipo concreto de dispositivo, debe editar la regla de instanciación en el archivo AOC. Utilice uno de los siguientes métodos para restringir el AOC al tipo de dispositivo elegido:
   - Si el tipo de dispositivo se puede identificar de forma única mediante EntiTiOid, utilice EntitYoID en la regla de instanciación. La mayoría de los archivos AOC predeterminados utilizan este método.
   - Si el tipo de dispositivo se puede identificar de forma única mediante cualquiera de los siguientes campos de la tabla de base de datos workingEntities.finalEntity, utilice su alias en la regla de instanciación.

     Tabla 51. Mapeos de tablas de base de datos, workingEntities.finalEntity

workingEntities.finalEntity	**Alias**
m_Name	EntityName
m_ObjectId	EntityOID
m_HaveAccess	IsActive
m_Description	Descripción
m_EntityType	EntityType

     Por ejemplo, el archivo Tellabs63xx.aoc utiliza el alias Description para hacer referencia al campo m_Description: instantiate_rule = "Description = 'Tellabs 6340_OLD'.
   - Si el tipo de dispositivo puede identificarse de forma exclusiva utilizando un campo diferente de la tabla de base de datos workingEntities.finalEntity, especifique el nombre del campo. Por ejemplo, el archivo VirtualHost.aoc utiliza el campo ExtraInfo->m_IsVirtualMachine en la tabla de base de datos workingEntities.finalEntity: instantiate_rule = "ExtraInfo->m_IsVirtualMachine = 1".
6. Si ha creado un archivo de AOC, añada una inserción a la tabla de base de datos class.classIds del archivo de configuración ClassSchema.cfg.
7. Edite las opciones de inicio del proceso **ncp_class** y establezca la opción -read_aocs_from para garantizar que se leen los archivos de AOC nuevos o modificados.
8. Reinicie el proceso **ncp_class** después de cambiar los archivos AOC. Después de reiniciar y ejecutar **ncp_class**, reinicie el proceso **ncp_disco**.
9. Asegúrese de que una nueva versión específica de dominio de cualquier archivo de AOC esté presente en el directorio NCHOME/precision/aoc.
10. Realice copias de seguridad y elimine los archivos de caché de clases en el directorio NCHOME/var/precision.

    Por ejemplo, elimine los siguientes archivos de caché:

    ```
    Class.Cache.class.activeClasses.NCOMS
    Class.Cache.class.staticClasses.NCOMS
    ```
11. Ejecute un descubrimiento completo y compruebe que los resultados coinciden con los cambios que ha realizado.

Aplicación de cambios de AOC a la topología y a los informes

Después de actualizar las definiciones AOC y pasar los cambios a **ncp_class**, puede aplicar estos cambios a la tipología esperando a que finalice el siguiente descubrimiento o reiniciando el descubrimiento en el momento en que se pase la topología de ncp_disco a ncp_model.

Acerca de esta tarea

Cuando finaliza el siguiente descubrimiento completo, los cambios de AOC que haya realizado se aplicarán de forma automática a la siguiente topología de red.

Si no desea esperar al siguiente descubrimiento completo, utilice el agrupador adecuado para reiniciar el descubrimiento en el punto necesario. Para volver a instanciar el modelo de contención, debe iniciar el agrupador que envía la topología desde **ncp_disco** a **ncp_model**.

Procedimiento

1. Inicie sesión en el proveedor de servicios OQL o acceda a **Acceso a la base de datos de gestión**.
2. Ejecute la siguiente consulta a la tabla disco.status para configurar que el proceso **ncp_disco** se encuentra en la modalidad de redescubrimiento.
   `select * from disco.status;`

   A continuación, se muestra un ejemplo de respuesta.

   ```
   m_DiscoveryMode=1;
   m_Phase=1;
   m_BlackoutState=0;
   m_CycleCount=0;
   m_ProcessingNeeded=0;
   m_FullDiscovery=0;
   ```

   A partir de los resultados devueltos por la consulta, podrá comprobar que **ncp_disco** se encuentra actualmente en la modalidad de redescubrimiento, es decir, m_DiscoveryMode=1.
3. Inicie el agrupador SendTopologyToModel.

   SendTopologyToModel envía la topología desde ncp_disco a ncp_model.

   a) Asegúrese de que se encuentra en el proveedor de servicios OQL o **Acceso a la base de datos de gestión**.

   b) Para insertar el agrupador en la tabla stitchers.actions, emita el siguiente mandato:

   ```
   insert into stitchers.actions
   ( m_Name )
   values
   ( 'SendTopologyToModel' );
   ```

   Una vez aceptada la inserción OQL, se invoca al agrupador y la topología de red se envía a ncp_model. Cuando se envía la topología, se instancia de acuerdo con la jerarquía de AOC modificada.
4. A fin de garantizar que los dispositivos recientemente clasificados se eliminen de Dispositivos con informes de ID de objeto SNMP sin clasificar y Dispositivos con informes de ID de objeto SNMP desconocido, lleve a cabo los siguientes pasos:

   a) Aclare con exactitud los valores sysObjectId nuevos se correlacionarán con los archivos de AOC nuevos o editados.
   Por ejemplo, los archivos de AOC originales se correlacionan con los siguientes valores sysObjectId:

   - 1.2.3.4
   - 1.5.6.*

   A continuación, se añaden dos nuevos valores sysObjectId al sistema: 1.9.8 y 1.5.6.7 En el archivo de AOC, el valor 1.5.6.7 de sysObjectId está comprendido en la correlación 1.5.6.*. Sin embargo, el archivo de AOC debe actualizarse para añadir el valor 1.9.8 del sysObjectId.

b) Aclare qué archivos de AOC se correlacionarán mediante la tabla de correlaciones de la base de datos de topología de NCIM.

El Dispositivos con informes de ID de objeto SNMP sin clasificar y el Dispositivos con informes de ID de objeto SNMP desconocido utilizan la tabla de correlaciones para determinar qué datos se mostrarán en los informes. Esta tabla no se actualiza de forma automática al editar los archivos de AOC y reiniciar el gestor de topología, `ncp_class`, y, por lo tanto, estos informes continúan mostrando valores sysObjectId como sin clasificar y desconocidos. Las correlaciones de la tabla de correlaciones son también más específicas que las de los archivos de AOC.

Por ejemplo, la tabla de base de datos de topología de NCIM puede incluir los siguientes datos:

Tabla 52. Ejemplo de datos

mappingGroup	mappingKey	mappingValue	Descripción
sysObjectId	1.2.3.4	Dispositivo de Tipo A	Descripción del dispositivo de Tipo A
sysObjectId	1.5.6.1	Dispositivo de Tipo B	Descripción del dispositivo de Tipo B
sysObjectId	1.5.6.2	Dispositivo de Tipo C	Descripción del dispositivo de Tipo C

En el archivo de AOC, solo es necesario añadir el valor 1.9.8 de sysObjectId porque la correlación genérica 1.5.6.* comprendía el valor 1.5.6.7 del sysObjectId nuevo. Sin embargo, en la tabla de correlaciones de base de datos de topología de NCIM, es necesario añadir los dos valores 1.9.8 y 1.5.6.7 de sysObjectId.

c) En la línea de mandatos, actualice la tabla de correlaciones de bases de datos de topología de NICM con registros pertinentes para los valores de sysObjectId nuevos.
Por ejemplo, para añadir registros para los dos valores nuevos 1.9.8 y 1.5.6.7 de sysObjectId, emita las siguientes sentencias de inserción SQL:

```
insert into mappings (mappingGroup, mappingKey, mappingValue) values
('sysObjectId', '1.9.8', 'device_type');
insert into mappings (mappingGroup, mappingKey, mappingValue) values
('sysObjectId', '1.5.6.7', 'device_type');
```

Donde *device_type* es el tipo de dispositivo con el que se debe correlacionar el valor sysObjectID.

Para obtener mas información sobre la tabla de correlaciones de bases de datos de topología de NCIM, consulte *Referencia de IBM Tivoli Network Manager*.

Resultados

Una vez aplicados los cambios de AOC a la topología, bien automáticamente esperando al siguiente descubrimiento, o manualmente realizando los pasos indicados en este tema, observará que se aplican los siguientes cambios a la visualización y el sondeo de red.

- Cuando defina la nueva política de sondeo, las clases nuevas que defina se mostrarán en el separador Clases de **Editor de políticas de sondeo**.
- Al visualizar la red mediante las vistas de red, el árbol de vistas de red ahora mostrará las clases definidas en la jerarquía de clases modificada.
- Si ha actualizado la tabla de correlaciones de bases de datos de topología de NICM como se ha descrito, el Dispositivos con informes de ID de objeto SNMP sin clasificar y el Dispositivos con informes de ID de objeto SNMP desconocido ya no devolverán ningún dispositivo.

Ejemplos de archivos AOC

Utilice los ejemplos de archivos AOC para comprender cómo Network Manager asigna dispositivos descubiertos a las clases de dispositivo en la jerarquía de clases.

Clase EndNode

Utilice este archivo AOC de clase EndNode de ejemplo para comprender cómo asigna Network Manager dispositivos descubiertos a la clase EndNode.

Ejemplo

El siguiente fragmento de archivo AOC de ejemplo asigna dispositivos a la clase EndNode mediante el filtro definido en la cláusula instantiate_rule.

```
//************************************************************
//
// File : EndNode.aoc
//
//************************************************************
active object 'EndNode'
{
super_class = 'Core';
instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.2021\.' OR
EntityOID = '1.3.6.1.4.1.2021' OR
EntityOID = '1.3.6.1.4.1.1575' OR
EntityOID like '1 \.3\.6\.1\.4\.1\.11\.2\.3\.9\.' OR
EntityOID = '1.3.6.1.4.1.11.2.3.9' OR
(EntityType = 1 AND EntityOID IS NULL)
OR
...
OR
(
EntityOID = '1.3.6.1.4.1.1977'
)
OR
(
EntityOID like '1\.3\.6\.1\.4\.1\.2136\.'
)
OR
...
```

Para la clase EndNode la instantiate_rule es muy larga. Se compone de varias líneas que comparan el EntityOID (el sysObjectID del dispositivo) con distintos valores, unidos por un operador OR. Hay diferentes versiones de la comparación OR:

EntityOID = '1.3.6.1.4.1.2021'
: Este filtro busca una coincidencia exacta del EntityOID con el valor 1.3.6.1.4.1.2021. Si la coincidencia no es exacta, la comparación falla y el dispositivo no se asigna a la clase EndNode.

EntityOID like '1\.3\.6\.1\.4\.1\.11\.2\.3\.9\.'
: Este filtro busca una coincidencia similar al valor 1\.3\.6\.1\.4\.1\.11\.2\.3\.9\. El signo \. es necesario para garantizar que el . (punto) se empareje. Asimismo, observe que el valor termina en \. Esto permite emparejar los OID que comienzan con el valor especificado pero tienen valores adicionales detrás del último . (punto) especificado.

Clase NetworkDevice

Utilice este archivo AOC de clase NetworkDevice de ejemplo para comprender cómo asigna Network Manager dispositivos descubiertos a la clase NetworkDevice.

Ejemplo

El siguiente fragmento de archivo AOC de ejemplo asigna dispositivos a la clase NetworkDevice mediante el filtro definido en la cláusula instantiate_rule.

```
//************************************************************
//
// File : NetworkDevice.aoc
//
//************************************************************
active object 'NetworkDevice'
{
super_class = 'Core';
instantiate_rule = 'EntityType = 1 OR // Chassis
EntityType = 2 OR // Interface
```

```
EntityType = 3 OR // LogicalInterface
EntityType = 5 OR // Card
EntityType = 6 OR // PSU
EntityType = 8 OR // Module
EntityType = 0';
...
```

Con la clase NetworkDevice, instantiate_rule intenta emparejar tipos de dispositivo. Los siguientes ejemplos son los filtros que se utilizan en la instantiate_rule.

EntityType = 1
Empareja todas las entidades descubiertas que son dispositivos de chasis. Los dispositivos de chasis tienen el campo entityType establecido en el valor 1 en la tabla entityData de la base de datos de topología de NCIM.

EntityType = 2
Empareja todas las entidades descubiertas que son puertos o interfaces. Los puertos y las interfaces tienen el campo entityType establecido en el valor 2 en la tabla entityData de la base de datos de topología de NCIM.

EntityType = 3
Empareja todas las entidades descubiertas que son interfaces lógicas. Las interfaces lógicas tienen el campo entityType establecido en el valor 3 en la tabla entityData de la base de datos de topología de NCIM.

EntityType = 5
Empareja todas las entidades descubiertas que son tarjetas. Las tarjetas tienen el campo entityType establecido en el valor 5 en la tabla entityData de la base de datos de topología de NCIM.

EntityType = 6
Empareja todas las entidades descubiertas que son unidades de fuente de alimentación (PSU). Las PSU tienen el campo entityType establecido en el valor 6 en la tabla entityData de la base de datos de topología de NCIM.

EntityType = 8
Empareja todas las entidades descubiertas que son módulos. Los módulos tienen el campo entityType establecido en el valor 8 en la tabla entityData de la base de datos de topología de NCIM.

AOC específico de clase de dispositivo

Utilice este archivo AOC de ejemplo para comprender cómoNetwork Manager asigna dispositivos descubiertos a la clase de dispositivo en un nivel inferior de la jerarquía de clases.

Ejemplo

El siguiente fragmento de archivo AOC de muestra asigna dispositivos a la clase EWindowsNetHarmoni utilizando el filtro definido en la cláusula instantiate_rule. Se trata de un dispositivo EndNode.

```
//************************************************************
//
// File : EWindowsNetHarmoni.aoc
//
//************************************************************
active object 'EWindowsNetHarmoni'
{
super_class ='EndNode';

instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.1977\.1\.6\.1279\.'";
...
```

En el caso de la clase EWindowsNetHarmoni, en el archivo AOC se definen los siguientes parámetros. El parámetro instantiate_rule es largo. Se compone de varias líneas que comparan el EntityOID (el sysObjectID del dispositivo) con distintos valores, unidos por un operador OR. Hay diferentes versiones de la comparación OR:

super_class ='EndNode'
Este parámetro establece el dispositivo como perteneciente a la clase EndNode. La clase EWindowsNetHarmoni hereda todos los atributos de la clase EndNode.

instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.1977\.1\.6\.1279\.'"
Este filtro busca una coincidencia con el valor 1\.3\.6\.1\.4\.1\.11\.2\.3\.9\. El signo \. es necesario para garantizar que el . (punto) se empareje. Asimismo, observe que el valor termina en \. Esto permite emparejar los OID que comienzan con el valor especificado pero tienen valores adicionales detrás del último . (punto) especificado.

Tipos de entidades

La tabla entityType contiene todos los tipos de entidades que están disponibles en la base de datos de topología de NCIM.

La tabla siguiente lista los tipos de entidades disponibles en la base de datos de topología.

Tabla 53. Entidades Network Manager

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
0	Desconocido	Elemento		
1	Chasis	Elemento	physicalChassis	Dispositivo de nodo principal.
2	Interfaz	Elemento	networkInterface	Las interfaces con entityType 2 pueden descubrirse y sondearse.
3	Interfaz lógica	Elemento	networkInterface	Las interfaces con entityType 3 se infieren, pero no están accesibles directamente. Las interfaces IP virtuales HSRP (Hot Standby Routing Protocol) son un ejemplo de interfaces lógicas.
4	VLAN local	Elemento	localVlan	Puerto VLAN en el dispositivo de nodo principal.
5	Módulo	Elemento	physicalCard	Tarjeta dentro de un conmutador o direccionador. El término *módulo* se utiliza para evitar confusión con el término *tarjeta* que se utiliza en las redes de capa 1.
6	PSU	Elemento	physicalPowerSupply	Unidad de fuente de alimentación dentro de un dispositivo de nodo principal.
7	Recopilación lógica	Recopilación		Ejemplos de colecciones lógicas incluyen VPN de MPLS, VLAN globales y subredes. NCIM también puede modelar áreas OSPF.
8	Tarjeta hija	Elemento		Hija de una tarjeta de red.
9	Ventilador	Elemento	physicalFan	Componente de ventilador dentro de un dispositivo de nodo principal.
10	Placa posterior	Elemento	physicalBackplane	Componente de placa posterior dentro del dispositivo de nodo principal. Las placas posteriores normalmente contienen entidades de ranura.
11	Ranura	Elemento	physicalSlot	Componente de ranura dentro del dispositivo de nodo principal. Las ranuras normalmente contienen entidades de módulo.
12	Sensor	Elemento	physicalSensor	Componente de sensor dentro del dispositivo de nodo principal.

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
13	Direccionador virtual	Elemento	virtualRouter	Representa una instancia de un direccionador virtual dentro de un dispositivo de chasis.
14	CPU	Elemento	cpu	Representa unidades centrales de proceso (CPU).
15	Subred	Recopilación	subred	Colección lógica que lista la dirección IP en una subred de clase A, B o C.
16	VLAN global	Recopilación	globalVlan	Colección de entidades VLAN entre dispositivos de varios chasis que se combina para formar una red virtual.
17	VPN	Recopilación	networkVpn	Colección lógica de dirección IP recopilada dentro de una VPN.
18	Grupo de HSRP	Recopilación	hsrpGroup	Representa una colección de grupo lógica de Hot Standby Routing Protocol (HSRP). El Cisco HRSP implementa un direccionador virtual con sus propias direcciones IP y MAC. Este direccionador virtual forma un grupo HSRP que consta de varias interfaces reales, sólo una de las cuales está activa en un momento determinado. La interfaz activa reenvía trafico IP que se envía al direccionador virtual y otras interfaces del grupo listas para activarse si la interfaz activa falla.
19	Pila	Elemento		Colección de dispositivos de chasis definidas por el MIB de entidad.
20	VRF	Elemento	vpnRouteForwarding	Representa un direccionamiento VPN y una tabla de reenvío.
21	Dominio de direccionamiento de OSPF	Recopilación	ospfRoutingDomain	Representa un dominio de direccionamiento de OSPF.
22	Servicio OSPF	Servicio	ospfService	Representa un servicio OSPF ejecutándose en un dispositivo.
23	Área OSPF	Recopilación	ospfArea	Representa un área de OSPF.
24	Dominio VTP	Recopilación	vtpDomain	Representa un dominio de protocolo de truncación de VLAN.
25	Otros	Elemento	physicalOther	Almacena atributos de un componente cuyo tipo de entidad que el descubrimiento no fue capaz de determinar. Esto ocurre si se conoce la clase de entidad física, pero no coincide con ninguno de los valores soportados.
26	Servicio BGP	Servicio	bgpService	Representa un servicio de BGP.
27	AS de BGP	Recopilación	bgpAutonomousSystem	Representa un sistema autónomo de BGP.
28	Ruta de BGP	Atributo	bgpRouteAttribute	Representa una ruta de BGP.

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
29	Clúster de BGP	Recopilación	bgpCluster	Representa un clúster de BGP.
30	red BGP	Servicio	bgpNetwork	Representa una red de BGP.
31	Servicios de ISIS	Recopilación		Representa un servicio de ISIS.
32	Nivel de ISIS	Elemento		Representa un nivel de ISIS.
33	Pseudo-nodo de OSPF	Elemento		Representa un pseudo nodo de OSPF.
34	Servicio de ITNM	Recopilación	itnmService	El tipo base para otros servicios como el servicio de ISIS.
35	Servicio MPLS TE	Servicio	mplsTEService	Representa un servicio de Ingeniería de tráfico de Multi Protocol Label Switching (TE de MPLS)
36	Túnel MPLS TE	Elemento	mplsTETunnel	Representa un túnel TE de MPLS
37	Recurso MPLS TE	Elemento	mplsTETunnel Resource	Representa un recurso TE de MPLS
38	LSP de MPLS	Elemento	mplsLSP	Representa una vía de acceso de conmutador de etiqueta (LSP) de MPLS
40	Conexión IP	Elemento	ipConnection	Representa una conexión utilizando TCP/IP.
41	Servicio PIM	Servicio	pimService	Representa un servicio de Protocol Independent Multicast (PIM).
42	Red PIM	Recopilación	pimNetwork	Representa una red PIM.
43	Servicio IPMRoute	Servicio	ipMRouteService	Representa un servicio de direccionamiento de multidifusión IP.
44	Corriente en sentido ascendente de IPMRoute	Elemento	ipMRouteUpstream	Almacena una estadística de ruta en sentido ascendente (RPF) para cada dispositivo o Multicast Distribution Tree (MDT).
45	Corriente en sentido descendente de IPMRoute	Elemento		Almacena una estadística de ruta en sentido descendente por dispositivo o MDT.
46	ipMRouteMdt	Recopilación	ipMRouteMdt	Almacena las entidades de colección representando los MDT para cada grupo u origen de multidifusión.
47	IPMRouteSource	Elemento	ipMRouteSource	Representa orígenes de multidifusión, como figuran en MDT.
48	ipMRouteGroup	Elemento	ipMRouteGroup	Representan grupos de multidifusión, como figuran en MDT.

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
49	Vía de acceso IP	Recopilación	ipPath	Representa una vía de acceso de la red entre los dispositivos IP.
50	Punto final de IP	Punto final de protocolo	ipEndPoint	Representa un punto final de IP lógico que se implementa por una interfaz física.
51	Punto final de conexión troncal de VLAN	Punto final de protocolo	vlanTrunkEndPoint	Representa un punto final de conexión troncal de VLAN lógico que se implementa a través de una interfaz física.
52	Punto final de frame relay	Punto final de protocolo	frameRelay EndPoint	Representa un Punto final de frame relay lógico que se implementa por una interfaz gráfica.
53	Punto final de OSPF	Punto final de protocolo	ospfEndPoint	Representa un punto final de OSPF lógico que se implementa por una interfaz física.
54	Punto final de ATM	Punto final de protocolo	atmEndPoint	Representa un punto final de ATM que se implementa por una interfaz física.
55	Punto final de VPWS	Punto final de protocolo	vpwsEndPoint	Representa un punto final de VPWS lógico que se implementa por una interfaz física.
56	Punto final de BGP	Punto final de protocolo	bgpEndPoint	Representa un punto final de BGP que se implementa por una interfaz física.
57	Punto final de ISIS	Punto final de protocolo		Representa un punto final de ISIS lógico que se implementa por una interfaz física.
58	Punto final de túnel MPLS	Punto final de protocolo	mplsTETunnelEnd Point	Representa un punto final de túnel MPLS lógico que se implementa por una interfaz física.
59	Punto final de TCP/UDP	Punto final de protocolo		Representa un punto final de TCP/UDP que se implementa por una interfaz física.
60	Punto final de PIM	Punto final de protocolo	pimEndpoint	Representa los puntos finales de Protocol Independent Multicast (PIM) descubiertos en la red y sus atributos asociados.

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
61	Punto final de IPMRoute	Punto final de protocolo	ipMRouteEndPoint	Almacena información en los puntos finales del protocolo de direccionamiento de difusión IP.
62	Punto final de IGMP	Punto final de protocolo	igmpEndPoint	Almacena información en los puntos finales del de protocolo de pertenencia a grupo de Internet (IGMP) .
63	Punto final de entidad de servicio de red	Punto final de protocolo	networkService Entity EndPoint	Permite modelar las relaciones relacionadas con la gestión de enlaces de frame relay.
67	Punto final de LAG	Punto final de protocolo	lagEndPoint	Representa un punto final de LAG (Link Aggregation Group) lógico implementado por una interfaz física.
68	Punto final de análisis	Punto final de protocolo	probeEndPoint	Fix Pack 3 Representa el punto final de origen o destino de una operación de análisis, implementado por una interfaz física.
70	Topología	Topología		Agrupación de conexiones que pertenecen a una topología.
71	Topología de capa 1	Topología		Agrupación de conexiones que pertenecen a una topología Capa 1.
72	Topología de capa 2	Topología		Agrupación de conexiones que pertenecen a una topología Capa 2.
73	Topología híbrida de capa 3	Topología		Agrupación de conexiones que pertenecen a una topología híbrida Capa 3.
74	Topología convergente (Capa 1 - Capa 3)	Topología		Basada en los datos disponibles en NCIM, agrupa las conexiones de la capa de datos más baja para la que hay datos disponibles.
75	Topología de MPLS TE	Topología		Agrupación de conexiones que pertenece a una topología TE de MPLS.
77	Topología de pseudocable	Topología		Agrupación de conexiones que pertenecen a una topología de pseudocable.
78	Topología OSPF	Topología		Representa una topología de OSPF.
79	Topología BGP	Topología		Representa a una topología de BGP.
80	Topología de vía de acceso IP	Topología	ipPath	Representa a una vía de acceso de IP.
81	Topología PIM	Topología		Representa topologías de PIM.

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
82	Topología de VLAN local	Topología		Representa topologías de VLAN locales.
83	Topología IPMRoute	Topología		Representa una topología de Direccionamiento de multidifusión IP.
84	Topología de pseudocable de VPLS	Topología		Representa una topología de pseudocable VPLS.
85	Topología de virtualización	Topología		Representa a una topología de virtualización.
86	Topología de microondas	Topología		Representa a una topología de microondas.
87	Topología de RAN	Topología		Representa a una topología de red de acceso mediante radio.
90	Nivel de control LTE	Topología		Representa los dispositivos y conectividad que constituyen el nivel de control LTE.
91	Nivel de usuario LTE	Topología		Representa los dispositivos y conectividad que constituyen el nivel de usuario LTE.
92	Topología de análisis	Topología		Representa la conectividad de origen/destino del análisis.
110	Recopilación genérica	Recopilación	genericCollection	Colección que no es de ningún otro tipo.
111	Ubicación geográfica	Elemento	geographicLocation	Representa una ubicación geográfica.
112	Región geográfica	Recopilación	geographicRegion	Representa una región geográfica.
113	Puertos de VLAN	Recopilación	vlanCollection	Representa una colección de puertos en una determinada VLAN con nombre o, si no se proporciona ningún nombre, en un identificador de VLAN específico.
120	Servicio IGMP	Servicio	igmpService	Representa un servicio Internet Group Management Protocol (IGMP).
121	Grupos IGMP	Recopilación	igmpGroup	Almacena colecciones de grupo de multidifusión para el que hay asociados puntos finales del protocolo de pertenencia a grupo de Internet (IGMP) en la tabla igmpEndPoint.
122	VSI (Virtual Switch Instance)	Elemento	virtualSwitch Instance	Representa una instancia de conmutador (VSI) configurada en un dispositivo de proveedor (PE) asociado con una instancia de red privada virtual (VPN) del servicio de LAN privada virtual (VPLS).
123	Centro de datos	Elemento		Representa un centro de datos.

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
124	Clúster virtual	Recopilación	virtualCluster	Representa un clúster de máquinas virtuales.
125	Servicio de gestión virtual	Servicio	virtualMgmtService	Representa un servicio de gestión virtual.
126	Hipervisor	Elemento	hypervisor	Representa un hipervisor.
127	Grupo de puertos	Recopilación	portGroup	Representa un grupo de puertos.
128	EMS System	Elemento	emsSystem	Representa un sistema EMS accedido por un recopilador.
130	RAN GSM Cell	Elemento	ranGSMCell	Representa una célula GSM.
131	RAN UTRAN Cell	Elemento	ranUtranCell	Representa una célula UTRAN.
132	RAN Sector	Elemento	ranSector	Representa un sector RAN.
133	RAN NodeB celular local	Elemento	ranNodeBLocalCell	Representa una célula local de NodeB.
134	Área de ubicación de RAN	Recopilación	ranLocationArea	Representa un área de ubicación de RAN.
135	Área de direccionamiento de RAN	Recopilación	ranRoutingArea	Representa un área de direccionamiento de RAN.
136	Core de paquete de RAN	Recopilación		Representa una entidad principal de conmutación de paquetes de RAN.
137	Core de circuito de RAN	Recopilación		Representa una entidad principal conmutada de circuito de RAN.
138	Core de radio de RAN	Recopilación	ranRadioCore	Representa una entidad principal de radio de RAN.
139	Transmisor/ receptor RAN	Recopilación	ranTransceiver	Representa un transmisor/receptor RAN.
150	Sector LTE	Elemento	eUtranSector	Representa un área geográfica de cobertura de radio y se implementa y obtiene soporte mediante equipo físico de radio. Un sector LTE implementa una o más celdas LTE.
151	Celda LTE	Elemento	eUtranCell	Representa un área geográfica de cobertura de radio y se implementa y obtiene soporte mediante equipo físico de radio, como torres, amplificadores y antenas.

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
152	Función MME	Elemento	mmeFunction	La entidad de gestión de movilidad (MME) es el elemento de control de señalización principal de la red troncal y es el nodo de control clave para permitir el acceso de equipo de usuario a la red troncal. El rol de la MME se implementa dentro de un nodo de hardware de red y está modelado mediante NCIM utilizando el tipo de entidad mmeFunction. Se pueden implementar varias instancias de mmeFunction dentro de un único nodo de hardware de red.
153	Área de rastreo	Recopilación	trackingArea	Representa un área de rastreo LTE.
154	Función SGW	Elemento	sgwFunction	La pasarela servidora (SGW) reside en el nivel de usuario donde reenvía y direcciona paquetes hacia y desde eNodeB y la pasarela de red de datos de paquete (PGW). El rol de la SGW se implementa dentro de un nodo de hardware de red y está modelado mediante NCIM utilizando el tipo de entidad sgwFunction. Se pueden implementar varias instancias de sgwFunction dentro de un único nodo de hardware de red.
155	Función PGW	Elemento	pgwFunction	La pasarela de red de datos de paquete (PGW) proporciona conectividad de nivel de usuario a las redes de datos de paquete. El rol de la PGW se implementa dentro de un nodo de hardware de red y está modelado mediante NCIM utilizando el tipo de entidad pgwFunction. Se pueden implementar varias instancias de pgwFunction dentro de un único nodo de hardware de red.
156	Función ENB	Elemento	enbFunction	El dispositivo eNodeB gestiona la comunicación de interfaz aérea de radio con usuarios de la red LTE. Cada dispositivo eNodeB controla una o más celdas, que son áreas geográficas de cobertura de radio. El rol de la eNodeB se implementa dentro de un nodo de hardware de red y está modelado mediante NCIM utilizando el tipo de entidad enbFunction. Se pueden implementar varias instancias de enbFunction dentro de un único nodo de hardware de red.
157	Agrupación LTE	Recopilación	ltePool	Mecanismo de modelado genérico para grupos de entidades LTE agrupadas, actualmente utilizado para modelar agrupaciones MME, agrupaciones PGW y agrupaciones SGW. Como ejemplo, para modelar una agrupación MME, la relación entre la entidad ltePool y las entidades mmeFunction asociadas se modela utilizando la tabla collects (recopilaciones).

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
158	PLMN	Elemento	plmn	Modela una red móvil terrestre pública (PLMN). Una PLMN es una red que proporciona servicios de telecomunicaciones móviles terrestres al público. Cada operador que proporciona servicios móviles tiene su propia PLMN.
159	Función HSS	Elemento	hssFunction	Modela el HSS (Home Subscriber Service) de LTE. El HSS gestiona las identidades de suscriptor, perfiles de servicio, autenticación, autorización y calidad de servicio (QoS), y actúa como el repositorio maestro para los perfiles de suscriptor, perfiles de dispositivo e información de estado.
160	Función PCRF	Elemento	pcrfFunction	Modela la PCRF (Policy and Charging Rules Function) de LTE. La PCRF gestiona la política y los cargos para los flujos de servicio ascendentes y descendentes y la QoS del portador EPS.
161	Función EIR	Elemento	eirFunction	Modela el EIR (Equipment Identity Register) de LTE. El EIR hace un seguimiento de dispositivos móviles a los que se debe supervisar o prohibir el uso de la red. Cuando un teléfono móvil ha sido robado, su identidad se añade a la lista negra de EIR y, como resultado, dicho teléfono no podrá conectarse nunca a la red de servicio. Normalmente, cada red tiene su propio EIR, que suele combinarse con el nodo HSS. Es posible que varios operadores compartan un EIR común, lo que permite que la información de la lista negra tenga una mayor y más sencilla disponibilidad.
163	Nivel de control LTE	Recopilación	controlPlane ViewCollection	Da soporte a las vistas de recopilación dinámicas en **Topología de red LTE** > **Nivel de control por área de rastreo** en las vistas de red. Cada instancia de esta entidad recopila los eNodeB del área de rastreo correspondiente, junto con los dispositivos a los que están conectados estos eNodeB en el nivel de control.
164	Nivel de usuario LTE	Recopilación	userPlane ViewCollection	Da soporte a las vistas de recopilación dinámicas en **Topología de red LTE** > **Nivel de usuario por área de rastreo** en las vistas de red. Cada instancia de esta entidad recopila los eNodeB del área de rastreo correspondiente, junto con los dispositivos a los que están conectados estos eNodeB en el nivel de usuario.
170	Enlace agregado	Recopilación	aggregatedLink	Representa un enlace de red entre LAG (Link Aggregation Groups)
171	Grupo de agregación de enlaces	Elemento	aggregationGroup	Representa un LAG (Link Aggregation Group).

Tabla 53. Entidades Network Manager (continuación)

Tipo de entidad	Nombre de tipo de entidad	Categoría	Tabla de NCIM	Descripción
190	Servicio de análisis	Servicio	probeService	Fix Pack 3 Representa el servicio que proporciona análisis de un dispositivo.
191	Analizador	Recopilación	Análisis	Fix Pack 3 Representa los análisis de red configurados y sus atributos.
192	Recopilación de análisis	Recopilación	probeCollection	Fix Pack 3 Proporciona un recurso de recopilación de análisis o colecciones de análisis.
200	LTE S1-U	Topología	entityData	Tipo de topología para la conectividad LTE S1-U.
201	LTE S5	Topología	entityData	Tipo de topología para la conectividad LTE S5.
202	LTE S8	Topología	entityData	Tipo de topología para la conectividad LTE S8.
203	LTE S1-MME	Topología	entityData	Tipo de topología para conectividad LTE S1-MME.
204	LTE S10	Topología	entityData	Tipo de topología para la conectividad LTE S10.
205	LTE S11	Topología	entityData	Tipo de topología para la conectividad LTE S11.
206	LTE SGi	Topología	entityData	Tipo de topología para la conectividad LTE SGi.
207	LTE Gx	Topología	entityData	Tipo de topología para la conectividad LTE Gx.
208	LTE S3	Topología	entityData	Tipo de topología para la conectividad LTE S3.
209	LTE S4	Topología	entityData	Tipo de topología para la conectividad LTE S4.
210	LTE S6a	Topología	entityData	Tipo de topología para la conectividad LTE S6a.
211	LTE S13	Topología	entityData	Tipo de topología para la conectividad LTE S13.
212	LTE X2	Topología	entityData	Tipo de topología para la conectividad LTE X2.

Capítulo 15. Cómo mantener la topología descubierta actualizada

Una vez haya finalizado un descubrimiento, puede guardar la topología descubierta actualizada planificando un descubrimiento, descubriendo dispositivos manualmente y eliminando dispositivos.

Planificación de descubrimientos

Después de que finalice un descubrimiento completo, puede planificar más descubrimientos insertando la hora, la fecha y el día en que deben ejecutarse en el archivo del agrupador `FullDiscovery.stch`.

Procedimiento

1. Realice una copia de seguridad del archivo `NCHOME/precision/disco/stitchers/FullDiscovery.stch`.
2. Cree instancias independientes del archivo `FullDiscovery.stch` para cada dominio de la red.

   Para crear una instancia específica de un dominio, inserte `.dominio` en el nombre del archivo.

   Por ejemplo, `FullDiscovery.NCOMS.stch`.

   Si no tiene archivos `FullDiscovery.stch` independientes para cada dominio, se descubren todos los dominios de la red.
3. Planifique el descubrimiento del primer dominio.

   En un archivo `FullDiscovery.dominio.stch`, elimine el comentario de una de las líneas de ActOnTimedTrigger. A continuación, modifíquela para que ejecute el descubrimiento a una hora determinada.

   Por ejemplo, para planificar el descubrimiento todos los días a las 11:00 PM, modifique la línea tal como se indica a continuación:

   ```
   ActOnTimedTrigger(( m_TimeOfDay ) values ( 2300 ) ; );
   ```
4. Repita los pasos del archivo `FullDiscovery.stch` para cada dominio de la red.

Ejemplos

- Para planificar un descubrimiento el sexto día de la semana desde el domingo (sábado) a las 11 PM:

  ```
  ActOnTimedTrigger(( m_DayOfWeek , m_TimeOfDay )
   values ( 6 , 2300 ) ; ) ;
  ```

  domingo = 0, lunes = 1, martes = 2, miércoles = 3, jueves = 4, viernes = 5, sábado = 6.
- Para planificar un descubrimiento en el día 13 de cada mes a las 2 PM:

  ```
  ActOnTimedTrigger(( m_DayOfMonth , m_TimeOfDay )
  values ( 13 , 1400 ) ; );
  ```
- Para planificar un descubrimiento en intervalos de 13 horas:

  ```
  ActOnTimedTrigger(( m_Interval ) values ( 13 ) ; );
  ```

Consulta del estado de descubrimiento de un dispositivo

En las GUI de topología puede ver información sobre un dispositivos, incluida la primera vez que fue descubierto, la última vez y la última vez que se arrancó.

Antes de empezar

Para realizar este procedimiento, debe encontrarse en **Vistas de red** o en la **Vista de saltos de red**, y el mapa de topología debe mostrar el dispositivo de interés.

Procedimiento

1. En el mapa de topología, seleccione con el botón derecho uno o varios dispositivos.
2. Seleccionar **Descubrimiento...** > **Mostrar una visión general del descubrimiento**.
3. La ventana **Visión general de descubrimiento** muestra la siguiente información:

IP de acceso

La dirección IP mediante la cual se ha descubierto y se supervisa esta entidad.

Nombre de clase

Clase de dispositivos a la que pertenece este dispositivo.

Actual

Fecha y hora actuales.

Nombre de entidad

Dirección IP, nombre DNS o nombre del sistema de este dispositivo. Por ejemplo, una dirección IP como 172.20.1.7, o un nombre DNS como company-abc.net.

Entidad creada

Fecha y hora en que se ha subido la entidad por primera vez a la base de datos de topología de NCIM.

Interfaz filtrada

Un distintivo que muestra si el dispositivo ha tenido un filtrado de interfaz aplicado o no. Si no puede ver toda la información que esperaba sobre el dispositivo, es posible que se haya filtrado la información. Puede hacer un recorrido SNMP del dispositivo utilizando el navegador de MIB con la opción de ignorar el filtrado.

Último descubrimiento

Fecha y hora a las que el agente Detalles accedió por última vez al dispositivo.

Última modificación

Fecha y hora a las que se reflejó en la base de datos de topología de NCIM el último cambio detectado en el dispositivo. Por ejemplo, si cambia el nombre de interfaz en el dispositivo, es la hora a la que se cargó ese cambio en NCIM.

Último arranque

Fecha y hora del último reinicio del dispositivo. Se calcula en función del valor de MIB sysUpTime obtenido del dispositivo; por lo tanto, **Último arranque** solo estará disponible si se ha recuperado el valor sysUpTime. Por ejemplo, para dispositivos sin acceso SNMP, el valor de **Último arranque** es NULL.

Descubrimiento manual de un dispositivo o subred

Puede descubrir manualmente dispositivos para que la topología de red en Network Manager coincida con la red.

Acerca de esta tarea

A veces tendrá que saber que uno o más dispositivos han cambiado su configuración y que quiere descubrirlos de nuevo independientemente de si el sistema ha detectado el cambio en las condiciones de excepción que los dispositivos han enviado.

Puede descubrir manualmente un dispositivo o subred de las siguientes maneras:

- Puede utilizar la GUI de configuración de descubrimiento para especificar dispositivos individuales o completar subredes que se van a descubrir.
- Puede descubrir dispositivos específicos o conjuntos de dispositivos desde la Vista de saltos o Vistas de red.
- Puede realizar inserciones en la tabla finders.rediscovery utilizando ncp_oql, especificando la dirección IP o la subred que se va a descubrir.

Nota: No utilice descubrimientos manuales para eliminar dispositivos de la topología. Los dispositivos que ya no son accesibles permanecen en la topología hasta su LingerTime llegue a cero y se ejecute otro descubrimiento, o hasta que los elimine utilizando el script RemoveNode.pl. Realice descubrimientos manuales solo en dispositivos que son operativos pero cuya configuración se ha cambiado.

Descubrimiento manual de un dispositivo o subred utilizando la GUI

Puede configurar e iniciar el descubrimiento de un dispositivo o subred desde la GUI de configuración de descubrimiento. Puede personalizar la configuración de descubrimiento para hacer que los descubrimientos parciales se ejecuten lo más rápido posible.

Habilitación de agentes de descubrimiento parcial

Puede configurar un descubrimiento parcial habilitando los agentes correspondientes en el separador **Agentes de descubrimiento parcial** en la GUI de configuración de descubrimiento.

Acerca de esta tarea

Puede acelerar el tiempo de un descubrimiento parcial seleccionando sólo aquellos agentes esenciales para descubrir dispositivos nuevos o modificados.

Configuración de valores avanzados de descubrimiento parcial

Entre los valores avanzados de descubrimiento parcial que puede configurar está la retroalimentación, la reconstrucción de la capa y los parámetros de vecinos remotos.

Configuración de valores de retroalimentación

Puede especificar valores de retroalimentación al configurar un descubrimiento parcial con la GUI.

Acerca de esta tarea

La retroalimentación es el mecanismo por el que los datos que han devuelto los agentes se utilizan para buscar otros dispositivos. Ejemplos de los datos de retroalimentación incluyen la dirección IP de vecinos remotos o la subred dentro de la cual existe un vecino local.

El mecanismo de retroalimentación permite que las nuevas direcciones IP se retroalimenten en el descubrimiento aumentando así el tamaño de la red que se ha descubierto. Es necesario que equilibre la totalidad de la topología descubierta (retroalimentación *activada*) con mayor velocidad de descubrimiento (retroalimentación *desactivada*).

Puede elegir entre las siguientes opciones una vez haya seleccionado el separador **Avanzado** en la opción de configuración de la GUI de configuración de descubrimiento:

- **No Feedback**: La retroalimentación está desactivada para todos los descubrimientos. Esta opción proporciona velocidad pero solo descubre aquellos dispositivos que se han especificado para los buscadores y, de esta manera, se proporciona una topología incompleta. Sin embargo, este valor garantiza que los descubrimientos finalizarán en el tiempo más breve posible.
- **Feedback**: La retroalimentación está activada para descubrimientos completos y parciales. Esta opción proporciona una topología completa en todas las situaciones pero es la que más tarda.
- **Feedback Only on Full**: La retroalimentación está activada para descubrimientos completos, garantizando una topología completa. No existe retroalimentación para descubrimientos parciales. Esto

garantiza que el descubrimiento parcial se ejecuta en el tiempo más breve posible. Este es el valor predeterminado.

Configuración de la reconstrucción de valores de capa

Puede permitir la reconstrucción de capas de topología para mostrar una topología precisa cuando configura un descubrimiento parcial.

Acerca de esta tarea

Para reconstruir las capas de topología que siguen a un descubrimiento parcial, seleccione el valor **Habilitar capas de reconstrucción de redescubrimiento** en el separador **Avanzado** en la opción configuración de la GUI de configuración de descubrimiento. Si especifica que *deben* reconstruirse las capas de topología después de un descubrimiento parcial, el resultado es una topología precisa que muestra toda la conectividad. Sin embargo, el proceso de agregar nuevos dispositivos tarda más tiempo.

Habilitación del descubrimiento de vecinos remotos para el descubrimiento parcial

Puede mejorar la precisión de las conexiones encontradas durante un descubrimiento parcial habilitando el descubrimiento de vecinos remotos.

Acerca de esta tarea

De forma predeterminada, el descubrimiento de vecinos remotos está desactivado. La habilitación del descubrimiento de vecinos remotos hace que el descubrimiento lleve más tiempo.

Con el descubrimiento de vecinos remotos activado, Network Manager comprueba, durante un descubrimiento parcial, si se ha modificado alguna conexión con vecinos remotos. (Los vecinos remotos en este contexto son dispositivos conectados que estaban dentro del ámbito del último descubrimiento completo, pero están fuera durante el descubrimiento parcial actual.)

Si las conexiones han cambiado, los dispositivos conectados se incluyen en el descubrimiento parcial, produciendo como resultado una topología más exacta.

Restricción: Si una conexión entre dispositivos ha cambiado, pero la información acerca de la conexión está almacenada solo en el dispositivo que está fuera del ámbito, el cambio no se registra y los dispositivos conectados no se incluyen en el descubrimiento parcial. La habilitación del descubrimiento de vecinos remotos aumenta la precisión de l topología, si se ha modificado, pero no garantiza que se descubran todos los cambios. Para obtener la topología más precisa posible, ejecute un descubrimiento completo.

Para habilitar el descubrimiento de vecinos remotos, seleccione **Habilitar redescubrimiento de dispositivos relacionados** en el separador **Avanzado** dentro de la opción **Configuración** en la GUI de configuración de descubrimiento.

Inicio de descubrimiento parcial desde la GUI

El inicio de un descubrimiento parcial implica la definición de una fuente y de ámbitos.

Acerca de esta tarea

Si no se ha ejecutado un descubrimiento completo desde la última vez que se inició el motor de descubrimiento, **`ncp_disco`**, no podrá iniciar un descubrimiento parcial.

Puede iniciar un descubrimiento parcial de un dispositivo o subred desde la ventana **Estado del descubrimiento activo**. También puede descubrir dispositivos específicos haciendo clic con el botón derecho sobre ellos en la vista de saltos y en las vistas de red.

Para iniciar un descubrimiento parcial desde la ventana **Estado del descubrimiento activo**, realice las siguientes tareas.

Procedimiento

1. Seleccione el dominio en el que desea ejecutar un descubrimiento desde el menú **Dominio**. Puede empezar a escribir el nombre del dominio y hacer coincidir los dominios que están enumerados bajo el campo **Dominio**.
2. Haga clic en la flecha que apunta hacia abajo junto al botón **Iniciar descubrimiento**  y seleccione **Iniciar descubrimiento parcial** desde el menú. Se muestra la ventana **Descubrimiento parcial**. Especifique las direcciones IP y las subredes que contienen los dispositivos que se van a descubrir
3. En **Descubrimiento parcial**, seleccione los nodos y subredes requeridas.
4. Para agregar una nueva subred o nodo, haga clic en **Nuevo.**
5. Cumplimente los campos como se indica a continuación y haga clic en **Aceptar**:

   Descubrir
   Seleccione una de las siguientes opciones:

   Identificador
   Escriba la dirección IP requerida.

   Subred
   Escriba la subred requerida y especifique el número de bits de máscara de red. El campo **Máscara de red** se actualiza automáticamente.

   Nombre de dispositivo de EMS
   Escriba el nombre de un dispositivo que se ha descubierto mediante un Sistema de gestión de elementos (EMS). Puede escribir el ID nativo, el nombre de entidad, el nombre de sistema o el nombre de visualización.

   Nota: Cuando ejecuta un descubrimiento parcial de un recopilador EMS desde la **GUI de estado de descubrimiento**, en la ventana **Nuevo nodo/subred de descubrimiento parcial**, debe especificar el valor del identificador del EMS en el campo **Nombre de dispositivo de EMS**, no en el campo **Identificador**. El campo **Identificador** sólo acepta direcciones IP.
6. Para agregar nuevas zonas de ámbito, haga clic en **Ámbito**.

   Nota: Si añade una zona de ámbito que no esté incluida en el ámbito del último descubrimiento completo, es posible que las conexiones entre dispositivos del nuevo ámbito y del anterior no sean exactas hasta que se realice el siguiente descubrimiento completo. La habilitación del descubrimiento de vecinos remotos puede mejorar la exactitud de estas conexiones.
7. Para agregar una nueva zona de descubrimiento, haga clic en **Nuevo**  . Para editar una zona de ámbito existente, haga clic en la entrada requerida en la lista.
8. Cumplimente los campos como se indica a continuación y haga clic en **Aceptar**:

   Acción
   Defina el rango de subred como una zona de inclusión o de exclusión. Si el rango de subred es una zona de inclusión en la que ejecutará ping durante el descubrimiento, haga clic en **Agregar a lista de fuentes de ping**. Al hacer clic en esta opción, se agregan automáticamente los dispositivos en la zona del ámbito como dispositivos de fuente de descubrimiento.

   Restricción: La opción `Agregar a lista de fuente de ping` no está disponible para zonas de ámbito de IPv6. Esto evita los barridos de ping de subredes IPv6, que potencialmente pueden contener billones de dispositivos para hacer ping. Por lo tanto, un barrido de ping de redes IPv6 puede provocar un descubrimiento interminable.
9. Haga clic en **Aceptar** y en **Ir**.

   Cuando se está ejecutando un descubrimiento parcial, se desactiva el botón **Iniciar descubrimiento**  .

Descubrimiento manual de un dispositivo o subred desde la línea de mandatos

Puede descubrir manualmente un dispositivo o subred desde la línea de mandatos.

Acerca de esta tarea

Para descubrir un dispositivo o una subred desde la línea de mandatos, realice inserciones en la tabla `finders.rediscovery` mediante `ncp_oql`, especificando la dirección IP o subred que debe descubrirse, como se describe en el siguiente ejemplo.

Descubrimiento manual

Para descubrir de forma manual el dispositivo con la dirección IP 192.168.1.2, inicie primero el proveedor de servicios OQL con el siguiente mandato:

```
ncp_oql -domain NCOMS -service Disco
```

Después de haber iniciado sesión en el proveedor de OQL, ejecute la siguiente consulta (tenga en cuenta que el mandato debe introducirse en una sola línea):

```
insert into finders.rediscovery (m_Address, m_RequestType) values
("192.168.1.2", 1);
```

Cuando el descubrimiento de un dispositivo se fuerza de esta manera, `ncp_disco` lo pasa inmediatamente al buscador de pings para confirmar que existe y, en caso afirmativo, activa los agentes adecuados para volver a analizarlo. Si las conexiones del dispositivo se han modificado, también se pueden descubrir los dispositivos vecinos.

Eliminación de un dispositivo de la red

Puede eliminar un dispositivo del que se sabe que se ha planificado para su eliminación permanente de la red.

Procedimiento

1. Elimine el dispositivo de la base de datos de topología utilizando el script **`RemoveNode.pl`**.
2. Elimine el dispositivo de la red físicamente.

Establecimiento del tiempo de espera para un dispositivo

El valor del campo LingerTime indica el número de descubrimientos que puede fallar un dispositivo antes de que se suponga que se ha eliminado de la red y que su registro se ha eliminado de la topología. El establecimiento del campo LingerTime en cero garantiza que cuando no se encuentre el dispositivo en el siguiente descubrimiento, su registro se eliminará inmediatamente de la topología.

Acerca de esta tarea

El establecimiento de LingerTime en la tabla ncimCache.lingerTime establece LingerTime sólo para el chasis. Las entidades contenidas como, por ejemplo, las interfaces y las tarjetas se eliminan de topología cuando un dispositivo descubierto tiene datos contención diferentes que muestran que la entidad contenida ya no está presente. LingerTime puede alterarse temporalmente para dispositivos específicos o entidades contenidas mediante la edición de los agrupadores de descubrimiento.

Para establecer el campo LingerTime en cero para un dispositivo, siga estos pasos:

Procedimiento

1. Emita un mandato similar a este para iniciar el proveedor de servicios OQL:

```
ncp_oql -domain NCOMS -service Model
```

2. Actualice el campo LingerTime en la tabla ncimCache.lingerTime para todas las entidades que representan al dispositivo. Por ejemplo, si el dispositivo se denomina `core-router.abcd.com`, escriba el siguiente mandato, en una sola línea:

```
update ncimCache.lingerTime set lingerTime->LINGERTIME = 0
where ENTITYNAME = 'core-router.abcd.com';
```

Capítulo 16. Resolución de problemas de descubrimiento

Puede solucionar problemas de descubrimiento supervisando los sucesos de descubrimiento y ejecutando informes de descubrimiento. También puede configurar sus propios agentes de descubrimiento.

Tareas relacionadas

Resolución de problemas de Network Manager

Consulte estas notas de resolución de problemas para ayudarse a determinar la causa del problema y cómo solucionarlo.

Resolución de problemas de descubrimiento con informes

Los informes de resolución de problemas proporcionan visibilidad fácil en los resultados del descubrimiento para ayudar con la verificación y la resolución de problemas de los resultados del descubrimiento y de la propia red.

Acerca de esta tarea

Network Manager usa el componente Cognos Analytics para generar informes.

Para obtener más información, consulte Cognos Analytics Knowledge Center, en https://www.ibm.com/support/knowledgecenter/SSEP7J.

Para acceder a los informes en la GUI de Network Manager, complete los pasos siguientes.

Pulse el icono **Informes** y seleccione **Informes comunes**. En el widget, seleccione **Network Manager**. Se muestra una lista de carpetas. Estas carpetas contienen todos los informes de Cognos para su acceso.

Puede utilizar informes para obtener resultados de verificación y resolución de problemas de descubrimiento como los ejemplos en Tabla 54 en la página 397.

Para obtener más información sobre los informes de Network Manager, consulte la publicación *IBM Tivoli Network Manager IP Edition Administration Guide*.

Tabla 54. Informe sobre las categorías que se van a utilizar para la resolución de problemas de descubrimiento

Tarea de resolución de problemas	Consulte esta categoría de informes e informe	Ventaja del informe
Identificación de todos los nodos e interfaces descubiertos	Informes de programa de utilidad: Lista de archivos sin formato de interfaces y nodos descubiertos	Este informe lista todos los nodos e interfaces que se han descubierto. También marca interfaces o puertos conectados a dispositivos de red. Le permite comprobar que los dispositivos e interfaces específicos se descubrieron en realidad.
Resolución de discrepancias	Informes de resolución de problemas Discrepancia de interfaces dúplex conectadas	Este informe proporciona una lista de conexiones que tienen discrepancias entre dispositivos de medio dúplex y dúplex completo, donde un extremo de la conexión es de medio dúplex y el otro extremo es de dúplex completo. Esta discrepancia es uno de los problemas de configuración clave que los gestores de red tienen que buscar para resolver problemas de rendimiento o disponibilidad.

Tabla 54. Informe sobre las categorías que se van a utilizar para la resolución de problemas de descubrimiento (continuación)

Tarea de resolución de problemas	Consulte esta categoría de informes e informe	Ventaja del informe
Resolución de dispositivos inaccesibles	Informes de resolución de problemas: Dispositivos sin acceso SNMP	Este informe identifica los dispositivos que no tienen acceso de SNMP. Puede identificar la causa del error de acceso SNMP.
Resolución de dispositivos no conectados	Informes de resolución de problemas: Dispositivos sin conexiones	Este informe lista dispositivos no conectados como un primer paso para determinar porqué no encontró el descubrimiento conexiones de red para un dispositivo.
Resolución de dispositivos no clasificados	Informes de resolución de problemas: Dispositivos con ID de objeto de SNMP sin clasificar	Al utilizar estos informes puede crear archivos AOC de nodo de hoja para la nueva clase de dispositivo.
	Informes de activo: • Disponibilidad de interfaz • Resumen por clase de dispositivo • Disponibilidad de proveedor y dispositivo	
Resolución de dispositivos con ID de objeto SNMP no registrado	Informes de resolución de problemas: Dispositivos con ID de objeto SNMP desconocido	Al utilizar la información de este informe, puede modificar los archivos AOC asociados con los dispositivos no registrados.
Identificación de dispositivos pendientes de supresión	Informes de resolución de problemas: Dispositivos pendientes de supresión en el siguiente descubrimiento	Este informe muestra información sobre dispositivos que se suprimirán de la topología si no se encuentran durante el siguiente ciclo de descubrimiento. El informe le permite comprobar que la eliminación de dispositivos de la topología está progresando, e identificar dispositivos planificados erróneamente para su eliminación.

Supervisión del estado de descubrimiento

Puede visualizar mensajes de estado de descubrimiento para entender el estado y el progreso del descubrimiento. También puede configurar sus propios agentes de descubrimiento.

Flujo de proceso para crear sucesos de descubrimiento

Los sucesos de descubrimiento se crean durante el proceso de descubrimiento y muestran el progreso de los agentes, los agrupadores y los buscadores. Esto sucesos se almacenan y envían a Tivoli Netcool/OMNIbus y se pueden ver utilizando GUI web.

Los sucesos de descubrimiento se crean en las siguientes etapas:

- Durante la fase de recopilación de datos de descubrimiento, los agrupadores dedicados (AgentStatus y FinderStatus) detectan si los buscadores o los agentes se han iniciado o detenido.
- Durante la fase de proceso de datos, un agrupador dedicado (CreateStchTimeEvent) detecta sucesos clave; por ejemplo, si el descubrimiento ha comenzado a crear la tabla de entidades que funcionan o la tabla de contención.

- Siempre que uno de los agrupadores mencionados más arriba detecta un suceso, graba ese suceso en la tabla `disco.events`.
- El agrupador responde a una inserción en la tabla `disco.events` y crea y envía el suceso apropiado a la sonda de Tivoli Netcool/OMNIbus, nco_p_ncpmonitor, que reenvía el suceso a ObjectServer.
- Puede iniciar o detener la generación de sucesos de descubrimiento mediante el establecimiento del campo `m_CreateStchrEvents` de la tabla `disco.config`.

Puede configurar sus propios sucesos de descubrimiento grabando un agrupador para detectar el suceso deseado y grabar los datos de ese suceso en la tabla `disco.events`.

Supervisión de mensajes de estado de descubrimiento

Puede visualizar mensajes de estado de descubrimiento para entender el estado y el progreso del descubrimiento.

Acerca de esta tarea

Los procesos de descubrimiento, incluyendo los agentes, agrupadores y buscadores, envían mensajes a IBM Tivoli Netcool/OMNIbus cuando se inician y se detienen. Puede visualizar estos mensajes para visualizar si los procesos de descubrimiento se ejecutan tal como se espera y para medir el progreso general del descubrimiento.

Para visualizar los mensajes de estado de proceso de descubrimiento, complete las siguientes tareas.

Procedimiento

1. Pulse el icono **Incidente** y seleccione **Sucesos** > **Visor de sucesos**.
2. Aplique un filtro a **Visor de sucesos** para que se visualicen únicamente sucesos con un `Agent` de `ncp_disco`.
3. Opcional: Refine el filtro u ordene en **EventId** para visualizar solo tipos específicos de sucesos de descubrimiento.
4. Asegúrese de que las columnas **LocalPriObj** y **LocalSecObj** se muestran en **Visor de sucesos**. Estas columnas contienen información para sucesos de descubrimiento. (No todas las columnas son utilizadas por todos los sucesos).

Error de recuperación de ID de entidad de NCIM

Si aparece un suceso de descubrimiento en la **Visor de sucesos** con la descripción "La recuperación de un ID de entidad de NCIM para una determinada entidad ha fallado", puede que la base de datos NCIM esté inactiva. Esto provocará una discordancia entre los ID de entidad en NCIM y en la base de datos de descubrimiento DNCIM incorporada; es decir, NCIM y DNCIM tendrán un conjunto diferente de ID de entidad para las mismas entidades de red.

Si la base de datos NCIM está inactiva por algún motivo mientras se ejecuta el agrupador RetrieveNCIMEntityId, habrá una discordancia entre los ID de entidad en DNCIM y NCIM. No es fundamental que los ID de entidad en DNCIM y NCIM coincidan; no obstante, en caso de una resolución de error de descubrimiento, es útil si los ID de entidad son coherentes en las bases de datos.

Si hay una discordancia entre los ID de entidad en DNCIM y NCIM, siga estos pasos para asegurarse de que las bases de datos están alineadas para el siguiente descubrimiento:

- Renueve la base de datos DNCIM antes del siguiente descubrimiento
- Inicie una sesión en la base de datos DNCIM de descubrimiento en ejecución y suprima todos los registros de entityNameCache para su dominio

Nota: Si la base de datos de topología NCIM se comparte entre varios dominios, la probabilidad de una discordancia en los ID de entidad de DNCIM y NCIM es mucho mayor.

Renueve la base de datos DNCIM antes del siguiente descubrimiento

Renueve la base de datos DNCIM sólo si el motor de descubrimiento, ncp_disco, no se está ejecutando.

Renueve la base de datos DNCIM suprimiendo el siguiente directorio y todo su contenido. La base de datos DNCIM almacena todos los archivos de base de datos en este directorio:

```
$NCHOME/precision/embeddedDb/sqlite/processName.domain
```

Donde:

- *nombre_proceso* es el nombre del proceso de Network Manager que utiliza DNCIM. En este caso, es el nombre del motor de descubrimiento, ncp_disco.
- *dominio* es el nombre del dominio actual.

Por ejemplo, si el nombre del dominio actual es NCOMS, los archivos de base de datos se encuentran en:

```
$NCHOME/precision/embeddedDb/sqlite/ncp_disco.NCOMS
```

Nota: Esto dará como resultado un pequeño retardo en el siguiente descubrimiento porque debe volver a crearse la base de datos DNCIM.

Inicio de una sesión en la base de datos DNCIM y suprima todos los registros de entityNameCache para su dominio

Siempre que el descubrimiento esté en el estado estático (fase 0), es seguro alterar la base de datos DNCIM de descubrimiento. Proceda como se explica a continuación:

1. Compruebe que el motor de descubrimiento, ncp_disco, esté en ejecución y que el descubrimiento esté en la fase 0 ejecutando la siguiente consulta. Si la consulta devuelve el valor 0, el descubrimiento están en la fase 0.

   ```
   select m_Phase from disco.status
   ```

2. Emita el siguiente mandato OQL para acceder a la base de datos DNCIM:

   ```
   ncp_oql -domain domain_name -service DNCIM
   ```

   Donde *domain_name* es el nombre del dominio de red actual.

3. Emita el siguiente mandato para suprimir todos los registros en entityNameCache:

   ```
   DELETE FROM entityNameCache
   ```

   Nota: Para una base de datos grande, la operación de supresión puede tardar un tiempo considerable.

Resolución de problemas de agentes de descubrimiento

Puede utilizar la GUI de estado de descubrimiento para resolver problemas de descubrimiento asociados con agentes de descubrimiento.

Resolución de problemas de un descubrimiento inusualmente largo

Un descubrimiento puede tardar bastante tiempo en completarse porque un agente no es capaz de completar el procesamiento en un dispositivo concreto. Utilice la sección **Estado de los agentes** para determinar qué agente tarda mucho tiempo en completar y en qué dispositivo está trabajando.

Acerca de esta tarea

Para utilizar la sección **Estado de los agentes** y determinar si la causa del problema es un agente que está bloqueado en un dispositivo, complete los siguientes pasos:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Estado del descubrimiento de red**.
2. En **Estado del descubrimiento de red**, pulse la ficha **Estado de los agentes**.
3. Defina la lista desplegable de fases situada por encima de la tabla superior de Agentes en Interrogando dispositivos.

   La tabla superior de Agentes muestra ahora solo los agentes que están planificados para finalizar en la primera fase del descubrimiento, Interrogando dispositivos.

   Nota: Este problema tiene lugar durante la primera fase de descubrimiento, Interrogando dispositivos.
4. Asegúrese de que la columna **Estado** está ordenada en orden descendiente.

   Los agentes aparecen de manera predeterminada en orden descendiente por estado de agente, tal y como aparecen numerados en la siguiente tabla.

Tabla 55. Estados del agente

Estado	Valor	Icono	Descripción
Concluido	5		El agente ha finalizado de forma inesperada. Este es un problema de descubrimiento potencial.
Finalizado	4		El agente se sigue ejecutando pero ha terminado el proceso de todas las entidades de la cola. El agente sigue estando disponible para procesar cualquier otro agente colocado en la cola.
En ejecución	3		El agente está procesando entidades actualmente.
Iniciando	2		El agente se está iniciando.
No ejecución	1		El agente no se está ejecutando.

5. Desplácese hacia abajo por la tabla para buscar los agentes que tienen el estado En ejecución  .

   Estos son los agentes que están procesando dispositivos todavía. Si se ha ejecutado el descubrimiento durante un periodo de tiempo inusualmente largo, puede que haya un único agente que todavía tenga el estado En ejecución  . Este es el agente bloqueado.
6. Seleccione uno de los agentes con el estado En ejecución  .

   De manera predeterminada, la tabla inferior muestra ahora todas las entidades que todavía están en cola para este agente.
7. Haga clic en el botón de selección **Todo** por encima de la tabla inferior.

   La tabla inferior muestra ahora todas las entidades que este agente ha procesado, que estos agentes están procesando todavía o que están en la cola de agente.
8. Asegúrese de que la columna **Estado** está ordenada en orden descendiente.

   Las entidades aparecen de manera predeterminada en orden descendiente por estado de agente, tal y como aparecen numerados en la siguiente tabla.

Tabla 56. Estados de entidad

Estado	Valor	Icono	Descripción
Concluido	5		El proceso de la entidad ha finalizado de forma inesperada. El agente se ha detenido manualmente o se ha producido un problema con el descubrimiento.

Tabla 56. Estados de entidad (continuación)			
Estado	**Valor**	**Icono**	**Descripción**
Finalizado	4		Un agente ha completado el proceso de esta entidad.
En ejecución	3		Un agente está procesando actualmente esta entidad.
Iniciando	2		Un agente está comenzando a procesar esta entidad.
No ejecución	1		Esta entidad no está procesándose actualmente.

9. Desplácese hacia abajo por la tabla para buscar las entidades que tienen el estado En ejecución .
   Estas son las identidades que este agente aún está procesando. Si el agente está bloqueado en un único dispositivo, solo habrá una entidad con el estado En ejecución .
10. Consulte el resto de la información de la tabla para saber más sobre esta entidad.
    La columna de tiempo transcurrido indica cuánto tiempo ha procesado el agente este dispositivo. La columna SNMP indica si el agente era capaz de conseguir acceso SNMP a este dispositivo. Si el agente no fue capaz de conseguir acceso SNMP al dispositivo, puede que haya un problema con los valores de cadena de comunidad SNMP. Es necesaria una investigación más detallada de este dispositivo.
11. Si el dispositivo tiene un gran número de interfaces, es posible que el descubrimiento parezca que se ha bloqueado en este dispositivo, ya que tarda mucho tiempo en descargar toda la información. Configure un filtro de interfaz para este dispositivo para excluir la información en la que no esté interesado. Cuando ejecute de nuevo el descubrimiento, el ayudante de SNMP recupera menos información desde el dispositivo, con lo cual podría resolverse el problema.

Identificación de agentes fallidos

El origen de un error de descubrimiento puede estar en la finalización inesperada de los agentes durante el descubrimiento. Utilice la sección **Estado de los agentes** para determinar si algún agente ha finalizado de forma inesperada.

Acerca de esta tarea

Para utilizar la sección **Estado de los agentes** para determinar si algún agente de descubrimiento no se está ejecutando de forma correcta, lleve a cabo los siguientes pasos:

Procedimiento

1. Pulse el icono **Descubrimiento** y seleccione **Estado del descubrimiento de red**.
2. En **Estado del descubrimiento de red**, pulse la ficha **Estado de los agentes**.
3. Asegúrese de que la lista desplegable de fases situada por encima de la tabla superior de Agentes se define como Todas las fases.
   La tabla de agentes superior muestra ahora todos los agentes que se han iniciado hasta el momento en este descubrimiento.
4. Haga clic en la columna **Estado** en la tabla de agentes superior para que los agentes estén situados en orden descendente de **Estado**.
   Los agentes aparecen ahora en la tabla por orden alfabético de estado.
5. Los agentes que hayan finalizado de forma inesperada se situarán en la parte superior de la tabla y tendrán el estado Concluido.

Qué hacer a continuación
Es necesario investigar más para determinar por qué este agente ha finalizado de forma inesperada.

Resolución de problemas de dispositivos ausentes

Si un dispositivo que espera encontrar en su topología de red no está presente, siga estos pasos para resolver el problema.

Antes de empezar
Antes de seguir estos pasos, ejecute un descubrimiento completo con la retroalimentación habilitada.

Acerca de esta tarea
Para comprobar algunas causas comunes para un dispositivo que no se encuentra en los mapas de red, complete los siguientes pasos.

Procedimiento
1. Compruebe que el dispositivo que busca se está ejecutando y está conectado a la red.
2. Buscar el dispositivo.
   a) Buscar el dispositivo en los mapas de red por nombre de host y después por dirección IP.
   b) Si sabe a qué dispositivos está conectado, intente encontrar uno de los dispositivos conectados en la **Vista de saltos de red**. A continuación, defina el número de saltos en 1 y vea si el dispositivo aparece como conectado.
3. Compruebe si el dispositivo está en el ámbito. Revise el ámbito de descubrimiento, incluidas las zonas de exclusión, en el separador **Ámbito** de la GUI de **Configuración de descubrimiento de red**.
4. Compruebe si el dispositivo se está filtrando fuera del dispositivo.
   a) Haga clic en **Filtros**.
   b) Revise los filtros de descubrimiento previo y posterior para asegurarse de que no se impide que el descubrimiento o la instanciación del dispositivo.
   c) Busque el nombre de dispositivo en el archivo `ncp_disco.`*`dominio`*`.log`.

      Si el dispositivo se ha filtrado mediante un filtro de postdescubrimiento, habrá mensajes de tipo:

      ```
      Filtering entity name and not sending to model
      ```

      ```
      name matches the instantiateFilter
      ```

      Si una relación de dispositivo se ha filtrado mediante un filtro de postdescubrimiento, habrá mensajes de tipo:

      ```
      Filter relationship involving name
      ```

Resolución de problemas de un descubrimiento inactivo

Si inicia el descubrimiento, y después de algunos minutos no se han descubierto dispositivos, siga estos pasos de resolución de problemas.

Acerca de esta tarea
Si el estado de descubrimiento se queda en la fase cero (inactivo) una vez lo haya iniciado, y no se han descubierto dispositivos, intente realizar los siguientes pasos de resolución de problemas.

Procedimiento

1. Si está utilizando el buscador de archivos, compruebe que ha especificado correctamente qué campo en el archivo de fuente contiene la dirección IP y qué archivo contiene el nombre de host. Puede verificar estos valores en la GUI de configuración de descubrimiento.
2. Si está utilizando el buscador de pings y está haciendo ping en direcciones IP individuales, compruebe que esas direcciones IP son accesibles. Si no lo son, es posible que se deba a una parada de la red o un problema del cortafuegos.
3. Verifique que las direcciones IP de fuente está en el ámbito. Incluso si agrega una dirección al buscador de pings o buscador de archivos, no se hará ping en el dispositivo o no se instanciará si no se incluye en el ámbito. Por ejemplo, si el ámbito de su descubrimiento es 172.16.1.0 /24 y las fuentes están en la red 192.168.1.0 /24, los buscadores no las podrán encontrar.
4. Si están haciendo ping en una subred grande y escasamente rellenada, por ejemplo, una subred de clase B que contiene solo 10 dispositivos, el buscador de pings puede tardar mucho tiempo en encontrar el primer dispositivo.

Qué hacer a continuación

Si necesita revisar los registros de descubrimiento, consulte la información sobre la ubicación de archivos de registro y de cambio de niveles de registro en *IBM Tivoli Network Manager IP Edition Administration Guide*.

Reparación de un descubrimiento dañado

Si el descubrimiento se detiene de forma anómala, por ejemplo, si el proceso ncp_disco se detiene de manera forzada desde la línea de mandatos, o se cierra de forma inesperada, es posible que necesite reparar el descubrimiento antes de ejecutar otro.

Acerca de esta tarea

Si el descubrimiento ha concluido con normalidad, todos los procesos dependientes tales como agentes de descubrimiento también se cierran, y la base de datos de descubrimientos está lista para otro descubrimiento. No obstante, si el proceso ncp_disco se ha detenido de manera forzada o inesperada, los procesos dependientes pueden seguir en ejecución, y los archivos de la memoria caché del descubrimiento se quedan en un estado en el que pueden interferir con el próximo descubrimiento. En este caso, se puede decir que el descubrimiento está *dañado*.

Para reparar un descubrimiento dañado, siga los pasos siguientes:

Procedimiento

1. Elimine la entrada para el proceso ncp_disco de la base de datos services.inTray de ncp_ctrl, si está presente. La eliminación de la entrada evita que el proceso ncp_ctrl reinicie ncp_disco.
2. Detenga el proceso ncp_disco, si aún está en ejecución, utilizando un mandato adecuado para su sistema operativo.
   Por ejemplo, en Unix, ejecute el mandato `kill -9` en el ID de proceso de ncp_disco.
3. Elimine los archivos de memoria caché de la base de datos dNCIM. Vaya al directorio `$PRECISION_HOME/embeddedDb/sqlite` y suprima el directorio `ncp_disco.`*`dominio`*.
4. Opcional: Archive o elimine los archivos de registro existentes para iniciar el siguiente descubrimiento con archivos de registro nuevos. Los archivos de registro son relevantes para los siguientes procesos:
   - **ncp_disco**
   - **ncp_df_***
   - **ncp_agent***
   - **ncp_disco_perl_agent***
5. Busque cualquier buscador de descubrimientos o agente que siga en ejecución en el dominio dañado. Los buscadores de descubrimientos tienen nombres de proceso que empiezan por ncp_df. Los agentes

de descubrimiento empiezan por ncp_agent, y los agentes de descubrimiento de Perl empiezan por ncp_disco_perl_agent. Detenga los agentes o buscadores que sigan en ejecución en el dominio dañado.

6. Si desea ejecutar el proceso ncp_disco como un proceso gestionado por el proceso ncp_ctrl, que es el valor predeterminado, inicie ncp_disco como un proceso gestionado. Consulte el tema sobre el inicio de procesos gestionados para obtener más información.

   El inicio de ncp_disco como un proceso gestionado inicia un nuevo descubrimiento.
7. Inicie o supervise el descubrimiento utilizando la GUI Configuración de descubrimiento.

Eliminación de archivos de memoria caché de descubrimiento

Elimine archivos de memoria caché de descubrimiento para realizar un descubrimiento nuevo y limpio.

Acerca de esta tarea

Para eliminar el descubrimiento de red actual para un dominio, debe eliminar todos los archivos de memoria caché de descubrimiento. Puede hacerlo cuando tenga que eliminar todos los datos de un descubrimiento anterior o cuando el servicio de soporte de IBM se lo solicite.

Este procedimiento suprime todos los archivos de memoria caché de descubrimiento actuales y borra la base de datos del descubrimiento, restableciendo de manera eficaz el descubrimiento. Después de realizar este procedimiento, debe ejecutar un nuevo descubrimiento completo de su red.

Nota: Ya que la topología de red está almacenada por separado en la base de datos de NCMI, este procedimiento no elimina los mapas de red. Sin embargo, los cambios que se hayan realizado en su red desde el último descubrimiento aparecerán reflejados en el próximo descubrimiento.

Realice el siguiente procedimiento para eliminar todos los archivos de memoria caché de descubrimiento:

Procedimiento

1. Detenga todos los procesos de Network Manager mediante el script `itnm_stop`.
2. Vaya al directorio `$NCHOME/var/precision` y elimine todos los archivos que pertenezcan el dominio que desea eliminar. Los archivos que pertenecen a un dominio particular tiene el dominio en el nombre de archivo. Por ejemplo, un archivo de configuración que pertenece al dominio NCOMS de puede llamar `file_name.NCOMS.cfg`.
3. Vaya al directorio `$PRECISION_HOME/embeddedDb/sqlite` y suprima el directorio `ncp_disco.`*`dominio`*.
4. Opcional: Archive o elimine los archivos de registro existentes para iniciar el siguiente descubrimiento con archivos de registro nuevos. Los archivos de registro son relevantes para los siguientes procesos:
   - **ncp_disco**
   - **ncp_df_***
   - **ncp_agent***
   - **ncp_disco_perl_agent***
5. Reinicie los procesos de Network Manager mediante el script `itnm_start`.

   Se crean de forma automática archivos de registro vacío cuando se reinician los procesos de Network Manager mediante los scripts `itnm_start`.
6. Ejecute un nuevo descubrimiento de red.

Resolución de problemas de caracteres no válidos

Si aparece un mensaje de error sobre caracteres no permitidos en las sentencias de inserción en la base de datos de topología, siga estos pasos para resolver el problema.

Acerca de esta tarea

Si tiene dispositivos de red con caracteres no permitidos en sus descripciones en el entorno local configurado en la base de datos, podría ver un mensaje de error similar al siguiente:

```
WARNING:  W-RIV-002-206: [4115626896t] CMdlDbEntityMgr.cc(647) Falló una
operación 'execute' de la base de datos: SQLRETURN = -1 CNcpODBCSth.cc line 233 : [<database>]
[<database> ODBC Driver]
[<database>]Se encontró un carácter ilegal en el enunciado.
```

Procedimiento

1. Haga una copia de seguridad y edite el archivo `SnmpStackSchema.cfg`.
2. Localice la línea de configuración de una inserción en la tabla `snmpStack.conversionCfg` y edítela del siguiente modo:

   insert into snmpStack.conversionCfg values (1);
3. Guarde y cierre el archivo.

Resultados

El ayudante de SNMP sustituye lo caracteres devueltos por los dispositivos que no están permitidos en el entorno local de la base de datos por el carácter de interrogación: '?'

El ayudante de SNMP sustituye los caracteres solo en aquellos objetos configurados en la tabla snmpStack.multibyteObjects.

Capítulo 17. Descubrimiento y uso de datos personalizados

Puede enriquecer la topología añadiendo datos personalizados a la información descubierta por el proceso de descubrimiento. Por ejemplo, puede añadir datos personalizados sobre entidades descubiertas procedentes de orígenes de terceros utilizando agentes o recopiladores. Estos datos personalizados se pueden utilizar posteriormente en el enriquecimiento de sucesos, la visualización de redes, los sondeos y la elaboración de informes.

Acerca de esta tarea

La adición de datos personalizados a la topología de red implica el descubrimiento de datos y su almacenamiento en la base de datos de topología. Existen varios métodos para descubrir datos. Elija el método adecuado basado en el origen y la complejidad de los datos.

Existen dos métodos que puede utilizar para almacenar datos personalizados. Elija el método adecuado basado en lo que desea hacer con los datos personalizados:

Almacenamiento de datos personalizados utilizando pares nombre-valor

Si desea utilizar los datos extra sólo para su uso en el enriquecimiento de suceso o su visualización en el Navegador de estructura, puede añadir datos personalizados utilizando pares nombre-valor. No necesita crear tablas de base de datos personalizadas.

Este método puede resultar más fácil de implementar y actualizar porque no necesita cambiar los esquemas de base de datos predeterminados.

Almacenamiento de datos personalizados en tablas de base de datos nuevas

Si desea utilizar los datos no sólo para el enriquecimiento de suceso o su visualización en el Navegador de estructura, sino también para el sondeo personalizado, encontrar dispositivos en la vista de saltos o para utilizarlos en la definición de vistas de red, debe crear tablas de base de datos nuevas.

Motivos para añadir datos personalizados

Los motivos para añadir datos personalizados determinan el método de almacenamiento de datos adecuado. Algunos motivos frecuentes para añadir datos personalizados a la topología incluyen el enriquecimiento de los datos asociados con un dispositivo o una interfaz y el modelado de una conectividad personalizada entre dispositivos.

Almacenamiento de datos personalizados en tablas de base de datos nuevas

Si desea filtrar o buscar en los datos, almacene los datos en tablas personalizadas. Este método de almacenamiento de datos personalizados es adecuado para los siguientes usos de ejemplo.

- Creación de diferentes informes para diferentes clientes
- Implementación de diferentes políticas de sondeo para diferentes proveedores basada en los acuerdos de nivel de servicio
- Creación de una vista de red basada en la ubicación

Todos los usos anteriores implican la identificación de entidades relevantes basadas en campos de datos personalizados. El almacenamiento de datos en tablas de base de datos nuevas es más eficientes para estos usos que el almacenamiento de datos como pares nombre-valor.

Almacenamiento de datos personalizados como pares nombre-valor en la tabla de base de datos entityDetails

Si desea incluir los datos personalizados como parte de otra operación, almacene los datos como pares de nombre-valor en la tabla de base de datos entityDetails. Este método de almacenamiento de datos personalizados es adecuado para los siguientes usos de ejemplo.

- Adición de nombres de cliente para informes que filtran otros datos
- Marcado de sucesos de red con ubicación o nombre de cliente

En estos casos, las entidades relevantes se seleccionan en base a otros campos de base de datos. Las entidades se seleccionan por consultas SQL o búsquedas de pasarela de sucesos. Los datos personalizados se extraen de las entidades seleccionadas si están presentes. Para estos usos, puede almacenar de forma alternativa los datos en tablas de base de datos nuevas, pero es más rápido almacenar datos como pares nombre-valor en la tabla de base de datos entityDetails.

Modelado de una conectividad personalizada entre entidades

La conectividad personalizada se modela en Network Manager utilizando capas. Algunos ejemplos de conectividad modelada de forma predeterminada mediante capas incluyen los tipos siguientes:

- Cisco Discovery Protocol, el protocolo utilizado entre dispositivos de comunicaciones Cisco.
- SynOptics Network Management Protocol, el protocolo utilizado entre dispositivos de comunicaciones Nortel.

Si desea modelar una conectividad personalizada entre entidades, debe almacenar los datos en tablas de base de datos nuevas. Debe grabar un agente personalizado para recuperar los datos personalizados pertinentes de sus entidades de red. También debe grabar un agrupador de capas personalizado para generar una conectividad personalizada a partir de los datos de agente. Algunos ejemplos de agrupadores de capa personalizados suministrados con Network Manager son `CDPLayer.stch`, `OSPFLayer.stch`, `SONMPLayer.stch` y `SRPLayer.stch`. Puede inspeccionar estos agrupadores para ayudarle a grabar el agrupador de capas personalizado.

Descubrimiento de datos personalizados

Para utilizar datos personalizados en el producto, primero debe añadir la información al descubrimiento.

Acerca de esta tarea

Puede utilizar diferentes métodos para descubrir datos personalizados.

Adición de pares nombre-valor a entidades utilizando el buscador de archivos

Si va a utilizar el buscador de archivos para iniciar el descubrimiento, puede añadir pares nombre-valor a entidades añadiendo columnas extra a la lectura de archivos de inicio mediante el buscador de archivos.

Acerca de esta tarea

En el procedimiento de ejemplo que figura a continuación, se supone que va a añadir columnas extra al archivo de inicio del buscador de archivos:

- cliente
- ubicación

El siguiente fragmento de archivo de texto muestra que el archivo de inicio podría ser similar a:

```
vi /var/tmp/logged_hosts

172.16.1.21       lnd-dharma-acme       acme        london
172.16.1.201      lnd-phoenix-acme      acme        london
172.16.1.25       prs-sun-acme          acme        paris
```

```
172.16.2.33       ranger1              telecorp    newyork
172.16.2.34       ranger2              telecorp    newyork
~
"/var/tmp/logged_hosts" [Read only] 4 lines, 190 characters
```

En este fragmento de ejemplo de archivo de texto, la tercera columna contiene la información del cliente, y la cuarta, información sobre la ubicación.

Procedimiento

1. Edite el archivo de configuración DiscoFileFinderParseRules.cfg.
2. En este archivo de configuración, configure el buscador de archivos para analizar el archivo de inicio mediante un inserto similar al del ejemplo. Asegúrese de configurar el campo `m_ColDefs` para que coincida con las nuevas columnas de etiqueta personalizadas.

```
insert into fileFinder.parseRules
(
            m_FileName,
            m_Delimiter,
            m_ColDefs
)
values
(
            "/var/tmp/logged_hosts",
            "[     ]",
            [
                {
                    m_VarName="m_UniqueAddress",
                    m_ColNum=1
                },
                {
                    m_VarName="m_Name",
                    m_ColNum=2
                },
                {
                    m_VarName="m_CustomTags->customer",
                    m_ColNum=3
                },
                {
                    m_VarName="m_CustomTags->location",
                    m_ColNum=4
                }
            ]
);
```

   Esta inserción indica al buscador de archivos que realice lo siguiente:

   - Analice `/var/tmp/logged_hosts`.
   - Considere al espacio en blanco como el separador de datos.
   - Utilice las siguientes definiciones de columna:
     - `m_UniqueAddress` para la primera columna
     - `m_Name` para la segunda columna
     - `m_CustomTags->customer` para la tercera columna
     - `m_CustomTags->location` para la cuarta columna
3. Edite el archivo DbEntityDetails.cfg y configure una inserción similar a la siguiente:

```
insert into dbModel.entityDetails
(
    EntityType,
    EntityDetails
)
values
(
    1,  -- chassis
    {
        Customer = "eval(text, '&m_ExtraInfo->m_CustomTags->customer')",
        Location = "eval(text, '&m_ExtraInfo->m_CustomTags->location')"
    }
);
insert into dbModel.entityDetails
```

```
(
     EntityType,
     EntityDetails
)
values
(
     2,  -- port/interface
     {
         Customer = "eval(text, '&m_ExtraInfo->m_CustomTags->customer')",
         Location = "eval(text, '&m_ExtraInfo->m_CustomTags->location')"
     }
);
```

4. Reinicie Network Manager para propagar los cambios en los archivos de configuración:

```
itnm_start ncp -domain domain
```

5. Ejecute un descubrimiento completo utilizando el buscador de archivos para descubrir la red con los pares nombre-valor añadidos.

Qué hacer a continuación

Asegúrese de que los nuevos datos se propagan entre los descubrimiento.

Desarrollo de agentes o recopiladores para obtener datos personalizados

Puede desarrollar agentes o recopiladores para recuperar datos personalizados y añadirlos al descubrimiento.

Acerca de esta tarea

Puede recuperar datos personalizados de un origen de terceros, como un archivo sin formato, una base de datos o un sistema de terceros. Para ello, desarrolle un agente Perl o un recopilador EMS.

Importante:

La grabación de agentes de descubrimiento o recopiladores personalizados es un procedimiento avanzado. Las inserciones incorrectas en las bases de datos de descubrimiento pueden corromper el descubrimiento y provocar resultados imprevisibles. Tenga en cuenta interactuar con IBM Services o un IBM Business Partner.

Utilice la siguiente información para determinar el mejor método para recuperar datos.

Tabla 57. Método para la recuperación de datos

Sistema origen	Método	Vínculo
EMS	Recopilador EMS	“Configuración de descubrimientos de EMS” en la página 228
Archivo sin formato o base de datos	Agente personalizado	Para obtener información sobre la escritura de agentes de descubrimiento, consulte la publicación *Referencia de IBM Tivoli Network Manager*.Para obtener información sobre la escritura de agentes de descubrimiento, consulte la publicación *Referencia de IBM Tivoli Network Manager*.

Adición de datos manualmente utilizando tablas de etiquetas personalizadas

Puede añadir etiquetas de par nombre-valor a entidades mediante la creación de inserciones que contengan los datos de par nombre-valor en las tablas disco.ipCustomTags o disco.filterCustomTags.

Adición de pares nombre-valor a entidades utilizando la tabla disco.ipCustomTags

Puede asociar etiquetas de par nombre-valor a direcciones IP únicas mediante la tabla disco.ipCustomTags. Utilice este método si conoce las direcciones IP individuales que desea etiquetar.

Acerca de esta tarea

En el procedimiento de ejemplo que figura a continuación, se supone que en el descubrimiento va a añadir estas dos etiquetas de par nombre-valor a las entidades:

- cliente
- ubicación

Este ejemplo utiliza la tabla disco.ipCustomTags para configurar estas etiquetas de par nombre-valor:

Tabla 58. Ejemplo de etiquetas de par nombre-valor

Dirección IP	Nombre	Valor
172.16.1.21	cliente	acme
172.16.1.21	ubicación	london
172.16.1.201	cliente	acme
172.16.1.201	ubicación	london
172.16.1.25	cliente	acme
172.16.1.25	ubicación	paris
172.16.2.33	cliente	telecorp
172.16.2.33	ubicación	newyork
172.16.2.34	cliente	telecorp
172.16.2.34	ubicación	newyork

Procedimiento

1. Edite el archivo de configuración `DiscoConfig.cfg`.
2. En este archivo de configuración. añada una inserción similar a esta.

```
insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.1.21',
            {
                customer="acme",
                location="london"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
```

```
            m_CustomTags
 )
values
(
            '172.16.1.201',
            {
                customer="acme",
                location="london"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.1.25',
            {
                customer="acme",
                location="paris"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.2.33',
            {
                customer="telecorp",
                location="newyork"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.2.34',
            {
                customer="telecorp",
                location="newyork"
            }
);
```

3. Guarde el archivo de configuración `DiscoConfig.cfg`.

Qué hacer a continuación

Puede ejecutar una búsqueda completa para descubrir su red con las etiquetas personalizadas.

Adición de pares nombre-valor a entidades utilizando la tabla disco.filterCustomTags

Puede asociar etiquetas de par nombre-valor a un conjunto filtrado de direcciones IP mediante la tabla disco.filterCustomTags. Utilice este método si desea etiquetar varias direcciones utilizando un atributo compartido de estos dispositivos.

Acerca de esta tarea

Puede filtrar las direcciones IP en función de una amplia variedad de criterios. Por ejemplo, puede filtrar según el nombre del dispositivo, la dirección IP o el identificador de VLAN. En el procedimiento de ejemplo que figura a continuación se aplica un filtro en función de una dirección IP y utiliza la tabla disco.filterCustomTags para configurar las siguientes etiquetas de par nombre-valor para todas las direcciones IP de la subred 172.20.3.0/24:

Tabla 59. Ejemplo de etiquetas de par nombre-valor		
Dirección IP	**Nombre**	**Valor**
172.20.3.0/24	cliente	acme
172.20.3.0/24	ubicación	london

Procedimiento

1. Edite el archivo de configuración DiscoConfig.cfg.
2. En este archivo de configuración, añada la siguiente inserción:

```
insert into disco.filterCustomTags
(
            m_Filter,
            m_CustomTags
 )
values
(
            "m_UniqueAddress LIKE '172.20.3'",
            {
                customer="acme",
                location="london"
            }
);
```

3. Guarde el archivo de configuración DiscoConfig.cfg.

Otros ejemplos de filtros

En el procedimiento anterior, se aplica un filtro en función de una dirección IP: `"m_UniqueAddress LIKE '172.20.3'"`.

Puede crear un filtro en función de cualquiera de los atributos asociados con las entidades descubiertas. Por ejemplo, puede aplicar los siguientes filtros:

- Filtro basado en el nombre de entidad: `"m_Name LIKE 'lon'"`
- Filtro basado en un identificador VLAN de una entidad VLAN: `"m_LocalNbr->m_VlanID = 102"`

Qué hacer a continuación

Puede ejecutar una búsqueda completa para descubrir su red con las etiquetas personalizadas.

Enriquecimiento de la topología con el agrupador GetCustomTag

Puede utilizar el agrupador GetCustomTag para añadir datos a entidades de topología. Puede elegir utilizar este método si tiene necesidades de personalización complejas.

Antes de empezar

Si desea aplicar una etiqueta fija a entidades coincidentes, puede utilizar el campo m_CustomTags, y no necesita utilizar el agrupador GetCustomTag.

Acerca de esta tarea

Si desea añadir datos más complejos, personalice el agrupador GetCustomTag.stch. La etiqueta configurada en el campo `m_StitcherTagName` se utiliza como nombre de campo, y el valor devuelto por el agrupador GetCustomTag se utiliza como valor de campo.

Nota: La edición de agrupadores es una tarea avanzada, que requiere conocimiento del idioma del agrupador y del flujo de datos de descubrimiento.

Para personalizar el agrupador `GetCustomTag.stch`, complete los pasos siguientes:

Procedimiento

1. Añadir datos a la tabla disco.filterCustomTags o disco.ipCustomTags para especificar qué entidades aplicar a las etiquetas personalizadas.
2. Editar el archivo de configuración `DiscoConfig.cfg` para configurar el agrupador GetCustomTag.
3. En este archivo de configuración, añada la siguiente inserción:

```
insert into disco.filterCustomTags
            (
                        m_Filter,
                        m_StitcherTagName,
             )
            values
            (
                        "m_UniqueAddress LIKE '172.20.3.'",
                        'customer'
            );
```

   Esta inserción configura el sistema para utilizar el agrupador `GetCustomTag.stch` para buscar el valor del campo `customer` para cada entidad en la subred 172.20.3.0/24. El agrupador `GetCustomTag.stch` debe modificarse para proporcionar esta información, en caso contrario, el para nombre-valor no se añade a la entidad.
4. Guarde el archivo de configuración `DiscoConfig.cfg`.
5. Modifique el agrupador `GetCustomTag.stch` para dar soporte a la etiqueta personalizada.

   El agrupador `GetCustomTag.stch` recibe el nombre de entidad y etiqueta como argumentos de agrupador 1 y 2 respectivamente y devuelve un valor de texto. Personalice el agrupador `GetCustomTag.stch` para determinar los valores de retorno adecuados, dependiendo de para qué desea utilizar los datos. En el ejemplo siguiente, el agrupador se personaliza para comprobar la serie `lon` en el nombre de entidad proporcionados. Si el nombre de entidad contiene la serie, se devuelve el valor `A-Z Inc., London` como valor para `customer`. Si el nombre de entidad no contiene la serie, se devuelve none.

```
                UserDefinedStitcher
                {
                    StitcherTrigger
                    {
                        // Called from another stitcher when tag criteria is met
                    }

                    StitcherRules
                    {
                        text tagName = eval(text,'$ARG_1');
                        text entityName = eval(text,'$ARG_2');

                        text value = NULL;

                        if(tagName == "customer")
                        {
                            // insert logic to retrieve custom tag
                            //
                            // As an example, here we use pattern matching to
                            // assign all entities with 'lon' in their name
                            // to the A-Z Inc. customer.
                            //
                            int count = MatchPattern(entityName, '(lon)');
                            if (count == 1)
                            {
                                value = "A-Z Inc., London";
                            }
                            else
                            {
                                // Not an A-Z Inc. device.
                                // If we leave value as NULL then no
                                // 'customer' custom tag will be
                                // created, however in this example we
                                // want such entities tagged with
                                // 'none'..
                                value = "none";
                            }
                        }
```

```
                    SetReturnValue(value);
                }
            }
```

Nota: Sólo las entidades que pasan los criterios configurados en la tabla `disco.filterCustomTags` o `disco.ipCustomTags` se pasan al agrupador `GetCustomTag.stch`.

Resultados

La siguiente etiqueta de par nombre-valor personalizada se añade a todas las direcciones IP de la subred 172.20.3.0/24:

Tabla 60. Datos añadidos a entidades

Dirección IP	Nombre	Valor
172.20.3.0/24	Cliente	A-Z Inc., London

Qué hacer a continuación

Ahora debe configurar el archivo de configuración `DbEntityDetails.cfg` para asegurarse de que, tras el descubrimiento, la tabla entityDetails de base de datos de topología de NCIM se actualiza con las etiquetas personalizadas.

Ejemplo del agrupador GetCustomTag

Este ejemplo explica cómo un agrupador GetCustomTag de ejemplo recupera el nombre de cliente asociado con un dispositivo.

¿Cómo se llama al agrupador GetCustomTag?

Al agrupador `GetCustomTag.stch` lo llama el agrupador `AddCustomTags.stch`. No necesita modificar el agrupador AddCustomTags. Necesita modificar el agrupador GetCustomTag.

El agrupador AddCustomTags recorre en bucle las etiquetas y las entidades de las tablas disco.ipCustomTags y disco.filterCustomTags. Si, en cualquiera de estas tablas, se establece el campo `m_StitcherTagName`, el agrupador AddCustomTags llama al agrupador GetCustomTag y pasa el nombre de entidad correspondiente y el campo `m_StitcherTagName` como parámetros. El campo `m_StitcherTagName` conserva la parte del nombre de una etiqueta de par nombre-valor, por ejemplo, `Customer`.

Si el agrupador GetCustomTags devuelve un valor no NULL para una etiqueta o entidad, el agrupador AddCustomTags actualiza el objeto `m_ExtraInfo->m_CustomTags` en el registro de tablas workingEntities.finalEntity para la entidad. La etiqueta se utiliza como nombre de campo y el valor de retorno se utiliza como valor de campo. En la tabla de base de datos workingEntities.finalEntity, los datos pasan a la base de datos DNCIM, la base de datos ncimCache y la base de datos NCIM.

Nota: El agrupador AddCustomTags recupera el nombre de entidad realizando una búsqueda en la tabla workingEntities.finalEntity. El agrupador utiliza la dirección IP de la tabla disco.ipCustomTags o m_Filter como cláusula WHERE proporcionada en la tabla disco.filterCustomTags.

Descripción de un agrupador GetCustomTag de ejemplo

El agrupador GetCustomTag toma como entrada un único nombre de entidad y una etiqueta (el campo `m_StitcherTagName`). Escriba lógica personalizada en el agrupador para evaluar la parte de valor del par nombre-valor. De forma predeterminada, el agrupador contiene un código de ejemplo similar al descrito aquí. Puede personalizar este agrupador para que funcione con distintos pares de nombre-valor y cambiar la lógica definiendo la forma en que se calculará el valor.

Tabla 61. Descripción línea a línea de un agrupador GetCustomTag de ejemplo	
Números de línea	**Descripción**
10	Establezca el valor de la variable tagName del primer argumento recibido del agrupador AddCustomTags. Este valor es el nombre de la etiqueta para la que se va a evaluar el valor.
11	Establezca el valor de la variable entityName del primer argumento recibido del agrupador AddCustomTags. La variable entityName conserva el nombre de entidad asociado con la dirección IP para la que el agrupador evalúa el valor de una etiqueta de par nombre-valor.
13	Establezca la variable de valor en NULL. El agrupador devuelve la variable del valor y conserva el valor evaluado de la etiqueta del par nombre-valor.
15	Prueba para una etiqueta soportada. En este caso la etiqueta es `customer`. Puede añadir soporte para etiquetas personalizadas añadiendo más bloques `else if`.
16-35	El código de búsqueda de la etiqueta `customer`. Si el nombre de entidad contiene el patrón de texto `lon`, establezca la variable de valor en el nombre personalizado `A-Z Inc. London`, en caso contrario, establézcalo en `none`.
37	Devuelva el valor de la etiqueta.

```
UserDefinedStitcher
     {
         StitcherTrigger
         {
             // Called from another stitcher when tag criteria
             // is met
         }

         StitcherRules
         {
            text tagName = eval(text,'$ARG_1');
            text entityName = eval(text,'$ARG_2');

            text value = NULL;

            if(tagName == "customer")
            {
                // insert logic to retrieve custom tag
                //
                // As an example, here we use pattern matching
                // to assign all entities with 'lon'
                //  in their name to the A-Z Inc. customer.
                //
               int count = MatchPattern(entityName, '(lon)');
                if (count == 1)
                {
                    value = "A-Z Inc., London";
              }
                else
                {
                    // Not an A-Z Inc. device.
                    // If we leave value as NULL then no 'customer'
                    // custom tag will be created,
                    // however in this example we want
                    // such entities tagged with 'none'..
                    value = "none";
                }
            }

            SetReturnValue(value);
        }
    }
```

Almacenamiento de datos personalizados como pares nombre-valor en la tabla entityDetails

Si desea utilizar datos extra para añadirlos a informes, enriquecer datos de red, o visualizarlos en **Navegador de estructura**, puede almacenar datos personalizados como pares nombre-valor en la tabla de base de datos entityDetails existente. No necesita crear tablas de base de datos nuevas.

Acerca de esta tarea

La tabla de base de datos entityDetails es una tabla de base de datos de topología predeterminada. Puede añadir datos personalizados a esta tabla insertándolos como pares nombre-valor. Este método es más fácil que crear nuevas tablas de base de datos, pero menos eficientes si necesita seleccionar entidades basadas en los datos.

Consejo: Si desea utilizar los datos para el sondeo personalizado, encontrar dispositivos en la Vista de saltos o utilizarlos en la definición de vistas de red, cree tablas de base de datos nuevas. Utilice el procedimiento en: "Almacenamiento de datos personalizados en tablas de base de datos nuevas" en la página 419.

Para descubrir datos personalizados y almacenarlos como pares nombre-valor, necesita descubrir los datos, asegurarse de que los datos persisten a través de varios descubrimientos y configurar cómo se añaden los datos a la base de datos de descubrimiento DNCIM.

El flujo de datos para el descubrimiento de datos personalizados y su almacenamiento como pares nombre-valor es el siguiente:

1. Los datos se recuperan del origen (archivo sin formato, EMS u otro origen) mediante un agente de descubrimiento, recopilador o buscador.
2. Los pares nombre-valor se insertan en la tabla de base de datos workingEntities.finalEntity.
3. El proceso **ncp_disco** utiliza la tabla de base de datos de descubrimiento dbModel.entityDetails para rellenar la tabla entityDetails de la base de datos de descubrimiento DNCIM con información de la tabla workingEntities.finalEntity.
4. Los datos de la tabla entityDetails en DNCIM se copian automáticamente a la tabla entityDetails en NCIM y la tabla ncimCache.entityData.
5. Desde la tabla ncimCache.entityData, los datos están disponibles en la Pasarela de sucesos para el enriquecimiento de suceso. Si los sucesos se enriquecen con los datos, la información está disponible en el **Visor de sucesos**.
6. Desde la base de datos de topología NCIM, los datos están disponibles para **Navegador de estructura**.

La tabla siguiente muestra un ejemplo de la clase de datos que puede añadir a un dispositivo como par nombre-valor.

Tabla 62. Ejemplo de etiquetas de par nombre-valor

Dirección IP	Nombre	Valor
172.20.3.20	`cliente`	`acme`
172.20.3.20	`ubicación`	`london`

Importación de pares nombre-valor a la base de datos de descubrimiento DNCIM

Una vez que se han descubierto los pares nombre-valor, debe insertarse en la base de datos de descubrimiento DNCIM. Configure el archivo de configuración `DbEntityDetails.cfg` para que se inserten los pares nombre-valor en la base de datos de descubrimiento DNCIM.

Acerca de esta tarea

El proceso **ncp_disco** utiliza la tabla de base de datos de descubrimiento dbModel.entityDetails para rellenar la tabla entityDetails de la base de datos de descubrimiento DNCIM con información de la tabla workingEntities.finalEntity. Para configurar una inserción en la tabla dbModel.entityDetails, complete los pasos siguientes:

Procedimiento

1. Edite el archivo de configuración `DbEntityDetails.cfg`.

   Nota: La edición del archivo de configuración `ModelNcimDb.cfg` hace que sea más difícil migrar las personalizaciones. En su lugar, edite el archivo de configuración `DbEntityDetails.cfg`.
2. Añada una inserción en la tabla de base de datos dbModel.entityDetails para ampliar el filtro EntityType predeterminado.

   Sólo puede tener una correlación entityDetails por filtro EntityType. Por ejemplo, añada una correlación similar al código siguiente:

```
insert into dbModel.entityDetails
(
    EntityType,
    EntityDetails
)
values
(
    1,  -- chassis
    {
        NetworkEdge = "eval(text, '&m_ExtraInfo->m_NetworkEdge')",
        CustomerName = "eval(text, '&m_ExtraInfo->m_CustomerName')",
        CustomerType = "eval(text, '&m_ExtraInfo->m_CustomerType')"
    }
);
```

3. Guarde y cierre el archivo de configuración `DbEntityDetails.cfg`.

Resultados

La próxima vez que se ejecute un descubrimiento completo, los pares nombre-valor se insertan en la tabla entityDetails en la base de datos de descubrimiento DNCIM. Los datos de la tabla entityDetails en DNCIM se copian automáticamente a la tabla entityDetails en NCIM y la tabla ncimCache.entityData.

Qué hacer a continuación

Asegúrese de que los pares nombre-valor personalizados se conservan entre descubrimientos.

Conservación de pares nombre-valor personalizados entre descubrimientos

De forma predeterminada, los datos personalizados añadidos a la tabla dbModel.entityDetails utilizando inserciones en el archivo DbEntityDetails.cfg, se suprimen si no están presentes en el siguiente descubrimiento. Puede configurar que el descubrimiento conserve estos datos personalizados.

Acerca de esta tarea

Para configurar el descubrimiento para que conserve los pares nombre-valor personalizados que se añadieron a la tabla dbModel.entityDetails, habilite el valor KeepOldEntityDetails.

Si el valor KeepOldEntityDetails está habilitado, los datos se conservan en descubrimientos posteriores. Los valores se actualizan si se descubre información nueva.

Para habilitar el valor KeepOldEntityDetails, realice los pasos siguientes:

Procedimiento

1. Realice una copia de seguridad y edite el archivo `NCHOME/etc/precision/ModelSchema.cfg`.

2. Localice la inserción dentro de la tabla model.config y establezca el campo KeepOldEntityDetails en 1 (habilitado).

   Por ejemplo, la inserción podría tener el aspecto siguiente:

```
insert into model.config
(
    LingerTime,
    ChassisCreationEvents,
    IpInterfaceCreationEvents,
    MaintenanceStateEvents,
    ManagedStatusUpdateInterval,
    DeleteRenamedDevices,
    KeepOldEntityDetails
)
values
(
    3,
    0,
    0,
    0,
    30,
    1,
    1,
);
```

Almacenamiento de datos personalizados en tablas de base de datos nuevas

Si desea utilizar los datos para el sondeo personalizado, encontrar dispositivos en la vista de saltos o para utilizarlos en la definición de vistas de red, debe crear tablas de base de datos nuevas.

Acerca de esta tarea

Si desea utilizar los datos personalizados para aplicaciones que implican seleccionar entidades basadas en los datos personalizados, es eficiente utilizar tablas de base de datos personalizadas.

Consejo: Si desea utilizar los datos extra sólo para aplicaciones donde las entidades se seleccionaron en base a otros campos de base de datos, por ejemplo, en el enriquecimiento de suceso o su visualización en el Navegador de estructura, no necesita crear tablas de base de datos personalizadas. Puede almacenar los datos personalizados de forma más sencilla como pares nombre-valore en la tabla de base de datos entityDetails, siguiendo el procedimiento en: “Almacenamiento de datos personalizados como pares nombre-valor en la tabla entityDetails” en la página 417.

Para almacenar datos personalizados en tablas de base de datos nuevas, necesita realizar las siguientes tareas:

- Crear nuevas tablas en la base de datos de topología NCIM.
- Crear las mismas tablas en la base de datos de descubrimiento DNCIM.
- Descubrir los datos.
- Configurar cómo se añaden los datos a la base de datos de descubrimiento.

El flujo de datos para el descubrimiento de datos personalizados creando tablas de base de datos es como sigue:

1. Los datos se recuperan del origen (archivo sin formato, EMS u otro origen) mediante un recopilador o agente de descubrimiento.
2. Los datos se insertan en la tabla de base de datos workingEntities.finalEntity.
3. El proceso **ncp_disco** utiliza la tabla de base de datos de descubrimiento dbModel.entityMap para rellenar la nueva tabla personalizada en la base de datos de descubrimiento DNCIM con la información de la tabla workingEntities.finalEntity.
4. Los datos de la nueva tabla personalizada en DNCIM se copian automáticamente a la tabla equivalente en NCIM y la tabla ncimCache.entityData.

5. Desde la tabla ncimCache.entityData, los datos están disponibles en la Pasarela de sucesos para el enriquecimiento de suceso. Si los sucesos se enriquecen con los datos, la información está disponible en **Visor de sucesos**.
6. Desde la base de datos de topología NCIM, los datos están disponibles para **Vista de saltos de red**, **Vistas de red** y **Navegador de estructura**.

Creación de nuevas tablas en la base de datos de topología NCIM

Creación de nuevas tablas en la base de datos NCIM para contener los datos personalizados que desea descubrir.

Acerca de esta tarea

Si crea las tablas de base de datos NCIM primero, puede planear para qué desea utilizar los datos antes de configurar cómo se descubren.

Procedimiento

1. Defina la nueva tabla en NCIM utilizando la herramienta de línea de mandatos para la base de datos o **ncp_oql**.
2. Llame al primer campo de la nueva tabla `entityID` y defina el campo como clave foránea para la tabla entityData.

   La definición del campo `entityID` de esta forma enlaza la información extra sobre la entidad al registro de entidad NCIM principal. Si la entidad se elimina de la tabla entityData, los datos también se eliminan de la tabla personalizada.
3. Reinicie Network Manager.
4. Opcional: Inserte algunos datos de ejemplo en la nueva tabla y pruebe si es adecuada para su propósito.

Creación de nuevas tablas en bases de datos diferentes

La siguiente sentencia SQL de ejemplo muestra cómo crear una tabla personalizada `exampleCustomData` en NCIM para Db2. La tabla utilizada en el ejemplo se basa en la personalización dNCIM definida en el archivo `createCustomization.sql` proporcionado con Network Manager.

```
CREATE TABLE exampleCustomData
(
    entityId INTEGER NOT NULL,
    slaId   VARCHAR(255),
    customerId              VARCHAR(255),
    customerContact         VARCHAR(255),

    CONSTRAINT example_cd_pk PRIMARY KEY (entityId),

    CONSTRAINT excd_entData_fk FOREIGN KEY (entityId)
    REFERENCES entityData(entityId) ON DELETE CASCADE
);
```

La siguiente sentencia SQL de ejemplo muestra cómo crear una tabla personalizada `exampleCustomData` en NCIM para Oracle. La tabla utilizada en el ejemplo se basa en la personalización dNCIM definida en el archivo `createCustomization.sql` proporcionado con Network Manager.

```
CREATE TABLE exampleCustomData
(
    entityId NUMBER(10) NOT NULL,
    slaId   VARCHAR2(255),
    customerId              VARCHAR2(255),
    customerContact         VARCHAR2(255),
--
    CONSTRAINT              example_cd_pk PRIMARY KEY (entityId),
--
    CONSTRAINT excd_entData_fk FOREIGN KEY (entityId)
```

```
    REFERENCES entityData(entityId) ON DELETE CASCADE
);
```

Qué hacer a continuación

Ahora cree la misma tabla en la base de datos de descubrimiento DNCIM.

Actualización de dNCIM para almacenar datos personalizados

Actualice dNCIM para almacenar datos personalizados escribiendo en primer lugar un script de SQL para definir las tablas donde se almacenarán los datos personalizados.

Acerca de esta tarea

Se proporcionan los siguientes fragmentos de código de ejemplo para servir de base a la creación del script SQL y garantizar que se vuelvan a crear las tablas personalizadas definidas en el script si se elimina la base de datos de dNCIM. Puede utilizar estos fragmentos de código como punto de partida.

Código para definir las tablas de dNCIM personalizadas

Se proporciona un script SQL denominado `createCustomization.sql`, que se encuentra ubicado en `$NCHOME/precision/scripts/sql/sqlite/createCustomization.sql`. Este script contiene un ejemplo del SQL necesario para crear una tabla personalizada para almacenar datos personalizados:

```
CREATE TABLE dncim.exampleCustomData
(
    entityId                    INTEGER NOT NULL,
    slaId                       VARCHAR(255),
    customerId                  VARCHAR(255),
    customerContact             VARCHAR(255),

    CONSTRAINT example_cd_pk PRIMARY KEY (entityId),

    CONSTRAINT exCd_entData_fk FOREIGN KEY (entityId)
    REFERENCES entityData(entityId) ON DELETE CASCADE
);
```

Para actualizar dNCIM para almacenar datos personalizados, lleve a cabo los siguientes pasos:

Procedimiento

1. Modifique el script SQL de ejemplo `createCustomization.sql` para definir las tablas para almacenar los datos personalizados.
2. Guarde el archivo `$NCHOME/precision/scripts/sql/sqlite/createCustomization.sql`.
3. Elimine el directorio de bases de datos de dNCIM antiguo `$NCHOME/precision/embeddedDb/sqlite/ncp_disco.`*`domain_name`*`/`.

   Donde *domain_name* es el nombre del dominio correspondiente.

   El directorio de bases de datos de dNCIM de `$NCHOME/precision/embeddedDb/sqlite/ncp_disco.`*`domain_name`*`/` se volverá a crear cuando reinicie el motor de descubrimiento, ncp_disco. El nuevo directorio de bases de datos de dNCIM seleccionará los cambios que haya especificado en el script SQL `createCustomization.sql`.

Qué hacer a continuación

También debe configurar NCIM para almacenar los datos personalizados.

Correlación de los datos recuperados con las tablas de datos personalizados DNCIM

Especifique cómo deben almacenarse los datos personalizados del descubrimiento en la base de datos de topología correlacionando los datos personalizados con las tablas personalizadas añadidas a dNCIM y NCIM.

Acerca de esta tarea

Defina las inserciones dentro del archivo de configuración de $NCHOME/etc/precision/DbEntityDetails.cfg para especificar cómo correlacionar los datos personalizados con las tablas personalizadas dNCIM.

Ejemplo: Añadir un única fila de datos personalizados sobre una entidad existente

Para añadir una única fila de datos personalizados, añada la inserción adecuada al archivo de configuración $NCHOME/etc/precision/DbEntityDetails.cfg.

Inserción de los datos descubiertos utilizando el buscador de archivos, un agentes de descubrimiento o un recopilador

La siguiente inserción añade una única fila de datos personalizados sobre una entidad existente. En la correlación, los valores de la izquierda son los nombres de campo de una tabla nueva llamada exampleCustomData. La tabla exampleCustomData debe crearse en dNCIM y NCIM. Las sentencias de evaluación de la derecha toman los valores de la tabla de base de datos workingEntities.finalEntity. Estos datos deben descubrirse utilizando uno de los métodos de descubrimiento de datos personalizados y deben añadirse a la tabla de base de datos workingEntities.finalEntity.

En este ejemplo, los datos de acuerdo a nivel de servicio para una entidad existente se correlacionan con la tabla de dNCIM personalizada exampleCustomData.

En este ejemplo, los datos se han descubierto utilizando el buscador de archivos, un agente de descubrimiento o un recopilador. Los datos se añaden a los campos personalizados dentro del campom_ExtraInfo en la tabla de base de datos workingEntities.finalEntity.

```
insert into dbModel.entityMap
(
   EntityFilter,
   TableName,
   FieldMap
)
values
(
   "m_ExtraInfo->m_CustomerSLA IS NOT NULL",
   "exampleCustomData",
   {
       entityId           = "eval(int, '&m_EntityId')",
       slaId  = "eval(text, '&m_ExtraInfo->m_CustomerSLA')",
       customerId         = "eval(text, '&m_ExtraInfo->m_CustomerId')",
       customerContact    = "eval(text, '&m_ExtraInfo->m_CustomerContact')"
    }
 );
```

En la tabla siguiente se describe la inserción.

Tabla 63. Descripción de la inserción

Línea	Descripción
9	Añadir solo filas a la tabla personalizada donde el campo personalizado m_ExtraInfo->m_CustomerSLA de la entidad tenga un valor. De esta forma, se filtrarán las entidades que no estén asociadas con un acuerdo de nivel de servicio.
10	Añadir las filas a la tabla dNCIM personalizada exampleCustomData.

Tabla 63. Descripción de la inserción (continuación)	
Línea	**Descripción**
11-16	Añadir los siguientes datos a cada fila: • Identificador de entidad. • Identificador de acuerdo de nivel de servicio. • Identificador del cliente. • Contacto del cliente.

Inserción de los datos descubiertos utilizando tablas de etiquetas personalizadas

La siguiente inserción añade una única fila de datos personalizados sobre una entidad existente. En la correlación, los valores de la izquierda son los nombres de campo de una tabla nueva llamada `exampleCustomData`. La tabla `exampleCustomData` debe crearse en dNCIM y NCIM. Las sentencias de evaluación de la derecha toman los valores de la tabla de base de datos `workingEntities.finalEntity`. Estos datos deben descubrirse utilizando uno de los métodos de descubrimiento de datos personalizados y deben añadirse a la tabla de base de datos `workingEntities.finalEntity`.

En este ejemplo, los datos de acuerdo a nivel de servicio para una entidad existente se correlacionan con la tabla de dNCIM personalizada `exampleCustomData`.

En este ejemplo, los datos se han descubierto utilizando tablas de etiquetas personalizadas. Los datos descubiertos mediante tablas de etiquetas personalizadas se añaden a los campos personalizados dentro del campo `m_ExtraInfo->m_CustomTags` en la tabla de base de datos `workingEntities.finalEntity`.

```
insert into dbModel.entityMap
(
   EntityFilter,
   TableName,
   FieldMap
)
values
(
   "m_ExtraInfo->m_CustomTags->m_CustomerSLA IS NOT NULL",
   "exampleCustomData",
   {
       entityId           = "eval(int, '&m_EntityId')",
       slaId              = "eval(text, '&m_ExtraInfo
                             ->m_CustomTags->m_CustomerSLA')",
       customerId         = "eval(text, '&m_ExtraInfo
                              ->m_CustomTags->m_CustomerId')",
       customerContact    = "eval(text, '&m_ExtraInfo
                                 ->m_CustomTags->m_CustomerContact')"
    }
 );
```

En la tabla siguiente se describe la inserción.

Tabla 64. Descripción de la inserción	
Línea	**Descripción**
9	Solamente añadir filas a la tabla personalizada donde el campo personalizado `m_ExtraInfo->m_CustomTags->m_CustomerSLA` de la entidad tenga un valor. De esta forma, se filtrarán las entidades que no estén asociadas con un acuerdo de nivel de servicio.
10	Añadir las filas a la tabla dNCIM personalizada `exampleCustomData`.

Tabla 64. Descripción de la inserción (continuación)	
Línea	**Descripción**
11-16	Añadir los siguientes datos a cada fila: • Identificador de entidad. • Identificador de acuerdo de nivel de servicio. • Identificador del cliente. • Contacto del cliente.

Utilización de datos personalizados para enriquecer sucesos

Puede utilizar datos personalizados en el enriquecimiento de sucesos de forma similar a los datos normales.

Antes de empezar

Asegúrese de que está familiarizado con la forma de enriquecer sucesos con datos normales. Si desea utilizar un campo nuevo en la tabla de ObjectServer alerts.status para almacenar datos enriquecidos, primero debe crear el campo en ObjectServer antes de seguir los pasos que se indican a continuación.

Para obtener información sobre cómo añadir un campo personalizado a una tabla de ObjectServer, consulte *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Acerca de esta tarea

El nombre de la interfaz está disponible en la tabla de interfaz de la base de datos de topología de NCIM. Se puede acceder a este campo utilizando la memoria caché de NCIM, contenida en la tabla ncimCache.entityData.

Para obtener más información sobre la estructura de los campos y tablas de memoria caché de NCIM, consulte *Referencia de IBM Tivoli Network Manager*.

Los pasos siguientes explican cómo configurar este enriquecimiento de suceso extra.

Procedimiento

1. Edite el archivo de esquema de la pasarela de sucesos, `$NCHOME/etc/precision/EventGatewaySchema.cfg`, para permitir que la pasarela de sucesos actualice el nuevo campo. Recuerde añadir una coma al final de la línea que contiene el campo `NmosSerial`, antes de la línea que contiene el nuevo campo `InterfaceName`.
   Por ejemplo, para configurar la Pasarela de sucesos para actualizar un campo `customer` nuevo, añada el texto en negrita al filtro de sucesos saliente.

```
insert into config.ncp2nco
(
    FieldFilter
)
values
(
    [
        "NmosCauseType",
        "NmosDomainName",
        "NmosEntityId",
        "NmosManagedStatus",
        "NmosObjInst",
        "NmosSerial",
        "Customer"
    ]
);
```

Nota: Los campos que se añaden al filtro de sucesos de salida se añaden automáticamente al filtro de campos de entrada, config.nco2ncp, asegurando que se recupera el valor actual del campo. Esto permite al agrupador StandardEventEnrichment comprobar el valor del campo InterfaceName antes de actualizarlo. Esta técnica garantiza que la pasarela de sucesos no sigue actualizando el mismo valor.

2. Edite los agrupadores de la pasarela de sucesos para recuperar la información del cliente de la base de datos de topología y llenar el campo Customer.

   Una forma de hacerlo es añadiendo código al agrupador StandardEventEnrichment. El código es diferente dependiendo de si ha añadido datos personalizados como pares nombre-valor a la tabla entityDetails o ha creado una tabla de base de datos personalizada. La adición de este código al agrupador asegura que este procedimiento se realiza para todos los sucesos de topología que coinciden en una entidad. Añada este código al agrupador inmediatamente antes de la línea final, la llamada a `GwEnrichEvent( enrichedFields )` y después de determinar el valor entityType. Para obtener más información sobre la regla del agrupador `GwEnrichEvent()`, consulte *Referencia de IBM Tivoli Network Manager*.

   El código de ejemplo siguiente toma el valor `customerId` de la tabla entityDetails en los archivos ncimCache. Utilice este método si ha añadido datos personalizados sin crear tablas de base de datos NCIM nuevas.

```
if ( entityType == 1 )
{
     text customerName = @entity.entityDetails.customerId;

    if ( customerName <> eval(text, '&Customer') )
    {
          @enrichedFields.Customer = customerName;
    }
}
```

Tabla 65. Líneas de código relevantes para el ejemplo de nombre de interfaz

Números de línea	Descripción
1	Este enriquecimiento de suceso sólo es relevante para los sucesos de chasis. Compruebe que este suceso se relaciona con un chasis garantizando que el valor entityType es 1, y si es así, continúe el proceso.
3	Recupera los datos de cliente de la tabla entityDetails. **Nota:** Los campos dentro de la memoria caché de NCIM normalmente están en mayúscula, por ejemplo, `@mainNode.chassis.SYSLOCATION`. En este ejemplo `customerName` hay mayúsculas y minúsculas porque está en la tabla entityDetails.
5 - 8	Rellene únicamente el campo Customer si el valor ya no está presente en el suceso dentro del ámbito.

El código de ejemplo siguiente toma el valor `customerName` de la tabla `customer` en los archivos ncimCache. Utilice este método si ha añadido datos personalizados a tablas de base de datos NCIM nuevas.

```
if ( entityType == 1 )
{
     text customerName = @entity.customer.CUSTOMERNAME;

    if ( customerName <> eval(text, '&CustomerName) )
    {
          @enrichedFields.CustomerName = customerName;
    }
}
```

Visualización de datos personalizados en Navegador de estructura

Si añade datos personalizados utilizando pares nombre-valor en la tabla `entityDetails` o creando tablas de base de datos nuevas, puede ver los datos en **Navegador de estructura**.

Acerca de esta tarea

No necesita realizar ningún paso de configuración extra para ver datos personalizados en la tabla `entityDetails` en **Navegador de estructura**.

Para ver tablas de base de datos nuevas en **Navegador de estructura**, complete los pasos siguientes.

Procedimiento

1. Vaya al directorio `$NMGUI_HOMEprofile/etc/tnm/`.
2. Edite el archivo `ncimMetaData.xml` y ubique la sección que define el `entityType` con el que desea asociar los datos personalizados. Este `entityType` generalmente es 1, es decir, un chasis.
3. Añada los datos personalizados añadiendo líneas similares a las siguientes líneas en negrita:

```
    <entityMetaData entityType="1" table="physicalChassis" manager="PrecisionIP"
               entitySearch="true">

        <dataField tableAlias="e" dataType="int" column="entityId"
         entitySearch="false"/>
        <dataField tableAlias="e" dataType="str" column="entityName"
         entitySearch="false"/>
        <dataField tableAlias="e" dataType="str" column="displayLabel"
         entitySearch="false"/>
        <dataField tableAlias="e" dataType="bool" column="manual"
         entitySearch="true"/>

...
 <dataField tableAlias="x" dataType="str" column="customerId"/> <dataField tableAlias="x"
dataType="str" column="slaId"/> <dataField tableAlias="x" dataType="str"
column="customerContact"/>

        <fromTables>
            FROM _ncim_.entityData e

...
 LEFT OUTER JOIN _ncim_.exampleCustomData x ON x.entityId = e.entityId
```

En el ejemplo anterior, se utiliza una unión a la izquierda en la tabla personalizada. Esta unión garantiza que se visualizan datos para dispositivos que no tienen una entrada en la tabla de base de datos personalizada. Se listan los campos que se van a visualizar y `tableAlias` coincide con el alias dado en la sentencia de unión a la izquierda.

Utilización de datos personalizados en sondeo

Puede sondear un conjunto de dispositivos de red basados en los datos personalizados.

Acerca de esta tarea

Para definir un ámbito de sondeo basado en datos personalizados, complete los pasos siguientes.

Procedimiento

1. Cree una vista de ref basada en los datos personalizados que desea utilizar. Consulte la tarea “Visualización de datos personalizados en las vistas de topología” en la página 427 para obtener más información.
2. Cree o edite una política de sondeo. Especifique la nueva vista de red como ámbito para la política de sondeo.

Visualización de datos personalizados en las vistas de topología

Si ha añadido datos personalizados a una tabla de base de datos NCIM nueva, puede buscar en los datos personalizados y puede crear vistas de red con los datos personalizados.

Acerca de esta tarea

Es posible crear vistas de red basadas en datos personalizados que se han añadido como pares nombre-valor, pero estas vistas de red no son eficientes. Para obtener un mejor rendimiento, cree vistas de red basadas en datos personalizados únicamente que se añadieron a las tablas de base de datos nuevas.

Para habilitar la visualización de atributos personalizados en las vistas de topología, complete las tareas siguientes:

Procedimiento

1. Vaya al directorio `$NMGUI_HOMEprofile/etc/tnm/`.
2. Edite el archivo `ncimMetaData.xml` añadiendo líneas similares al siguiente ejemplo:

```
<entityMetaData table="customer" manager="AllManagers" entitySearch="true">
     <dataField dataType="str" column="customerName"/>
     <dataField dataType="str" column="customerType"/>
</entityMetaData>
```

   En el ejemplo anterior, se añade la tabla personalizada `customer` El atributo `manager` debe establecerse siempre en `AllManagers`. Establezca el atributo `entitySearch` en `true` para utilizar los datos en las búsquedas. Cada `dataField` es una sola columna de la tabla que se va a visualizar y debe tener el `dataType` correcto.

Resultados

Los operadores pueden seleccionar ahora la tabla cuando realicen un búsqueda en la **Vista de saltos** o cuando creen una vista de red dinámica.

Parte 3. Sondeo de la red

Sondea la red para recuperar información de dispositivos de red que pueden utilizarse para supervisar el comportamiento de los dispositivos.

Acerca de esta tarea

Para obtener más información acerca de las tareas de administrador relacionadas con el sondeo de red, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Capítulo 18. Acerca del sondeo de la red

Para sondear la red, Network Manager envía consultas periódicamente a los dispositivos en la red. Estas consultas determinan el comportamiento de los dispositivos, por ejemplo el estado operativo o los datos en las variables de la base de información de gestión (MIB) de los dispositivos.

El sondeo de red está controlado por políticas de sondeo. Las políticas de sondeo están formadas por:

- Definiciones de sondeo, que definen los datos que se recuperarán.
- Ámbito de sondeo, que incluye los dispositivos que se sondearán. El ámbito también puede modificarse a nivel de definición de sondeo para filtrar por clase de dispositivo e interfaz.
- Intervalo de sondeo y otras propiedades de sondeo.

Nota: Network Manager no sondea entidades que no son IP, como los dispositivos ópticos de capa 1 y los dispositivos de red de acceso mediante radio. Estos dispositivos se establecen automáticamente en el estado no gestionado.

Network Manager utiliza la sonda de condición de excepción IBM Tivoli Netcool/OMNIbus SNMP y la sonda Syslog para supervisar la red. Para ejecutar las sondas de Tivoli Netcool/OMNIbus, utilice el control de proceso de Tivoli Netcool/OMNIbus.

Para obtener más información sobre cómo utilizar el control de procesos de Tivoli Netcool/OMNIbus, consulte la publicación *IBM Tivoli Netcool/OMNIbus Administration Guide*.

El proceso ncp_poller controla el proceso de sondeo. El proceso ncp_poller almacena información de SNMP en la base de datos ncmonitor; el resto de datos están almacenados en la memoria.

Network Manager tiene un mecanismo de varios sondeadores para distribuir la carga. Si los sondeadores predeterminados no pueden atender a todas las demandas de sondeos de la red, es posible que necesite configurar sondeadores adicionales.

Tareas relacionadas

Administración de varios sondeadores
Si se necesitan más sondeadores para sondear la red, puede configurar nuevos sondeadores. Puede añadir o quitar sondeadores o utilizar un ID de sondeador para asociar un sondeador concreto con una política.

Políticas de sondeo

Las políticas de sondeo contienen todas las propiedades de una operación de sondeo de red. Especifican con qué frecuencia se sondea un dispositivo, el tipo de mecanismos de sondeo utilizados para realizar el sondeo y los dispositivos que se van a sondear.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Parámetros de política de sondeo

Utilice esta información para entender los parámetros de una política de sondeo.

Utilice la política de sondeo para definir los siguientes parámetros:

- Nombre de la política de sondeo
- Habilitación o inhabilitación: Se debe habilitar una política de sondeo para que el sondeo tenga lugar.
- Definiciones de sondeo: Si es necesario el filtrado a nivel de interfaz, la definición de sondeo debe contener algunos valores. Para cada definición de sondeo asociada con la política, puede especificar si almacenar datos sondeados para obtener informes históricos. Si se define este parámetro, los datos de almacenan en el esquema de base de datos ncpolldata.

Nota: Una política de sondeo puede tener una o más definiciones de sondeo asociadas. Esto puede ser útil, por ejemplo, cuando desee sondear información que es específica del proveedor del dispositivo. En estos casos debe configurar una definición de sondeo para cada proveedor (ya que cada proveedor puede tener MIB diferentes), pero solo tener una política con todas las definiciones de sondeo agregadas para obtener los datos de toda su red.

Restricción: El almacenamiento de datos de sondeo no está soportado para el Ping remoto de Cisco, el Ping remoto de Juniper y las Definiciones de sondeo de umbral genérico.

- Intervalo de sondeo
- Sondeador al que se asigna al política de sondeo, si está definido la característica de varios sondeadores.
- Ámbito. Contiene:
  - Vistas de red: Especifica las vistas de red que contienen los dispositivos que desea sondear.
  - Filtros de dispositivos: Refina la lista de dispositivos que desea sondear filtrándolos en los valores de los campos en la tabla `mainNodeDetails` de la base de datos NCIM (Network Connectivity and Inventory Model). Se pueden combinar varios filtros en una relación booleana.

Network Manager proporciona políticas y definiciones de sondeo predeterminadas. Puede tener otros sondeos disponibles si ha migrado valores de sondeo durante el proceso de instalación de Network Manager.

Ámbito de la política de sondeo

El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Una política de sondeo se puede describir como una serie de filtros. Si, en alguna fase, no se define un filtro, pasarán todos los dispositivos. La salida de este conjunto de filtros puede ser un conjunto de dispositivos o, si se ha definido un filtro de interfaz, un conjunto de interfaces de dispositivos. Esto aparece ilustrado en la siguiente figura.

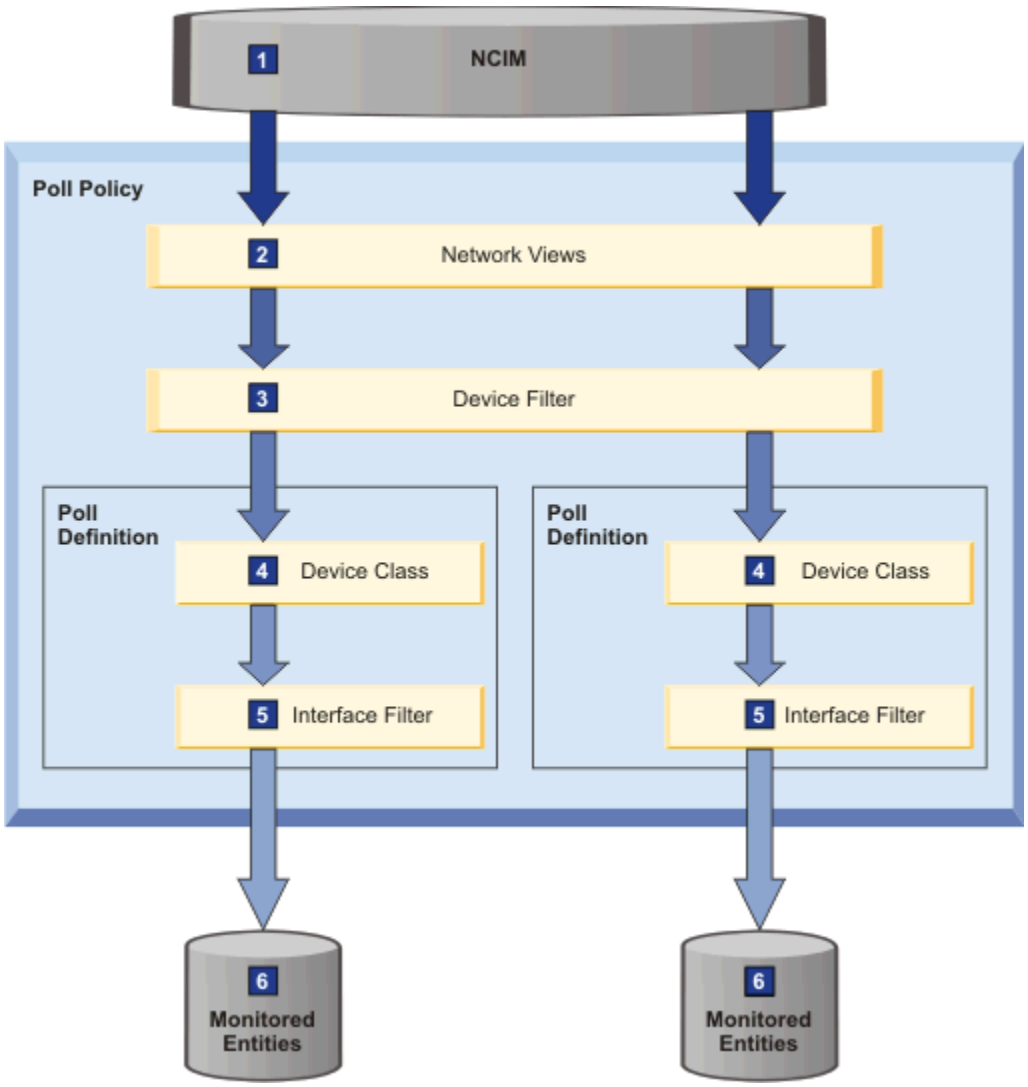


Figura 7. Ámbito de la política de sondeo

1 NCIM
Empieza con todos los dispositivos definidos para un único dominio en la base de datos de topología de NCIM.

2 Vistas de red
Si no hay vistas de red asociadas con las políticas de sondeo, el ámbito de la política se restringirá a los dispositivos que esas vistas contienen. Si no hay vistas de red asociadas a la política de sondeo, los dispositivos pasan esta fase. Esta segunda situación es equivalente a la selección de la opción **Todos los dispositivos** en el separador **Vistas de red** del **Editor de políticas de sondeo** y del **Asistente de políticas de sondeo**.

3 Filtro de dispositivo
Si hay un filtro de dispositivo definido para la política de sondeo, la política de sondeo se restringirá más al conjunto de dispositivos que coinciden con el filtro. Si no hay ningún filtro de dispositivo definido, los dispositivos que han pasado el filtro de vistas de red pasan esta fase. En este punto, hay un conjunto de dispositivos disponibles que están en el ámbito de esta política de sondeo. Para cada definición de sondeo que se asigna a la política puede haber un conjunto diferente de entidades de red que están en ámbito basadas en un filtrado más intenso.

4 Clase de dispositivo
Para cada definición de sondeo asignado a la política, la clase de dispositivo restringe los dispositivos que están en ámbito basándose en la selección de clase. Si no se han seleccionado clases de dispositivo no se llevará a cabo ningún tipo de filtrado.

5 Filtro de interfaz
Si se define un filtro de interfaz, presuponiendo que este filtro de interfaz es válido para el sondeo en cuestión, este filtro de interfaz se aplicará a todas las interfaces que contienen los dispositivos que han pasado los filtros anteriores. La salida es un conjunto de interfaces en ámbito. Si no define ningún filtro de interfaz, la salida es el conjunto de dispositivos que han pasado el filtro de Clase de dispositivo.

definiciones de sondeo

Las definiciones de sondeo determinan cómo sondear una entidad de red. Debe asociar cada política de sondeo al menos con una definición de sondeo. Una política de sondeo se puede asociar con varias definiciones de sondeo.

Referencia relacionada

Definiciones de sondeo predeterminadas

Network Manager proporciona un número de definiciones de sondeo predeterminadas que cumplen los requisitos de sondeo más comunes.

Parámetros de definición de sondeo

Utilice esta información para entender los parámetros de una definición de sondeo.

Network Manager proporciona políticas y definiciones de sondeo predeterminadas.

Utilice la definición de sondeo para definir los siguientes parámetros:

- Nombre de definición de sondeo
- Tipo de definición de sondeo: Esto determina el *mecanismo de sondeo* que utiliza la definición de sondeo. Se utilizan los siguientes mecanismos de sondeo:
  - Sondeo de ping
  - sondeo de SNMP
- Nivel de gravedad del suceso que se genera

  Importante: El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de los niveles de gravedad disponibles, consulte *Guía del usuario de IBM Tivoli Network Manager*.
- Breve descripción de la definición de sondeo.
- Solo tipo básico de definición de sondeo de umbral: etiqueta de datos. Una etiqueta que se utiliza para asociar datos que recopila una definición básica de sondeo de umbral con un informe. Al definir el informe, debe seleccionar los datos que va a presentar en el informe utilizando la etiqueta de datos. Esto habilita un informe para presentar datos marcados con la misma etiqueta de datos pero recopilados por más de una definición de sondeo. Para obtener una lista de informes de resumen, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.
- Tipo de definición de sondeo de umbral básico: unidades de datos.

  Recuentos
  Las definiciones de sondeos en las que un valor es un recuento de algún elemento. Los ejemplos son:
  - dot3StatsAlignmentErrors
  - ifInDiscards
  - ifInErrors

  En este tipo de definición de sondeo especifique una unidad de datos de #.

  Porcentajes
  Las definiciones de sondeos en las que el valor es un porcentaje. Los ejemplos son:
  - cpuBusyPoll
  - ciscoCPUTotal5min

En este tipo de definición de sondeo especifique una unidad de datos de %.

Unidades de medida específicas
Las definiciones de sondeos en las que un valor es una unidad de medida especificada. Los ejemplos son:

– memoryPoll

En este tipo de definición de sondeo especifique la unidad de medida adecuada. Por ejemplo, en el caso de memoryPoll, la unidad de medida adecuada es `bytes`.

- Ámbito de la definición de sondeo: de manera opcional la clase de dispositivo y los filtros de interfaz que se van a aplicar.
- Solo definiciones de sondeo de ámbito: los valores de umbral para generar y borrar una alerta.

Mecanismos de sondeo

Las definiciones de sondeo utilizan uno de dos posibles mecanismos de sondeo. sondeo de ping y sondeo de SNMP. Todas las definiciones de sondeo se basan en uno de estos mecanismos.

Sondeo de ping

El sondeo de ping determina la disponibilidad de un dispositivo de red o interfaz utilizando una solicitud de eco ICMP.

El proceso de ping garantiza que un dispositivo esté presente, vivo y se pueda contactar en la red enviando periódicamente un paquete ICMP a una dirección IP y esperando una respuesta.

Un sondeo de ping puede tener los siguientes resultados:

Satisfactorio
Se recibe una respuesta a los paquetes de ping. No se generan alertas.

Fallo
No se recibe ninguna respuesta a los paquetes de ping dentro del tiempo especificado en la definición de sondeo. Se generan alertas para las entidades de red que no responden.

Restaurar
Un dispositivo que no era alcanzable en el último intento de ping se vuelve alcanzable de nuevo. Se genera una alerta para borrar la alerta de fallo de ping.

El sondeo de ping se puede realizar en un chasis o en la interfaz de un dispositivo. En el caso de un chasis, se envían los paquetes ICMP a la dirección IP de un dispositivo de nodo principal. La dirección IP del nodo principal está asociada también con una interfaz. En el caso de las interfaces, los paquetes ICMP se envían a la dirección IP de cada interfaz. Por lo tanto, si habilita el sondeo de ping para el chasis y las interfaces, el tráfico en las direcciones IP del nodo principal se duplica.

Recuerde: De forma predeterminara, sólo la política de ping de chasis está habilitada en todos los dispositivos dentro de la topología de red descubierta, con la excepción de dispositivos de nodo final, como escritorios e impresoras.

Puede optar por almacenar los resultados de los sondeos de ping junto con las dos métricas siguientes:

- tiempo de ida y vuelta (RTT
- Pérdida de paquetes

El resultado de la operación ping siempre se almacena si está establecida la opción de almacenamiento. Las otras dos métricas son opcionales. El tiempo de RTT son los milisegundos entre el momento en que se envía el ping y el momento en que se procesa la respuesta, o -1 si no se recibe una respuesta. La pérdida de paquetes es un porcentaje de pérdidas de paquete, el cual se determina enviando varias solicitudes ping y cuadrando la pérdida de paquetes. El resultado del ping real es 0 si falla el ping o 100 si es correcto.

sondeo de SNMP

El sondeo de SNMP implica la recuperación de variables de base de información de gestión (MIB) de los dispositivos para determinar comportamientos con fallos o problemas de conexión. Los dispositivos o conexiones con fallos se diagnostican aplicando fórmulas predefinidas a las variables MIB extraídas.

Sondeo de estado de enlace

El sondeo de estado de enlace supervisa los cambios en el estado de las siguientes variables MIB: ifOperStatus e ifAdminStatus.

Si el valor de una de estas variables MIB cambia entre los intervalos de sondeo, se generará un suceso.

El estado inicial de los sondeos de estado de enlace se determina mediante los sucesos de estado de enlace existentes en la interfaz. Si no existen sucesos de estado de enlace, el estado inicial se establece en Clear (sin estado). Si hay varias interfaces en la red que no tienen establecido el estado administrativo, es posible que desee determinar el estado de interfaz inicial mediante el sondeo de la interfaz en su lugar. Para establecer el estado inicial de la interfaz utilizando un sondeo, establezca la opción de configuración `UseFirstPollForInitialState` del archivo de configuración `NcPollerSchema.cfg`.

Al almacenar datos de estado de enlaces de SNMP en la base de datos de sondeo NCPOLLDATA los datos no se almacenan con cada ciclo de sondeo. Los datos se almacenan al detectar un cambio de estado o tras 15 minutos, lo que suceda primero. Si se produce un cambio de estado se almacenan los valores anterior y actual. Si no hay cambio de estado entonces se almacena el valor actual.

La interfaz puede estar en uno de los siguientes estados:

- 3: disponible
- 2: la interfaz administrativa está inactiva
- 1: no disponible

Ejemplo

Si el valor de ifOperStatus era 1 (arriba) durante el sondeo anterior y cambia a 2 (abajo) en el sondeo actual, se generará un suceso.

La siguiente tabla muestra los sucesos que se generan como resultado de los cambios en el estado de interfaz. Además, se genera un suceso cuando un sondeo no puede devolver datos y se genera un suceso con una gravedad clara cuando posteriormente se realiza un sondeo con éxito en el mismo dispositivo.

Tabla 66. Sucesos que genera el sondeo de estado de enlace SNMP

Estado de la variable de MIB ifAdminStatus entre intervalos de sondeo	Estado de la variable de MIB ifOperStatus entre intervalos de sondeo	Suceso generado	Gravedad de suceso
Permanece en 1 (arriba)	Cambia de 1 (arriba) a 2 (abajo)	`La interfaz está inactiva.`	Menor
Permanece en 1 (arriba)	Cambia de 2 (abajo) a 1 (arriba)	`La interfaz se ha activado de nuevo.`	Borrar
Cambia de 1 (arriba) a 2 (abajo)	Cambia de 2 (abajo) a 1 (arriba)	`La interfaz se ha activado, aunque debería estar inactiva.`	Borrar
Cambia de 1 (arriba) a 2 (abajo)	Permanece en 2 (abajo)	`Un administrador ha confirmado que la interfaz debería estar inactiva.`	Borrar

Tabla 66. Sucesos que genera el sondeo de estado de enlace SNMP (continuación)			
Estado de la variable de MIB ifAdminStatus entre intervalos de sondeo	**Estado de la variable de MIB ifOperStatus entre intervalos de sondeo**	**Suceso generado**	**Gravedad de suceso**
Cambia de 2 (abajo) a 1 (arriba)	Cambia de 1 (arriba) a 2 (abajo)	`La interfaz está inactiva.`	Menor
Cambia de 2 (abajo) a 1 (arriba)	Permanece en 2 (abajo)	`Un administrador le ha ordenado a la interfaz que se active, pero no lo ha hecho.`	Menor

Tareas relacionadas

Cambio de las definiciones de sondeo de estado de enlace y ping remoto
Utilice el **Editor de definiciones de sondeos** para cambiar los siguientes tipos de definición de sondeo: Ping remoto de Cisco, ping remoto de Juniper y estado de enlace de SNMP.

Configuración del sondeo de estado de enlace
Puede especificar cómo el proceso de ncp_poller determina el estado inicial de los sondeos de estado de enlace cuando no hay ningún suceso existente.

Sondeo de ping remoto

Durante el sondeo de ping remoto, los MIB de dispositivo específicos de empresa se utilizan para verificar el estado de la vía de acceso entre dispositivos. En redes de Multi Protocol Label Switching (MPLS), el sondeo de ping remoto puede ser útil en el extremo de la red, donde el redireccionamiento MPLS automático es menos probable que ocurra. Los módulos MIB específicos permiten una estación de gestión para iniciar operaciones de ping de forma remota. Con las operaciones de ping remotas de SNMP puede supervisar errores de ping utilizando SNMP.

Durante las operaciones de sondeo de ping remoto, Network Manager indica a un direccionador de proveedor (PE) que haga ping periódicamente en el dispositivo CE (cliente) al que está adjunto. El resultado de esa operación de ping remoto proporciona información sobre si el direccionador desde el dispositivo PE al dispositivo CE está disponible o inactivo.

Restricción: Las operaciones de ping remoto están actualmente disponibles solo para dispositivos Cisco y Juniper.

Para obtener información sobre cómo definir contraseñas de SNMP, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Requisitos previos para el sondeo de ping remoto

Antes de que el sondeo de ping remoto se pueda realizar, se deben cumplir los siguientes requisitos previos:

- Debe tener acceso de escritura al dispositivo PE.
- Las vías de acceso de MPLS se deben haber descubierto y los datos transferidos a la base de datos NCIM. En NCIM, los datos se deben ubicar de la siguiente manera:
  - Las tablas VRF (Virtual Private Network Router Forwarding) deben estar listadas en la tabla VPNRouteForwarding.
  - Los enlaces de los dispositivos PE a CE deben estar listados en la tabla `connects`.
- Para el sondeo de ping remoto de Juniper, también necesita acceso a dispositivos de Juniper a través de VACM (View-Based Access Control Model).

Para obtener más información sobre la tabla VPNRouteForwarding y la tabla `connects`, consulte *Referencia de IBM Tivoli Network Manager*.

Sondeo de umbral

Durante el sondeo de umbral, se aplican fórmulas predefinidas a las variables de MIB seleccionadas y si la variable de MIB excede el umbral, se generará un suceso. Se genera un suceso de borrado cuando el valor de la variable de MIB cae por debajo del valor de umbral o cae por debajo de un valor de borrado diferente.

Puede definir dos umbrales:

Umbral de desencadenante
Necesaria: Se genera un suceso cuando el valor de la variable o variables de MIB excede el umbral.

Umbral de borrado
Opcional: Se genera un suceso de borrado cuando el valor de la variable de MIB cae por debajo del umbral.

Si no especifica un umbral de borrado, el suceso generado se borra automáticamente cuando el valor de la variable o variables de MIB ya no exceden el valor del umbral de generación.

Ejemplo de sondeo de umbral

El administrador de supervisión quiere identificar todos los direccionadores 29xx de Cisco que tienen un uso de CPU por encima del 75%. Al utilizar el sondeo de SNMP, el administrador puede supervisar el comportamiento de todos los direccionadores 29xx de Cisco en la red y establecer que un suceso se genera para cada uno de estos direccionadores cuando el uso de CPU supera el 75%. Se puede definir también un umbral del borrado para generar una notificación cuando el uso de la CPU cae por debajo del 60%; si no se especifica ningún umbral de borrado, se genera un suceso de borrado cuando el uso de la CPU ya no supera el 75%.

Sondeo de umbral básico y genérico

Utilice el *sondeo de umbral básico* para aplicar fórmulas simples a las variables de MIB o para filtrar el ámbito a nivel de dispositivo e interfaz. Para filtrar a nivel de interfaz, se debe configurar la definición de sondeo para el filtrado de interfaz.

Utilice el *sondeo de umbral genérico* para fórmulas complejas o para filtrar el ámbito solo a nivel de dispositivo.

Tipos de definición de sondeo

Cada definición de sondeo se basa en un tipo de definición de sondeo. Los tipos de definición de sondeo se pueden agrupar de acuerdo con el mecanismo de sondeo que utilizan.

Basándose en los mecanismos de sondeo, el tipo de definición de sondeo restringe el ámbito de la operación de sondeo en el que se utiliza.

Mecanismo de sondeo de ping

El mecanismo de sondeo de ping tiene los siguientes tipos de definición de sondeo:

Ping de chasis
Se utiliza para hacer ping a la interfaz de gestión de un dispositivo de red o la interfaz principal de un nodo final.

Ping de interfaz
Se utiliza para operaciones de ping en interfaces dentro de dispositivos. Una definición de sondeo de ping posee un filtrado de nivel de interfaz opcional.

Mecanismo de sondeo de SNMP

El mecanismo de sondeo de SNMP tiene los siguientes tipos de definición de sondeo:

Umbral genérico
Se utiliza para definir fórmulas para aplicar en variables de MIB. Una definición de sondeo de umbral consiste en los siguientes umbrales:

Umbral de desencadenante
Necesaria: Se genera un suceso cuando el valor de la variable o variables de MIB excede el umbral.

Umbral de borrado
Opcional: Se genera un suceso de borrado cuando el valor de la variable de MIB cae por debajo del umbral.

Umbral básico
Utilice un umbral básico para recopilar datos de sondeo para una única variable o expresión de MIB. Puede presentar los datos recopilados en los informes o mostrarlos en gráficos MIB. Se genera un suceso cuando se cumple la condición del umbral de desencadenante definida en la definición de sondeo y se borra cuando se cumple la condición de umbral de borrado.

Estado de enlace SNMP
Se utiliza para comprobar el estado administrativo y operativo. Una definición de sondeo de estado de enlace de SNMP posee un filtrado de nivel de interfaz opcional.

Ping remoto de Cisco
Se utiliza para comprobar la disponibilidad de los dispositivos utilizando los MIB específicos de Cisco.

Ping remoto de Juniper
Se utiliza para comprobar la disponibilidad de los dispositivos utilizando los MIB específicos de Juniper.

Etiquetas de datos

Las etiquetas de datos son un mecanismo que permite agrupar varias definiciones de sondeo que recopilan los mismos datos de sondeo dentro de un único informe. Las etiquetas de datos solo están disponibles en definiciones de sondeo de umbral básico. De forma predeterminada, la etiqueta de datos tiene el mismo nombre que la definición de sondeo, pero puede cambiarlo para que se ajuste a sus necesidades de etiquetado de datos.

Los siguientes ejemplos describen el uso de etiquetas de datos para habilitar un único informe para recuperar datos de varias definiciones de sondeo. Algunos informes de resumen de Network Manager utilizan etiquetas de datos de manera predeterminada. Para obtener una lista de informes de resumen, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Varias definiciones de sondeo específicas del proveedor

Un informe de resumen que presenta datos según porcentaje de uso de memoria en diferentes dispositivos de proveedor recuperan datos de sondeo de varias definiciones de sondeo específicas del proveedor. Definiendo una etiqueta de datos `memoryPercentageUsage` común dentro de cada definición de sondeo específica del proveedor, los datos recuperados por cada una de las definiciones de sondeo diferentes se pueden agrupar en un informe.

Definiciones de sondeo con diferentes umbrales y gravedades de suceso

Un informe de resumen que presenta datos en descartes de entrada en interfaces de dispositivo recupera los datos de varias definiciones de sondeo. Cada una de estas definiciones de sondeo recopilan los mismos datos de sondeo pero aplican umbrales y gravedades de suceso diferentes estos datos. Al definir una etiqueta de datos `ifInDiscards` común dentro de cada una de las definiciones de sondeo diferentes, los datos recuperados por cada una de estas definiciones de sondeo se pueden agrupar en un único informe.

Informe predeterminado para la correlación de etiquetas de datos

La siguiente tabla enumera los informes de resumen y las etiquetas de datos que estos informes de resumen utilizan de manera predeterminada.

Tabla 67. Informe predeterminado para la correlación de etiquetas de datos	
Informe	**etiqueta de datos**
Resumen de estado de direccionador	memoryPercentageUsage
	cpuBusy
Resumen de disponibilidad de dispositivos	systemUptime

Propiedades de sondeo de ping y métricas

Para sondeos de ping de chasis e interfaz, puede especificar propiedades de ping como los periodos de tiempo de espera y el número de reintento de ping. También puede recopilar métricas de ping, como el tiempo de respuesta y la pérdida de paquetes.

Puede especificar las siguientes propiedades de ping al crear un sondeo de ping de un chasis o interfaz.

Tiempo de espera excedido
Especifique, en milisegundos, cuánto tiempo desea que el proceso de sondeo espere una respuesta del dispositivo de destino antes de volver a enviar un nuevo paquete de ping.

Reintentos
Especifique cuántas veces desea que el proceso de sondeo intente hacer ping del dispositivo de destino antes de abandonar. Cuando la recopilación de métrica **Pérdida de paquetes** está habilitada, el proceso de sondeo envía este número de paquetes de ping independientemente de si se ha recibido una respuesta.

Tamaño de carga
Seleccione el tamaño del paquete ICMP que se utilizará para la solicitud de ping. Seleccione el valor predeterminado (32 bytes) o seleccione un tamaño personalizado. Este valor sustituye el valor de IcmpData en el archivo de configuración `NcPollerSchema.cfg`.

PRECAUCIÓN: El uso de un tamaño menor de 32 bytes puede provocar que se descarten paquetes.

Puede recopilar las siguientes métricas de ping al crear un sondeo de ping de un chasis o interfaz.

Tiempo de respuesta
Puede optar por recopilar datos sobre el tiempo de ida y vuelta en pruebas de ping. Esta representado en milisegundos. Cuando también se recopila la **Pérdida de paquetes**, se trata del tiempo de respuesta medio de cada prueba satisfactoria.

Pérdida de paquetes
Puede optar por recopilar datos sobre el número de paquetes de ping de los que el proceso de sondeo no ha recibido respuesta. Se almacena como un porcentaje.

Datos multibyte en definiciones de sondeo

Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Para obtener información sobre cómo configurar Network Manager para utilizar caracteres multibyte, consulte *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Capítulo 19. Habilitación e inhabilitación de sondeos

Para activar el sondeo de Network Manager, deberá habilitar las políticas de sondeo.

Antes de empezar

Consejo: Puede cambiar los valores de un sondeo antes de habilitarlo. Al crear sus propias políticas de sondeo, utilice las políticas de sondeo predeterminadas como ejemplos.

Acerca de esta tarea

De forma predeterminada, sólo está habilitado el sondeo de ping de chasis. Debe habilitar las demás políticas de sondeo que desee utilizar.

Nota: Si está habilitando políticas de sondeo para un gran número de dispositivos, es recomendable esperar hasta que las políticas de sondeo estén totalmente habilitadas antes de utilizar la GUI del Sondeo de redes para realizar cualquier cambio a las políticas de sondeo. Cualquier cambio en una política de sondeo hace que el Motor de sondeo, `ncp_poller`, reinicie la política de sondeo, y esto puede causar resultados impredecibles si `ncp_poller` estaba en el proceso de habilitación de políticas de sondeo. Utilice las columnas **Estado** y **Habilitado** en la sección **Configuración de políticas de sondeo** de **GUI de sondeo de red** para determinar si una política de sondeo se ha habilitado.

Para habilitar o inhabilitar sondeos:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Marque el recuadro de selección junto a la o las políticas requeridas.
3. Opcional: Para habilitar la o las políticas seleccionadas, haga clic en **Habilitar políticas seleccionadas**  .
4. Opcional: Para inhabilitar políticas, haga clic en **Inhabilitar políticas seleccionadas**  .
5. Haga clic en **Aceptar**.

Capítulo 20. Creación de sondeos

Cree sondeos si las políticas y definiciones de sondeo existentes no satisfacen sus requisitos. Personalice una copia de un sondeo existente o predeterminado o cree un nuevo sondeo a partir desde cero.

Acerca de esta tarea

Utilice el **Editor de políticas de sondeo** para crear una política de sondeo completa con varias definiciones de sondeo y recursos de ámbito completos. De forma alternativa, utilice el **Asistente de política de sondeo** para que le guíe en la creación de una política de sondeo; sin embargo, solo puede utilizar el asistente para crear una política de sondeo simple con una única definición de sondeo existente y recursos de ámbito limitados.

Recuerde: El sistema obliga a que los nombres de políticas de sondeo sean exclusivos dentro de un dominio.

Nota: Si está habilitando políticas de sondeo para un gran número de dispositivos, es recomendable esperar hasta que las políticas de sondeo estén totalmente habilitadas antes de utilizar la GUI del Sondeo de redes para realizar cualquier cambio a las políticas de sondeo. Cualquier cambio en una política de sondeo hace que el Motor de sondeo, `ncp_poller`, reinicie la política de sondeo, y esto puede causar resultados impredecibles si `ncp_poller` estaba en el proceso de habilitación de políticas de sondeo. Utilice las columnas **Estado** y **Habilitado** en la sección **Configuración de políticas de sondeo** de **GUI de sondeo de red** para determinar si una política de sondeo se ha habilitado.

Conceptos relacionados

Tipos de definición de sondeo
Cada definición de sondeo se basa en un tipo de definición de sondeo. Los tipos de definición de sondeo se pueden agrupar de acuerdo con el mecanismo de sondeo que utilizan.

Tareas relacionadas

Modificación de sondeos
Para modificar un sondeo, haga cambios en la política de sondeo, o en la definición de sondeo en la cual se basa el sondeo.

Modificación de definiciones de sondeo
Modifique las definiciones de sondeo existentes para personalizarlas según sus requisitos de sondeo. Las definiciones de sondeo se modifican en el **Editor de definiciones de sondeos**; los pasos que deberá seguir varían dependiendo del *tipo de definición de sondeo*.

Creación de sondeos adaptativos
Crear sondeos adaptativos para permitir que el sistema reaccione de forma dinámica a los sucesos de la red.

Creación de políticas de sondeo completas

Utilice el **Editor de políticas de sondeo** para crear una política de sondeo completa con varias definiciones de sondeo y características de ámbito completas.

Acerca de esta tarea

Al utilizar el **Editor de políticas de sondeo** puede crear una política de sondeo con las siguientes características:

- *Varias definiciones de sondeo*. Puede utilizar definiciones de sondeo existentes o puede crear nuevas definiciones de sondeo.
- *Network views*. Puede restringir el conjunto de dispositivos que se van a sondear a los que contienen las vistas de red seleccionadas.
- *Filtro de dispositivo*. Puede refinar aun más la lista de dispositivos seleccionados por las vistas de red utilizando este filtro simple en la tabla mainNodeDetails.

Nota: Puede restringir todavía más el ámbito de la política de sondeo filtrando el ámbito de cada una de las definiciones de sondeo incluidas dentro de esta política de sondeo. Puede filtrar el ámbito de las definiciones de sondeo por clase de dispositivo e interfaz.

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Cree una nueva política siguiendo estos pasos:
   - Para crear una nueva política desde cero, haga clic en **Agregar nueva**  . Se abre **Editor de políticas de sondeo**.
   - Para clonar una política existente, siga los siguientes pasos:
     a. En la columna **Seleccionar**, marque el recuadro de selección junto a la fila requerida y haga clic en **Copiar elementos seleccionados**  .
     b. Haga clic en **Aceptar**. El nombre de la copia utiliza el siguiente convenio: *nombrepolítica*_1, donde *nombrepolítica* es el nombre de la política copiada. Por ejemplo, si copió la política bgpPeerState, la copia se denominará bgpPeerState_1. Las políticas de sondeo están ordenadas alfabéticamente; por lo tanto, en este ejemplo, la copia bgpPeerState_1 aparecería en la lista después de la política copiada bgpPeerState.
     c. Haga clic en el nombre de la copia de la política de sondeo en la lista para abrir el **Editor de políticas de sondeo**.
3. Desde el separador **Propiedades de política de sondeo**, especifique un valor para cada propiedad:

   Nombre
   Escriba el nombre exclusivo que desea otorgar a la política de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Sondeo habilitado
   Marque este recuadro de selección para habilitar la política de sondeo. Asegúrese de que ha especificado como mínimo una definición de sondeo para la política antes de habilitarla.

   Definiciones de sondeo
   Utilice esta tabla para especificar una o varias definiciones de sondeo para la política de sondeo.

   Renovar 
   Renueve los datos de la tabla. Esto actualiza la tabla con cualquier cambio realizado por cualquier usuario desde que inició sesión o desde que hizo clic por última vez en **Renovar**.

   Suprimir elementos seleccionados 
   Suprime las filas seleccionadas.

   Agregar definiciones de sondeo a esta política 
   Abre el panel Definiciones de sondeo donde puede especificar una o varias definiciones de sondeo para agregar a la política de sondeo.

   Buscar 
   Buscar en la tabla texto especificado en el campo **Buscar**. De forma predeterminada, la búsqueda se realiza en todas las columnas de la tabla. Haga clic en la flecha hacia abajo a la izquierda del campo **Buscar** para limitar la búsqueda a una o varias columnas de la tabla.
   - Seleccione los recuadros de selección correspondientes a las columnas a las que desee limitar la búsqueda.
   - Seleccione **Todas las columnas** para revertir a las configuraciones de búsqueda predeterminadas.
   - Haga clic en **Aceptar** una vez que haya realizado la selección.

Tabla Definiciones de sondeo
La lista de definiciones de sondeo asociada a esta política de sondeo se presenta en una tabla. Puede realizar las acciones siguientes en esta tabla. Cualquier configuración realizada es válida sólo para esta sesión.

Ocultar barra de herramientas
Oculta la barra de herramientas. Si la barra de herramientas se oculta, haga clic en Mostrar barra de herramientas para mostrar la barra de herramientas.

Columna de ordenación
Haga clic en la cabecera de columna para ordenar dicha columna en orden descendente. Haga clic en la columna por segunda vez para ordenar la columna en orden ascendente. Los clics posteriores conmutarán la columna entre el orden descendente y el orden ascendente. El significado del orden ascendente y descendente varía según el tipo de datos de la columna:

Datos alfabéticos
El orden ascendente ordena los datos de a hasta z. El orden descendente ordena los datos de z hasta a.

Datos numéricos
El orden ascendente ordena los datos de menor a mayor. El orden descendente ordena los datos de mayor a menor.

Icono
El orden ascendente ordena los iconos del de mayor valor al de menor valor asociado con el icono. El orden descendente ordena los iconos del de menor valor al de mayor valor asociado con el icono. Los valores asociados con cada icono están listados a continuación.

Cambiar el tamaño de una columna
Haga clic y arrastre el separador de línea vertical a la derecha de la cabecera de columna.

Seleccionar todo/Desmarcar todo
Seleccione el recuadro de selección para seleccionar todas las filas. Si todas las filas están seleccionadas, desmarque el recuadro de selección para desmarcar todas las filas. Seleccione el recuadro de selección al lado de una fila para seleccionar una única fila o para desmarcar una única fila seleccionada.

¿Almacenar?
Seleccione el recuadro de selección para almacenar datos recopilados por esta definición de sondeo para fines de gráfica de MIB de informe e históricos.

Nota: Esta opción sólo está disponible para definiciones de sondeo de tipo Umbral básico.

Nombre
El nombre de una definición de sondeo asociada a esta política de sondeo. Haga clic en el nombre para editar las propiedades de esta definición de sondeo.

Tipo
El tipo de definición de sondeo.

Estado
Indica si la definición de sondeo es un error. La lista completa de valores se proporciona en la siguiente tabla.

Tabla 68. Estado de la definición de sondeo

Estado	Valor	Icono	Descripción
Desconocido	-1		El estado es desconocido porque la definición de sondeo no se ha ejecutado aún.
Sin errores	0		Ningún error. La definición de sondeo se ha ejecutado sin errores.

Tabla 68. Estado de la definición de sondeo (continuación)			
Estado	**Valor**	**Icono**	**Descripción**
Error	Mayor que 0		Hay un error en la definición de sondeo. La definición de sondeo no se puede ejecutar. El error debe arreglarse antes de que se utilice la definición de sondeo. Pase el ratón por encima del icono de estado para ver un mensaje emergente con una indicación del error.

Intervalo de sondeo
Especifique el intervalo requerido en segundos entre las operaciones de sondeo. Haga clic en las flechas para cambiar el valor.

Descripción
Descripción de la definición de sondeo.

Asignar a instancia de sondeador
Seleccione el sondeador en el que ejecutar la política de sondeo.

Regular política
El número de dispositivos en algunos tipos de vistas de red, especialmente en las vistas de red basadas en sucesos, puede fluctuar y aumentar. Para evitar que el motor de sondeo, ncp_poller, se sobrecargue por causa de un gran número de dispositivos en las vistas de red adjuntos a una política, puede poner un límite al número de dispositivos adjuntos a una política de sondeo. Este límite se denomina regulador de política.

Especifique el número máximo de entidades a las que limitar el sondeo. La política de sondeo sondeará a no más del número de entidades especificadas aquí.

Nota: Inhabilite la regulación de políticas estableciendo este valor en cero. Todas las nuevas políticas de sondeo tienen la regulación de políticas inhabilitada de forma predeterminada.

4. Si decide agregar una definición de sondeo a la política de sondeo, especifique las definiciones de sondeo que se van a agregar en el panel **Definiciones de sondeo** utilizando los siguientes botones y campos:

Renovar 
Renueve los datos de la tabla. Esto actualiza la tabla con cualquier cambio realizado por cualquier usuario desde que inició sesión o desde que hizo clic por última vez en **Renovar**.

Buscar 
Buscar en la tabla texto especificado en el campo **Buscar**. De forma predeterminada, la búsqueda se realiza en todas las columnas de la tabla. Haga clic en la flecha hacia abajo a la izquierda del campo **Buscar** para limitar la búsqueda a una o varias columnas de la tabla.

- Seleccione los recuadros de selección correspondientes a las columnas a las que desee limitar la búsqueda.
- Seleccione **Todas las columnas** para revertir a las configuraciones de búsqueda predeterminadas.
- Haga clic en **Aceptar** una vez que haya realizado la selección.

Tabla Definiciones de sondeo
La lista completa de definiciones de sondeo definidas en el sistema. Las definiciones de sondeo que ya están asociadas a esta política de sondeo tienen un recuadro de selección inhabilitado. Puede realizar las acciones siguientes en esta tabla. Cualquier configuración realizada es válida sólo para esta sesión.

Ocultar barra de herramientas 
Oculta la barra de herramientas. Si la barra de herramientas se oculta, haga clic en Mostrar barra de herramientas  para mostrar la barra de herramientas.

Columna de ordenación
Haga clic en la cabecera de columna para ordenar dicha columna en orden descendente. Haga clic en la columna por segunda vez para ordenar la columna en orden ascendente. Los clics posteriores conmutarán la columna entre el orden descendente y el orden ascendente. El significado del orden ascendente y descendente varía según el tipo de datos de la columna:

Datos alfabéticos
El orden ascendente ordena los datos de a hasta z. El orden descendente ordena los datos de z hasta a.

Datos numéricos
El orden ascendente ordena los datos de menor a mayor. El orden descendente ordena los datos de mayor a menor.

Icono
El orden ascendente ordena los iconos del de mayor valor al de menor valor asociado con el icono. El orden descendente ordena los iconos del de menor valor al de mayor valor asociado con el icono. Los valores asociados con cada icono están listados a continuación.

Cambiar el tamaño de una columna
Haga clic y arrastre el separador de línea vertical a la derecha de la cabecera de columna.

Seleccionar todo/Desmarcar todo
Seleccione el recuadro de selección para seleccionar todas las filas. Si todas las filas están seleccionadas, desmarque el recuadro de selección para desmarcar todas las filas. Seleccione el recuadro de selección al lado de una fila para seleccionar una única fila o para desmarcar una única fila seleccionada.

Nombre
El nombre de una definición de sondeo asociada a esta política de sondeo. Haga clic en el nombre para editar las propiedades de esta definición de sondeo.

Tipo
El tipo de definición de sondeo.

Descripción
Descripción de la definición de sondeo.

Almacenar datos de sondeo
Marque este recuadro de selección para almacenar los datos de sondeo para que puedan ser recuperados posteriormente para informes. Los datos se almacenan en la base de datos ncpolldata.

Restricción: El almacenamiento de datos de sondeo no está soportado para el Ping remoto de Cisco, el Ping remoto de Juniper y las Definiciones de sondeo de umbral genérico.

Intervalo
Especifique el intervalo requerido en segundos entre las operaciones de sondeo. Haga clic en las flechas para cambiar el valor.

5. Haga clic en el separador **Vistas de red** para establecer el ámbito de sondeo. En el árbol **Vistas de red**, seleccione los recuadros de selección de las vistas de red requeridas.

   El árbol **Vistas de red** muestra sólo aquellas vistas de red que pertenecen al dominio de red en el que se define esta política de sondeo. No aparecen vistas de red de dominios cruzados, ya que las políticas de sondeo se aplican a un solo dominio.

   Atención: Si selecciona la opción **Todos los dispositivos**, el sistema sondea todos los dispositivos que coinciden con el ámbito definido en el separador **Filtro de dispositivo**. Si no se establece ningún ámbito y selecciona la opción **Todos los dispositivos**, el sondeo que cree sondeará todos los dispositivos en el dominio de red actual.

   Puede filtrar todavía más el ámbito de la política de sondeo filtrando el ámbito de cada una de las definiciones de sondeo incluidas dentro de esta política de sondeo. Puede filtrar el ámbito de las definiciones de sondeo por clase de dispositivo e interfaz.

6. Opcional: Haga clic en el separador **Filtro de dispositivo**. Filtra dispositivos solo en la tabla de dispositivos mainNodeDetails. Defina el filtro utilizando uno de los siguientes métodos:
   - Escriba una sentencia WHERE de SQL en el campo de la columna Filtro.

     Nota: La sintaxis SQL es diferente para las distintas bases de datos. Consulte la documentación de la base de datos de topología que utilice para ver cuál es la sintaxis SQL correcta.
   - Haga clic en **Editar** para configurar el filtro utilizando el Constructor de filtros.
7. Opcional: En el **Constructor de filtros**, cree la consulta requerida en uno de los dos separadores y haga clic en **Aceptar**:
   - En el separador **Básico**, seleccione un campo, un comparador y escriba un valor. Utilice el carácter % como comodín. El campo está restringido a la tabla de atributo seleccionado.
   - En el separador **Avanzado**, escriba la sentencia WHERE de SQL requerida.

     Nota: La sintaxis SQL es diferente para las distintas bases de datos. Consulte la documentación de la base de datos de topología que utilice para ver cuál es la sintaxis SQL correcta.

   La información especificada en el separador **Básico** se escribe automáticamente en el separador **Avanzado**.
8. Opcional: Para agregar filtros a otras tablas de atributos, haga clic en **Agregar nueva fila** y repita los pasos para editar la fila y crear el filtro.
9. Opcional: Para combinar varios filtros, haga clic en **Todos** o **Cualquiera**:
   - **Todo**: Solo se sondearán aquellas entidades de red que coincidan con todos los filtros especificados. Por ejemplo, si crea dos filtros, una entidad de red deberá coincidir con ambos filtros.
   - **Cualquiera**: Se sondearán aquellas entidades de red que coincidan con cualquiera de los filtros especificados.
10. Haga clic en **Guardar**.

Conceptos relacionados

Ámbito de la política de sondeo

El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Tareas relacionadas

Ajuste del ancho de banda de sondeo

Puede configurar la cantidad de datos transferidos por el motor de sondeo, ncp _ poller, y la frecuencia. Es posible que desee ajustar el ancho de banda del sondeo para evitar la congestión de la red o reducir el impacto de un gran número de sucesos de sondeo que se producen de forma simultánea.

Creación de políticas de sondeo simples

Utilice el **Asistente de política de sondeo** para que le guíe en la creación de una política de sondeo; sin embargo, solo puede utilizar el asistente para crear una política de sondeo simple con una única definición de sondeo existente y características de ámbito limitadas.

Acerca de esta tarea

Al utilizar el **Asistente de política de sondeo** puede crear una política de sondeo simple con la siguiente definición de sondeo limitado y las características del ámbito.

- *Definición de sondeo único*. Puede utilizar solo una definición de sondeo existente único.
- *Network views*. Puede restringir el conjunto de dispositivos que se van a sondear a los que contienen las vistas de red seleccionadas.

  Restricción: El **Asistente de política de sondeo** no proporciona un filtro para matizar la lista de dispositivos que las vistas de red seleccionan.

Si necesita una política de sondeo completa con varias definiciones de sondeo y características de ámbito completas, utilice el **Editor de políticas de sondeo**.

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en **Iniciar Asistente de configuración de sondeos**  .
3. Haga clic en **Siguiente**. Complete la página **Detalles de política de sondeo** tal como se muestra a continuación:

   Nombre
   Especifique un nombre para la política de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Intervalo
   Especifique el intervalo requerido en segundos entre las operaciones de sondeo. Haga clic en las flechas para cambiar el valor.

   Sondeo habilitado
   Especifique si el sondeo debe estar habilitado. El sondeo estará habilitado de forma predeterminada. Para inhabilitar el sondeo, desmarque este recuadro de selección.

   Almacenar datos de sondeo
   Marque este recuadro de selección para almacenar los datos de sondeo para que puedan ser recuperados posteriormente para informes. Los datos se almacenan en la base de datos ncpolldata.

   Restricción: El almacenamiento de datos de sondeo no está soportado para el Ping remoto de Cisco, el Ping remoto de Juniper y las Definiciones de sondeo de umbral genérico.

   Definición
   Seleccione una definición de sondeo de la lista.

   Asignar a instancia de sondeador
   Seleccione el sondeador en el que ejecutar la política de sondeo.

   Regular política
   El número de dispositivos en algunos tipos de vistas de red, especialmente en las vistas de red basadas en sucesos, puede fluctuar y aumentar. Para evitar que el motor de sondeo, ncp_poller, se sobrecargue por causa de un gran número de dispositivos en las vistas de red adjuntos a una política, puede poner un límite al número de dispositivos adjuntos a una política de sondeo. Este límite se denomina regulador de política.

   Especifique el número máximo de entidades a las que limitar el sondeo. La política de sondeo sondeará a no más del número de entidades especificadas aquí.

   Nota: Inhabilite la regulación de políticas estableciendo este valor en cero. Todas las nuevas políticas de sondeo tienen la regulación de políticas inhabilitada de forma predeterminada.
4. Haga clic en **Siguiente**. En la página **Detalles de ámbito de política de sondeo**, marque los recuadros de selección de las vistas de red requeridas. En el árbol **Vistas de red**, seleccione los recuadros de selección de las vistas de red requeridas.

   El árbol **Vistas de red** muestra sólo aquellas vistas de red que pertenecen al dominio de red en el que se define esta política de sondeo. No aparecen vistas de red de dominios cruzados, ya que las políticas de sondeo se aplican a un solo dominio.

   Atención: Si selecciona la opción **Todos los dispositivos**, el sondeo que cree sondeará todos los dispositivos en el dominio de red actual.
5. Haga clic en **Siguiente**. En la página **Resumen de política de sondeo**, revise la información que ha especificado y haga clic en **Finalizar**.

Conceptos relacionados

Ámbito de la política de sondeo

El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Políticas de sondeo predeterminadas

Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Políticas de ping predeterminadas

Network Manager proporciona políticas de sondeo predeterminadas para operaciones de ping.

La tabla siguiente proporciona información sobre las políticas de sondeo predeterminadas.

Tabla 69. Políticas de sondeo de ping predeterminadas

Nombre de la política de sondeo	**Descripción**
Ping de chasis predeterminado	Utiliza la definición de sondeo Ping de chasis predeterminado para hacer ping a todos los dispositivos de red. El filtro de clase restringe el tipo de dispositivo al que se le ha hecho ping en la definición de sondeo de ping de chasis predeterminado. Esta es la única política de sondeo que está habilitada de forma predeterminada.
Ping de interfaz predeterminado	Utiliza la definición de sondeo Ping de interfaz determinado para realizar operaciones de ping en todas las interfaces que están dentro de un nodo principal con una dirección IP válida. Esta política utiliza la definición de sondeo Ping de interfaz determinado para hacer ping a interfaces en todos los dispositivos de red. Las interfaces a las que se hace ping está restringidas de acuerdo a lo siguiente: • El filtro de interfaz de la definición de sondeo. Se puede mejorar más añadiendo filtros de definición de sondeo extra. • El estado gestionado de cada interfaz. El estado de gestionado se puede cambiar mediante las GUI del navegador de estructura o Topoviz o mediante los scripts `ManagedNode.pl`, `UnManagedNode.pl` o `RemoveNode.pl`.
Ping de nodo final	Utiliza la definición de sondeo Ping de nodo final para realizar las operaciones de ping en todos los nodos finales, como definen los valores de clase.
ConfirmDeviceDown	Utilice la definición de sondeo Ping de chasis predeterminado con una frecuencia de sondeo aumentada y un alcance de política que incluye únicamente esos sucesos en los que se ha producido el suceso NmosPingFail. Esta política se utiliza como parte de un escenario de sondeo adaptativo y tiene el objetivo de acelerar el sondeo ping de dispositivos que no pudieron responder a un sondeo ping para identificar los dispositivos que estaban realmente inactivos.

Políticas de ping remotas predeterminadas

Network Manager proporciona políticas de ping remotas predeterminadas para operaciones de ping remotas. Estas políticas utilizan operaciones de grabación de SNMP para controlar las extensiones específicas del proveedor para DISMAN-PING-MIB.

La tabla siguiente proporciona información sobre las políticas de sondeo de ping remotas predeterminadas.

Tabla 70. Políticas de sondeo de ping remotas predeterminadas	
Nombre de la política de sondeo	**Descripción**
Ping remoto de Cisco	Utiliza la definición de sondeo de ping remoto de Cisco para comprobar la disponibilidad de las vías de acceso de MPLS entre los dispositivos Cisco Provider Edge (PE) y Customer Edge (CE) a través de operaciones de ping remotas de SNMP. Esta política de sondeo se aplica únicamente a dispositivos de Cisco.
Ping remoto de Juniper	Utiliza la definición de sondeo de ping remoto de Juniper para comprobar la disponibilidad de rutas MPLS entre los dispositivos PE de Juniper y CE de Juniper a través de SNMP operaciones de mesa de ping remoto, definida por los valores de la clase. Esta política de sondeo se aplica únicamente a dispositivos de Juniper.

Restricción: El almacenamiento de datos de sondeo no está soportado para el Ping remoto de Cisco, el Ping remoto de Juniper y las Definiciones de sondeo de umbral genérico.

Políticas de umbral SNMP predeterminadas

Se proporcionan políticas de sondeo de umbral SNMP predeterminadas con el producto. Estas políticas de sondeo están clasificadas como *básicas* o *genéricas*; además, algunas son específicas del proveedor.

Políticas de umbral

La siguiente tabla describe las políticas de sondeo de umbral de SNMP.

Tabla 71. Políticas de sondeo de umbral de SNMP básicas	
Nombre	**Descripción**
dot3StatsAlignmentErrors	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo dot3StatsAlignmentErrors para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
frCircuitReceivedBECNs	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo frCircuitReceivedBECNs para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
frCircuitReceivedFECNs	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo frCircuitReceivedFECNs para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.

Tabla 71. Políticas de sondeo de umbral de SNMP básicas (continuación)	
Nombre	**Descripción**
ifInDiscards	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo ifInDiscards para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
ifInErrors	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo ifInErrors para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
ifOutDiscards	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo ifOutDiscards para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
ifOutErrors	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo ifOutErrors para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
snmpInBandwidth	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo snmpInBandwidth para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
snmpOutBandwidth	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo snmpOutBandwidth para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
bgpPeerState	Tipo de definición de sondeo: Umbral genérico. Utiliza la definición de sondeo bgpPeerState para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
frCircuitState	Tipo de definición de sondeo: Umbral genérico. Utiliza la definición de sondeo frCircuitState para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
isdnLinkUp	Tipo de definición de sondeo: Umbral genérico. Utiliza la definición de sondeo isdnLinkUp para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.

Tabla 71. Políticas de sondeo de umbral de SNMP básicas (continuación)	
Nombre	**Descripción**
rebootDetection	Tipo de definición de sondeo: Umbral genérico. Utiliza la definición de sondeo rebootDetection para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase.
HighDiscardRate	Tipo de definición de sondeo: Umbral básico. Utiliza la definición de sondeo HighDiscardRate para realizar el sondeo de umbral en todos los dispositivos de red, como definen los valores de clase. La política sondea esta información cada 30 minutos.
ConfirmHighDiscardRate	Tipo de definición de sondeo: Umbral básico. Proporciona un sondeo de SNMP acelerado. Utiliza la definición de sondeo HighDiscardRate para realizar el sondeo de umbral en todos los dispositivos de red que tienen al menos una interfaz que infringe el 5% del umbral del porcentaje de descarte del paquete, y como definieron los valores de clase. Esta política se utiliza como parte de un escenario de sondeo y tiene el objetivo de acelerar el sondeo para confirmar las violaciones de umbral en las interfaces de dispositivo.

Políticas de sondeo de umbral de Foundry SNMP

La siguiente tabla describe las políticas de umbral de SNMP que suministran los dispositivos Foundry.

Tabla 72. Políticas de sondeo de umbral de SNMP para dispositivos Foundry	
Nombre	**Descripción**
snChasActualTemperature	Utiliza la definición de sondeo snChasActualTemperature para realizar el sondeo de umbral en todos los dispositivos Foundry, como definen los valores de clase.
snChasFanOperStatus	Utiliza la definición de sondeo snChasFanOperStatus para realizar el sondeo de umbral en todos los dispositivos Foundry, como definen los valores de clase.
snChasPwrSupplyOperStatus	Utiliza la definición de sondeo snChasPwrSupplyOperStatus para realizar el sondeo de umbral en todos los dispositivos Foundry, como definen los valores de clase.

Políticas de umbral de Cisco SNMP

La siguiente tabla describe las políticas de sondeo de umbral de SNMP que proporcionan los dispositivos Cisco.

Tabla 73. Políticas de sondeo de umbral de SNMP para dispositivos Cisco	
Nombre	**Descripción**
bufferPoll	Utiliza la definición de sondeo bufferPoll para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
ciscoEnvMonFanState	Utiliza la definición de sondeo ciscoEnvMonFanState para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
ciscoEnvMonSupplyState	Utiliza la definición de sondeo ciscoEnvMonSupplyState para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
ciscoEnvMonTemperature State	Utiliza la definición de sondeo ciscoEnvMonTemperatureState para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
memoryPoll	Utiliza la definición de sondeo ciscoMemoryPool para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
cpuBusyPoll	Utiliza la definición de sondeo cpuBusyPoll para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
locIfInCrcErrors	Utiliza la definición de sondeo locIfInCrcErrors para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
memoryPoll	Utiliza la definición de sondeo memoryPoll para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.
sysTrafficPoll	Utiliza la definición de sondeo sysTrafficPoll para realizar el sondeo de umbral en todos los dispositivos Cisco, como definen los valores de clase.

Políticas de estado de enlace SNMP predeterminadas

La política de sondeo de estado de enlace SNMP predeterminada utiliza la definición de sondeo SNMP `Link State` para comprobar estados operativos y administrativos de todos los dispositivos de red, como se define en la configuración de clases. Los sucesos se generan si hay cambios en el estado de la interfaz.

Capítulo 21. Creación de nuevas definiciones de sondeo

Utilice el **Editor de definiciones de sondeos** como guía para crear una nueva definición de sondeo.

Antes de empezar

Antes de crear o cambiar una definición de sondeo, vea una definición de sondeo existente para determinar si puede utilizarlo como una plantilla para crear una nueva definición de sondeo.

Recuerde: El sistema obliga a que los nombres de definiciones de sondeo sean exclusivos dentro de un dominio.

Acerca de esta tarea

Debido a que los tipos de definiciones de sondeo son diferentes, el **Editor de definiciones de sondeos** mostrará páginas diferentes en función del tipo de definición de sondeo seleccione.

Tareas relacionadas

Modificación de definiciones de sondeo
Modifique las definiciones de sondeo existentes para personalizarlas según sus requisitos de sondeo. Las definiciones de sondeo se modifican en el **Editor de definiciones de sondeos**; los pasos que deberá seguir varían dependiendo del *tipo de definición de sondeo*.

Creación de sondeos
Cree sondeos si las políticas y definiciones de sondeo existentes no satisfacen sus requisitos. Personalice una copia de un sondeo existente o predeterminado o cree un nuevo sondeo a partir desde cero.

Referencia relacionada

Definiciones de sondeo predeterminadas
Network Manager proporciona un número de definiciones de sondeo predeterminadas que cumplen los requisitos de sondeo más comunes.

Creación de definiciones de sondeo de umbral básico

Cree una definición de sondeo de umbral básico para ejecutar fórmulas sencillas en variables de MIB o para crear sondeos de umbrales con filtrado a nivel de interfaz..

Antes de empezar

Antes de crear o cambiar una definición de sondeo, vea una definición de sondeo existente para determinar si puede utilizarlo como una plantilla para crear una nueva definición de sondeo.

Acerca de esta tarea

Para crear una definición de sondeo de umbral básico:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en **Agregar nuevo**  .
   Aparecerá la página **Nueva selección de tipo de definición de sondeo**.
3. Seleccione `Umbral básico` en la lista y haga clic en **Aceptar**.

4. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

   ID de suceso
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

   - Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor POLL-*defsondeo*, donde *defsondeo* es el nombre de la definición de sondeo actual.
   - Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

   Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación POLL-*defsondeo*.

   Gravedad de suceso
   Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

   Descripción
   Escriba una breve descripción de la definición de sondeo.

   Etiqueta de datos
   Haga clic en la lista de etiqueta de datos y seleccione una de las etiquetas de datos de la lista. De forma predeterminada, la etiqueta de datos tiene el mismo nombre que la definición de sondeo actual. Para definir una etiqueta de datos nueva, seleccione <Agregar nueva etiqueta de datos>. El campo a la derecha de la lista se convertirá en activo. Escriba el nombre de la nueva etiqueta de datos en este campo.

   Unidades de datos
   Especifique las unidades de datos para esta definición de sondeo. La unidad de datos adecuada varía en función del tipo de datos de la definición del sondeo. Los siguientes son algunos tipos de datos y unidades de datos típicos que corresponden a dichos tipos de datos, junto con ejemplos de las definiciones de sondeos de Network Manager predeterminadas:

   Recuentos
   Las definiciones de sondeos en las que un valor es un recuento de algún elemento. Los ejemplos son:

   - dot3StatsAlignmentErrors
   - ifInDiscards
   - ifInErrors

   En este tipo de definición de sondeo especifique una unidad de datos de #.

   Porcentajes
   Las definiciones de sondeos en las que el valor es un porcentaje. Los ejemplos son:

   - cpuBusyPoll
   - ciscoCPUTotal5min

   En este tipo de definición de sondeo especifique una unidad de datos de %.

Unidades de medida específicas

Las definiciones de sondeos en las que un valor es una unidad de medida especificada. Los ejemplos son:

- memoryPoll

En este tipo de definición de sondeo especifique la unidad de medida adecuada. Por ejemplo, en el caso de memoryPoll, la unidad de medida adecuada es `bytes`.

5. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.

6. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

   El campo **Tabla** será rellenado con la tabla `interfaces`.

   Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.

7. Haga clic en el separador **Datos de sondeo** y especifique la fórmula requerida:

   - Para especificar un OID (identificador de objeto) de MIB, seleccione **OID único**. Especifique el valor actual o delta de la variable de MIB requerida y escriba la variable en el siguiente campo.
   - Para especificar una expresión compleja, seleccione **Expresión** y escriba la fórmula en el campo.

   Para seleccionar variables directamente del árbol MIB, haga clic en **Agregar objeto de MIB**. Desde el árbol de MIB, puede especificar el valor o valores actuales de la variable de MIB seleccionada o resuelva el valor actual de la variable en el índice SNMP.

8. Haga clic en el separador **Umbral** y especifique las fórmulas para desencadenar sucesos y borrar sucesos.

   El OID de MIB o expresión especificada en el separador **Datos de sondeo** se escribe automáticamente en las fórmulas.

   a) En el área **Umbral de desencadenante**, seleccione un comparador en la lista y escriba el valor que desea filtrar del OID de MIB.

   b) En el campo **Descripción**, escriba una descripción de la fórmula desencadenante. Agregue la variable de MIB a la descripción en paréntesis.

   La descripción que se muestra en el **Visor de sucesos** cuando se genera un suceso.

   Por ejemplo:

   ```
   CPU usage high (avgBusy5=)
   ```

   c) Para insertar la sentencia eval subyacente en la descripción, posicione el cursor antes del paréntesis de cierre, haga clic en **Agregar objeto de MIB** y navegue hasta la variable especificada. Especifique si el valor actual o anterior de la variable debe evaluarse, o si el valor será resuelto en el índice SNMP y haga clic en **Aceptar**.

   La sentencia está insertada, por ejemplo:

   ```
   CPU usage high (avgBusy5=eval(text,"&SNMP.VALUE.sysName"))
   ```

   d) Repeat steps 6a to 6c for the **Clear Threshold** area.

9. Haga clic en **Guardar**.

Conceptos relacionados

Datos multibyte en definiciones de sondeo
Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Ámbito de la política de sondeo
El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Referencia relacionada

Ejemplo de expresión de umbral básico
Utilice este ejemplo de expresión de umbral básico para entender cómo componer expresiones complejas de umbral básico.

Creación de definiciones de sondeo de umbral genérico

Utilice el **Editor de definición de sondeo** para crear nuevas definiciones de sondeo de umbral genérico.

Acerca de esta tarea

Cuando se crea una definición de umbral genérico, establecerá fórmulas y combinará fórmulas.

Para crear una definición de sondeo de umbral genérico:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en **Agregar nuevo**  .
   Aparecerá la página **Nueva selección de tipo de definición de sondeo**.
3. Seleccione `Umbral genérico` en la lista y haga clic en **Aceptar**.
4. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

   ID de suceso
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

   - Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor `POLL-`*`defsondeo`*, donde *defsondeo* es el nombre de la definición de sondeo actual.
   - Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

   Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación `POLL-`*`defsondeo`*.

   Gravedad de suceso
   Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

Descripción
Escriba una breve descripción de la definición de sondeo.

5. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

   Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.

6. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

   El campo **Tabla** será rellenado con la tabla `interfaces`.

   Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.

7. Haga clic en **Umbral de desencadenante**. Construya la fórmula que especifica el umbral utilizando uno de los siguientes métodos:
   - En el área **Básica**, utilice los campos y opciones para construir una fórmula. Para seleccionar valores en el árbol de MIB, haga clic en **Abrir árbol de MIB**.
   - En el área **Avanzada**, escriba la sentencia **`eval`** requerida en OQL (lenguaje de consulta de objetos).

8. Especifique el mensaje que se muestra en el **Visor de sucesos** para el suceso generado:
   a) En el campo **Descripción de suceso**, escriba el mensaje.
   b) Para insertar las variables de MIB en el campo, haga clic en **Abrir árbol de MIB**. Establezca el mensaje para que incluya el valor actual o anterior de SNMP, o el índice de SNMP y haga clic en **Aceptar**.

9. Necesario: Haga clic en el separador **Umbral de borrado**. Cada definición de umbral de la encuesta genérica requiere un umbral claro. Construya la fórmula que especifica el umbral utilizando uno de los siguientes métodos:
   - En el área **Básica**, utilice los campos y opciones para construir una fórmula. Para seleccionar valores en el árbol de MIB, haga clic en **Abrir árbol de MIB**.
   - En el área **Avanzada**, escriba la sentencia **`eval`** requerida en OQL (lenguaje de consulta de objetos).

   Consejo: Si desea borrar el umbral de forma manual, cree un umbral de borrado que no pueda alcanzarse.

10. Especifique el mensaje que se muestra en el **Visor de sucesos** para el suceso generado:
    a) En el campo **Descripción de suceso**, escriba el mensaje.
    b) Para insertar las variables de MIB en el campo, haga clic en **Abrir árbol de MIB**. Establezca el mensaje para que incluya el valor actual o anterior de SNMP, o el índice de SNMP y haga clic en **Aceptar**.

11. Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Qué hacer a continuación

La definición de sondeo se agrega al final de la lista.

Conceptos relacionados

Datos multibyte en definiciones de sondeo
Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Ámbito de la política de sondeo
El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Referencia relacionada

Ejemplo de expresión de umbral genérico
Utilice este ejemplo de expresión de umbral genérico para entender cómo componer expresiones complejas de umbral básico.

Creación de las definiciones de sondeo de ping de interfaz y chasis

Utilice el **Editor de definiciones de sondeos** para crear los tipos de definición de sondeo de ping de interfaz y chasis. Los resultados del sondeo de ping se almacenan como 0 si la operación ping falla o 100 si la operación ping es satisfactoria.

Acerca de esta tarea

Los pasos para crear una definición de sondeo basada en todos los tipos de definiciones de sondeo anteriores son idénticos a estos.

Para crear una definición de sondeo de ping de interfaz o chasis:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en **Agregar nuevo**  .
   Aparecerá la página **Nueva selección de tipo de definición de sondeo**.
3. Seleccione Ping de chasis o Ping de interfaz en la lista.
4. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

   ID de suceso
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

   - Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor POLL-*defsondeo*, donde *defsondeo* es el nombre de la definición de sondeo actual.
   - Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

   Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación POLL-*defsondeo*.

   Gravedad de suceso
   Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado

de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

Descripción
Escriba una breve descripción de la definición de sondeo.

5. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.

6. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

   El campo **Tabla** será rellenado con la tabla `interfaces`.

   Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.

7. Haga clic en el separador **Ping** y cumplimente los campos en **Propiedades de ping** tal como se muestra a continuación:

   Tiempo de espera excedido
   Especifique, en milisegundos, cuánto tiempo desea que el proceso de sondeo espere una respuesta del dispositivo de destino antes de volver a enviar un nuevo paquete de ping.

   Reintentos
   Especifique cuántas veces desea que el proceso de sondeo intente hacer ping del dispositivo de destino antes de abandonar. Cuando la recopilación de métrica **Pérdida de paquetes** está habilitada, el proceso de sondeo envía este número de paquetes de ping independientemente de si se ha recibido una respuesta.

   Recopilar métricas de ping

   Tiempo de respuesta
   Marque el recuadro para recopilar el tiempo que llevan los dispositivos en responder a una solicitud de ping. El tiempo de respuesta se almacena como el tiempo en milisegundos entre el momento en que se ha enviado la solicitud de ping y el momento en que se ha procesado la respuesta. Si no se recibe ninguna respuesta, se almacena el valor de -1.

   Pérdida de paquetes
   Marque el recuadro para recopilar datos sobre los paquetes perdidos. La pérdida de paquetes se almacenan como el porcentaje de paquetes perdidos, que a su vez viene determinado por el envío de varias solicitudes de ping y el cálculo del porcentaje de paquetes perdidos.

   Tamaño de carga
   Seleccione el tamaño del paquete ICMP que se utilizará para la solicitud de ping. Seleccione el valor predeterminado (32 bytes) o seleccione un tamaño personalizado. Este valor sustituye el valor de IcmpData en el archivo de configuración `NcPollerSchema.cfg`.

PRECAUCIÓN: El uso de un tamaño menor de 32 bytes puede provocar que se descarten paquetes.

8. Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Conceptos relacionados

Ámbito de la política de sondeo

El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Creación de definiciones de sondeo de estado de enlace y ping remoto

Utilice el **Editor de definiciones de sondeos** para crear nuevas definiciones de sondeo con los siguientes tipos de definición de sondeo: Ping remoto de Cisco, ping remoto de Juniper y estado de enlace de SNMP.

Acerca de esta tarea

Los pasos para crear una definición de sondeo basada en todos los tipos de definiciones de sondeo anteriores son idénticos a estos.

Para crear una definición de sondeo de ping remoto o una definición de sondeo de estado de enlace SNMP:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en **Agregar nuevo**  .
   Aparecerá la página **Nueva selección de tipo de definición de sondeo**.
3. Seleccione el tipo de definición requerido en la lista:
   - `Ping remoto de Cisco`
   - `Ping remoto de Juniper`
   - `Estado de enlace SNMP`
4. Haga clic en **Aceptar**.
5. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

   ID de suceso
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

   - Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor POLL-*defsondeo*, donde *defsondeo* es el nombre de la definición de sondeo actual.
   - Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

   Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación POLL-*defsondeo*.

   Gravedad de suceso
   Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

   Descripción
   Escriba una breve descripción de la definición de sondeo.
6. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.

7. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

   El campo **Tabla** será rellenado con la tabla `interfaces`.

   Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.

8. Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Conceptos relacionados

Ámbito de la política de sondeo
El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Definiciones de sondeo predeterminadas

Network Manager proporciona un número de definiciones de sondeo predeterminadas que cumplen los requisitos de sondeo más comunes.

La tabla siguiente describe las definiciones de sondeo predeterminadas que proporciona Network Manager.

Nota: Las definiciones de sondeo de umbral básico requieren valores de unidad de datos. La tabla incluye los valores de unidad de datos predeterminados para cada definición de sondeo de umbral básico.

Definiciones de sondeo de SNMP predeterminadas

bgpPeerState

Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación de estado similar de BGP. Surgirá una alerta cuando BGP (Border Gateway Patrol) busque cambiar a un estado no establecido. Esta definición de sondeo sondea la variable de MIB de bgpPeerState, que tiene la siguiente vía de acceso y OID:

Vía de acceso: `iso/org/dod/mgmt/mib-2/bgpPeerTable/bgpPeerEntry/bgpPeerState`
OID DE MIB 1.3.6.1.2.1.15.3.1.2

bufferPoll

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de límite de almacenamiento intermedio. Se genera una alerta cuando el número de elementos de almacenamiento intermedio libres está debajo de 100. Esta definición de sondeo sondea la variable de MIB de bufferElFree, que tiene la vía de acceso y OID siguientes:

Vía de acceso de MIB: `iso/org/dod/private/enterprises/cisco/local/bufferElFree`
OID DE MIB: 1.3.6.1.4.1.9.2.1.9

ciscoCPUTotal5min

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: %

Esta definición de sondeo define la comprobación de uso de CPU. Se genera una alerta cuando el valor de la variable de MIB de Cisco de cpmCPUTotal5min supera el 80%. Esta definición de sondeo

sondea la variable de MIB de cpmCPUTotal5min, que muestra el porcentaje ocupado de CPU general en el último periodo de cinco minutos. Este objeto deja en desuso el objeto avgBusy5 de OLD-CISCO-SYSTEM-MIB. La variable de MIB de cpmCPUTotal5min tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/private/enterprises/cisco/local/cpmCPUTotal5min`
OID DE MIB: 1.3.6.1.4.1.9.9.109.1.1.1.1.5

ciscoEnvMonFanState
Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación del estado del ventilador para dispositivos Cisco. Se genera una alerta si el estado cambia a cualquiera distinto a 1 (normal). Esta definición de sondeo sondea la variable de MIB de ciscoEnvMonFanState, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/cisco/ciscoMgmt/ciscoEnvMonMIB/ciscoEnvMonObjects/ciscoEnvMonFanStatusTable/ciscoEnvMonFanStatusEntry/ciscoEnvMonFanState`
OID DE MIB: 1.3.6.1.4.1.9.9.13.1.4.1.3

ciscoEnvMonSupplyState
Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación del estado del suministro de energía para dispositivos Cisco. Se genera una alerta si el estado cambia a cualquiera distinto a 1 (normal). Esta definición de sondeo sondea la variable de MIB de ciscoEnvMonSupplyState, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/cisco/ciscoMgmt/ciscoEnvMonMIB/ciscoEnvMonObjects/ciscoEnvMonSupplyStatusTable/ciscoEnvMonSupplyStatusEntry/ciscoEnvMonSupplyState`
OID DE MIB: 1.3.6.1.4.1.9.9.13.1.5.1.3

ciscoEnvMonTemperatureState
Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación del estado de la temperatura del ventilador para los dispositivos Cisco. Se genera una alerta si el estado cambia a cualquiera distinto a 1 (normal). Esta definición de sondeo sondea la variable de MIB de ciscoEnvMonTemperatureState, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/cisco/ciscoMgmt/ciscoEnvMonMIB/ciscoEnvMonObjects/ciscoEnvMonTemperatureStatusTable/ciscoEnvMonTemperateureStatusEntry/ciscoEnvMonTemperatureState`
OID DE MIB: 1.3.6.1.4.1.9.9.13.1.3.1.6

Ping remoto de Cisco
Tipo de definición de sondeo: Ping remoto de Cisco.

Esta definición de sondeo define operaciones de ping remoto que utilizan MIB específicas de Cisco.

cpuBusyPoll
Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de uso de CPU. Se genera una alerta cuando el valor de la variable de MIB de Cisco de avgBusy5 supera el 80%. Esta definición de sondeo sondea la variable de MIB de avgBusy5, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/private/enterprises/cisco/local/avgBusy5`
OID DE MIB: 1.3.6.1.4.1.9.2.1.58

Restricción: La variable de MIB de aveBusy5 no está soportada en algunos direccionadores de Cisco recientes. Para tales direccionadores, utilice la definición de sondeo de ciscoCPUTotal5min.

dot3StatsAlignmentErrors

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de tasas de error para las alineaciones. Se genera una alerta cuando la tasa de error supera el 0 por segundo. Esta definición de sondeo sondea la variable de MIB de dot3StatsAlignmentErrors, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/transmission/dot3/dot3StatsTable/dot3StatusEntry/dot3StatsAlignmentErrors`
OID DE MIB: 1.3.6.1.2.1.10.7.2.1.2

frCircuitReceivedBECNs

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de la congestión regresiva de Frame Relay para un identificador de conexión de enlace de datos (DLCI). Se genera una alerta cuando se reciben avisos de congestión regresiva para DLCI. Esta definición de sondeo sondea la variable de MIB de frCircuitReceivedBECNs, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/transmission/frameRelayDTE/frCircuitTable/frCircuitEntry/frCircuitReceivedBECNs`
OID DE MIB: 1.3.6.1.2.1.10.32.2.1.5

frCircuitReceivedFECNs

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de la congestión progresiva de Frame Relay para DLCI. Se genera una alerta cuando se reciben avisos de congestión progresiva para DLCI. Esta definición de sondeo sondea la variable de MIB de frCircuitReceivedFECNs, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/transmission/frameRelayDTE/frCircuitTable/frCircuitEntry/frCircuitReceivedFECNs`
OID DE MIB: 1.3.6.1.2.1.10.32.2.1.4

frCircuitState

Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación del estado del circuito de Frame Relay. Se genera una alerta cuando un circuito se vuelve inactivo. Para evitar la generación de alertas para circuitos que están inactivos al inicio, la definición buscará circuitos inactivos. Esta definición de sondeo sondea la variable de MIB de frCircuitState, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/transmission/frameRelayDTE/frCircuitTable/frCircuitEntry/frCircuitState`
OID DE MIB: 1.3.6.1.2.1.10.32.2.1.3

HighDiscardRate

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Se genera una alerta cuando la tasa de descarte de paquete en al menos una interfaz de un dispositivo supere el 5%. Esta definición de sondeo sondea las siguientes variables de MIB:

ifInDiscards

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInDiscards`
OID DE MIB: 1.3.6.1.2.1.2.2.1.13

ifInNUcastPkts

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInNUcastPkts`
OID DE MIB: 1.3.6.1.2.1.2.2.1.12

ifInUcastPkts

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInUcastPkts`
OID DE MIB: 1.3.6.1.2.1.2.2.1.11

ifInDiscards

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de la tasa de descarte de entrada. Se genera una alerta cuando la tasa supera el 0 por segundo. Esta definición de sondeo sondea la variable de MIB de ifInDiscards, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInDiscards`
OID DE MIB: 1.3.6.1.2.1.2.2.1.13

ifInErrors

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de la tasa de error de la interfaz de entrada. Se genera una alerta cuando la tasa supera el 0 por segundo. Esta definición de sondeo sondea la variable de MIB de ifInErrors, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB:`iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInErrors`
OID DE MIB: 1.3.6.1.2.1.2.2.1.14

ifOutDiscards

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de la tasa de descarte de salida. Se genera una alerta cuando la tasa supera el 0 por segundo. Esta definición de sondeo sondea la variable de MIB de ifOutDiscards, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifOutDiscards`
OID DE MIB: 1.3.6.1.2.1.2.2.1.19

ifOutErrors

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de la tasa de error para interfaces de salida. Se genera una alerta cuando la tasa supera el 0 por segundo. Esta definición de sondeo sondea la variable de MIB de ifOutErrors, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB:`iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifOutErrors`
OID DE MIB: 1.3.6.1.2.1.2.2.1.20

isdnLinkUp

Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación del estado de enlace de ISDN. Se genera una alerta cuando se activa un enlace ISDN. La activación de un enlace ISDN puede indicar que un enlace

primario correspondiente se ha desactivado. Esta definición de sondeo sondea las siguientes variables de MIB:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifOperStatus`
OID DE MIB: 1.3.6.1.2.1.2.2.1.8
Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifAdminStatus`
OID DE MIB: 1.3.6.1.2.1.2.2.1.7

Ping remoto de Juniper
Tipo de definición de sondeo: Ping remoto de Juniper.

Esta definición de sondeo define operaciones de ping remoto que utilizan MIB específicas de Juniper.

locIfInCrcErrors
Tipo de definición de sondeo: Umbral básico.

Unidades de datos: #

Esta definición de sondeo define la comprobación de redundancia cíclica de entrada (CRC)/ comprobación de error de alineación. Se genera una alerta cuando se producen los errores de alineación de CRC de entrada. Esta definición de sondeo sondea la variable de MIB de locIfInCRC, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/cisco/local/linterfaces/lifTable/lifEntry/locIfInCRC`
OID DE MIB: 1.3.6.1.4.1.9.2.2.1.1.12

memoryPoll
Tipo de definición de sondeo: Umbral básico.

Unidades de datos: Bytes

Esta definición de sondeo define la comprobación del límite de memoria. Se genera una alerta cuando la cantidad de memoria libre cae por debajo de los 100 bytes. Esta definición de sondeo sondea la variable de MIB de freeMem, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/cisco/local/lsystem/freeMem`
OID DE MIB: 1.3.6.1.4.1.9.2.1.8

rebootDetection
Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación de detección de rearranque de un dispositivo, donde se genera una alerta si un dispositivo se rearranca. El motivo del rearranque de un dispositivo puede ser que el subsistema de SNMP de un dispositivo se haya restablecido.

Consejo: Para supervisar el tiempo de actividad del sistema, cambie la variable de MIB de sysUpTime a la variable de MIB de hrSystemUptime. La variable de MIB de hrSystemUptime está disponible únicamente si HOSTRES-MIB está soportado por el dispositivo.

Esta definición de sondeo sondea la variable de MIB de sysUpTime, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/system/sysUpTime`
OID DE MIB: 1.3.6.1.2.1.1.3

snChasActualTemperature
Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación de temperatura para dispositivos Foundry. Se genera una alerta cuando la temperatura real del chasis supera el valor establecido para un aviso cerca del nivel de la temperatura. Esta definición de sondeo sondea las siguientes variables de MIB:

snChasActualTemperature

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/foundry/foundryProducts/switch/snChassis/snChassGen/snChasActualTemperature`
OID DE MIB: 1.3.6.1.4.1.1991.1.1.1.1.18

snChasWarningTemperature

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/foundry/foundryProducts/switch/snChassis/snChassGen/snChasWarningTemperature`
OID DE MIB: 1.3.6.1.4.1.1991.1.1.1.1.19

snChasFanOperStatus
Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación del estado del ventilador para dispositivos Foundry. Se genera una alerta cuando el estado del ventilador cambia de 2 (normal) a 3 (fallo). Esta definición de sondeo sondea la variable de MIB de snChasFanOperStatus, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/foundry/foundryProducts/switch/snChassis/snChasFan/snChasFanTable/snChasFanEntry/snChasFanOperStatus`
OID DE MIB: 1.3.6.1.4.1.1991.1.1.1.3.1.1.3

snChasPwrSupplyOperStatus
Tipo de definición de sondeo: Umbral genérico.

Esta definición de sondeo define la comprobación del estado del suministro de energía para dispositivos Foundry. Se genera una alerta cuando el estado del suministro de energía cambia de 2 (normal) a 3 (fallo). Esta definición de sondeo sondea la variable de MIB de snChasPwrSupplyOperStatus, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/private/enterprises/foundry/foundryProducts/switch/snChassis/snChasPwr/snChasPwrSupplyTable/snChasPwrSupplyEntry/snChasPwrSupplyOperStatus`
OID DE MIB: 1.3.6.1.4.1.1991.1.1.1.2.1.1.3

Estado de enlace SNMP
Tipo de definición de sondeo: Estado de enlace SNMP.

Esta definición de sondeo define la comprobación del estado de administración y operativo. Se genera una alerta si se produce una discrepancia entre los estados administrativos y operativos. Esta definición de sondeo sondea las siguientes variables de MIB:

ifAdminStatus

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifAdminStatus`
OID DE MIB: 1.3.6.1.2.1.2.2.1.7

ifOperStatus

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifOperStatus`
OID DE MIB: 1.3.6.1.2.1.2.2.1.8

snmpInBandwidth
Tipo de definición de sondeo: Umbral básico.

Unidades de datos: %

Esta definición de sondeo define la comprobación de la utilización del ancho de banda entrante. Se genera una alerta cuando el uso de ancho de banda entrante supera el 40%. Esta definición de sondeo sondea las siguientes variables de MIB:

ifInOctets

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInOctets`
OID DE MIB: 1.3.6.1.2.1.2.2.1.10

ifSpeed

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifSpeed`
OID DE MIB: 1.3.6.1.2.1.2.2.1.5

snmpOutBandwidth

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: %

Esta definición de sondeo define la comprobación de la utilización del ancho de banda de SNMP de salida. Se genera una alerta cuando la utilización del ancho de banda de SNMP de salida está por encima del 40% para una interfaz. Esta definición de sondeo sondea las siguientes variables de MIB:

ifOutOctets

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifOutOctets`
OID DE MIB: 1.3.6.1.2.1.2.2.1.16

ifSpeed

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/interfaces/ifTable/ifEntry/ifSpeed`
OID DE MIB: 1.3.6.1.2.1.2.2.1.5

sysUpTime

Tipo de definición de sondeo: Umbral básico.

Unidades de datos: Tiempo, milisegundos

Este sondeo recupera el valor de la variable de MIB de sysUpTime, que tiene la siguiente vía de acceso y OID:

Vía de acceso de MIB: `iso/org/dod/mgmt/mib-2/system/sysUpTime`
OID DE MIB: 1.3.6.1.2.1.1.3

Definiciones de sondeo de Ping predeterminadas

Ping de chasis predeterminado

Tipo de definición de sondeo: Ping de chasis.

Esta definición de sondeo define operaciones de ping para los dispositivos de nodo principal. Envía paquetes de ICMP a la dirección ID de nodo principal de un dispositivo.

Ping de interfaz predeterminado

Tipo de definición de sondeo: Ping de interfaz.

Esta definición de sondeo define operaciones de ping para interfaces dentro de dispositivos. Envía paquetes de ICMP a la dirección IP de cada interfaz.

Ping de nodo final

Tipo de definición de sondeo: Ping de chasis.

Esta definición de sondeo define operaciones de ping para nodos finales, como por ejemplo impresoras y estaciones de trabajo. Envía paquetes de ICMP a la dirección IP de cada nodo final.

Para cada una de estas definiciones de sondeo de ping, se pueden recopilar las siguientes métricas de ping: tiempo de respuesta y pérdida de paquete.

Ejemplo de umbrales de activador y borrado

Utilice las fórmulas de umbral de ejemplo para configurar los umbrales de activador y borrado para las definiciones de sondeo de umbral genérico.

Ejemplo de umbral de activador

El siguiente ejemplo provocaría suceso en los casos siguientes:

- Cuando el valor actual de la variable MIB `avgBusy5` MIB es igual o mayor al valor de la variable MIB `avgBusy6`

Para crear este umbral, especifique la siguiente información en el separador **Umbral de desencadenante** del **Editor de definiciones de sondeos**:

1. Seleccione **Básico**.
2. Especifique el primer umbral:
   a. Seleccione **Actual**.
   b. Haga clic en **Añadir objeto MIB**  .
   c. Expanda el **árbol de MIB** en la siguiente vía de acceso:

      ```
      iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy5
      ```

      Haga clic en **Insertar**
   d. Seleccione el comparador >=.
   e. Seleccione **actual**.
   f. Haga clic en **Añadir objeto MIB**  .
   g. Expanda el árbol de MIB en la siguiente vía de acceso:

      ```
      iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy6
      ```

      Haga clic en **Insertar**.
3. Especifique el mensaje que se visualiza en **Visor de sucesos** cuando surge el suceso:
   a. En el campo **Descripción del suceso**, escriba `CPU usage high (avgBusy5= .`
   b. Haga clic en **Añadir objeto MIB**  .
   c. Expanda el **árbol de MIB** en la siguiente vía de acceso:

      ```
      iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy5
      ```

   d. Seleccione **Valor SNMP actual** y haga clic en **Insertar**.
   e. Tipo >=.
   f. Haga clic en **Añadir objeto MIB**  .
   g. Expanda el **árbol de MIB** en la siguiente vía de acceso:

      ```
      iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy6
      ```

   h. Escriba).

   La descripción para la **Visor de sucesos** ahora debe leerse de la siguiente manera:

   ```
   CPU usage high (avgBusy5=eval(text,"SNMP.VALUE.avgBusy5")>=eval
   (text,"SNMP.VALUE.avgBusy6"))
   ```

Ejemplo de umbral de borrado

El siguiente ejemplo provoca un ejemplo de borrado en los casos siguientes:

- Cuando el valor de la variable de MIB avgBusy5 es menor de 80.

Para crear este umbral, especifique la siguiente información en el separador **Umbral de borrado** del **Editor de definición de sondeo**:

1. Seleccione **Básico**.
2. Especifique el umbral:
   a. Seleccione **Actual**.
   b. Haga clic en **Añadir objeto MIB**  .
   c. Expanda el **árbol de MIB** en la siguiente vía de acceso:

      ```
      iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy5
      ```

      Haga clic en **Insertar**
   d. Seleccione el comparador <=.
   e. Seleccione **Literal**.
   f. Escriba 80.
3. Especifique el mensaje que se visualiza en **Visor de sucesos** cuando surge el suceso:
   a. En el campo **Descripción del suceso**, escriba `CPU usage high (avgBusy5= .`
   b. Haga clic en **Añadir objeto MIB**  .
   c. Expanda el **árbol de MIB** en la siguiente vía de acceso:

      ```
      iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy5
      ```

   d. Seleccione **Valor SNMP actual** y haga clic en **Insertar**.
   e. Escriba <=.
   f. Escriba 80.
   g. Escriba `).`

   La descripción para la **Visor de sucesos** ahora debe leerse de la siguiente manera:

   ```
   CPU usage high (avgBusy5=eval(text,"SNMP.VALUE.avgBusy5")<=80)
   ```

Capítulo 22. Modificación de sondeos

Para modificar un sondeo, haga cambios en la política de sondeo, o en la definición de sondeo en la cual se basa el sondeo.

Conceptos relacionados

Políticas de sondeo
Las políticas de sondeo contienen todas las propiedades de una operación de sondeo de red. Especifican con qué frecuencia se sondea un dispositivo, el tipo de mecanismos de sondeo utilizados para realizar el sondeo y los dispositivos que se van a sondear.

definiciones de sondeo
Las definiciones de sondeo determinan cómo sondear una entidad de red. Debe asociar cada política de sondeo al menos con una definición de sondeo. Una política de sondeo se puede asociar con varias definiciones de sondeo.

Tareas relacionadas

Creación de sondeos
Cree sondeos si las políticas y definiciones de sondeo existentes no satisfacen sus requisitos. Personalice una copia de un sondeo existente o predeterminado o cree un nuevo sondeo a partir desde cero.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Modificación de políticas de sondeo

Utilice el **Editor de políticas de sondeo** para modificar los valores de políticas de sondeo existentes.

Antes de empezar

Nota: Si está habilitando políticas de sondeo para un gran número de dispositivos, es recomendable esperar hasta que las políticas de sondeo estén totalmente habilitadas antes de utilizar la GUI del Sondeo de redes para realizar cualquier cambio a las políticas de sondeo. Cualquier cambio en una política de sondeo hace que el Motor de sondeo, `ncp_poller`, reinicie la política de sondeo, y esto puede causar resultados impredecibles si `ncp_poller` estaba en el proceso de habilitación de políticas de sondeo. Utilice las columnas **Estado** y **Habilitado** en la sección **Configuración de políticas de sondeo** de **GUI de sondeo de red** para determinar si una política de sondeo se ha habilitado.

Acerca de esta tarea

Para cambiar una política de sondeo:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en la política de sondeo requerida.
   Aparecerá el **Editor de políticas de sondeo**; los valores de la política de sondeo seleccionada se cargan automáticamente en los campos.
3. En **Propiedades de política de sondeo**, especifique un valor para los siguientes campos:

   Nombre
   Escriba el nombre exclusivo que desea otorgar a la política de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

Sondeo habilitado
Marque este recuadro de selección para habilitar la política de sondeo. Asegúrese de que ha especificado como mínimo una definición de sondeo para la política antes de habilitarla.

Definiciones de sondeo
Utilice esta tabla para especificar una o varias definiciones de sondeo para la política de sondeo.

Renovar
Renueve los datos de la tabla. Esto actualiza la tabla con cualquier cambio realizado por cualquier usuario desde que inició sesión o desde que hizo clic por última vez en **Renovar**.

Suprimir elementos seleccionados
Suprime las filas seleccionadas.

Agregar definiciones de sondeo a esta política
Abre el panel Definiciones de sondeo donde puede especificar una o varias definiciones de sondeo para agregar a la política de sondeo.

Buscar 
Buscar en la tabla texto especificado en el campo **Buscar**. De forma predeterminada, la búsqueda se realiza en todas las columnas de la tabla. Haga clic en la flecha hacia abajo a la izquierda del campo **Buscar** para limitar la búsqueda a una o varias columnas de la tabla.

- Seleccione los recuadros de selección correspondientes a las columnas a las que desee limitar la búsqueda.
- Seleccione **Todas las columnas** para revertir a las configuraciones de búsqueda predeterminadas.
- Haga clic en **Aceptar** una vez que haya realizado la selección.

Tabla Definiciones de sondeo
La lista de definiciones de sondeo asociada a esta política de sondeo se presenta en una tabla. Puede realizar las acciones siguientes en esta tabla. Cualquier configuración realizada es válida sólo para esta sesión.

Ocultar barra de herramientas
Oculta la barra de herramientas. Si la barra de herramientas se oculta, haga clic en Mostrar barra de herramientas para mostrar la barra de herramientas.

Columna de ordenación
Haga clic en la cabecera de columna para ordenar dicha columna en orden descendente. Haga clic en la columna por segunda vez para ordenar la columna en orden ascendente. Los clics posteriores conmutarán la columna entre el orden descendente y el orden ascendente. El significado del orden ascendente y descendente varía según el tipo de datos de la columna:

Datos alfabéticos
El orden ascendente ordena los datos de a hasta z. El orden descendente ordena los datos de z hasta a.

Datos numéricos
El orden ascendente ordena los datos de menor a mayor. El orden descendente ordena los datos de mayor a menor.

Icono
El orden ascendente ordena los iconos del de mayor valor al de menor valor asociado con el icono. El orden descendente ordena los iconos del de menor valor al de mayor valor asociado con el icono. Los valores asociados con cada icono están listados a continuación.

Cambiar el tamaño de una columna
Haga clic y arrastre el separador de línea vertical a la derecha de la cabecera de columna.

Seleccionar todo/Desmarcar todo
Seleccione el recuadro de selección para seleccionar todas las filas. Si todas las filas están seleccionadas, desmarque el recuadro de selección para desmarcar todas las filas. Seleccione el recuadro de selección al lado de una fila para seleccionar una única fila o para desmarcar una única fila seleccionada.

¿Almacenar?
Seleccione el recuadro de selección para almacenar datos recopilados por esta definición de sondeo para fines de gráfica de MIB de informe e históricos.

Nota: Esta opción sólo está disponible para definiciones de sondeo de tipo Umbral básico.

Nombre
El nombre de una definición de sondeo asociada a esta política de sondeo. Haga clic en el nombre para editar las propiedades de esta definición de sondeo.

Tipo
El tipo de definición de sondeo.

Estado
Indica si la definición de sondeo es un error. La lista completa de valores se proporciona en la siguiente tabla.

Tabla 74. Estado de la definición de sondeo

Estado	Valor	Icono	Descripción
Desconocido	-1		El estado es desconocido porque la definición de sondeo no se ha ejecutado aún.
Sin errores	0		Ningún error. La definición de sondeo se ha ejecutado sin errores.
Error	Mayor que 0		Hay un error en la definición de sondeo. La definición de sondeo no se puede ejecutar. El error debe arreglarse antes de que se utilice la definición de sondeo. Pase el ratón por encima del icono de estado para ver un mensaje emergente con una indicación del error.

Intervalo de sondeo
Especifique el intervalo requerido en segundos entre las operaciones de sondeo. Haga clic en las flechas para cambiar el valor.

Descripción
Descripción de la definición de sondeo.

Asignar a instancia de sondeador
Seleccione el sondeador en el que ejecutar la política de sondeo.

Regular política
El número de dispositivos en algunos tipos de vistas de red, especialmente en las vistas de red basadas en sucesos, puede fluctuar y aumentar. Para evitar que el motor de sondeo, ncp_poller, se sobrecargue por causa de un gran número de dispositivos en las vistas de red adjuntos a una política, puede poner un límite al número de dispositivos adjuntos a una política de sondeo. Este límite se denomina regulador de política.

Especifique el número máximo de entidades a las que limitar el sondeo. La política de sondeo sondeará a no más del número de entidades especificadas aquí.

Nota: Inhabilite la regulación de políticas estableciendo este valor en cero. Todas las nuevas políticas de sondeo tienen la regulación de políticas inhabilitada de forma predeterminada.

4. Haga clic en el separador **Vistas de red**. En el árbol **Vistas de red**, seleccione los recuadros de selección de las vistas de red requeridas.

El árbol **Vistas de red** muestra sólo aquellas vistas de red que pertenecen al dominio de red en el que se define esta política de sondeo.

Atención: Si selecciona la opción **Todos los dispositivos**, el sistema sondea todos los dispositivos que coinciden con el ámbito definido en el separador **Filtro de dispositivo**. Si no se establece ningún ámbito y selecciona la opción **Todos los dispositivos**, el sondeo que cree sondeará todos los dispositivos en el dominio de red actual.

5. Opcional: Haga clic en el separador **Filtro de dispositivo**. Filtra dispositivos solo en la tabla de dispositivos mainNodeDetails. Defina el filtro utilizando uno de los siguientes métodos:
   - Escriba una sentencia WHERE de SQL en el campo de la columna Filtro.

     Nota: La sintaxis SQL es diferente para las distintas bases de datos. Consulte la documentación de la base de datos de topología que utilice para ver cuál es la sintaxis SQL correcta.
   - Haga clic en **Editar** para configurar el filtro utilizando el Constructor de filtros.
6. En el **Constructor de filtros**, cree la consulta requerida en uno de los dos separadores y haga clic en **Aceptar**:
   - En el separador **Básico**, seleccione un campo, un comparador y escriba un valor. Utilice el carácter % como comodín. El campo está restringido a la tabla de atributo seleccionado.
   - En el separador **Avanzado**, escriba la sentencia WHERE de SQL requerida.

     Nota: La sintaxis SQL es diferente para las distintas bases de datos. Consulte la documentación de la base de datos de topología que utilice para ver cuál es la sintaxis SQL correcta.

   La información especificada en el separador **Básico** se escribe automáticamente en el separador **Avanzado**.
7. Para agregar filtros a otras tablas de atributos, haga clic en **Agregar nueva fila** y repita los pasos para editar la fila y crear el filtro.
8. Para combinar varios filtros, haga clic en **Todos** o **Cualquiera**:
   - **Todo**: Solo se sondearán aquellas entidades de red que coincidan con todos los filtros especificados. Por ejemplo, si crea dos filtros, una entidad de red deberá coincidir con ambos filtros.
   - **Cualquiera**: Se sondearán aquellas entidades de red que coincidan con cualquiera de los filtros especificados.
9. Haga clic en **Guardar**.

Referencia relacionada

Políticas de sondeo predeterminadas

Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Política de sondeo de ejemplo

Utilice este ejemplo de política de sondeo personalizada para ayudarle a copiar una política existente y personalizarla para sondear dispositivos específicos en subredes de clase C.

Situación

Debe personalizar una política de sondeo para cumplir los siguientes requisitos:

- La política de sondeo debe comprobar la red para obtener los dispositivos en las subredes de clase C que tienen la dirección IP 9.1.2.* o 10.123.46*
- La política de sondeo debe comprobar la red en intervalos de 60 segundos
- La política de sondeo debe empezar sondeando la red una vez se haya guardado

Valores requeridos

Para crear un sondeo que responda a los requisitos descritos en la situación anterior, realice los siguientes cambios:

1. En la página **Configurar políticas de sondeo**, haga una copia de una política de sondeo, por ejemplo, la política ciscoMemoryPctgUsage. La copia de la política de sondeo aparece como una nueva fila en la tabla de política de sondeo.
2. Encuentre la fila que contiene la copia de la política de sondeo ciscoMemoryPctgUsage y haga clic en el nombre de la copia de la política de sondeo. Esto le permite editar la copia de la política de sondeo en el **Editor de políticas de sondeo**.
3. En el separador **Propiedades de política de sondeo**, realice los siguientes cambios:

   Nombre
   Escriba un nombre significativo, por ejemplo `ciscoMemoryPctgUsage para subredes de clase C con 9.1.2* y 10.123.46*`.

   Sondeo habilitado:
   Marque este recuadro de selección.

   Intervalo de sondeo
   En la tabla **Definiciones de sondeo**, desplácese por la pantalla y escriba `60` en la columna **Intervalo de sondeo**.
4. En el separador **Vistas de red**, asegúrese de que está seleccionado **Todos los dispositivos**.
5. En el separador **Filtro de dispositivo**, realice los siguientes cambios:
   a. Seleccione **Cualquiera**.
   b. Para especificar el filtro en los campos de la tabla mainNodeDetails, haga clic en **Abrir constructor de filtros**  .
   c. En el separador **Básico** del **Constructor de filtros**, complete los campos de la siguiente manera:

Field	Comparator	Value
ipAddress	like	9.1.2.%

   d. Haga clic en **Aceptar**.
   e. Haga clic en **Agregar**  .
   f. Para especificar otro filtro en los campos de la tabla mainNodeDetails, haga clic en **Abrir constructor de filtros**  .
   g. En el separador **Básico** del **Constructor de filtros**, complete los campos de la siguiente manera:

Field	Comparator	Value
ipAddress	like	10.123.46.%

   h. Haga clic en **Aceptar**.
6. Haga clic en **Guardar**.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Modificación de definiciones de sondeo

Modifique las definiciones de sondeo existentes para personalizarlas según sus requisitos de sondeo. Las definiciones de sondeo se modifican en el **Editor de definiciones de sondeos**; los pasos que deberá seguir varían dependiendo del *tipo de definición de sondeo*.

Antes de empezar

Antes de crear o cambiar una definición de sondeo, vea una definición de sondeo existente para determinar si puede utilizarlo como una plantilla para crear una nueva definición de sondeo.

Tareas relacionadas

Creación de nuevas definiciones de sondeo
Utilice el **Editor de definiciones de sondeos** como guía para crear una nueva definición de sondeo.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Modificación de las definiciones de sondeo de umbral

Utilice el **Editor de definiciones de sondeos** para cambiar definiciones de sondeo de umbral básico.

Acerca de esta tarea

Puede cambiar algunas de las propiedades generales de la definición de sondeo y las propiedades asociadas con el tipo de definición de sondeo. No puede, sin embargo, cambiar el tipo de definición de sondeo.

Para cambiar una definición de sondeo de umbral básico:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en la definición de sondeo requerida.
   La definición de sondeo debe tener el tipo de definición de sondeo Umbral básico.
3. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

   ID de suceso
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

   - Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor POLL-*defsondeo*, donde *defsondeo* es el nombre de la definición de sondeo actual.
   - Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

   Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación POLL-*defsondeo*.

   Gravedad de suceso
   Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

Descripción
Escriba una breve descripción de la definición de sondeo.

Etiqueta de datos
Haga clic en la lista de etiqueta de datos y seleccione una de las etiquetas de datos de la lista. De forma predeterminada, la etiqueta de datos tiene el mismo nombre que la definición de sondeo actual. Para definir una etiqueta de datos nueva, seleccione <Agregar nueva etiqueta de datos>. El campo a la derecha de la lista se convertirá en activo. Escriba el nombre de la nueva etiqueta de datos en este campo.

Unidades de datos
Especifique las unidades de datos para esta definición de sondeo. La unidad de datos adecuada varía en función del tipo de datos de la definición del sondeo. Los siguientes son algunos tipos de datos y unidades de datos típicos que corresponden a dichos tipos de datos, junto con ejemplos de las definiciones de sondeos de Network Manager predeterminadas:

Recuentos
Las definiciones de sondeos en las que un valor es un recuento de algún elemento. Los ejemplos son:

- dot3StatsAlignmentErrors
- ifInDiscards
- ifInErrors

En este tipo de definición de sondeo especifique una unidad de datos de #.

Porcentajes
Las definiciones de sondeos en las que el valor es un porcentaje. Los ejemplos son:

- cpuBusyPoll
- ciscoCPUTotal5min

En este tipo de definición de sondeo especifique una unidad de datos de %.

Unidades de medida específicas
Las definiciones de sondeos en las que un valor es una unidad de medida especificada. Los ejemplos son:

- memoryPoll

En este tipo de definición de sondeo especifique la unidad de medida adecuada. Por ejemplo, en el caso de memoryPoll, la unidad de medida adecuada es bytes.

4. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.

5. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

El campo **Tabla** será rellenado con la tabla interfaces.

Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.

6. Haga clic en el separador **Datos de sondeo** y especifique la fórmula requerida:

- Para especificar un OID (identificador de objeto) de MIB, seleccione **OID único**. Especifique el valor actual o delta de la variable de MIB requerida y escriba la variable en el siguiente campo.

- Para especificar una expresión compleja, seleccione **Expresión** y escriba la fórmula en el campo.

Para seleccionar variables directamente del árbol MIB, haga clic en **Agregar objeto de MIB**  . Desde el árbol de MIB, puede especificar el valor o valores actuales de la variable de MIB seleccionada o resuelva el valor actual de la variable en el índice SNMP.

7. Haga clic en el separador **Umbral** y especifique las fórmulas para desencadenar sucesos y borrar sucesos.

   El OID de MIB o expresión especificada en el separador **Datos de sondeo** se escribe automáticamente en las fórmulas.

   a) En el área **Umbral de desencadenante**, seleccione un comparador en la lista y escriba el valor que desea filtrar del OID de MIB.

   b) En el campo **Descripción**, escriba una descripción de la fórmula desencadenante. Agregue la variable de MIB a la descripción en paréntesis.

   La descripción que se muestra en el **Visor de sucesos** cuando se genera un suceso.

   Por ejemplo:

   ```
   CPU usage high (avgBusy5=)
   ```

   c) Para insertar la sentencia eval subyacente en la descripción, posicione el cursor antes del paréntesis de cierre, haga clic en **Agregar objeto de MIB**  y navegue hasta la variable especificada. Especifique si el valor actual o anterior de la variable debe evaluarse, o si el valor será resuelto en el índice SNMP y haga clic en **Aceptar**.

   La sentencia está insertada, por ejemplo:

   ```
   CPU usage high (avgBusy5=eval(text,"&SNMP.VALUE.sysName"))
   ```

   d) Repeat steps 6a to 6c for the **Clear Threshold** area.

8. Haga clic en **Guardar**.

Conceptos relacionados

Datos multibyte en definiciones de sondeo
Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Ámbito de la política de sondeo
El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Referencia relacionada

Ejemplo de expresión de umbral básico
Utilice este ejemplo de expresión de umbral básico para entender cómo componer expresiones complejas de umbral básico.

Modificación de definiciones de sondeo de umbral genérico

Utilice el **Editor de definiciones de sondeos** para cambiar definiciones de sondeo genérico.

Acerca de esta tarea

Puede cambiar algunas de las propiedades generales de la definición de sondeo y las propiedades asociadas con el tipo de definición de sondeo. No puede, sin embargo, cambiar el tipo de definición de sondeo.

Para cambiar una definición de sondeo de umbral genérico:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.

2. Haga clic en la definición de sondeo requerida.

   La definición de sondeo debe tener el tipo de definición de sondeo Umbral genérico.
3. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

   ID de suceso
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

   - Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor POLL-*defsondeo*, donde *defsondeo* es el nombre de la definición de sondeo actual.
   - Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

   Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación POLL-*defsondeo*.

   Gravedad de suceso
   Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

   Descripción
   Escriba una breve descripción de la definición de sondeo.
4. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

   Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.
5. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

   El campo **Tabla** será rellenado con la tabla `interfaces`.

   Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.
6. Haga clic en **Umbral de desencadenante**. Construya la fórmula que especifica el umbral utilizando uno de los siguientes métodos:

   - En el área **Básica**, utilice los campos y opciones para construir una fórmula. Para seleccionar valores en el árbol de MIB, haga clic en **Abrir árbol de MIB** .
   - En el área **Avanzada**, escriba la sentencia **`eval`** requerida en OQL (lenguaje de consulta de objetos).
7. Especifique el mensaje que se muestra en el **Visor de sucesos** para el suceso generado:

a) En el campo **Descripción de suceso**, escriba el mensaje.

b) Para insertar las variables de MIB en el campo, haga clic en **Abrir árbol de MIB**. Establezca el mensaje para que incluya el valor actual o anterior de SNMP, o el índice de SNMP y haga clic en **Aceptar**.

8. Necesario: Haga clic en el separador **Umbral de borrado**. Cada definición de umbral de la encuesta genérica requiere un umbral claro. Construya la fórmula que especifica el umbral utilizando uno de los siguientes métodos:
   - En el área **Básica**, utilice los campos y opciones para construir una fórmula. Para seleccionar valores en el árbol de MIB, haga clic en **Abrir árbol de MIB**.
   - En el área **Avanzada**, escriba la sentencia **`eval`** requerida en OQL (lenguaje de consulta de objetos).

   Consejo: Si desea borrar el umbral de forma manual, cree un umbral de borrado que no pueda alcanzarse.
9. Especifique el mensaje que se muestra en el **Visor de sucesos** para el suceso generado:
   a) En el campo **Descripción de suceso**, escriba el mensaje.

   b) Para insertar las variables de MIB en el campo, haga clic en **Abrir árbol de MIB**. Establezca el mensaje para que incluya el valor actual o anterior de SNMP, o el índice de SNMP y haga clic en **Aceptar**.
10. Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Conceptos relacionados

Datos multibyte en definiciones de sondeo
Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Ámbito de la política de sondeo
El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Ejemplo de expresión de umbral genérico
Utilice este ejemplo de expresión de umbral genérico para entender cómo componer expresiones complejas de umbral básico.

Cambio de las definiciones de sondeo de ping de interfaz y chasis

Utilice el **Editor de definiciones de sondeos** para cambiar los tipos de definición de sondeo de ping de interfaz y chasis.

Acerca de esta tarea

Puede cambiar algunas de las propiedades generales de la definición de sondeo y las propiedades asociadas con el tipo de definición de sondeo. No puede, sin embargo, cambiar el tipo de definición de sondeo.

Para cambiar una definición de sondeo de ping de interfaz o chasis:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en la definición de sondeo requerida.

La definición de sondeo debe tener el tipo de definición de sondeo Ping de chasis o Ping de interfaz.

3. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

   ID de suceso
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

   - Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor POLL-*defsondeo*, donde *defsondeo* es el nombre de la definición de sondeo actual.
   - Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

   Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación POLL-*defsondeo*.

   Gravedad de suceso
   Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

   Descripción
   Escriba una breve descripción de la definición de sondeo.

4. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

   Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.

5. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

   El campo **Tabla** será rellenado con la tabla `interfaces`.

   Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.

6. Haga clic en el separador **Ping** y cumplimente los campos en **Propiedades de ping** tal como se muestra a continuación:

   Tiempo de espera excedido
   Especifique, en milisegundos, cuánto tiempo desea que el proceso de sondeo espere una respuesta del dispositivo de destino antes de volver a enviar un nuevo paquete de ping.

   Reintentos
   Especifique cuántas veces desea que el proceso de sondeo intente hacer ping del dispositivo de destino antes de abandonar. Cuando la recopilación de métrica **Pérdida de paquetes** está habilitada, el proceso de sondeo envía este número de paquetes de ping independientemente de si se ha recibido una respuesta.

Recopilar métricas de ping

Tiempo de respuesta
Marque el recuadro para recopilar el tiempo que llevan los dispositivos en responder a una solicitud de ping. El tiempo de respuesta se almacena como el tiempo en milisegundos entre el momento en que se ha enviado la solicitud de ping y el momento en que se ha procesado la respuesta. Si no se recibe ninguna respuesta, se almacena el valor de `-1`.

Pérdida de paquetes
Marque el recuadro para recopilar datos sobre los paquetes perdidos. La pérdida de paquetes se almacenan como el porcentaje de paquetes perdidos, que a su vez viene determinado por el envío de varias solicitudes de ping y el cálculo del porcentaje de paquetes perdidos.

Tamaño de carga
Seleccione el tamaño del paquete ICMP que se utilizará para la solicitud de ping. Seleccione el valor predeterminado (32 bytes) o seleccione un tamaño personalizado. Este valor sustituye el valor de IcmpData en el archivo de configuración `NcPollerSchema.cfg`.

PRECAUCIÓN: El uso de un tamaño menor de 32 bytes puede provocar que se descarten paquetes.

7. Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Conceptos relacionados

Ámbito de la política de sondeo
El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Cambio de las definiciones de sondeo de estado de enlace y ping remoto

Utilice el **Editor de definiciones de sondeos** para cambiar los siguientes tipos de definición de sondeo: Ping remoto de Cisco, ping remoto de Juniper y estado de enlace de SNMP.

Acerca de esta tarea

Puede cambiar algunas de las propiedades generales de la definición de sondeo y las propiedades asociadas con el tipo de definición de sondeo. No puede, sin embargo, cambiar el tipo de definición de sondeo.

Para cambiar una definición de sondeo de ping remoto o una definición de sondeo de estado de enlace SNMP:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. Haga clic en la definición de sondeo requerida.
   La definición de sondeo debe tener uno de los siguientes tipos de definición de sondeo:
   - Ping remoto de Cisco
   - Ping remoto de Juniper
   - Estado de enlace SNMP
3. En el **Editor de definiciones de sondeos**, en el separador **General**, complete los campos en **Propiedades generales** tal como se muestra a continuación:

   Nombre
   Especifique un nombre exclusivo para la definición de sondeo. Sólo se permiten caracteres alfanuméricos, espacios y subrayados.

   Tipo
   Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política de sondeo habilitada.

ID de suceso
Este campo está inhabilitado. El motor de sondeo, ncp_poller, rellena automáticamente este campo tras incluir esta definición de sondeo como parte de una política habilitada. El campo **ID de suceso** se rellena como se indica a continuación:

- Si se trata de una nueva definición de sondeo, el campo **ID de suceso** se rellena con el valor POLL-*defsondeo*, donde *defsondeo* es el nombre de la definición de sondeo actual.
- Si ha creado una definición de sondeo copiando otra ya existente, **ID de suceso** contiene el mismo valor que la definición de sondeo copiada.

Nota: Algunos de los sondeos predeterminados más antiguos tienen campos **ID de suceso** que no utilizan el convenio de denominación POLL-*defsondeo*.

Gravedad de suceso
Especifique un número válido como gravedad. El nivel de gravedad debe corresponder con un nivel de gravedad válido como se ha definido en IBM Tivoli Netcool/OMNIbus. Para obtener un listado de niveles de gravedad disponibles, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*

Descripción
Escriba una breve descripción de la definición de sondeo.

4. Haga clic en el separador **Clases**. En el árbol **Clases**, seleccione los recuadros de selección de las clases requeridas.

   Atención: Si deja todas las clases sin marcar, el sistema sondeará todos los dispositivos que coincidan con el ámbito definido en la política de sondeo que utiliza esta definición de sondeo.

5. Opcional: Haga clic en el separador **Filtro de interfaz** y cree el filtro para los campos requeridos.

   El campo **Tabla** será rellenado con la tabla `interfaces`.

   Nota: Al realizar un sondeo para obtener datos de interfaz (no sondeo de ping ni sondeo de ping remoto), de forma predeterminada, se sondean todas las interfaces de la tabla de interfaces SNMP del dispositivo, tanto si se han descubierto como si no. Es posible que no se descubran las interfaces si ha configurado el filtrado de interfaz para el descubrimiento, o por algún otro motivo, por ejemplo que no estuvieran accesibles en el momento del descubrimiento. También se sondean las interfaces no descubiertas, a menos que configure un filtro sobre los registros de interfaz en la base de datos de NCIM para el sondeo. Si añade un filtro de interfaz a este sondeo, el filtro se aplica a los registros de interfaz de la base de datos de topología de NCIM, y sólo se sondean dichas interfaces. Únicamente se sondea el subconjunto de las interfaces descubiertas que también coincida con el filtro.

6. Haga clic en **Guardar** y, a continuación, haga clic en **Aceptar**.

Conceptos relacionados

Sondeo de estado de enlace
El sondeo de estado de enlace supervisa los cambios en el estado de las siguientes variables MIB: ifOperStatus e ifAdminStatus.

Ámbito de la política de sondeo
El ámbito de la política de sondeo define los dispositivos o interfaces de dispositivo que se van a sondear.

Tareas relacionadas

Configuración del sondeo de estado de enlace
Puede especificar cómo el proceso de ncp_poller determina el estado inicial de los sondeos de estado de enlace cuando no hay ningún suceso existente.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Definición personalizada de sondeo de ejemplo

Utilice este ejemplo de una definición personalizada de sondeo para ayudarle a copiar una definición existente y personalizarla para satisfacer sus requisitos.

Situación

Necesita una definición de sondeo que alerte al operador cuando un dispositivo esté utilizando demasiada potencia de proceso. Desea que se genere un suceso si la utilización media de la CPU supera el 80% y que el suceso sea borrado si la utilización media de la CPU cae por debajo del 70%.

Valores requeridos

Para crear una definición de sondeo que responda a los requisitos descritos en el apartado "Situación" en la página 486, haga los siguientes cambios:

- En el panel **Nueva selección de definición de sondeo**, seleccione `Umbral básico`.
- En el separador **Datos de sondeo** del **Editor de definiciones de sondeos**, haga los siguientes cambios:
  - Asegúrese de que **OID único** está seleccionado.
  - Complete el área **OID único** tal como se muestra en el siguiente ejemplo. El texto en negrita indica entradas que debe escribir; el texto sin formato indica selecciones que debe realizar utilizando las listas:

```
current          avgBusy5
```

- En el separador **Umbral** del **Editor de definiciones de sondeos** realice los siguientes cambios:
  - Complete el área **Umbral de desencadenante** tal como se muestra en el siguiente ejemplo. El texto en negrita indica entradas que debe escribir; el texto sin formato indica selecciones que debe realizar utilizando las listas. El texto en cursiva representa elementos que no puede editar:

```
current          avgBusy5          >=          80
```

  - Complete el campo **Descripción** tal como se muestra a continuación:
    1. Escriba `CPU usage high (avgBusy5=)`.
    2. Coloque el cursor dentro del paréntesis de cierre y haga clic en **Agregar objeto de MIB**.
    3. Navegue hasta la siguiente vía de acceso: `iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy5`.
    4. Seleccione **Valor SNMP actual** y haga clic en **Insertar**.
  - Complete el área **Umbral de borrado** tal como se muestra en el siguiente ejemplo. El texto en negrita indica entradas que debe escribir; el texto sin formato indica selecciones que debe realizar utilizando las listas. El texto en cursiva representa elementos que no puede editar:

```
current          avgBusy5          <          70
```

  - Complete el campo **Descripción** tal como se muestra a continuación:
    1. Escriba `CPU usage high (avgBusy5=)`.
    2. Coloque el cursor dentro del paréntesis de cierre y haga clic en **Agregar objeto de MIB**.
    3. Navegue hasta la siguiente vía de acceso: `iso/org/dod/internet/private/enterprises/cisco/local/lsystem/avgBusy5`.
    4. Seleccione **Valor SNMP actual** y haga clic en **Insertar**.

Conceptos relacionados

Datos multibyte en definiciones de sondeo

Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Ejemplo de expresión de umbral básico

Utilice este ejemplo de expresión de umbral básico para entender cómo componer expresiones complejas de umbral básico.

Ejemplo: snmpInBandwidth

La definición de sondeo snmpInBandwidth es una de las definiciones de sondeo predeterminadas. Esta definición de sondeo define la comprobación de la utilización del ancho de banda entrante. Se genera una alerta cuando el uso de ancho de banda entrante supera el 40%. La siguiente expresión muestra cómo utilizar las sentencias `eval` para definir esta condición y está definida dentro del separador **Datos de sondeo** bajo el botón de selección **Expresión**.

```
((eval(long64,"&SNMP.DELTA.ifInOctets") / eval(long64,"&POLL.POLLINTERVAL"))
/(eval(long64,"&SNMP.VALUE.ifSpeed")))
*800
```

Dentro del separador **Umbral**, el umbral está definido para desencadenarse si el valor de esta expresión es mayor que 40.

Conceptos relacionados

Datos multibyte en definiciones de sondeo

Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Tareas relacionadas

Modificación de las definiciones de sondeo de umbral

Utilice el **Editor de definiciones de sondeos** para cambiar definiciones de sondeo de umbral básico.

Creación de definiciones de sondeo de umbral básico

Cree una definición de sondeo de umbral básico para ejecutar fórmulas sencillas en variables de MIB o para crear sondeos de umbrales con filtrado a nivel de interfaz..

Ejemplo de expresión de umbral genérico

Utilice este ejemplo de expresión de umbral genérico para entender cómo componer expresiones complejas de umbral básico.

Ejemplo: memoryPoll

La definición de sondeo memoryPoll es una de las definiciones de sondeo predeterminadas. Esta definición de sondeo define la comprobación de la utilización de la agrupación de memoria para dispositivos Cisco. Se genera una alerta cuando el uso de la agrupación de memoria supera el 80%. La siguiente expresión muestra cómo utilizar las sentencias `eval` para definir esta condición y está definida dentro del separador **Desencadenar umbral** bajo el botón de selección **Avanzado**.

```
((eval(int,"&SNMP.VALUE.ciscoMemoryPoolValid") = 1)
AND
((eval(long64,"&SNMP.VALUE.ciscoMemoryPoolUsed")/
(eval(long64,"&SNMP.VALUE.ciscoMemoryPoolFree") +
eval(long64,"&SNMP.VALUE.ciscoMemoryPoolUsed")))*100
> 80))
```

Conceptos relacionados

Datos multibyte en definiciones de sondeo

Si está ejecutando Network Manager en un dominio que usa caracteres multibyte, como el chino simplificado, debe asegurarse de que Network Manager esté configurado para usar caracteres multibyte antes de configurar definiciones de sondeo de umbral básicas o genéricas.

Tareas relacionadas

Modificación de definiciones de sondeo de umbral genérico
Utilice el **Editor de definiciones de sondeos** para cambiar definiciones de sondeo genérico.

Creación de definiciones de sondeo de umbral genérico
Utilice el **Editor de definición de sondeo** para crear nuevas definiciones de sondeo de umbral genérico.

Capítulo 23. Supresión de políticas de sondeo

Suprima políticas de sondeo cuando ya no son necesarias.

Acerca de esta tarea

Para suprimir una política de sondeo:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. En la columna **Seleccionar**, seleccione las políticas de sondeo requeridas.
3. Haga clic en **Suprimir**  .
4. Haga clic en **Aceptar** para confirmar la supresión.

Qué hacer a continuación

Se suprimirán las políticas de sondeo seleccionadas.

Capítulo 24. Supresión de definiciones de sondeo

Suprimir definiciones de sondeo cuando ya no son necesarias.

Acerca de esta tarea

Para suprimir una definición de sondeo:

Procedimiento

1. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes**.
2. En la columna **Seleccionar**, seleccione las definiciones de sondeo requeridas.
3. Haga clic en **Suprimir**  .
4. Haga clic en **Aceptar** para confirmar la supresión.

Qué hacer a continuación

Se suprimirán las definiciones de sondeo seleccionadas.

Capítulo 25. Gestión del sondeo adaptativo

Los sondeos adaptativos reaccionan de forma dinámica a los sucesos en la red. Puede crear sondeos adaptativos que gestionen una amplia gama de situaciones de problemas de red.

Conceptos relacionados

Plug-in de sondeo adaptativo

Utilice esta información para comprender los requisitos previos del conector, la forma en que el conector de sondeo adaptativo rellena campos en la tabla activeEvent, así como los detalles de configuración asociados con el conector. La tabla activeEvent se encuentra en el esquema NCMONITOR.

Situaciones de sondeo adaptativo

Network Manager proporciona sondeos adaptativos predeterminados para manejar automáticamente situaciones clave de problemas de red. Utilice estos sondeos adaptativos predeterminados para entender cómo crear sus propios sondeos adaptativos.

Confirmación rápida de que el dispositivo está inactivo

Utilice el sondeo adaptativo que se describe en esta situación para determinar tan rápido como sea posible cuando un dispositivo está inactivo. Puede activar este sondeo adaptativo habilitando la política de sondeo ConfirmDeviceDown.

Rationale

La política de sondeo de ping de chasis predeterminada sondea todos los dispositivos de chasis en el dominio de red actual cada dos minutos. Por diferentes razones los dispositivos sanos no pueden responder a veces a esta política de sondeo, generando sucesos NmosPingFail erróneos en la **Visor de sucesos**. Estos sucesos no se borran hasta que se produzca una respuesta de ping satisfactoria al menos dos minutos más tarde. Durante este tiempo estos sucesos erróneos pueden hacer que los operadores de red realicen acciones innecesarias.

El sondeo adaptativo que se describe en esta situación evita el riesgo de actividad de operaciones de red innecesarias haciendo un ping más rápido de todos los dispositivos en los que un suceso NmosPingFail se genera por primera vez. Una política de sondeo diferente hace ping a estos dispositivos cada 10 segundos durante tres minutos, con la intención de borrar el suceso tan pronto como responda el dispositivo. Los dispositivos que todavía muestran un suceso NmosPingFail después de que se les haya hecho un ping acelerado durante tres minutos se considera que están inactivos y no se les vuelve a hacer ping. El operador de red puede realizar acciones en esos dispositivos o las automatizaciones se pueden escribir para que realicen una acción relevante, con la confianza de que los sucesos se puedan accionar.

Nota: Se fuerzan estos tres minutos especificando los dispositivos de ámbito de política con un suceso NmosPingFail y un valor Cuadrar menor que 18. El valor Cuadrar se calcula asumiendo que un dispositivo con fallos no podrá responder a todos los sondeos acelerados. Cada minuto se producen seis sondeos de ping acelerados, por lo que en un período de tres minutos habrá 18 y el valor Cuadrar de esos dispositivos que todavía no responden alcanzará 18.

Los valores de ping acelerados son totalmente configurables. Por ejemplo, puede especificar un intervalo de sondeo de ping acelerado de 20 segundos (en vez de un intervalo de 10 segundos) para aligerar la carga en la red. También puede continuar el sondeo acelerado durante más de tres minutos (aumentando el valor Cuadrar) si necesita más tiempo para verificar que los dispositivos están inactivos.

Políticas de sondeo encadenadas

El sondeo adaptativo descrito en esta situación está formado por los siguientes sondeos encadenados:

Ping de chasis predeterminado
Esta política de sondeo hace ping en todos los dispositivos en la red cada dos minutos. Está habilitado de manera predeterminada.

ConfirmDeviceDown
Esta política de sondeo proporciona un ping acelerado en intervalos de 10 segundos de dispositivos que no pueden responder a la política de sondeo de ping de chasis predeterminada. La política ConfirmDeviceDown debe asignarse a una vista de red.

Importante: La política de sondeo ConfirmDeviceDown está inhabilitada de manera predeterminada. Debe habilitar esta política de sondeo para activar el sondeo adaptativo descrito en esta situación.

Explicación de la situación

La siguiente sección le explica este sondeo adaptativo.

1. La política de sondeo de ping de chasis predeterminada sondea todos los dispositivos de chasis en el dominio de red actual. Puede modificar el ámbito de esta política modificando las vistas de red asociadas y el filtro de dispositivo.
2. Se genera un suceso NmosPingFail para todos los dispositivos que no responden a la política de ping de chasis predeterminada.
3. Los dispositivos que tienen un suceso NmosPingFail asociado se agregan automáticamente a la vista de red de sucesos de error de ping inicial. La vista de red de sucesos de error de ping inicial es una vista de red filtrada que se define de la siguiente forma:

```
EventId = NmosPingFail
Tally < 18
```

   La vista de red de sucesos de error de ping inicial se puede encontrar en **Vistas de red**, en el árbol Vista de red, en el nodo **Vistas de supervisión** > **Sucesos de error de ping inicial**. Para obtener más información sobre los nodos en el árbol de vista de red, consulte *Guía del usuario de IBM Tivoli Network Manager*.

   Puede cambiar la duración del sondeo acelerado modificando la cláusula de filtro `Tally < 18`. Por ejemplo, si quiere aumentar la duración del sondeo acelerado a cinco minutos, cambie esta cláusula a `Tally < 30`. Este valor se determina con el siguiente cálculo basado en un intervalo de sondeo de 10 segundos: cada minuto hay seis sondeos de ping acelerados, por lo que en un periodo de cinco minutos habrá 30. Para obtener más información sobre cómo cambiar las vistas red filtradas por sucesos, consulte *Guía del usuario de IBM Tivoli Network Manager*.
4. La política de sondeo ConfirmDeviceDown sondea todos los dispositivos dentro de la vista de red de sucesos de error de ping inicial cada 10 segundos. Cada vez que el dispositivo no responde, se recibe otro valor Cuadrar NmosPingFail para el dispositivo y se incrementa el valor Cuadrar NmosPingFail para el dispositivo.

   Importante: De forma predeterminada, tiene que realizar las siguientes acciones para activar el sondeo adaptativo descrito en este escenario:

   - La política de sondeo ConfirmDeviceDown está inhabilitada de manera predeterminada. Debe habilitar esta política de sondeo.
   - La política de sondeo ConfirmDeviceDown no tiene alcance de forma predeterminada. Debe asignar vista de red de sucesos de error de ping inicial como ámbito de la política de sondeo de ConfirmDeviceDown.

   Puede cambiar la frecuencia del sondeo de ping acelerado editando la política de sondeo de ConfirmDeviceDown y modificando el intervalo en segundos entre las operaciones de sondeo. Por ejemplo, si desea disminuir la frecuencia de sondeo a intervalos de sondeo de 20 segundos (tres sondeos por minuto en vez de seis), abra la política de sondeo ConfirmDeviceDown en el **Editor de políticas de sondeo** y defina el valor del **Intervalo de sondeo** en 20.

   Nota: Al cambiar el intervalo de política de sondeo cambia el valor Cuadrar para la misma duración de sondeo acelerado. Por ejemplo, si cambia el valor del **Intervalo de sondeo** a 20 este disminuye la

frecuencia del sondeo de ping acelerado a 3 sondeos por minuto. En este caso el valor Cuadrar asociado para un sondeo acelerado de tres minutos es 9. Este valor se determina con el siguiente cálculo basado en un intervalo de sondeo de 20 segundos: cada minuto hay tres sondeos de ping acelerados, por lo que en un periodo de tres minutos habrá 9.

5. El sondeo acelerado de dispositivos puede concluir de una de las siguientes maneras:

   Dispositivo sano
   Durante un periodo de sondeo acelerados de tres minutos se recibe una respuesta de ping satisfactoria para un dispositivo. El suceso NmosPingFail para ese dispositivo se borra y será suprimido posteriormente de la **Visor de sucesos**. El dispositivo se elimina automáticamente de la vista de red de sucesos de error de ping inicial y, por lo tanto, ya no existe un sujeto para el sondeo acelerado.

   Dispositivo con fallos
   El dispositivo sigue siendo sondeado con ping hasta el final del periodo de tres minutos. El valor Cuadrar para el suceso en ese dispositivo alcanza 18 y el dispositivo se elimina automáticamente de la vista de red de sucesos de error de ping inicial y, por lo tanto, ya no existe un sujeto para el sondeo acelerado. La **Visor de sucesos** contiene ahora un suceso que se puede accionar, es decir, un suceso NmosPingFail con un valor cuadrar de 18 o mayor.

Tareas relacionadas

Habilitación e inhabilitación de sondeos
Para activar el sondeo de Network Manager, deberá habilitar las políticas de sondeo.

Modificación de políticas de sondeo
Utilice el **Editor de políticas de sondeo** para modificar los valores de políticas de sondeo existentes.

Creación de sondeos adaptativos
Crear sondeos adaptativos para permitir que el sistema reaccione de forma dinámica a los sucesos de la red.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Definiciones de sondeo predeterminadas
Network Manager proporciona un número de definiciones de sondeo predeterminadas que cumplen los requisitos de sondeo más comunes.

Confirmación rápida de una violación de umbral

Utilice el sondeo adaptativo definido en esta situación para utilizar un sondeo SNMP lento la mayor parte del tiempo para crear un mínimo impacto en los dispositivos de red y acelerar el sondeo cuando se ha vulnerado un umbral. Puede activar este sondeo adaptativo habilitando la política de sondeo ConfirmHighDiscardRate.

Rationale

La política de sondeo HighDiscardRate estándar realiza un sondeo de umbral SNMP en todos los direccionadores en el dominio de red actual cada 30 minutos para determinar si la tasa de descarte de paquete porcentual en alguna de las interfaces del direccionador excede el 5%. Si la política de sondeo detecta que una interfaz en un direccionador ha excedido el umbral, el sondeo genera un suceso POLL-HighDiscardRate para el direccionador. Las interfaces de direccionador sano pueden estar ocupadas ocasionalmente y tendrán que soltar paquetes, haciendo que vulneren el 5% del umbral durante un intervalo de 30 minutos, generando sucesos HighDiscardRate erróneos en la **Visor de sucesos**. Estos sucesos no se borran hasta que se produzca una respuesta de política de sondeo POLL-HighDiscardRate satisfactoria al menos treinta minutos más tarde. Durante este tiempo estos sucesos erróneos pueden hacer que los operadores de red realicen acciones innecesarias.

El sondeo adaptativo que se describe en esta situación evita el riesgo de actividad de operaciones de red innecesarias acelerando el sondeo SNMP de todos los dispositivos en los que un suceso POLL-

HighDiscardRate se genera por primera vez. Una política de sondeo SNMP distinta sondea estos dispositivos cada cinco minutos, con la intención de borrar el suceso tan pronto como las interfaces en el dispositivo respondan con una tasa de descarte de paquete porcentual que quede en el umbral del 5%. Se ha confirmado que estos dispositivos que siguen exhibiendo el suceso POLL-HighDiscardRate tienen una o más interfaces con fallos. El operador de red puede realizar acciones en esos dispositivos o las automatizaciones se pueden escribir para que realicen una acción relevante, con la confianza de que los sucesos se puedan accionar.

Los valores de sondeo acelerados son totalmente configurables. Por ejemplo, puede especificar un intervalo de sondeo de SNMP acelerado de 10 minutos (en vez de un intervalo de 5 segundos) para aligerar la carga en la red.

Políticas de sondeo encadenadas

El sondeo adaptativo descrito en esta situación está formado por los siguientes sondeos encadenados:

HighDiscardRate
Esta política de sondeo determina si una interfaz en un dispositivo está soltando más del porcentaje mínimo del total de paquetes que están procesando. La política sondea esta información cada 30 minutos.

ConfirmHighDiscardRate
Esta política de sondeo proporciona sondeo SNMP acelerado en intervalos de cinco minutos de dispositivos que tienen al menos una interfaz que ha vulnerado el umbral de 5% de la tasa de descarte de paquete. El ámbito de la política ConfirmHighDiscardRate debe asignarse a una vista de red.

Importante: La política de sondeo ConfirmHighDiscardRate está inhabilitada de manera predeterminada. Debe habilitar esta política de sondeo para activar el sondeo adaptativo descrito en esta situación.

Explicación de la situación

La siguiente sección le explica este sondeo adaptativo.

1. La política de sondeo HighDiscardRate realiza un sondeo de umbral SNMP en todos los direccionadores en el actual dominio de red cada 30 minutos. Puede modificar el ámbito de esta política modificando las vistas de red asociadas y el filtro de dispositivo.
2. Se genera un suceso POLL-HighDiscardRate para todos los dispositivos que tienen al menos una interfaz que ha vulnerado el umbral de 5% de la tasa de descarte de paquete.
3. Los dispositivos que tienen un suceso POLL-HighDiscardRate asociado se agregan automáticamente a los dispositivos que tienen al menos un suceso de interfaz para la vista de red HighDiscardRate. Esta vista de red es una vista de red filtrada que se define de la siguiente forma:

   ```
   EventId = POLL-HighDiscardRate
   ```

   Los dispositivos que tienen al menos un suceso de interfaz para la vista de red HighDiscardRate se pueden encontrar en **Vistas de red**, en el árbol de vista de red, en **Supervisión de vistas** > **Dispositivos que tienen al menos un suceso de interfaz para el nodo HighDiscardRate**. Para obtener más información sobre los nodos en el árbol de vista de red, consulte *Guía del usuario de IBM Tivoli Network Manager*.
4. La política de sondeo ConfirmHighDiscardRate sondea todos los dispositivos dentro de los dispositivos que tienen al menos un suceso de interfaz para la vista de red HighDiscardRate cada cinco minutos.

   Importante: De forma predeterminada, tiene que realizar las siguientes acciones para activar el sondeo adaptativo descrito en este escenario:

   - La política de sondeo ConfirmHighDiscardRate está inhabilitada de manera predeterminada. Debe habilitar esta política de sondeo.

- La política de sondeo ConfirmHighDiscardRate no tiene alcance de manera predeterminada. Debe asignar los dispositivos que tengan al menos un suceso de interfaz para la vista de red HighDiscardRate como alcance de la política de sondeo de ConfirmHighDiscardRate.

Importante: La política de sondeo ConfirmHighDiscardRate está inhabilitada de manera predeterminada. Debe habilitar esta política de sondeo para activar el sondeo adaptativo descrito en esta situación.

Puede cambiar la frecuencia del sondeo de ámbito de SNMP acelerado editando la política de sondeo de ConfirmHighDiscardRate y modificando el intervalo en segundos entre las operaciones de sondeo. Por ejemplo, si desea disminuir la frecuencia de sondeo a intervalos de sondeo a intervalos de sondeo de 10 minutos, abra la política de sondeo ConfirmHighDiscardRate en el **Editor de políticas de sondeo** y defina el valor del **Intervalo de sondeo** en 600.

5. El sondeo de ámbito SNMP acelerado de dispositivos puede concluir de una de las siguientes maneras:

Dispositivo sano
Todas las interfaces en el dispositivo responden al sondeo acelerado con una tasa de descarte de paquete porcentual que quede en el umbral del 5%. El suceso POLL-HighDiscardRate para ese dispositivo se borra y será suprimido posteriormente de la **Visor de sucesos**. El dispositivo se elimina automáticamente de los dispositivos que tienen al menos un suceso de interfaz para la vista de red HighDiscardRate y, por lo tanto, ya no existe un sujeto para el sondeo acelerado.

Dispositivo con fallos
Al menos una interfaz en el dispositivo sigue respondiendo al sondeo SNMP acelerado con una vulneración del 5% de la tasa de descarte de paquete. El suceso POLL-HighDiscardRate permanece en la **Visor de sucesos** con un valor Cuadrar que aumenta continuamente. La **Visor de sucesos** contiene ahora un suceso POLL-HighDiscardRate que se puede accionar.

Tareas relacionadas

Habilitación e inhabilitación de sondeos
Para activar el sondeo de Network Manager, deberá habilitar las políticas de sondeo.

Modificación de políticas de sondeo
Utilice el **Editor de políticas de sondeo** para modificar los valores de políticas de sondeo existentes.

Creación de sondeos adaptativos
Crear sondeos adaptativos para permitir que el sistema reaccione de forma dinámica a los sucesos de la red.

Referencia relacionada

Políticas de sondeo predeterminadas
Network Manager proporciona un conjunto de políticas de sondeo predeterminadas. Utilice esta información para familiarizarse con estas políticas.

Definiciones de sondeo predeterminadas
Network Manager proporciona un número de definiciones de sondeo predeterminadas que cumplen los requisitos de sondeo más comunes.

Creación de sondeos adaptativos

Crear sondeos adaptativos para permitir que el sistema reaccione de forma dinámica a los sucesos de la red.

Antes de empezar

Antes de crear un sondeo adaptativo, debe identificar en primer lugar una condición de red que se beneficie de un sondeo adaptativo. Por ejemplo, el sondeo adaptativo que se proporciona de manera predeterminada con Network Manager proporciona un sondeo acelerado de un conjunto seleccionado de dispositivos para que realicen una de las siguientes acciones:

- Confirme que un dispositivo que no ha podido hacer un ping ICMP está inactivo.
- Confirme que se ha violado el umbral en un dispositivo.

Acerca de esta tarea

Siga de la siguiente manera para crear un sondeo adaptativo que cree una cadena de dos políticas de sondeo. Las columnas Confirmar inactividad de dispositivo y confirmar violación de umbral proporcionan ejemplos de sondeo adaptativo que se proporciona de manera predeterminada con Network Manager.

Procedimiento	Confirmar inactividad de dispositivo	Confirmar violación de umbral
1. Identificar una política de sondeo existente que recupere una condición de error en dispositivos que se encuentren en la red.	Política de sondeo utilizada: **Default Chassis Ping** Realiza sondeo de ping en todos los dispositivos en el dominio de red cada dos minutos.	Política de sondeo utilizada: **Default Chassis Ping** Determina si una interfaz en un dispositivo está soltando más del porcentaje mínimo del total de paquetes que están procesando. Se realizan sondeos para esta información cada 30 minutos.
2. Crear una vista de red filtrada por sucesos que filtre dispositivos basándose en el suceso generado por el sondeo que ha identificado en el paso anterior. Los dispositivos en esta vista de red tienen, por lo general, una condición de error asociada que se puede diagnosticar aún más mediante un sondeo más intenso. Para obtener información sobre la creación de vistas de red filtradas por sucesos, consulte *Guía del usuario de IBM Tivoli Network Manager*.	Vista de red: **Vistas de supervisión** > **Sucesos de error de ping inicial** Contiene todos los dispositivos en los que se ha generado un suceso NmosPingFail y el valor Cuadrar es menor que un valor especificado. El suceso NmosPingFail se genera en sucesos que no pasan la política de sondeo Ping de chasis predeterminado.	Vista de red: **Vistas de supervisión** > **Dispositivos que tienen al menos un suceso de interfaz para HighDiscardRate** Determina si una interfaz en un dispositivo está soltando más del porcentaje mínimo del total de paquetes que están procesando.
3. Crear un política de sondeo que tiene como ámbito la vista de red que ha creado en el paso anterior y que proporciona un sondeo más intenso de los dispositivos en esa vista de red. El objetivo de sondear de forma más intensa esos dispositivos es diagnosticar el problema más intensamente como introducción a acciones posteriores.	Política de sondeo: **ConfirmDeviceDown** Propósito del sondeo intenso: acelerar el sondeo de ping de dispositivos en la red de sucesos de error de ping inicial a intervalos de sondeo de 10 segundos para identificar los dispositivos que están inactivos realmente. Los dispositivos sanos proporcionan una respuesta satisfactoria a este sondeo intenso y sus sucesos son borrados.	Política de sondeo: **ConfirmHighDiscardRate** Propósito del sondeo intenso: Acelerar el sondeo de dispositivos en los dispositivos que tienen al menos un suceso de interfaz para la vista de red HighDiscardRate para proporcionar información más actualizada antes de reaccionar. Esta política de sondeo continúa generando los sucesos POLL_HighDiscardRate, confirmando así el problema en un dispositivo, o emite un suceso resuelto que borra el suceso de error y se elimina así el dispositivo asociado de la vista HighDiscardRate.

En el paso 2, en la columna *Confirmar inactividad de dispositivo*, la vista de red *Sucesos de error de ping inicial* incluye un criterio de salida que se implementa utilizando el valor Cuadrar: una vez el valor Cuadrar para un suceso supere un valor especificado, el dispositivo relacionado se elimina automáticamente de la vista de red. Esto es útil si quiere acelerar el sondeo para un periodo de tiempo limitado para establecer una condición en ese dispositivo. Una vez se ha establecido la condición, ya se puede eliminar el dispositivo de la vista. Por ejemplo, en el caso de los valores predeterminados para esta vista de red, puede acelerar el sondeo de los dispositivos que no han podido hacer el sondeo de ping durante tres minutos. Si el dispositivo todavía tiene un suceso NmosPingFail asociado después de tres minutos, se confirmará como que está inactivo.

También es posible encadenar más de dos políticas de sondeo creando vistas de red extra y políticas de sondeo y encadenándolas como apropiadas para responder a condiciones de red y para realizar el diagnóstico necesario.

Conceptos relacionados

Confirmación rápida de que el dispositivo está inactivo
Utilice el sondeo adaptativo que se describe en esta situación para determinar tan rápido como sea posible cuando un dispositivo está inactivo. Puede activar este sondeo adaptativo habilitando la política de sondeo ConfirmDeviceDown.

Confirmación rápida de una violación de umbral
Utilice el sondeo adaptativo definido en esta situación para utilizar un sondeo SNMP lento la mayor parte del tiempo para crear un mínimo impacto en los dispositivos de red y acelerar el sondeo cuando se ha vulnerado un umbral. Puede activar este sondeo adaptativo habilitando la política de sondeo ConfirmHighDiscardRate.

Tareas relacionadas

Creación de sondeos
Cree sondeos si las políticas y definiciones de sondeo existentes no satisfacen sus requisitos. Personalice una copia de un sondeo existente o predeterminado o cree un nuevo sondeo a partir desde cero.

Capítulo 26. Administración de sondeo de red

Utilice la interfaz de línea de mandatos para realizar una amplia gama de tareas de administración de sondeo, incluidas la gestión de varias características de sondeador, la copia de sondeos de red en dominios de red, la suspensión de sondeo de red, la habilitación e inhabilitación de sondeos, la recuperación del estado de sondeo y la renovación de sondeos.

Acerca de esta tarea

También puede configurar el ayudante SNMP para utilizar la operación GetBulk cuando se utiliza SNMP v2 o v3. El uso de la operación GetBulk mejora la eficiencia del sondeo. Para obtener más información, consulte la publicación *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Tareas relacionadas

Administración de Network Manager
Para administrar el producto, debe iniciarlo y detenerlo. Podrá administrar procesos, registros, puertos, usuarios, contraseñas, informes y bases de datos.

Administración de sondeos

Utilice la interfaz de línea de mandatos para administrar las políticas de sondeo.

Inicio de ncp_poller más rápido al no comprobar las credenciales SNMP

La inhabilitación de la comprobación de credenciales de acceso SNMP en el inicio de **ncp_poller** puede mejorar los tiempos de inicio.

Acerca de esta tarea

Si está seguro de que las credenciales de acceso de los dispositivos que desea sondear son precisas, puede configurar el proceso de sondeo, **ncp_poller**, para que no las compruebe en el inicio.

Procedimiento

1. Haga una copia de seguridad y edite el archivo `NCHOME/etc/precision/NcPollerSchema.DOMAIN.cfg`
2. Localice la línea que define el valor de la opción DiscoverInitialAccess.
3. Si desea que el proceso **ncp_poller** compruebe las credenciales SNMP cada vez que se inicie, deje el valor de DiscoverInitialAccess establecido en 1.
4. Para desactivar la comprobación inicial de las credenciales de acceso SNMP, establezca el valor de DiscoverInitialAccess en 0. El proceso **ncp_poller** continúa comprobando las credenciales SNMP para un determinado dispositivo si se produce una anomalía de sondeo.
5. Reinicie el proceso **ncp_poller**.

Recuperación del estado de sondeo

Utilice el script **itnm_poller.pl** para mostrar el estado de las políticas de sondeo.

Acerca de esta tarea

El dominio que se proporciona en la interfaz de línea de mandatos (CLI) debe tener una entrada en la tabla de NCIM domainMgr.

Para obtener más información sobre el script **itnm_poller.pl**, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Procedimiento

1. Cambie al directorio de $NCHOME/precision/scripts/perl/scripts y localice el script **itnm_poller.pl**
2. Ejecute el programa de script **itnm_poller.pl** para recuperar el estado de las políticas de sondeo. El siguiente ejemplo muestra cómo recuperar el estado de todas las políticas de sondeo.

   ```
   ncp_perl itnm_poller.pl -domain NCOMS -status all
   ```

   También puede recuperar el estado de políticas de sondeo estáticas o en tiempo real especificando `-status realtime` o `-status static`.

Habilitación e inhabilitación de sondeos

Utilice el script itnm_poller.pl para habilitar e inhabilitar políticas de sondeo individuales.

Acerca de esta tarea

El dominio que se proporciona en la interfaz de línea de mandatos (CLI) debe tener una entrada en la tabla de NCIM domainMgr.

Para obtener más información sobre el script itnm_poller.pl, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Procedimiento

1. Cambie al directorio de $NCHOME/precision/scripts/perl/scripts y localice el script itnm_poller.pl.
2. Ejecute el programa de script de itnm_poller.pl para recuperar el estado de las diversas políticas de sondeo, como se muestra en el siguiente ejemplo:

   ```
   ncp_perl itnm_poller.pl -domain NCOMS -status all
   ```

   En la salida del mandato, puede ver el ID de cada política de sondeo. Anote el ID de la política de sondeo que desea habilitar o inhabilitar.
3. Ejecute el programa de scripts itnm_poller.pl para habilitar o inhabilitar políticas de sondeo individuales, especificando el ID de política de sondeo como un parámetro.
   El siguiente ejemplo muestra cómo habilitar una política de sondeo con un ID de política de 10.

   ```
   ncp_perl itnm_poller.pl -domain NCOMS -enable 10
   ```

   El siguiente ejemplo muestra cómo inhabilitar una política de sondeo con un ID de política de 15.

   ```
   ncp_perl itnm_poller.pl -domain NCOMS -disable 15
   ```

Renovación de sondeos

Utilice el script itnm_poller.pl para renovar una configuración de política de sondeo y su lista de entidad.

Acerca de esta tarea

El dominio proporcionado en la interfaz de línea de mandatos (CLI) debe tener una entrada en la tabla domainMgr de la base de datos de topología de NCIM.

Para obtener más información sobre el script itnm_poller.pl, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Procedimiento

1. Cambie al directorio de $NCHOME/precision/scripts/perl/scripts y localice el script itnm_poller.pl.

2. Ejecute el programa de script de itnm_poller.pl para recuperar el estado de las diversas políticas de sondeo, como se muestra en el siguiente ejemplo:

```
ncp_perl itnm_poller.pl -domain NCOMS -status all
```

En la salida del mandato, puede ver el ID de cada política de sondeo. Anote el ID de la política de sondeo que desea habilitar o inhabilitar.

3. Ejecute el programa de script itnm_poller.pl para renovar una simple política de sondeo o varias políticas de sondeo.
El siguiente ejemplo muestra cómo renovar un política de sondeo con un ID de política de 10.

```
ncp_perl itnm_poller.pl -domain NCOMS -refresh 10
```

El siguiente ejemplo muestra cómo renovar todas las políticas de sondeo.

```
ncp_perl itnm_poller.pl -domain NCOMS -refresh all
```

Copia de los sondeos entre dominios

Utilice el programa `get_policies.pl` para copiar las políticas de sondeo de uno de los dominios de red a otro, o entre un archivo y un dominio.

Antes de empezar

Si proporciona un nombre de dominio con las opciones `-to` o `-from`, tiene que estar conectado a las bases de datos NCIM y NCMONITOR. Las conexiones se crean basándose en los valores del archivo `DbLogins.`*`DOMAIN`*`.cfg` o del archivo `DbLogins.cfg` si no se encuentra un archivo específico del dominio.

El dominio que se proporciona en la interfaz de línea de mandatos (CLI) debe tener una entrada en la tabla de NCIM domainMgr.

Procedimiento

1. Cambie al directorio `NCHOME/precision/scripts/perl/scripts` y ubique el programa `get_policies.pl`.
2. Ejecute el programa `get_policies.pl` para copiar las políticas de sondeo.
La tabla siguiente describe las posibles acciones y qué entrar en la CLI.

Acción	Entrada en la CLI
Copiar todas las políticas de sondeo directamente de un dominio a otro	`ncp_perl get_policies.pl -from domain=`*`SOURCE`* `-to domain=`*`DESTINATION`* `-ncim_password` *`NCIM_password`* `-ncmonitor_password` *`NCMONITOR_password`*
Copiar sólo las políticas de sondeo seleccionadas de un dominio a otro	`ncp_perl get_policies.pl -from domain=`*`SOURCE`* `-to domain=`*`DESTINATION`* `-policy "`*`policy_name1`*`" -policy "`*`policy_name2`*`"`
Copiar todas las políticas de sondeo de un dominio a un archivo XML	`ncp_perl get_policies.pl -from domain=`*`DOMAIN_name`* `-to file=`*`filename`*`.xml -password` *`NCIM_password`*
Copiar todas las políticas de sondeo de un archivo XML a un dominio	`ncp_perl get_policies.pl -from file=`*`filename`*`.xml -to domain=`*`DOMAIN_name`*
Copiar solo las políticas seleccionadas de un dominio a un archivo	`ncp_perl get_policies.pl -from domain=`*`DOMAIN_name`* `-to file=`*`filename`*`.xml -`

Acción	Entrada en la CLI
	policy "*policy_name1*" -policy "*policy_name2*"

Opciones de suspensión de sondeo

Establezca un dispositivo o componente en un estado no gestionado para suspenderlo del sondeo de red de Network Manager.

Cuando un dispositivo o componente está no gestionado, no se sondea mediante Network Manager, y los sucesos no se generan para el dispositivo o componente. Igualmente, no se realiza ningún análisis de causa raíz (RCA) en sucesos para dicho dispositivo.

Restricciones

Establecer el dispositivo a "no gestionado" afecta únicamente al sondeo de Network Manager, no detiene otros sondeos de recuperar información del dispositivo ni de sus componentes ni de generar alertas cuando sea aplicable. Sin embargo, las alertas de otros orígenes se etiquetan como no gestionadas para indicar que el dispositivo o el componente contra los que se generaron se encuentran en estado de mantenimiento.

Para obtener más información acerca de la configuración de dispositivos no gestionados, consulte la publicación *IBM Tivoli Network Manager IP Edition Administration Guide*.

Opciones para suspender el sondeo

Para suspender un dispositivo o sus componentes de las operaciones de sondeo activas, tiene las siguientes opciones:

Establecer un dispositivo o componente a no gestionado
Tiene las opciones siguientes:

- Utilizar las **Vistas de red** o la **Vista de saltos**
- Utilizar la herramienta **`No gestionar nodo`**

Si configura un dispositivo como no gestionado, todos los componentes dentro de dicho dispositivo también se convertirán en no gestionados. Si un componente individual dentro de un dispositivo se configura como no gestionado, únicamente dicho componente y cualquier componente contenido dentro se convertirá en no gestionado y el propio dispositivo permanecerá en estado no gestionado. Un componente puede ser gestionado o no gestionado únicamente si el dispositivo dentro del que reside se encuentra en estado gestionado. Igualmente, la configuración de la interfaz de gestión asociada con el chasis al estado no gestionado no suspende los sondeos para todo el dispositivo.

Configurar los tipos de interfaces específicos para que no se gestionen de forma permanente
Esto significa que los tipos de interfaz especificados no son sondeados por Network Manager. Igualmente, puede configurar nuevos dispositivos para que no se sondeen de forma inicial una vez que se descubran y se agreguen a la topología. Estos valores los determinan el archivo `PopulateDNCIM_ManagedStatus.stch` y las tablas de base de datos de NCIM.

Para obtener más información sobre las **Vistas de red** y la **Vista de saltos**, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*. Para obtener más información sobre la configuración de dispositivos y componentes a un estado no gestionado, consulte la publicación *Guía del usuario de IBM Tivoli Network Manager*.

Ajuste del ancho de banda de sondeo

Puede configurar la cantidad de datos transferidos por el motor de sondeo, ncp _ poller, y la frecuencia. Es posible que desee ajustar el ancho de banda del sondeo para evitar la congestión de la red o reducir el impacto de un gran número de sucesos de sondeo que se producen de forma simultánea.

Configuración de la cantidad que sucesos que lee el sondeador

Grandes aumentos en el número de sucesos de red pueden ralentizar el proceso de sondeo, ncp_poller. Para minimizar el impacto en el rendimiento de repentinos aumentos en sucesos, puede definir la cantidad de sucesos de red que lee el sondeador.

Acerca de esta tarea

El proceso de sondeo, ncp_poller, lee sucesos de la tabla NCMONITOR.activeEvent en la memoria a intervalos para determinar el estado inicial de los sucesos de sondeo. Puede poner un límite superior en el número de sucesos que lee el sondeador. Los sucesos adicionales no se leen en memoria. Cuando el número de sucesos disminuye nuevamente por debajo del límite, el sondeador reanuda la lectura de sucesos.

Para configurar un límite para el número de sucesos que lee el sondeador, realice los pasos siguientes:

Procedimiento

1. Realice una copia de seguridad del archivo siguiente y edítelo: `NcPollerSchema.cfg`.
2. Edite, quite como comentario o añada la línea siguiente:

   ```
   update config.properties set EventThrottle = number_of_events
   ```

   donde *número_de_sucesos* es el número máximo de sucesos que leerá el sondeador. Si esta línea no está presente, no hay límite en el número de sucesos que el sondeador intenta procesar.
3. Guarde y cierre el archivo.

Cambio del intervalo para comprobar el tamaño de pertenencia de la política de sondeo

Puede cambiar el intervalo para comprobar el tamaño de pertenencia de la política de sondeo para todas las políticas de sondeo.

Acerca de esta tarea

Antes de cambiar el intervalo para comprobar el tamaño de pertenencia de la política de sondeo, debe tener en cuenta lo siguiente:

- Un intervalo mayor significa menos carga en le red debido a un tiempo mayor entren comprobaciones.
- Un intervalo más corto significa que ncp_poller se mantiene actualizado con cambios, especialmente el tamaño de pertenencia de vista de red.

Procedimiento

1. Edite el siguiente archivo de configuración: `$NCHOME/etc/precision/NcPollerSchema.cfg`.
2. Añada la línea siguiente al final del archivo:

   ```
   update config.properties set PolicyUpdateInterval= update_interval;
   ```

   donde: *update_interval* es el intervalo para comprobar el tamaño de pertenencia de la política de sondeo, en segundos. El valor predeterminado es de 30 segundos.
3. Reinicie el motor de sondeo, ncp_poller.

Habilitación e inhabilitación de las actualizaciones de vista de red para políticas de sondeo

De forma predeterminada, las actualizaciones de vista están habilitadas para todas las políticas de sondeo. Puede inhabilitar las actualizaciones de vista de red si está sondeando vistas de red estables. Esto impedirá problemas de rendimiento asociados con la actualización.

Procedimiento

1. Edite el siguiente archivo de configuración: $NCHOME/etc/precision/NcPollerSchema.cfg.
2. Añada la línea siguiente al final del archivo:

   ```
   update config.properties set UpdateNetworkViewCache = enable_or_disable_update;
   ```

   Donde: *enable_or_disable_update* es 1 (habilitar) o 0 (inhabilitar). El valor predeterminado es 1 (habilitar).
3. Reinicie el motor de sondeo, ncp_poller.

Ajuste del tamaño de las colas de datos de sondeo

Los problemas de base de datos o las altas cargas de sondeo pueden provocar que los sondeadores agoten la memoria si la cola de datos de sondeo para escribir en la base de datos NCPOLLDATA se hace demasiado grande. Para supervisar y evitar este problema, puede establecer un límite en el tamaño de la cola. El límite se define como el número de lotes. Si se sobrepasa el límite, se alertará en el registro y en la **Visor de sucesos**. A continuación, el sondeador reduce el tamaño de la cola descartando los datos en cola. Los datos descartados se graban en otro archivo.

Antes de empezar

Establezca el nivel de depuración del sondeador en 4.

Procedimiento

1. Para definir el límite, en el archivo $NCHOME/etc/precision/NcPollerSchema.cfg del sondeador, establezca el parámetro **PollDataQueueLimit** en el número de lotes adecuado. El ejemplo siguiente muestra cómo definir el límite en 50 lotes de datos en cola:

   ```
   update config.properties set PollDataQueueLimit = 50;
   ```
2. Supervise el archivo de registro del sondeador en $NCHOME/log/precision y **Visor de sucesos** para mensajes y alertas.

Resultados

Cuando la cola sobrepase el límite especificado por el parámetro **PollDataQueueLimit**, se realizan las acciones siguientes:

- En **Visor de sucesos**, se visualiza una alerta. Por ejemplo:

  ```
  ItnmPollerPolicyDataQueueFull: sondeador NCOMS; la cola de datos de sondeo ha
  sobrepasado su capacidad, descargando datos en archivo
  ```
- Se escribe un mensaje en el registro. Por ejemplo:

  ```
  2013-04-19T12:37:58 [CDataQueue::ProcessValue] El tamaño de cola ha sobrepasado el umbral,
  descartando datos: policyId:122:templateId:39:monitoredInstanceId:2212
  :monitoredObjectId:3:pollTime:1387232947:
  tdwTime:1131216222944000:errorCode:111:value:0
  ```
- Los datos de sondeo se descartan de la cola y se graban en un archivo $NCHOME/log/precision/ ncp_poller.*nombre_sondeador*.*dominio*.polldata, por ejemplo, ncp_poller.*nombre_sondeador*.*dominio*.data. Los datos sólo se muestran a título informativo y no se pueden insertar de nuevo en la base e datos de sondeo. Por ejemplo:

  ```
  MONITOREDOBJECTID,5, MONITOREDINSTID,184, POLLTIME,1447960873, ERRORCODE,100,
  VALUE, 0
  MONITOREDOBJECTID,6, MONITOREDINSTID,184, POLLTIME,1447960873, ERRORCODE,100,
  VALUE, -1
  MONITOREDOBJECTID,5, MONITOREDINSTID,248, POLLTIME,1447960873, ERRORCODE,100,
  VALUE, 100
  ```

Qué hacer a continuación

Si se sobrepasa el límite:

- Resuelva el tamaño de las colas de datos de sondeo. Por ejemplo, cree más sondeadores o póngase en contacto con el administrador de la base de datos.
- Borre la alerta de **Visor de sucesos**.
- Borre el archivo `.polldata`. El contenido del archivo no se borra ni se sustituye automáticamente.

Tareas relacionadas

Cambio del nivel de registro para los procesos
Cambie el nivel de registro de un proceso antes de iniciar el proceso o mientras este se está ejecutando.

Ubicación de archivos de registro para un proceso
Ubique archivos de registro para un proceso para obtener información que pueda ser útil para resolver problemas en el proceso.

Configuración de un sondeador adicional
Configure un sondeador adicional en el servidor de Network Manager si los sondeadores predeterminados no son suficientes para manejar la carga de red.

Supervisión de la capacidad del sondeador

Inicio de ncp_poller más rápido al no comprobar las credenciales SNMP

La inhabilitación de la comprobación de credenciales de acceso SNMP en el inicio de **ncp_poller** puede mejorar los tiempos de inicio.

Acerca de esta tarea

Si está seguro de que las credenciales de acceso de los dispositivos que desea sondear son precisas, puede configurar el proceso de sondeo, **ncp_poller**, para que no las compruebe en el inicio.

Procedimiento

1. Haga una copia de seguridad y edite el archivo `NCHOME/etc/precision/NcPollerSchema.`*`DOMAIN`*`.cfg`
2. Localice la línea que define el valor de la opción DiscoverInitialAccess.
3. Si desea que el proceso **ncp_poller** compruebe las credenciales SNMP cada vez que se inicie, deje el valor de DiscoverInitialAccess establecido en 1.
4. Para desactivar la comprobación inicial de las credenciales de acceso SNMP, establezca el valor de DiscoverInitialAccess en `0`. El proceso **ncp_poller** continúa comprobando las credenciales SNMP para un determinado dispositivo si se produce una anomalía de sondeo.
5. Reinicie el proceso **ncp_poller**.

Configuración del sondeo de estado de enlace

Puede especificar cómo el proceso de ncp_poller determina el estado inicial de los sondeos de estado de enlace cuando no hay ningún suceso existente.

Acerca de esta tarea

El proceso ncp_poller puede utilizar el primer sondeo para determinar el estado inicial de los sondeos de estado de enlace o suponer un estado de borrado.

Procedimiento

1. Edite el archivo `NCHOME/etc/precision/NcPollerSchema.cfg`.
2. Localice la sección `config.properties`.

3. Edite el valor de `UseFirstPollForInitialState`.
   - Establézcalo en 0 para establecer el estado inicial en Borrado.
   - Establézcalo en 1 para configurar el estado inicial para que se determine en el primer sondeo.

Conceptos relacionados

Sondeo de estado de enlace

El sondeo de estado de enlace supervisa los cambios en el estado de las siguientes variables MIB: ifOperStatus e ifAdminStatus.

Tareas relacionadas

Cambio de las definiciones de sondeo de estado de enlace y ping remoto

Utilice el **Editor de definiciones de sondeos** para cambiar los siguientes tipos de definición de sondeo: Ping remoto de Cisco, ping remoto de Juniper y estado de enlace de SNMP.

Administración de varios sondeadores

Si se necesitan más sondeadores para sondear la red, puede configurar nuevos sondeadores. Puede añadir o quitar sondeadores o utilizar un ID de sondeador para asociar un sondeador concreto con una política.

Descripción general de varios sondeadores

Puede utilizar sondeadores adicionales para escalar el sondeo a más dispositivos y por motivos de rendimiento.

El proceso del sondeador tiene dos funciones: sondear los dispositivos de red y realizar tareas administrativas, como actualizar memorias caché, el descarte de particiones y el soporte de **Gráfico de MIB de SNMP**. De forma predeterminada, el sondeador `ncp_poller_admin` se inicia con la opción `-admin` y realiza las tareas administrativas. El sondeador `ncp_poller_default` se inicia con la opción `-noadmin` y se utiliza para el sondeo de SNMP y Ping. Si tiene muchos dispositivos a sondear de forma regular, considere la posibilidad de utilizar varios sondeadores para el sondeo. Un sondeador debe iniciarse siempre con la opción `-admin` para realizar las funciones administrativas necesarias.

Nota: Puede crear versiones específicas de dominio y específicas de sondeador del archivo de configuración de sondeador, `NcPollerSchema.cfg`. Para crear una versión específica de dominio, añada el nombre de dominio al nombre de archivo; por ejemplo, `NcPollerSchema.`*`DOMINIO`*`.cfg`. Para crear una versión específica del sondeador, añada el nombre del sondeador y el nombre del dominio al nombre de archivo; por ejemplo, `NcPollerSchema.`*`NOMBRE_SONDEADOR`*`.`*`DOMINIO`*`.cfg`. Una instancia de sondeador utiliza el archivo de configuración más específico disponible.

Si utiliza la migración tras error, duplique en el servidor de copia de seguridad la misma disposición de sondeadores que tiene en el servidor primario.

Cada sondeador se registra con un nombre que puede utilizar el administrador para asociar una política con un sondeador.

Restricción: Para cualquier dominio proporcionado, en un entorno distribuido, todos los sondeadores deben iniciarse en el mismo servidor que el motor de descubrimiento.

Puede supervisar los motores de sondeo con las vistas de estado de Network Manager en IBM Tivoli Monitoring.

Para obtener más información, consulte la publicación *IBM Tivoli Network Manager IP Edition Administration Guide*.

Supervisión de Editor de políticas

El administrador controla qué sondeador utiliza una política. De forma predeterminada, cada política utiliza el sondeador `ncp_poller_default` en el servidor de Network Manager. El administrador puede seleccionar otro sondeador en una lista de sondeadores registrados.

Gráficos MIB en tiempo real

El administrador define el sondeador utilizado para los sondeos en tiempo real. De forma predeterminada, el sondeador `ncp_poller_admin` realiza esta función.

Información relacionada

Best Practices Guide for Remote Discovery en la página Network Manager Best PracticesPara obtener más información sobre la arquitectura distribuida, consulte la guía de prácticas recomendadas para el descubrimiento remoto en la página Network Manager Best Practices.

Configuración de un sondeador adicional

Configure un sondeador adicional en el servidor de Network Manager si los sondeadores predeterminados no son suficientes para manejar la carga de red.

Acerca de esta tarea

Los sondeadores predeterminados se instalan automáticamente al instalar Network Manager.De forma predeterminada, el sondeador `ncp_poller_admin` se inicia con la opción `-admin` y realiza las tareas administrativas. El sondeador `ncp_poller_default` se inicia con la opción `-noadmin` y se utiliza para el sondeo de SNMP y Ping.

Complete los siguientes pasos para registrar una nueva instancia del sondeador e iniciarlo automáticamente.

Procedimiento

1. Edite el archivo `CtrlServices.cfg`.
   a) Localice la entrada del proceso **`ncp_poller`**.
   b) Copie la entrada y cambie el valor de serviceName de esta nueva entrada de ncp_poller para que coincida con el nombre que utilizó para registrar el sondeador. De manera alternativa, edite el ejemplo comentado de un sondeador adicional en la versión predeterminada del archivo `CtrlServices.cfg` y establezca el valor de serviceName para que sea un nombre exclusivo para el sondeador.

      Importante: Asegúrese de que sólo uno de los sondeadores se haya iniciado utilizando la opción `-admin`, que configura el sondeador para que realice funciones administrativas esenciales. De forma predeterminada, este es el sondeador `ncp_poller_admin`. Inicie todos los demás sondeadores utilizando la opción -noadmin, que configura los sondeadores para no realizar funciones administrativas. Consulte las opciones de línea de comandos de ncp_poller para obtener información sobre otras opciones que puede utilizar para iniciar los sondeadores.
   c) Guarde y cierre el archivo.
2. Reinicie el proceso ncp_ctrl con el dominio especificado.

   El proceso **`ncp_ctrl`** reinicia todos los procesos **`ncp_`** en ejecución, incluido el nuevo sondeador. El sondeador registra automáticamente cualquier nuevo sondeador con nombre cuando se inicia.

Ejemplo

El ejemplo siguiente crea un sondeador, en el dominio NCOMS, que puede utilizar para determinados sondeos de ping y otro sondeador que puede utilizar para determinadas consultas de SNMP.

1. En el archivo `CtrlServices.cfg`, deje la entrada ncp_poller con el serviceName de ncp_poller_default tal cual. Este sondeador realiza las funciones administrativas y se utiliza para la creación de gráficos de MIB.
2. Elimine los comentarios de la entrada ncp_poller_ping. Esta inserción debería verse de la siguiente manera:

```
insert into services.inTray
(
    serviceName,
    binaryName,
    servicePath,
```

```
    domainName,
    argList,
    dependsOn,
    retryCount
)
values
(
    "ncp_poller_ping",
    "ncp_poller",
    "$PRECISION_HOME/platform/$PLATFORM/bin",
    "$PRECISION_DOMAIN",
    [ "-domain" , "$PRECISION_DOMAIN" , "-latency" ,  "200000", "-debug",  "0",
 "-messagelevel", "warn", "-name", "ncp_poller_ping", "-noadmin" ],
    [ "nco_p_ncpmonitor", "ncp_g_event" ],
    5
);
```

3. Añada una entrada similar para el sondeador snmpPoller. Esta inserción es idéntica a la inserción de PingPoller, salvo por el valor de serviceName, la opción -name en el parámetro argList.

```
insert into services.inTray
(
    serviceName,
    binaryName,
    servicePath,
    domainName,
    argList,
    dependsOn,
    retryCount
)
values
(
    "snmpPoller",
    "ncp_poller",
    "$PRECISION_HOME/platform/$PLATFORM/bin",
    "$PRECISION_DOMAIN",
    [ "-domain" , "$PRECISION_DOMAIN" , "-latency" , "60000", "-debug", "0",
"-messagelevel", "warn", "-name", "snmpPoller" "-noadmin"
 ],
    [ "nco_p_ncpmonitor", "ncp_g_event" ],
    5
);
```

Qué hacer a continuación

Una vez configurados los sondeadores, lleve a cabo los siguientes pasos:

1. Reinicie Network Manager, y, a continuación, inicie sesión en Network Manager.
2. Pulse el icono **Administración** y seleccione **Red** > **Sondeo de redes** para editar las definiciones de sondeo.
3. En **Propiedades de política de política de sondeo**, elija **Asignar a instancia de sondeador**.
4. Asigne un sondeo al sondeador existente y, a continuación, asigne otro sondeo al sondeador nuevo.

Asignación de un sondeador a gráficos MIB

Si desea cambiar el sondeador asignado para gestionar los gráficos MIB, edite el archivo de propiedades.

Antes de empezar

Es necesario que haya creado el sondeador que desea utilizar con los gráficos MIB antes de editar el archivo.

Acerca de esta tarea

Para asignar un sondeador para gráficos MIB:

Procedimiento

1. Abra el siguiente archivo: `$NMGUI_HOMEprofile/etc/tnm/tnm.properties`.

2. Cambie el valor del parámetro **tnm.graph.poller** del valor predeterminado ncp_poller_admin al nombre del sondeador necesario.
3. Guarde y cierre el archivo.

Eliminación de un sondeador

Si un sondeador no se utiliza para supervisar la red, puede eliminar el sondeador del sistema de supervisión.

Acerca de esta tarea

Para eliminar un sondeador del sistema de supervisión, anule el registro del sondeador en la línea de mandatos. El sondeador se elimina del editor Política de supervisor.

Lleve a cambio las siguientes tareas para eliminar un sondeador del sistema de supervisión.

Procedimiento

1. Antes de eliminar el sondeador, edite cada política activa asociada con el sondeador que desea eliminar. En el **Editor de políticas de supervisor**, edite las políticas para utilizar otro sondeador válido.
2. Detenga todos los procesos de Network Manager en ejecución.
3. En el servidor Network Manager, ejecute el siguiente mandato.

   ```
   ncp_poller -deregister -domain [nombre_dominio] -name [nombre_sondeador]
   ```

   Si no hay políticas activas asociadas con el sondeador, se anula el registro del sondeador. Si todavía hay políticas activas asociadas con el sondeador, el script no anula el registro del sondeador.
4. Si todavía hay políticas activas asociadas con el sondeador, asígnelas a otro sondeador o vuelva a ejecutar el script con la opción `-force`. Si ejecuta el script con la opción `-force`, también se suprimen todas las políticas de sondeo asociadas con el sondeador.
5. Edite el archivo `CtrlServices.cfg` para eliminar o eliminar el comentario de la entrada **ncp_poller** para el sondeador que ha eliminado.
6. Reinicie los procesos de Network Manager.

Administración de datos de sondeo históricos

Network Manager procesa los datos de sondeo históricos sin procesar y los transforma en datos de sondeo y almacena un año entero de datos de sondeo históricos agregados de.

Acerca de esta tarea

Network Manager utiliza el sistema de cálculo en tiempo real de Apache Storm para agregar datos de sondeo sin procesar a datos de sondeo históricos, y almacena los datos de sondeo sin procesar e históricos en la base de datos NCPOLLDATA.

Los datos de sondeo sin procesar e históricos se presentan en gráficos y tablas en **Panel de instrumentos de estado de red** y en los informes de rendimiento.

También puede acceder a estos datos dispositivo por dispositivo o haciendo clic en cada uno de los enlaces del mapa de topología dentro de la GUI de **Vista de saltos de red**, la GUI de **Vistas de red** y **GUI de las vistas de vías de acceso**.

Acerca de la agregación de datos de sondeo

La agregación de datos es el proceso en virtud del cual los datos de sondeo sin procesar se agregan a datos de sondeo históricos y se almacenan en la base de datos, desde donde pueden recuperarse para su presentación en gráficos, informes y paneles de control. Este es un sistema totalmente automatizado que comienza a procesar los datos cuando se inicia.

En los releases anteriores, la agregación de datos de sondeo para almacenar como datos históricos la realizaba Tivoli Data Warehouse. A partir de la versión 4.2, la agregación de datos de sonde se realiza por completo dentro de Network Manager

Nota: No existe ninguna vía de acceso de migración para los datos de sondeo históricos almacenados en una integración de Tivoli Data Warehouse antigua.

Una vez configurado, no es necesario realizar tareas de mantenimiento en el sistema. Existen mecanismos integrados que protegen el sistema si comienza a recibir más datos de los que puede manejar y métricas que hacen que sea más fácil de supervisar durante la fase de planificación.

Los usuarios pueden realizar un número muy limitado de tareas de configuración como, por ejemplo, definir si se agregarán datos de periodos de tiempo concretos. Por ejemplo, puede desactivar la agregación de datos para el período de datos anual.

Para muchos clientes, especialmente aquellos con grandes redes, la velocidad a la que se pueden recopilar los datos de sondeo puede ser alta. Es importante que el mecanismo utilizado para realizar la tarea de resumen sea capaz de gestionar la carga de datos sin provocar interrupciones en el sondeador. Apache Storm es un sistema de computación sistema en tiempo real distribuido que puede procesar secuencias de datos en vivo de forma eficiente. Apache Storm utiliza una topología que define las tareas de agregar los datos de sondeo y Storm gestiona a continuación las tareas y la carga de datos. La topología define cómo se procesan los datos en bruto para generar datos de sondeos agregados diarios, semanales, mensuales y anuales que se pueden almacenar en la base de datos NCPOLLDATA. De forma predeterminada, esta topología recibirá el nombre de NMStormTopology.

Agregación de datos de sondeo

El proceso de datos de sondeo históricos y el sistema de almacenamiento están diseñados para aceptar datos de todas las instancias del motor de sondeo, ncp_poller, en todos los dominios. Dentro de estas instancias de ncp_poller, solo los datos procedentes de políticas sondeo que se han configurado para almacenar datos se agregarán a los datos históricos.

El sistema agrega de forma automática datos a cuatro colecciones, cada una de las cuales representa un periodo de tiempo diferente:

- Último día
- Última semana
- Último mes
- Último año

Cada una de estas recopilaciones, incluida una recopilación adicional que recibe los datos sin procesar, se depuran de forma automática a medida que la antigüedad de los datos supera su periodo de tiempo. Los datos sin procesar se recopilan en una tabla de bases de datos que mantiene los datos de la última hora.

Los datos de sondeo sin procesar, y los resultados de la agregación de datos de los cuatro periodos temporales, se almacenan en la base de datos NCPOLLDATA. Todo el proceso de Apache Storm necesario para generar estos datos agregados se configura de forma predeterminada. Esto permite a Network Manager ofrecer una vista de los datos de sondeo de todo el año anterior.

Los datos de sondeo sin procesar, y los resultados de la agregación de datos de los cuatro periodos temporales, se almacenan en las siguientes tablas de bases de datos dentro de la base de datos NCPOLLDATA.

- Los datos de sondeo sin procesar se almacenan en la tabla pollData.
- Existen cuatro tablas de datos de resumen, una por cada periodo de tiempo. Para rellenar estas tablas con datos de sondeo históricos, Apache Storm lee continuamente datos de la tabla de datos de sondeo sin procesar, pollData, y calcula los datos de sondeo agregados en función de intervalos predeterminados independientes para cada periodo de tiempo utilizando el promedio de variación exponencialmente ponderada (EWMA) de los datos de sondeo sin procesar. Storm graba estos datos en la tabla de datos de sondeo agregados correspondiente. Por ejemplo, para el último día del periodo de tiempo, Storm calcula un promedio de los datos de sondeo sin procesar cada 15 minutos y graba este

promedio en la tabla pdEwmaForDay. Las siguientes tablas de bases de datos NCPOLLDATA almacenan datos de sondeo históricos.

Nota: Los datos agregados se almacenan en la base de datos NCPOLLDATA sin tener en cuenta el dominio.

Tabla pdEwmaForDay
Almacena el último día agregado de datos de sondeo con una media móvil de 15 minutos.

Tabla pdEwmaForWeek
Almacena la última semana agregada de datos de sondeos con una media móvil de dos horas.

Tabla pdEwmaForMonth
Almacena el último mes agregado de datos de sondeos con una media móvil de 8 horas.

Tabla pdEwmaForYear.
Almacena el último año agregado de datos de sondeos con un promedio oscilante de 4 días.

Depuración de datos de sondeo

La depuración de los datos de sondeos históricos y sin formato se maneja automáticamente, utilizando el particionamiento de datos para una mayor eficacia.

Cada tabla de datos de sondeos históricos tiene un límite de tiempo y la tabla se particiona en ranuras de tiempo. Por ejemplo, la tabla pdEwmaForDay que almacena datos de sondeos históricos del último día, contiene 25 horas de datos divididos en 25 particiones de 1 hora cada una.

Las inserciones en las tablas se realizan en la partición más reciente y se depura la partición más antigua. Este método disminuye los conflictos entre las operaciones de inserción y supresión, por lo que mejora la depuración y la eficacia de la inserción. La depuración automática está basada en un factor de antigüedad, adecuado a cada tabla. instanciaPor ejemplo, en la tabla forDay, se descartan las particiones cuando la antigüedad de los datos supera las 24 horas. Este método de depuración garantiza que, cuando el número total de entidades sondeadas y KPI sondeados es fijo, el tamaño de cada tabla de datos de sondeos históricos permanece estable y dentro de los límites recomendados.

Nota: Todas las consultas SQL en estas tablas se pueden realizar sin hacer referencia a, o sin conocer, las particiones.

Directrices de capacidad para sondeos de datos históricos

Utilice esta información para ayudar a calcular la carga de sondeo y determinar si la carga de sondeo está dentro de los límites de almacenamiento recomendados para tener un sistema de sondeo estable y que funcione perfectamente.

Consideraciones sobre el dimensionamiento

La carga de sondeo de un servidor se puede expresar calculando el índice general de inserciones de sondeos en la base de datos NCPOLLDATA. Cuanto más alto sea el índice de inserción, más grande será la capacidad necesaria dentro de las tablas de almacenamiento de datos sin procesar e históricos para almacenar datos de sondeos. Una vez que las tablas de datos de sondeo históricos sobrepasen un determinado tamaño, el rendimiento de las consultas de las tablas por parte de los paneles de control y los informes posiblemente se degradará; por lo tanto, el índice de inserciones para la tabla de datos de sondeo sin formato POLLDATA y el número total de filas en las tablas de datos de sondeo históricos no debe sobrepasar el límite recomendado para garantizar la estabilidad del sistema.

Se recomienda que el índice de inserción de sondeos a la tabla de datos de sondeo sin formato POLLDATA no supere los 20 millones de inserciones a la hora y que el número total de filas para las tablas de datos agregadas no supere los 200 millones de filas. Esto garantiza que el tamaño de las tablas de datos de sondeo históricos se mantendrán dentro de unos límites aceptables.

Tablas de dimensionamiento

Utilice estas tablas como ayuda para determinar la carga de sondeo adecuada para su sistema, en concreto, el número de entidades y de KPI que debe sondear y el intervalo de sondeo que se ha de establecer para sus políticas de sondeo.

Utilice la tabla siguiente para determinar la tasa de inserción de sondeo aproximada y el número de filas que generará esta tasa de inserción en cada una de las tablas de datos de sondeos históricos. Utilice estas tablas revisando las columnas siguientes y buscando los valores que más se aproximen a los valores de su red:

En cada uno de los ejemplos que se presentan en la tabla, se presupone que el número de KPI (definiciones de sondeos) por política de sondeo y el intervalo de sondeo para cada política de sondeo son los siguientes:

Tabla 75. Número de KPI y de intervalos de sondeo por política de sondeo

	Número de KPI	**Intervalo de sondeo en minutos**	**Número de sondeos por hora**
Sondeos de chasis	3	5	36
Sondeos de chasis	5	5	60

Los siguientes ejemplos muestran cómo cambian los valores de la tasa de inserción y el número de filas de las tablas de datos de sondeos históricos, a medida que varía el número de entidades sondeadas de su red.

Ejemplo que entra dentro de los límites recomendados

Los ejemplos siguientes entran dentro de los límites recomendados para un sistema de sondeo estable.

Número de entidades sondeadas

- Dispositivos de chasis: 15.000
- Interfaces: 300.000

Tabla 76. tasa de inserción y el número de filas en millones por tabla de datos de sondeos históricos

	Tasa de inserción [Inserciones/ hora]	**Último día [Millones de filas]**	**Última semana [Millones de filas]**	**Último mes [Millones de filas]**	**Último año [Millones de filas]**
Sondeos de chasis	0,72	5,76	5,04	5,4	5,475
Sondeos de chasis	18,56	153,6	134,4	144	146
Total	19,28	159,36	139,44	149,4	151,475

Ejemplo que queda fuera de los límites de almacenamiento recomendados

Los ejemplos siguientes quedan fuera de los límites del recomendado para un sondeo de sistema estable.

Número de entidades sondeadas

- Dispositivos de chasis: 30.000
- Interfaces: 500.000

Tabla 77. tasa de inserción y el número de filas en millones por tabla de datos de sondeos históricos					
	Tasa de inserción [Inserciones/ hora]	**Último día [Millones de filas]**	**Última semana [Millones de filas]**	**Último mes [Millones de filas]**	**Último año [Millones de filas]**
Sondeos de chasis	1.080.000	8,64	30,24	32,4	32,85
Sondeos de chasis	30.000.000	240	840	900	912,5
Total	31.080.000	248,64	870,24	932,4	945,35

Realice la prueba

Utilice la calculadora de la hoja de cálculo disponible en SMC para calcular estos valores:

- Número estimado de entidades sondeadas en su red
- Promedio de KPI y de intervalos de sondeo entre las políticas de sondeo

La hoja de cálculo realiza el cálculo de la tasa de inserciones y el número de filas de las tablas de datos de sondeos históricos de red, basándose en los valores estimados.

Información relacionada

Network Manager Calculadora para el tamaño del sistema y el almacenamiento de datos por sondeo En esta página puede encontrar la calculadora de la hoja de cálculo que calcula la tasa de inserción y el número de filas en las tablas de datos históricos de los sondeos en función de valores estimados.

Límites de tolerancia del sistema

Los orígenes principales de las potenciales interrupciones del sistema son la pérdida de conexión con la base de datos NCPOLLDATA y la detención del proceso de Apache Storm. El sistema es tolerante con todas estas eventualidades y si todas las conexiones y procesos se restauran dentro de unos determinados periodos de tiempo, no se perderá ningún dato.

Apache Storm está inactivo

En las siguientes secciones se describe con más detalle la tolerancia del sistema:

Si Apache Storm se detiene y continúa así durante menos de una hora, no se verán afectados la colección de datos de sondeo sin procesar y el almacenamiento en la tabla pollData. Al reiniciarse, Storm continuará procesando de forma automática las filas de pollData desde el punto donde se detuvo, asegurándose de que todos los datos de sondeo sin procesar dentro de esa hora se hayan procesado correctamente e incluido en los datos de sondeo históricos. Tenga en cuenta que durante el tiempo que Apache Storm esté detenido, no se añadirá ningún dato a las tablas de datos de sondeo históricos.

Si Apache Storm se detiene y continúa así durante más de una hora, los datos de la tabla pollData empezarán a caducar y no se procesarán en incluirán en las tablas de datos de sondeo históricos.

La base de datos NCPOLLDATA está inactiva

En las siguientes secciones se describe con más detalle la tolerancia del sistema:

Si la base de datos NCPOLLDATA está inactiva durante menos de 5 minutos, todas las instancias de ncp_poller retendrán datos en una almacenamiento intermedio y cuando se restablezca la conexión con la base de datos, los datos del almacenamiento intermedio se grabaran de forma automática en la tabla pollData.

Si la base de datos NCPOLLDATA está inactiva durante más de 5 minutos, en algún momento, el almacenamiento intermedio en memoria se agotará y los datos más antiguos se pierden hasta que la conexión a la base de datos se reanuda.

Inicio y detención de Apache Storm

Puede iniciar, detener y obtener el estado del sistema Apache Storm mediante los mandatos itnm_start, itnm_stop e itnm_status.

Acerca de esta tarea

Para obtener más información, consulte la *IBM Tivoli Network Manager IP Edition Administration Guide*.

Configuración de la agregación de datos de sondeo

Todo el proceso de Apache Storm necesario para generar estos datos de sondeo históricos se configura de forma predeterminada. Sin embargo, puede llevar a cabo un conjunto limitado de tareas de configuración.

Especificación de los periodos de datos de sondeo históricos que se van a almacenar

De forma predeterminada, Network Manager almacena datos de sondeo histórico en periodos de tiempo diarios, semanales, mensuales y anuales. Puede desactivar el almacenamiento de datos de sondeo históricos para cualquiera de estos periodos.

Acerca de esta tarea

Para desactivar los datos de sondeo históricos diarios, semanales, mensuales o anuales, lleve a cabo los pasos siguientes.

Procedimiento

1. Edite el archivo de propiedades para la topología Storm utilizando un editor de texto como vi.

   De forma predeterminada, la topología Apache Storm toma el nombre `NMStormTopology` y utiliza el archivo de propiedades llamado `NMStormTopology.properties`.

   ```
   vi $NCHOME/precision/storm/conf/NMStormTopology.properties
   ```

2. Busque una de las siguientes propiedades en el archivo y establézcala en 0, para desactivar el almacenamiento de datos de sondeo históricos para el periodo de tiempo correspondiente.

   ewma.day.storage.enabled
   Establecer en false para desactivar el almacenamiento de datos de sondeo históricos diario

   ewma.week.storage.enabled
   Establecer en false para desactivar el almacenamiento de datos de sondeo históricos semanal

   ewma.month.storage.enabled
   Establecer en false para desactivar el almacenamiento de datos de sondeo históricos mensual

   ewma.year.storage.enabled
   Establecer en false para desactivar el almacenamiento de datos de sondeo históricos anual
3. Guarde el archivo.
4. Reinicie la topología Apache Storm.

Otras opciones de configuración de datos de sondeo históricos

El archivo de configuración `NMStormTopology.properties` también contiene los siguientes parámetros. Se recomienda encarecidamente dejar estos valores en los valores predeterminados.

Periodos de agregación

ewma.day.window.period.minutes
La ventana, en minutos, sobre qué datos de sondeo sin procesar de entrada se agregan para un único punto de datos en la tabla agregada para el día. Se genera un punto de datos únicamente si hay nuevos datos disponibles dentro de cada ventana, por lo que no tiene sentido que sea inferior al intervalo de sondeo del sondeador más pequeño. El rango permitido es de 1 a 60 minutos. El valor predeterminado es de 15 minutos

ewma.week.window.period.minutes
La ventana, en minutos, sobre qué datos de sondeo sin procesar de entrada se agregan para un único punto de datos en la tabla agregada para la semana. Se genera un punto de datos únicamente si hay nuevos datos disponibles dentro de cada ventana. El rango permitido es de 1 a 300 minutos. El valor predeterminado es de 120 minutos.

ewma.month.window.period.hours
La ventana, en minutos, sobre qué datos de sondeo sin procesar de entrada se agregan para un único punto de datos en la tabla agregada para el mes. Se genera un punto de datos únicamente si hay nuevos datos disponibles dentro de cada ventana. El rango permitido es de 1 a 24 horas. El valor predeterminado es de 8 horas.

ewma.year.window.period.days
La ventana, en minutos, sobre qué datos de sondeo sin procesar de entrada se agregan para un único punto de datos en la tabla agregada para el año. Se genera un punto de datos únicamente si hay nuevos datos disponibles dentro de cada ventana. El rango permitido es de 1 a 30 días. El valor predeterminado es un día.

Acceso a base de datos

nm.domain
El servidor Apache Storm utiliza este parámetro para encontrar credenciales que le permitan acceder a la base de datos NCPOLLDATA. Storm busca los archivos `DbLogins.`*`domain_name`*`.cfg` y `tnm.`*`domain_name`*`.properties` específicos de dominio. El parámetro `nm.domain` se establece durante la instalación. Storm retrocederá a las versiones genéricas de estos archivos (`DbLogins.cfg` y `tnm.properties`) si no se han encontrado versiones específicas de dominio de los archivos

Intervalo de lectura de la tabla de datos sin procesar

ncpolldata.read.interval.seconds

El intervalo al que se consulta la tabla de datos de sondeo. El rango permitido es de 5 a 3000 segundos. El valor predeterminado es 60 segundos.

Número de conexiones JDBC

ewma.day.jdbc.connection.count
ewma.week.jdbc.connection.count
ewma.month.jdbc.connection.count
ewma.hour.jdbc.connection.count

El número de conexiones JDBC para insertar datos a las distintas tablas de agregación. El rango permitido es de 1 a 10.

Supervisión de la capacidad del sondeador

Para evitar que se produzcan problemas en los sondeadores, supervise las métricas del sondeador mostrándolas como salida en la interfaz de línea de mandatos. Las métricas se muestran como gráficos de barras. Las métricas muestran cuándo un sondeador alcanza su capacidad, por ejemplo, si el bajo rendimiento de base de datos provoca que quede por debajo.

De forma predeterminada, las métricas se escriben en un rastreo en `NCHOME/log/precision` cada 2 minutos. Existe un rastreo para cada sondeador. El nombre del archivo de rastreo tiene el formato `ncp_poller.SnmpPoller.`*`dominio`*`.metrics` para el sondeador predeterminado y `ncp_poller.SnmpPoller.`*`nombre_sondeador`*`.`*`dominio`*`.metrics` para todos los demás

sondeadores. Por ejemplo, `ncp_poller.SnmpPoller.Poller23507.NCOMS.metrics`. La tabla siguiente describe las métricas.

Tabla 78. Métricas de sondeador

Métrica	Mide	Medido en (las unidades del eje y de cada gráfico de barras)
Health	El porcentaje de dispositivos que se sondean durante un ciclo de política. Si el valor es 100%, el sondeador está funcionando correctamente. Si el valor es inferior a 100%, no todos los dispositivos se sondean durante el intervalo de sondeo. El sondeador no puede seguir el ritmo de la carga de política.	%
Memoria	La memoria que utiliza el sondeador. El uso de memoria aumenta a medida que se descubren los dispositivos o que se habilitan más políticas.	MB
BatchQueueSize	El número de lotes que están esperando una hebra.	Recuento
PollDataQueueSize	El número de sentencias INSERT en cola en la base de datos NCPOLLDATA. Muestra si el sondeador está almacenando correctamente los datos de sondeo.	Recuento
PollDataRowCount	La velocidad de inserción en la tabla de datos de sondeo en bruto ncpolldata.pollData, expresada como el número de registros insertados a lo largo de una hora. Esta métrica es útil sólo si se utiliza el sondeo histórico.	Recuento

Antes de empezar

Asegúrese de que el terminal en el que se van a mostrar los gráficos de barras tiene una anchura mínima de 140 caracteres. De lo contrario, el gráfico de barras no se visualizará correctamente debido a la acomodación de líneas.

Procedimiento

Ejecute el script `itnm_poller.pl` tal como se muestra en los ejemplos.
El siguiente ejemplo muestra cómo visualizar los gráficos para el sondeador predeterminado, en el dominio NCOMS, desde la indicación de fecha y hora más reciente, por encima de un periodo predeterminado de 4 horas:

```
ncp_perl itnm_poller.pl -domain NCOMS -metrics
```

El ejemplo siguiente muestra cómo ejecutar el script para el mismo dominio para un sondeador concreto, durante las últimas 12 horas:

```
ncp_perl itnm_poller.pl -domain NCOMS -poller Poller23507 -metrics -window 12
```

El ejemplo siguiente muestra cómo ejecutar el script para el mismo dominio y sondeador, desde una indicación de fecha y hora concreta, durante un periodo de 8 horas:

```
ncp_perl itnm_poller.pl -domain NCOMS -poller Poller23507 -metrics
-timestamp 2013-12-10T17:30:36 -window 8
```

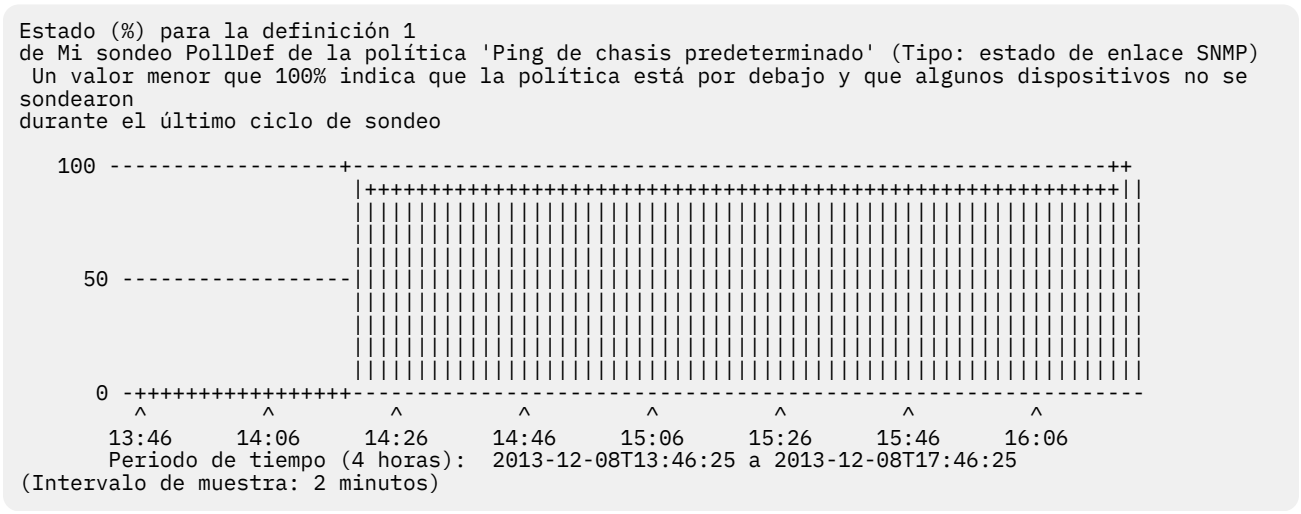
No ejecute el script con la opción `-metrics` y la opción `-status` simultáneamente.

Resultados

Preste especial atención a la escala del eje Y. Un gráfico de barras que aparece sin cambios durante un largo periodo de tiempo, por ejemplo 24 horas, podría mostrar diferencias en los valores cuando se visualiza durante un periodo más corto, por ejemplo 4 horas.

Ejemplo

El ejemplo siguiente muestra un gráfico de ejemplo para la métrica Health (estado).



Qué hacer a continuación

Revise los problemas y las posibles causas en las tablas siguiente y realice la acción adecuada.

Tabla 79. Posibles causas de problemas con las métricas de sondeador

Métrica	Problema	Causa posible	Acciones
Health	El valor está de forma constante por debajo de 100%.	El porcentaje puede caer de forma temporal por debajo de 100% después de que se inicie el sondeador, o si se recibe información de cambio de la base de datos MODEL.	• Aumente el intervalo de sondeo modificando la política de sondeo • Añada más sondeadores.

Tabla 79. Posibles causas de problemas con las métricas de sondeador (continuación)

Métrica	Problema	Causa posible	Acciones
Memoria	La memoria crece de forma ilimitada	Se ha perdido la conexión con la base de datos. O también, la carga de sondeo es demasiado alta para que se pueda mantener, o la tasa de almacenamiento de datos es demasiado alta para que se pueda mantener.	• Póngase en contacto con el administrador de base de datos. • Añada más sondeadores.
BatchQueue	El número de lotes que están esperando una hebra es mayor que 0 y sigue aumentando.	El número de hebras se ha agotado, lo que puede indicar que el asignador SNMP de bajada está cerca de la capacidad.	Aunque es posible aumentar el número de hebras estableciendo la propiedad **`BatchExtraThreads`** en el archivo `NcPollerSchema.cfg`, no es la mejor solución. Es posible que aumentar el número de hebras empeore el problema. Las soluciones más seguras son las siguientes: • Añada más sondeadores. • Póngase en contacto con el administrador del sistema para analizar si se debe añadir RAM al host. **Consejo:** Defina un umbral sobre el número de lotes que se encuentran en la cola para su proceso. Si se sobrepasa el umbral, se alertará en el archivo de registro del sondeador."1" en la página 521
PollDataQueueSize	El número de sentencias INSERT en la cola crece de forma exponencial.	Se ha perdido la conexión a la base de datos o la frecuencia de sentencias INSERT es mayor que la que puede gestionar el sondeador.	• Póngase en contacto con el administrador de base de datos. • Añada más sondeadores.

Tabla 79. Posibles causas de problemas con las métricas de sondeador (continuación)

Métrica	Problema	Causa posible	Acciones
PollDataRowCount	El número de filas sobrepasa el umbral después de que se haya completado la poda. El umbral predeterminado es 5.000.000 y el intervalo de poda predeterminado es de 1 hora.	La carga de sondeo es demasiado pesada y, por tanto, el número de filas es demasiado alto para que se pueda recortar dentro del intervalo de poda. O también, se han producido problemas en la base de datos, lo que provoca problemas con la poda.	Póngase en contacto con el administrador de base de datos.

Notas de la tabla:

1. Para definir un umbral, cambie el valor de la propiedad **BatchQueueThreshold** de $NCHOME/etc/precision/NcPollerSchema.cfg a un valor adecuado. Por ejemplo, para definir el umbral en 10 lotes de sondeos en cola:

   ```
   update config.properties set BatchQueueThreshold = 10;
   ```

   Cuando la cola sobrepase el umbral especificado, se escribe un mensaje similar al ejemplo siguiente:

   ```
   2013-04-19T12:37:58:Poller:NCOMS:DataQueueSize:10;
   ```

Si se muestra un error, compruebe el archivo $NCHOME/etc/precision/NcPollerSchema.cfg para ver si el parámetro **CollectPollerMetrics** está inhabilitado. Este parámetro está habilitado de forma predeterminada pero, si se encuentra inhabilitado, habilítelo. Puede utilizar la interfaz OQL para habilitar el parámetro en tiempo de ejecución. Por ejemplo:

```
ncp_oql -domain NCOMS -service SnmpPoller -poller Poller23507
-query “update config.properties set CollectPollerMetrics=1;”
```

Tareas relacionadas

Configuración de un sondeador adicional
Configure un sondeador adicional en el servidor de Network Manager si los sondeadores predeterminados no son suficientes para manejar la carga de red.

Modificación de políticas de sondeo
Utilice el **Editor de políticas de sondeo** para modificar los valores de políticas de sondeo existentes.

Ajuste del tamaño de las colas de datos de sondeo

Capítulo 27. Resolución de problemas del sondeo de red

Utilice esta información para entender cómo resolver los problemas de sondeo de red.

Resolución de problemas del sondeo ping de la red

Utilice esta información para que le ayude a asegurarse de que el sondeo ping de las direcciones IP importantes de la red realizado por Network Manager es el previsto o, en caso contrario, para proporcionar información para solucionar el problema.

Antes de empezar

De forma predeterminada, las tablas y vistas definidas en el archivo `$NCHOME/precision/scripts/sql/`*`tipo_base_datos`*`/createPollLogTables.sql` se añaden al esquema NCMONITOR como parte de la instalación de Network Manager. Estas tablas y vistas almacenan los resultados de las operaciones de diagnóstico realizadas en este procedimiento.

Nota: Este mecanismo se refiere solo a las políticas de sondeo ping y no a las políticas de sondeo SNMP.

Este procedimiento incluye un paso para tomar una instantánea del estado de sondeo de ping actual dentro de un dominio de red específico. Después de iniciar el Network Manager proceso de sondeo, debe permitir al menos dos intervalos de sondeo antes de tomar la primera instantánea. No es necesario reiniciar el sistema.

Acerca de esta tarea

Dado un conjunto de direcciones IP, los scripts descritos en esta tarea ayudan a comprender mejor si el sondeador está haciendo ping a esas direcciones IP y, si no lo está haciendo, proporcionan una indicación de lo que es el problema. Existen varias razones por las que no es posible hacer sondeo a las direcciones IP incluyendo lo siguiente:

- No se ha descubierto el dispositivo especificado en la política de sondeo.
- El dispositivo o interfaz no está incluido en ninguno de los ámbitos de política de ping.
- El dispositivo o interfaz se ha marcado como no gestionado desde una de las GUI de visualización de topología.
- La interfaz se marcó como no gestionada en el momento de descubrimiento o se ha determinado que no se puede crear una ruta hacia ella.

Para obtener más información sobre los scripts descritos en esta tarea, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Nota: Estos scripts son únicamente una herramienta de diagnóstico y verificación y no tienen efecto en el sondeo real de los dispositivos; el sondeo de dispositivos se rige únicamente por las políticas de sondeo establecidas utilizando la GUI de sondeo de red.

Procedimiento

1. Agregue la lista de direcciones IP cuyo sondeo quiere supervisar utilizando el script `ncp_upload_expected_ips.pl`.

   Emita el siguiente mandato:`$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/ncp_upload_expected_ips.pl -domain` *`DOMAIN_NAME`* `-file` *`FILENAME`* `-password` *`PASSWORD`*

   Donde:

- *NOMBRE_DOMINIO* es el nombre del dominio que contiene las direcciones IP. La lista de direcciones IP solo se comparará con las direcciones IP de este dominio.
- *NOMBREARCHIVO* es un archivo de texto plano de direcciones IP, separadas por espacios en blanco (por ejemplo, una dirección IP por línea). Solo acepta direcciones IPv4. Se supone que el archivo solo contiene direcciones IP en notación de punto estándar.
- *CONTRASEÑA* es la contraseña de la base de datos utilizada para acceder a los esquemas NCIM y NCMONITOR.

Nota: Repita esta operación solo si hay cambios en la lista de direcciones IP cuyo sondeo quiera supervisar. De lo contrario, se convierte en una única operación por dominio.

2. De forma periódica, o cuando sea necesario para resolver problemas, tome una instantánea del estado de sondeo de ping actual dentro del dominio especificado en el paso anterior.

   Emita el siguiente mandato:`$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/ ncp_ping_poller_snapshot.pl -domain DOMAIN_NAME -password PASSWORD`

   Donde:

   - *NOMBRE_DOMINIO* es nombre del dominio dentro del cual de debe tomar la instantánea del estado de sondeo de ping actual.
   - *CONTRASEÑA* es la contraseña de la base de datos utilizada para acceder a los esquemas NCIM y NCMONITOR.

   Los resultados de la operación están almacenados en la tabla de la base de datos pollLog dentro del esquema NCMONITOR.
3. Informe sobre las entidades que no están siendo sondeadas. Ejecute el informe de estado de las entidades sondeadas o no por el proceso de sondeo de Network Manager.

   Emita el siguiente mandato:`$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/ ncp_polling_exceptions.pl -domain DOMAIN_NAME [ -notpolled ] [-format LIST | REPORT ]`

   Donde:

   - *NOMBRE_DOMINIO* es el nombre del dominio dentro del que se informa sobre el estado de sondeo de ping actual.
   - `-notpolled`: este parámetro opcional devuelve una lista de direcciones IP que no se sondean, en comparación con la lista de direcciones IP esperadas. Esta salida sólo está disponible en formato LIST.
   - `-format LIST | REPORT`: este parámetro opcional especifica si la salida debe ser en formato de informe o lista.

   Este mandato devuelve dos listas: una lista de las direcciones IP que desea sondear y una lista de las direcciones IP que no se están sondeando. Puede ver de un vistazo si alguna de las direcciones IP que desea sondear no se está sondeando.

Tareas relacionadas

Resolución de problemas de Network Manager
Consulte estas notas de resolución de problemas para ayudarse a determinar la causa del problema y cómo solucionarlo.

Resolución de problemas del sondeo de SNMP

Hay un valor de configuración en el sondeador denominado AggregationLimit. Este valor se aplica únicamente a políticas de sondeo de SNMP que tienen habilitado el filtrado de interfaz. El valor de AggregationLimit determina cómo el proceso `ncp_poller` divide los sondeos que contienen varias solicitudes SNMP GET. Es posible que tenga que modificar el valor predeterminado dependiendo de los datos que está sondeando en la red.

Acerca de esta tarea

El proceso `ncp_poller` divide las solicitudes de sondeo en paquetes de Unidad de datos de protocolo SNMP (PDU) hasta el límite de agregación inferior. Por ejemplo, cuando el valor del límite de agregación se establece en el valor predeterminado de 30, el proceso `ncp_poller` crea PDU con no menos de 30 solicitudes SNMP GET individuales. Este valor predeterminado, `AggregationLimit = 30`, puede generar errores en las siguientes situaciones. En ambos casos, debe disminuir el valor del parámetro `AggregationLimit`.

- En datos de sondeo grandes, los resultados recuperados por las 30 solicitudes 30 SNMP GET pueden sobrecargar las PDU de resultados. Esta situación se puede producir al emitir solicitudes de sondeo de ancho de banda.
- Si uno de los OID que se está solicitando dentro de la PDU no existe, se devuelve la PDU de resultados con un código de error y se descarta todo el sondeo. Este problema se puede producir cuando se trabaja con tablas dispersas. Cuando esto sucede el sondeo se descartará si sólo falta una entrada.

Nota: Disminuir el valor del parámetro `AggregationLimit` tiene el siguiente impacto sobre el rendimiento del sistema:

- Aumento en el volumen de datos de tráfico de SNMP transmitidos a través de la red. Por ejemplo, un descenso del valor de `AggregationLimit` de 30 a 1 da como resultado un aumento multiplicado por cuatro aproximadamente del volumen de datos de tráfico de SNMP transmitidos a través de la red.
- El aumento correspondiente en la utilización de CPU para el proceso ncp_poller: Por ejemplo; un descenso del valor de `AggregationLimit` de 30 a 1 da como resultado un aumento de aproximadamente el 50% de utilización de CPU para el proceso ncp_poller.

Hay un impacto proporcional de valores entre 30 y 1. Por ejemplo, si el valor del parámetro `AggregationLimit` disminuye de 30 a 15, este cambio da como resultado un aumento aproximadamente doble del volumen de datos de tráfico de SNMP transmitidos a través de la red. El aumento correspondiente en la utilización de CPU debe estar en el orden del 25%.

Después de un cambio en el valor de `AggregationLimit`, debe supervisar el rendimiento del proceso ncp_poller supervisando la métrica de ncp_poller.

Para cambiar el valor de AggregationLimit predeterminado, lleve a cabo los siguientes pasos.

Procedimiento

1. Edite el archivo NcPollerSchema.cfg ubicado en `$NCHOME/etc/precision`.
2. Añada la línea siguiente al final del archivo:

   ```
   update config.properties set AggregationLimit = aggregationLimit;
   ```

   Donde *aggregationLimit* es el valor del límite de agregación. De forma predeterminada es 30.
3. Reinicie el proceso `ncp_poller`.

Tareas relacionadas

Supervisión de la capacidad del sondeador

Resolución de problemas del proceso de datos de sondeo históricos

Puede definir umbrales relacionados con la antigüedad de los datos de las tablas de datos de sondeo históricos y relacionados con el tamaño de las tablas de datos de sondeo. Si se sobrepasan estos umbrales, es señal de que la carga de sondeos es demasiado grande o de que existe un problema con el sistema de datos de sondeo históricos o con la base de datos de los sondeos. Las violaciones de umbral generan mensajes de registro, así como alertas de Tivoli Netcool/OMNIbus ObjectServer que se pueden ver en el GUI web de Tivoli Netcool/OMNIbus **Visor de sucesos**.

Acerca de esta tarea

Si se produce alguno de estos sucesos, se generará una alerta de Tivoli Netcool/OMNIbus ObjectServer. Estas alertas tienen un grupo de alertas definido como Estado de ITNM:

Se ha sobrepasado la velocidad máxima de inserción para la tabla de datos de sondeo sin procesar.
La velocidad máxima de inserción en la tabla de datos de sondeo sin procesar ncpolldata.pollData se define en la tabla de bases de datos de configuración, `config.tableMonitor`. Si se superan estos valores, se genera una alerta de Estado de ITNM en el GUI web de Tivoli Netcool/OMNIbus **Visor de sucesos**, y se graba un mensaje de registro en el archivo de registro de `NCHOME/log/precision/ncp_poller.SnmpPoller.`*`nombre_sondeador.dominio`*.

Si se sobrepasa la velocidad máxima de inserción, es señal de que la carga de sondeo es demasiado grande. Es posible que necesite ajustar la carga de sondeos reduciendo el número de dispositivos que se van a sondear y también el número de métricas que se van a recopilar en estos dispositivos o modificando los intervalos de sondeo.

Los recuentos de antigüedad se han sobrepasado en las tablas de datos de sondeo históricos
Los ajustes de antigüedad máxima para las tablas de datos de sondeo históricos en la base de datos ncpolldata se definen en la tabla de bases de datos `config.tableMonitor`. Si se sobrepasan estos valores, se emite una alerta de Estado de ITNM en el GUI web de Tivoli Netcool/OMNIbus **Visor de sucesos** y se graba un mensaje de registro en el archivo de registro de `NCHOME/log/precision/ncp_poller.SnmpPoller.`*`nombre_sondeador.dominio`*.

Si se sobrepasa algunos de estos valores de antigüedad máxima, es señal de que el mecanismo de depuración de datos no funciona. Es posible que el sistema Apache Storm, que procesa datos de sondeo históricos, no funcione o que no se adapte al ritmo de los sondeos y las depuraciones. También, podría indicar que se ha producido un problema con el servidor de bases de datos que aloja la base de datos ncpolldata.

No se ha recibido ninguna señal de monitorización de Apache Storm
El sistema comprueba la indicación de fecha y hora dentro de una base de datos ncpolldata. Si esta indicación de fecha y hora no se actualiza, indica que no se ha recibido ninguna señal de monitorización del sistema Apache Storm, que procesa datos de sondeo históricos. En este caso, se generará una alerta de Estado de ITNM en el GUI web de Tivoli Netcool/OMNIbus **Visor de sucesos**.

Si no se recibe la señal de monitorización de Apache Storm, podría significar que Apache Storm no se está ejecutando o necesita atención.

Los lotes procesados por Apache Storm llevan retraso con respecto a los lotes de sondeo.
El motor de sondeo ncp_poller recopila datos de sondeo sin procesar en lotes y les asigna un ID de lote a cada uno. Al procesar estos datos de sondeo sin procesar y convertirlos en datos históricos, Apache Storm marca cada lote para indicar que se ha procesado. El estado del ID de los lotes de datos de sondeo más recientes se comprueba de forma periódica. Si los tiempos asociados con el identificador del lote del último conjunto de sondeos sin procesar muestran que los datos procesados por Apache Storm llevan retraso con respecto a los últimos lotes grabados por ncp_poller, se genera una alerta de Estado de ITNM en el GUI web de Tivoli Netcool/OMNIbus **Visor de sucesos**.

Si el proceso por lotes se retrasa, podría indicar que Apache Storm no se está ejecutando o que necesita atención.

Tareas relacionadas

Inicio y detención de Apache Storm
Puede iniciar, detener y obtener el estado del sistema Apache Storm mediante los mandatos itnm_start, itnm_stop e itnm_status.

Referencia relacionada

Sucesos de estado de Network Manager
Network Manager puede generar sucesos que muestren el estado de varios procesos de Network Manager. Estos sucesos se conocen como sucesos de estado de Network Manager y tienen el valor del campo de AlertGroup de alerts.status de `Estado ITNM`.

Capítulo 28. Acerca de la correlación y enriquecimiento de sucesos

Network Manager utiliza la Pasarela de sucesos para correlacionar sucesos con datos de topología y enriquecer sucesos con un conjunto predeterminado de campos de topología. Una vez que un suceso se ha enriquecido, se pasa a procesos de conector como por ejemplo el análisis de causa raíz (RCA) y migración tras error, que realizan más acciones según los datos del suceso enriquecido. El suceso enriquecido también se devuelve a ObjectServer.

Enriquecimiento de sucesos

El proceso de enriquecimiento de suceso se produce dentro de la Pasarela de sucesos y se compone de distintos pasos. Cada uno de estos pasos se pueden personalizar.

Conceptos relacionados

Categorías de sucesos de Network Manager

Los sucesos que se generan mediante Network Manager están en dos categorías: sucesos acerca de la red que se supervisa y sucesos acerca de los procesos de Network Manager.

Referencia rápida de enriquecimiento de sucesos

Utilice esta información para comprender cómo se procesan los sucesos y se pasan a través de la Pasarela de sucesos.

Nota: Al acceder a un ObjectServer de Tivoli Netcool/OMNIbus protegido por un cortafuegos, debe especificar un puerto IDUC y proporcionar acceso a ese puerto utilizando el cortafuegos.Para obtener más información sobre cómo especificar un puerto IDUC para ObjectServer, consulte *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Los pasos están descritos en la tabla siguiente.

Tabla 80. Referencia rápida de enriquecimiento de sucesos

Acción	Información adicional	Los datos pasan al siguiente paso
1. Se recibe un suceso del ObjectServer y se aplica el filtro del suceso entrante al suceso. El filtro predeterminado comprueba el campo LocalNodeAlias del suceso. Si el campo LocalNodeAlias no está vacío, el suceso pasa el filtro y avanza al Paso 3. **Nota:** El campo LocalNodeAlias por lo general contiene datos que apuntan al dispositivo de nodo principal en el que se produjo el suceso. Los datos exactos incluidos en el campo LocalNodeAlias varían y pueden incluir lo siguiente: • Dirección IP • nombre de DNS • sysName	"Filtro de sucesos entrantes" en la página 530	Suceso
2. La Pasarela de sucesos asigna un estado al suceso en función de los campos Severity y Tally del suceso. Este estado es una representación interna de la Pasarela de sucesos y se utiliza posteriormente por los conectores como parte del mecanismo de suscripción a sucesos.	"Estados de suceso" en la página 535	Suceso Estado de suceso

Tabla 80. Referencia rápida de enriquecimiento de sucesos (continuación)

Acción	Información adicional	Los datos pasan al siguiente paso
3. El filtro de campo entrante se aplica al suceso. Este filtro de campo filtra los campos de alerts.status que no participan en el proceso de la Pasarela de sucesos.	"Filtro de campo entrante" en la página 532	Suceso con campos filtrados Estado de suceso
4. La Pasarela de sucesos determina cómo tratar este suceso, determinando qué correlación de suceso se utilizará. Las correlaciones de sucesos definen cómo tratar un suceso. Al mismo tiempo, un valor de precedencia numérica se asocia con un suceso. El conector RCA utiliza el valor de precedencia en los casos en los que hay varios sucesos en la misma entidad. El suceso con el valor de precedencia más alto de la entidad se utiliza para suprimir otros sucesos.	"Selección de correlaciones de sucesos" en la página 539 "Prioridad de valor" en la página 566	Suceso con campos filtrados Estado de suceso Campos de correlación de sucesos, como un nombre de correlación de sucesos y un agrupador de enriquecimiento de sucesos Prioridad de valor
5. La Pasarela de sucesos determina el ID de entidad del servidor de Network Manager o de la interfaz de ingreso, la interfaz dentro del ámbito de descubrimiento desde la que se transmiten los paquetes de red desde y hacia el servidor de Network Manager. El conector RCA utiliza este valor para realizar un supresión aislada.	"Entidad de sondeador" en la página 567	Suceso con campos filtrados Estado de suceso Campos de correlación de sucesos, como un nombre de correlación de sucesos y un agrupador de enriquecimiento de sucesos Prioridad de valor PollerEntityId
6. La Pasarela de sucesos ejecuta una búsqueda de topología para recuperar datos de entidad asociados con este suceso y, a continuación, enriquece el suceso al usar parte de estos datos de entidad. Para ejecutar la búsqueda de topología y el enriquecimiento de sucesos, la Pasarela de sucesos llama el agrupador definido en la correlación de sucesos.	"Agrupadores de la pasarela de sucesos" en la página 548	Para los pasos 8 y 9 Suceso con campos filtrados y campos enriquecidos Estado de suceso Prioridad de valor PollerEntityId Valor de devolución del agrupador

Tabla 80. Referencia rápida de enriquecimiento de sucesos (continuación)		
Acción	**Información adicional**	**Los datos pasan al siguiente paso**
7. El filtro de campo saliente se aplica al suceso. Este filtro solo pasa los campos enriquecidos por la Pasarela de sucesos y, en concreto, por la regla de agrupador GwEnrichEvent. Los campos enriquecidos se colocan en la cola de la Pasarela de sucesos, desde donde se envían los datos al ObjectServer en un intervalo de tiempo configurable (el valor predeterminado es de 5 segundos).	"Filtro de campos salientes" en la página 533 "Cola de pasarela de sucesos salientes" en la página 534	Campos enriquecidos por la Pasarela de sucesos
8. En función del valor de devolución del agrupador definido en la correlación de sucesos (Paso 7), la Pasarela de sucesos determina si se enviará el suceso enriquecido a los conectores. • Si el valor de devolución es 1, la Pasarela de sucesos envía el suceso enriquecido a los conectores. Vaya al siguiente paso. • Si el valor de devolución es 0, la Pasarela de sucesos no envía el suceso enriquecido a los conectores. El proceso de enriquecimiento de sucesos de este suceso finaliza aquí.	"Agrupadores de enriquecimiento de sucesos" en la página 558	Suceso con campos filtrados y campos enriquecidos Estado de suceso Nombre de correlación de sucesos Prioridad de valor PollerEntityId
9. Cada conector determina si está interesado en el suceso enriquecido. Esto se realiza en función del nombre de la correlación de sucesos y el estado de suceso. Los conectores que está interesados en el suceso ejecutan un enriquecimiento de sucesos posterior o llevan a cabo otro tipo de acción.	"Conector de Análisis de causa raíz (RCA)" en la página 565 "Conectores de la Pasarela de sucesos" en la página 589	Suceso con campos filtrados y campos enriquecidos
10. Al finalizar el proceso, los campos enriquecidos se colocan en la cola de la Pasarela de sucesos, desde donde se envían los datos al ObjectServer en un intervalo de tiempo configurable (el valor predeterminado es de 5 segundos).	"Cola de pasarela de sucesos salientes" en la página 534	A ObjectServer Campos enriquecidos por los conectores

Conceptos relacionados

Ejemplo: Enriquecimiento predeterminado de un suceso de interrupción de Tivoli Netcool/OMNIbus
Utilice esta información para comprender cómo se procesa un suceso de Tivoli Netcool/OMNIbus y pasa a través de la Pasarela de sucesos.

Tareas relacionadas

Modificación de las suscripciones de mapas de sucesos
Puede cambiar los mapas de sucesos que se suscriben a un plug-in. Por ejemplo, si añade un mapa de sucesos nuevo y quiere que el sistema realice RCA en los sucesos gestionados por ese mapa de sucesos, debe añadir el mapa de sucesos a la lista de subscripciones para el plug-in RCA.

Filtro de sucesos

Los sucesos se filtran al principio del proceso de enriquecimiento cuando los sucesos se reciben desde el ObjectServer. Los sucesos también se filtran al final del proceso cuando los sucesos enriquecidos se envían de vuelta a ObjectServer.

Filtro entrante

El filtro entrante garantiza que solo los sucesos y los campos de interés se pasan a la Pasarela de sucesos para el enriquecimiento de sucesos.

Filtro de sucesos entrantes

El filtro de sucesos entrantes filtra sucesos desde ObjectServer y sólo pasa sucesos que cumplen ciertos criterios.

El filtro de sucesos entrantes se utiliza tanto en instalaciones sin migración tras error como en instalaciones con migración tras error. En el caso de una instalación con migración tras error, el mecanismo de filtro se aplica a sucesos en el dominio activo, es decir, el dominio principal cuando el servidor principal está sano, o el dominio de copia de seguridad cuando el servidor principal está inactivo.

El filtro de sucesos entrantes sólo pasa sucesos que cumplen las condiciones siguientes:

- Se rellenará el campo LocalNodeAlias del suceso. Este campo debe contener la dirección IP o el nombre DNS del dispositivo relacionado.
- El nombre de dominio especificado en el campo NmosDomainName del suceso es el mismo que el dominio manejado por la Pasarela de sucesos actual. De forma alternativa, no hay ningún dominio asociado con este suceso, y el campo NmosDomainName está vacío.

El filtro de sucesos entrantes puede manejar sucesos tanto en dominio único como en sistemas multidominio.

Manejo de dominio único y multidominio

En un sistema de dominio único, sólo hay un proceso de Pasarela de sucesos. Todos los sucesos que tienen un conjunto de dominios en el campo NmosDomainName tienen la misma asignación de dominios que esta Pasarela de sucesos.

En un sistema de dominios múltiples, hay varios procesos de la Pasarela de sucesos, uno para cada dominio. Cada proceso de la Pasarela de sucesos recibe sucesos desde el ObjectServer y filtra los sucesos para que sólo reciba sucesos para su propio dominio. El ObjectServer realiza la deduplicación y la coincidencia de sucesos de problemas y de resolución según los siguientes campos alerts.status: AlertKey, Identifier, y Domain. La inclusión del campo Dominio asegura que toda la deduplicación y la coincidencia de los sucesos de problemas y de resolución es específico del dominio.

Sucesos sin dominio

Los sucesos que provienen de orígenes externos a Network Manager, como por ejemplo el syslog de Tivoli Netcool/OMNIbus o la sonda de condición de excepción, no tienen un valor de dominio la primera vez que pasen por una Pasarela de sucesos. En un único sistema de dominio, los sucesos sin pase del valor de dominios, el filtro del suceso entrante y la Pasarela de sucesos determinará el dominio asociado con el suceso como parte de la búsqueda de topología realizada durante el enriquecimiento de sucesos.

En un sistema multidominio, la primera Pasarela de sucesos que se encuentra el suceso sin dominio la pasará por el filtro del suceso entrante y procederá a procesarlo. Sin embargo, si la búsqueda de topología no encuentra una entidad para el suceso, el suceso se rechazará mediante la Pasarela de sucesos sin ningún enriquecimiento de sucesos. El suceso se recogerá mediante una Pasarela de sucesos distinta, que también intentará hacer coincidir el suceso hasta un dispositivo de su dominio. Este proceso continuará hasta que el suceso se procese mediante una Pasarela de sucesos que pueda hacer coincidir una entidad con el suceso.

Filtro de sucesos entrantes: configuración predeterminada

Este ejemplo muestra cómo se configura el filtro de sucesos entrantes en el archivo de configuración EventGatewaySchema.cfg. Esta inserción estándar para el filtro de sucesos entrantes maneja tanto sistemas de dominio único como de múltiple dominio.

El filtro de sucesos entrantes está configurado en el archivo de configuración EventGatewaySchema.cfg. Este archivo se encuentra ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

La tabla siguiente describe las líneas relevantes de esta inserción.

Tabla 81. Líneas de código relevantes para el filtro de sucesos entrantes

Números de línea	Descripción
1	Configure el filtro entrante realizando una inserción en la tabla config.nco2ncp.
3	Especifique una inserción en el campo EventFilter de la tabla config.nco2ncp.
9 - 10	Establezca el filtro como sigue: `"LocalNodeAlias <> '' and (NmosDomainName = '$DOMAIN_NAME' or NmosDomainName = '')"` Esta cláusula comprueba que la columna LocalNodeAlias del suceso se haya rellenado. Además, el filtro comprueba si el nombre del dominio especificado en el suceso (contenido en el campo NmosDomainName) es el mismo que el dominio que contiene la Pasarela de sucesos (contenido en la variable $DOMAIN_NAME). Si hay una coincidencia, o si el suceso no tiene un dominio asociado (`NmosDomainName - ''`), y la columna LocalNodeAlias se ha rellenado, el suceso pasará el filtro.

La tabla siguiente describe las líneas relevantes desde esta inserción.

```
insert into config.nco2ncp
(
    EventFilter,
    StandbyEventFilter,
    FieldFilter
)
values
(
    "LocalNodeAlias <> '' and (NmosDomainName =
         '$DOMAIN_NAME' or NmosDomainName = '')",
    "EventId in ('ItnmHealthChk', 'ItnmDatabaseConnection')",
    [
        "Acknowledged",
        "AlertGroup",
        "EventId",
        "FirstOccurrence",
        "LastOccurrence",
        "LocalNodeAlias",
        "LocalPriObj",
        "LocalRootObj",
        "Manager",
        "NmosCauseType",
        "NmosDomainName",
        "NmosEntityId",
        "NmosEventMap",
        "NmosManagedStatus",
        "NmosObjInst",
        "NmosSerial",
        "Node",
        "RemoteNodeAlias",
        "EventId",
        "Serial",
        "ServerName",
        "Severity",
        "Summary",
        "SuppressEscl",
        "Tally",
        "Type"
    ]
);
```

Filtro en espera

En un despliegue de migración tras error, el filtro en espera lo utiliza el dominio de copia de seguridad en un par de migración tras error. Ello significa el dominio de copia de seguridad cuando la principal está activa, o el dominio principal si la copia de seguridad está activa. El filtro en espera sólo permite los sucesos de comprobación de estado (ItnmHealthCheck) mediante la Pasarela de sucesos. Estos sucesos

se pasan al Conector de migración tras error y dicen al sistema que vuelva a la modalidad principal. Tenga en cuenta que para el comportamiento de migración tras error, cualquier modificación a este filtro debe asegurar que el filtro en espera acepta los sucesos de comprobación de error.

Cuando el servidor principal está activo, la Pasarela de sucesos en el servidor de copia de seguridad no realizará ningún enriquecimiento de sucesos. Cuando el servidor principal está inactivo, la Pasarela de sucesos en el servidor de copia de seguridad realizará enriquecimiento de sucesos en el ObjectServer.

El filtro en espera se configura en el archivo de configuración EventGatewaySchema.cfg. Este archivo se encuentra ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

El ejemplo listado en "Filtro de sucesos entrantes: configuración predeterminada" en la página 530 muestra cómo está configurado el filtro en espera en el archivo de configuración EventGatewaySchema.cfg.

La sección de código que es relevante para el filtro en espera se lista en las líneas siguientes. Esta inserción configura la Pasarela de sucesos para pasar únicamente sucesos de ItnmHealthCheck cuando el servidor principal esté inactivo y el servidor de copia de seguridad esté activo.

La tabla siguiente describe las líneas relevantes desde esta inserción:

Tabla 82. Líneas de código relevantes para el filtro en espera

Números de línea	Descripción
1	Configure el filtro entrante realizando una inserción en la tabla config.nco2ncp.
4	Especifique una inserción en el campo StandbyEventFilter de la tabla config.nco2ncp.
11	Establezca el filtro como sigue: `"EventId in ('ItnmHealthChk', 'ItnmDatabaseConnection')",` Esta cláusula sólo pasará sucesos que tengan el ID de suceso establecido en el valor `ItnmHealthChk` o `ItnmDatabaseConnection`.

Filtro de campo entrante

Para cada suceso que pasa el filtro de sucesos entrantes, el filtro de campo especifica un subconjunto de campos de alerts.status que se pasan a través del proceso de enriquecimiento de sucesos. Si el filtro de campo está vacío, todos los campos de alerts.status se pasan a través del proceso de enriquecimiento de sucesos. El fin de este filtro es limitar los campos que se pasan a través al conjunto mínimo requerido para aligerar la carga del proceso.

El filtro de sucesos entrantes está configurado en el archivo de configuración EventGatewaySchema.cfg. Este archivo se encuentra ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

El ejemplo listado en "Filtro de sucesos entrantes: configuración predeterminada" en la página 530 muestra cómo está configurado el filtro de campos entrantes en el archivo de configuración EventGatewaySchema.cfg.

La sección de código que es relevante para el filtro de campos entrantes se lista en las líneas siguientes del ejemplo. Para cada suceso que el ObjectServer pasa a la Pasarela de sucesos, el filtro de campos entrantes especifica un subconjunto de campos de alerts.status que se pasan a través del proceso de enriquecimiento de sucesos.

La tabla siguiente describe las líneas relevantes de este ejemplo:

Tabla 83. Líneas de código relevantes para el filtro de campos entrantes

Números de línea	Descripción
1	Configure el filtro entrante realizando una inserción en la tabla config.ncp2nco.
5	Especifique una inserción en el campo FieldFilter de la tabla config.ncp2nco.

Tabla 83. Líneas de código relevantes para el filtro de campos entrantes (continuación)	
Números de línea	**Descripción**
11-38	Pasar solo los campos de alerts.status especificados en las líneas 13 a 38. **Nota:** Si configura un enriquecimiento de sucesos adicional, puede que tenga que agregar campos a la lista.

Filtro de campos salientes

El filtro de campos salientes define el conjunto de campos de ObjectServer que puede actualizar la Pasarela de sucesos.

El enriquecimiento de sucesos se realiza mediante la regla de agrupador `GwEnrichEvent()`. De los campos enriquecidos con esa regla, solo los que figuran en este filtro se transmiten al servidor de objetos. Algunos enriquecimientos de sucesos están destinados únicamente a proporcionar datos para su uso por los conectores de la Pasarela de sucesos. No es necesario especificar en el filtro de campos salientes los campos enriquecidos destinados únicamente para su uso por los conectores. El filtro de campos salientes solo funciona con los datos pasados a la regla `GwEnrichEvent()`

Nota: Si personaliza el enriquecimiento de sucesos para añadir campos adicionales enriquecidos al suceso, debe actualizar el filtro de campos salientes para incluir estos campos adicionales enriquecidos. Por ejemplo, si desea enriquecer sucesos para que las alertas de un direccionador de Cisco aumente hasta alcanzar el nivel más alto de gravedad (gravedad 5), debe añadir el campo Severity a la lista de campos del filtro de campos salientes.

El filtro de campos salientes se configura en el archivo de configuración EventGatewaySchema.cfg. Este archivo se encuentra ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

El ejemplo que aparece a continuación muestra cómo está configurado el filtro de campos salientes en el archivo de configuración EventGatewaySchema.cfg.

La sección de código que es relevante para el filtro de campos salientes se lista en las líneas siguientes del ejemplo. Cada vez que la Pasarela de sucesos vuelve a pasar los campos enriquecidos al ObjectServer, solo se transmiten los campos incluidos en este filtro. Los demás campos se omiten.

La tabla siguiente describe las líneas relevantes de este ejemplo:

Tabla 84. Líneas de código relevantes para el filtro de sucesos entrantes	
Números de línea	**Descripción**
1	Configure el filtro saliente realizando una inserción en la tabla config.ncp2nco.
3	Especifique una inserción en el campo FieldFilter de la tabla config.ncp2nco.
5-14	Solo se vuelven a pasar al ObjectServer los campos especificados en las líneas 5 a 14. **Nota:** Si configura un enriquecimiento de sucesos adicional, tendrá que agregar campos a la lista.

```
insert into config.ncp2nco
(
    FieldFilter
)
values
(
    [
        "NmosCauseType",
        "NmosDomainName",
        "NmosEntityId",
        "NmosManagedStatus",
        "NmosObjInst",
        "NmosSerial"
```

```
    ]
);
```

Tareas relacionadas

Ejemplo: Enriquecimiento de un suceso con la ubicación del dispositivo de nodo principal
Puede configurar el enriquecimiento de suceso para que la ubicación del dispositivo de nodo principal asociado con el suceso se añada a un campo del suceso.

Ejemplo: Enriquecimiento de un suceso con un nombre de interfaz
Puede configurar el enriquecimiento de sucesos para que todos los sucesos de interfaz, el nombre de la interfaz en la que se produce el suceso se añadan a un campo del suceso.

Cola de pasarela de sucesos salientes

La cola de la pasarela de sucesos de salida recibe sucesos enriquecidos de los agrupadores de la pasarela de sucesos (enriquecimiento de sucesos principal) y de los plug-ins. Con el fin de minimizar el número de actualizaciones y, por lo tanto, minimizar la carga del ObjectServer, las actualizaciones de este se colocan en una cola, se agregan y se envían al ObjectServer en un período de tiempo especificado. El valor predeterminado es de 5 segundos.

La cola de Pasarela de sucesos saliente recibe sucesos enriquecidos de los agrupadores de la Pasarela de sucesos (enriquecimiento de suceso principal) y de los conectores, como se muestra en el siguiente diagrama.

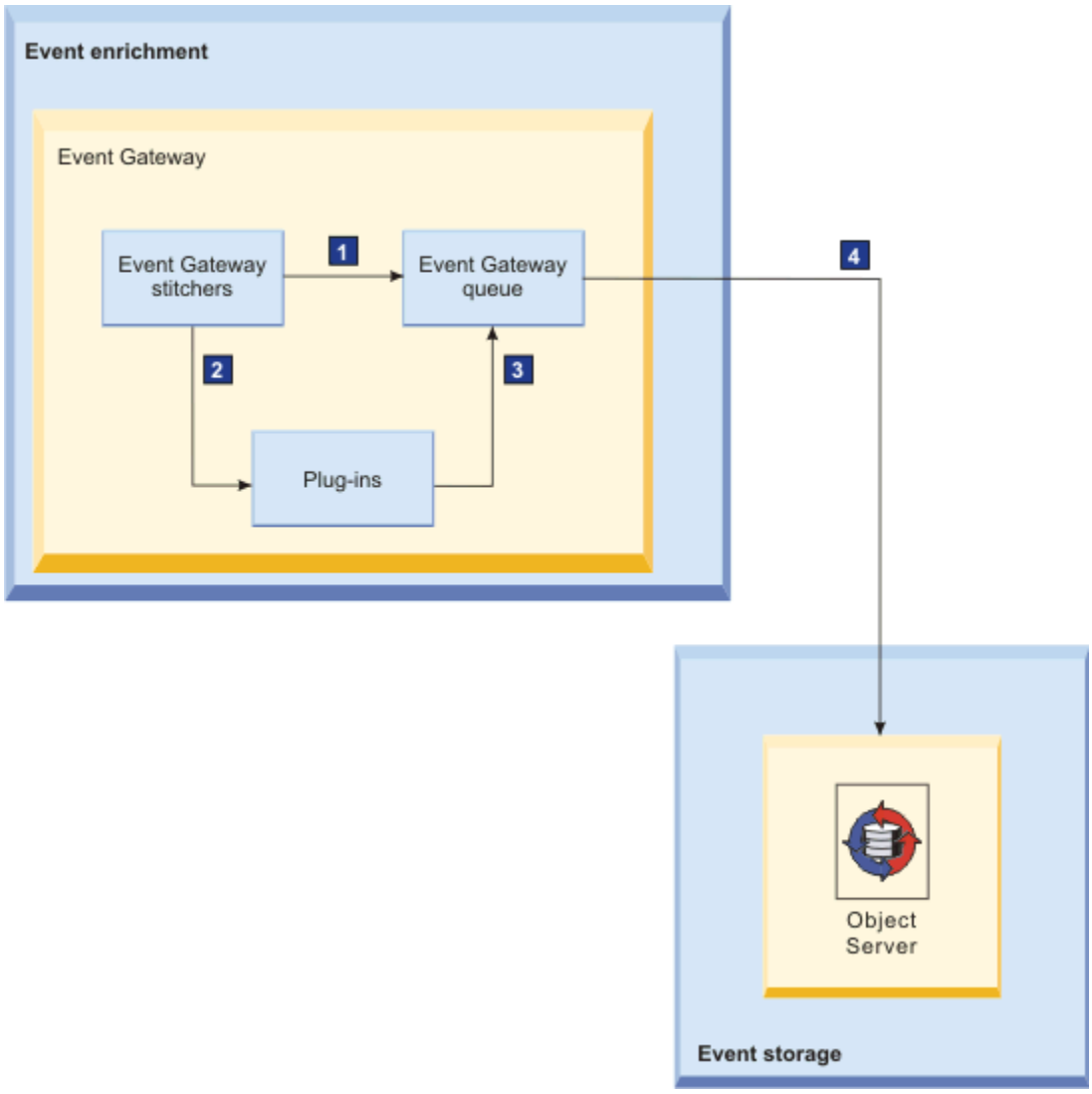


Figura 8. Cola de pasarela de sucesos salientes

1 Sucesos enriquecidos estándar colocados en la cola de la Pasarela de sucesos
Tras el enriquecimiento de sucesos estándar, los agrupadores de la Pasarela de sucesos colocan los datos enriquecidos en la cola de la Pasarela de sucesos.

2 Sucesos pasados a los conectores
Si los agrupadores de la Pasarela de sucesos devuelven el valor 1, los sucesos relacionados se pasan a los conectores para un enriquecimiento posterior. Los conectores seleccionan los sucesos para enriquecer en función de la correlación de sucesos y el estado de suceso asociados.

3 Los sucesos enriquecidos por los conectores se colocan en la cola de la Pasarela de sucesos
Los conectores colocan los sucesos que han enriquecido en la cola de la Pasarela de sucesos.

4 Los sucesos enriquecidos se envían al ObjectServer
Los datos de sucesos enriquecidos se envían al ObjectServer cada 5 segundos. El intervalo de 5 segundos es configurable.

De forma predeterminada, los agrupadores de la Pasarela de sucesos enriquecen el suceso rellenando los campos NmosManagedStatus, NmosEntityId, NmosObjInst y NmosDomainName. Estos sucesos se colocan en la cola de la Pasarela de sucesos y esperan a la siguiente actualización. Mientras tanto, el suceso se pasa al conector RCA. El conector RCA enriquece el suceso al rellenar los campos NmosSerial y NmosCauseType y luego coloca estos sucesos en la cola de la Pasarela de sucesos. Ambas actualizaciones llegan a la cola de la Pasarela de sucesos en un intervalo de 5 segundos. Por lo tanto, en lugar de realizar dos actualizaciones, la Pasarela de sucesos coloca en la cola los datos para ejecutar solo una actualización del ObjectServer para todos estos campos.

Tareas relacionadas

Configuración del campo de intervalo de actualización de ObjectServer
Puede configurar el intervalo que utiliza la pasarela de sucesos para poner en cola las actualizaciones de enriquecimiento de sucesos para ObjectServer.

Modificación de las suscripciones de mapas de sucesos
Puede cambiar los mapas de sucesos que se suscriben a un plug-in. Por ejemplo, si añade un mapa de sucesos nuevo y quiere que el sistema realice RCA en los sucesos gestionados por ese mapa de sucesos, debe añadir el mapa de sucesos a la lista de subscripciones para el plug-in RCA.

Estados de suceso

La Pasarela de sucesos asigna un estado al suceso en función del tipo de suceso y de los campos Severity y Tally del suceso. El estado del suceso es uno de los parámetros utilizados por los conectores de suceso al suscribirse a sucesos.

Conceptos relacionados

Descripciones del agrupador de RCA
Utilice esta información para comprender qué es lo que realiza el agrupador de RCA.

Secuencia del agrupador de análisis de causa raíz
Los agrupadores invocados por el plugin RCA y la secuencia en la que aquéllos se ejecutan para determinar la causa raíz.

Tipos de suceso

A efectos de la Pasarela de sucesos, los tipos de suceso se dividen en tres categorías amplias: Problema, Resolución e Información.

A efectos de la Pasarela de sucesos, los tipos de suceso se dividen en las siguientes categorías:

Tipo = 1: Problema
La Pasarela de sucesos asigna un número de estado a los sucesos de problema en función del estado anterior y de los campos Severity y Tally del suceso.

Tipo = 2: Resolución
A los sucesos de resolución se les asigna inmediatamente el estado Resolución.

Tipo = 13: Información
A los sucesos de información se les asigna inmediatamente el estado Información.

La lista completa de los tipos de sucesos definidos en la tabla alerts.status se presenta en la siguiente tabla y se correlaciona con una de las tres categorías mencionadas anteriormente.

Tabla 85. Etiquetas de transición

Valor del campo Type en alerts.status	**El tipo de suceso es comprendido por la Pasarela de sucesos**
0: Tipo no establecido	Desconocido
1: Problema	Problema
2: Resolución	Resolución
3: Problema Netcool/ Visionary	Problema
4: Resolución Netcool/ Visionary	Resolución
7: Nueva alarma Netcool/ISM	Problema
8: Antigua alarma Netcool/ISM	Problema
11: Más grave	Problema
12: Menos grave	Problema
13: Información	Información

Diagrama de estado de suceso

El diagrama de estado de suceso muestra posibles estados de suceso y describe cómo se producen las transiciones entre estos estados en función de los valores de los campos Severity y Tally de alerts.status. El diagrama muestra también cómo se gestionan los distintos tipos de suceso.

El diagrama de estado de suceso se muestra más abajo. A cada uno de los sucesos se le asigna uno de estos estados a medida que pasa a través de la Pasarela de sucesos. Cada transición de estado se corresponde con un suceso actualizado recibido del ObjectServer. Los estados de suceso se muestran con un color asociado del siguiente modo:

- El color rojo indica un estado de problema activo.
- El color verde indica un estado de borrado activo.
- El color blanco indica que no es un estado activo.

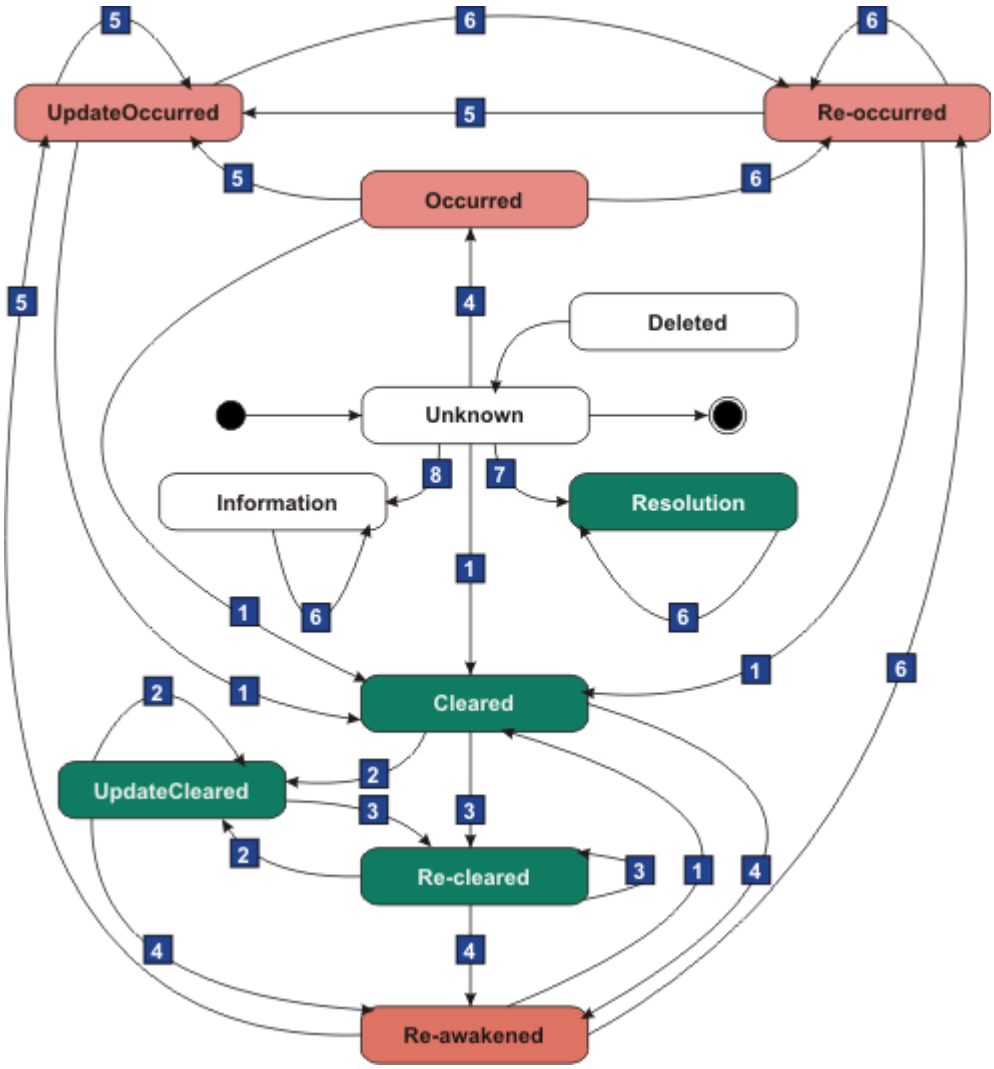


Figura 9. Diagrama de estado de suceso

Transiciones de estado de sucesos

Cada transición se etiqueta en el diagrama con un número del 1 al 8. La tabla siguiente muestra las transiciones asociadas con cada etiqueta.

Tabla 86. Etiquetas de transición

Etiqueta	Valores de campo de un suceso actualizado
1	Severity =0
2	Severity = 0 Cuadrar: Sin cambios desde el suceso anterior
3	Gravedad: 0 Cuadrar: Modificado desde el suceso anterior
4	Gravedad: Diferente a cero
5	Gravedad: Diferente a cero Cuadrar: Sin cambios desde el suceso anterior

Tabla 86. Etiquetas de transición (continuación)	
Etiqueta	**Valores de campo de un suceso actualizado**
6	Gravedad: Diferente a cero Cuadrar: Modificado desde el suceso anterior
7	Tipo = 2: Resolución
8	Type = 13:Información

Descripciones de estados de sucesos

Los estados se sucesos se muestran en la tabla siguiente. Todos los estados mostrados se refiere a sucesos de Type = 1 (Suceso de problema), salvo que se especifique otra cosa.

Tabla 87. Estados de suceso	
Estado	**Descripción**
Borrado	El suceso de gravedad cero no era conocido para la Pasarela de sucesos o se encontraba en un estado de problema activo.
Suprimido	El suceso se ha eliminado del ObjectServer. Como esto puede suceder en cualquier momento, a este estado se puede llegar desde cualquier otro estado, excepto Desconocido. Las eliminaciones se envían a los conectores a través de la interfaz de conectores y el estado del suceso en la Pasarela de sucesos pasa a ser Desconocido.
Información	Cualquier suceso de entrada que tenga el tipo Información (Type = 13) recibe el estado Información, independientemente de otros valores de campo.
Sucedido	El suceso de gravedad no cero no era anteriormente conocido para la Pasarela de sucesos.
Reactivado	El suceso de gravedad no cero era conocido para la Pasarela de sucesos, pero no se encontraba en un estado de problema activo.
Borrado otra vez	El suceso de gravedad cero era anteriormente conocido para la Pasarela de sucesos y ha vuelto a suceder.
Sucedido de nuevo	El suceso de gravedad no cero era anteriormente conocido para la Pasarela de suceso y se ha producido una nueva aparición de ese suceso de problema.
Resincronizado	La Pasarela de sucesos se ha vuelto a sincronizar con el ObjectServer. Se trata de un estado sintético que no se corresponde con ningún suceso único de ObjectServer.
Resolución	Cualquier suceso de entrada que tenga el tipo Resolución (Type = 2) recibe el estado Resolución, independientemente de otros valores de campo.
Desconocido	El suceso no ha sido detectado por la Pasarela de sucesos. Este es el estado inicial y final.
ActualizarBorrado	El suceso de gravedad cero era anteriormente conocido para la Pasarela de sucesos y se ha detectado una actualización, en oposición a una nueva aparición.
ActualizarSucedido	El suceso de gravedad no cero era anteriormente conocido para la Pasarela de sucesos y se ha detectado una actualización, en oposición a una nueva aparición.

Gestión de sucesos

La gestión de sucesos implica determinar cómo debe correlacionarse cada tipo de suceso de ObjectServer con una entidad de los datos de topología.

Correlaciones de sucesos

La gestión de sucesos se realiza utilizando correlaciones de sucesos. La función principal de una correlación de sucesos es llamar a un conjunto de agrupadores que ejecutarán una búsqueda de topologías para determinar la entidad asociada con el suceso y, a continuación, enriquece el suceso con datos de topología.

Selección de correlaciones de sucesos

La Pasarela de sucesos determina qué correlación de sucesos se utilizará en función de la clase de suceso, según se haya definido en el campo alerts.status EventId. Un ejemplo de esta clase de suceso es un suceso de enlace inactivo de interrupción de SNMP.

Selección de correlaciones de sucesos mediante la Pasarela de sucesos

Utilice esta información para comprender cómo configurar la Pasarela de sucesos para seleccionar correlaciones de sucesos para utilizarlas en la gestión de sucesos.

Si opta por configurar la selección de correlaciones de sucesos mediante la Pasarela de sucesos, debe configurar la tabla config.precedence de la Pasarela de sucesos. La tabla config.precedence se configura en el archivo de configuración EventGatewaySchema.cfg. Este archivo se encuentra ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

A continuación, figura un ejemplo de cómo configurar la tabla config.precedence en el archivo de configuración EventGatewaySchema.cfg.

La sección de código que es relevante para la selección de correlaciones de sucesos para utilizar en la gestión de sucesos se muestra en las siguientes líneas del ejemplo. Esta inserción de ejemplo configura la Pasarela de sucesos para utilizar la correlación LinkDownIfIndex para todos los sucesos que tengan el campo EventId establecido en SNMPTRAP-LinkDown. Se trata de sucesos de interrupción que se originan desde un analizador de Tivoli Netcool/OMNIbus.

La tabla siguiente describe las líneas relevantes de este ejemplo:

Tabla 88. Líneas de código relevantes para el filtro de sucesos entrantes

Números de línea	Descripción
1	Configure el filtro entrante realizando una inserción en la tabla config.precedence.
4-5	Especifique una inserción en los campos EventMapName y NcoEventIds de la tabla config.precedence.
10	Establezca el campo EventMapName en el valor LinkDownIfIndex.
11	Establezca el campo NcoEventId en el valor del campo EventId en la tabla alerts.status; en este ejemplo, la correlación de sucesos LinkDownIfIndex se selecciona para todos los sucesos en los que el valor EventId de alerts.status es SNMPTRAP-LinkDown.

```
insert into config.precedence
(
    Precedence,
    EventMapName,
    NcoEventId
)
values
(
    910,
    "LinkDownIfIndex",
```

```
    "SNMPTRAP-LinkDown"
);
```

Métodos de selección de correlaciones de sucesos
La correlación de sucesos y la prioridad pueden asignarse directamente desde el archivo de reglas del analizador de Tivoli Netcool/OMNIbus o en el archivo de configuración de la pasarela de sucesos.

Utilice uno de los métodos siguientes para configurar la correlación de sucesos y la prioridad.

Archivos de reglas del analizador de Tivoli Netcool/OMNIbus
Configure los archivos de reglas del analizador para rellenar el campo NmosEventMap del registro de sucesos alerts.status con el nombre de la correlación de sucesos y un valor de precedencia opcional. En la sección adecuada del archivo de reglas para el tipo de suceso que desea modificar, añada una línea similar al ejemplo siguiente:

```
@NmosEventMap = "LinkDownIfIndex.910"
```

Pasarela de sucesos
Rellene la tabla config.precedence utilizando la inserción definida en el archivo de configuración de la Pasarela de sucesos, EventGatewaySchema.cfg. Para obtener un ejemplo, consulte “Selección de correlaciones de sucesos mediante la Pasarela de sucesos” en la página 539.

Las inserciones eventPrecedence configuradas en la paralela de sucesos sustituyen las inserciones eventPrecedence configuradas en los archivos de reglas del analizador de Tivoli Netcool/OMNIbus. Esto permite sustituir de forma local las inserciones eventPrecedence configuradas en la red.

Correlaciones de sucesos predeterminadas
Network Manager proporciona una configuración predeterminada de estas correlaciones de sucesos. Utilice esta información para conocer las correlaciones de sucesos disponibles y qué realiza cada una de ellas y para comprender cómo las correlaciones de sucesos delegadas se delegan en las correlaciones de sucesos actuales.

Correlaciones de sucesos predeterminadas
En la tabla siguiente se describen las correlaciones de sucesos predeterminadas.

Tabla 89. Correlaciones de sucesos predeterminadas

Correlación de sucesos	Agrupador llamado por la correlación de sucesos	Descripción de la correlación de sucesos
ChassisFailure	LookupMainNode	Gestiona sucesos en los que `LocalNodeAlias` especifica suficientemente la entidad del chasis (nodo principal). Campos de entrada esperados: • `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: – Dirección IP – Nombre de entidad – nombre de DNS – sysName – entityId

Tabla 89. Correlaciones de sucesos predeterminadas (continuación)

Correlación de sucesos	Agrupador llamado por la correlación de sucesos	Descripción de la correlación de sucesos
EMSNonPollingEvent	LookupEMSEntity	Maneja los sucesos de sondeo de los sistemas de gestión de elementos (EMS). Campos de entrada esperados: • `LocalNodeAlias`. • `LocalPriObj`. • `RemoteNodeAlias`, donde este campo contiene la dirección IP o el nombre DNS de la estación de sondeo.
EMSPollingEvent	LookupEMSEntity	Maneja los sucesos no de sondeo de los sistemas de gestión de elementos (EMS). Campos de entrada esperados: • `LocalNodeAlias`. • `LocalPriObj`. • `RemoteNodeAlias`.
EntityFailure	LookupIp	Maneja sucesos en los que el `LocalNodeAlias` es suficiente para especificar la entidad o si no se dispone de más datos. Campo de entrada esperado: `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: • Dirección IP • Nombre de entidad • nombre de DNS • sysName • entityId
EntityMibTrap	LookupEntPhysEntry	Gestiona las interrupciones del MIB ENTITY. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: – Dirección IP – Nombre de entidad – nombre de DNS – sysName – entityId • `LocalPriObj`, donde este campo incluye un índice de entPhysicalTable; por ejemplo, `'entPhysicalEntry.2'`.

Tabla 89. Correlaciones de sucesos predeterminadas (continuación)

Correlación de sucesos	Agrupador llamado por la correlación de sucesos	Descripción de la correlación de sucesos
EntityStateChange	LookupEntityId	Maneja los sucesos generados por el gestor de topología, ncp_model. Ningún conector registra interés actualmente en esta correlación de sucesos. No obstante, la correlación permite el rellenado de campos estándar. Los sucesos generados por ncp_model son los siguientes: • ItnmEntityCreation • ItnmEntityDeletion • ItnmMaintenanceState Campo de entrada esperado: `NmosEntityId`.
genericip-event	LookupMainNode	Procesa los sucesos que no coinciden con ninguna otra correlación de sucesos. **Nota:** Esta correlación de sucesos está pensada como una correlación multiusos. Los conectores no deben registrar interés en esta correlación de sucesos. En su lugar, los sucesos de interés deben pasarse a la correlación de sucesos EntityFailure. Campo de entrada esperado: `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: • Dirección IP • Nombre de entidad • nombre de DNS • sysName • entityId
ItncmResourceEvent	LookupMainNode	Se utiliza para manejar los sucesos generados por Netcool Configuration Manager. Esta correlación de sucesos correlaciona el identificador de entidad (`entityId`) en Network Manager con sus credenciales de Netcool Configuration Manager correspondientes. Campos de entrada esperados: `NmosEntityId`. Si este campo no está disponible, utiliza como entrada lo siguiente: `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: • Dirección IP • Nombre de entidad • nombre de DNS • sysName • entityId

Tabla 89. Correlaciones de sucesos predeterminadas (continuación)

Correlación de sucesos	Agrupador llamado por la correlación de sucesos	Descripción de la correlación de sucesos
ItnmHealthChk	Ningún agrupador relacionado	Utilizada por el conector de migración tras error para procesar sucesos de comprobación de estado de Network Manager. Campo de entrada esperado: `Node`, donde este campo incluye el nombre del dominio para el que se realizará la comprobación de estado.
ItnmLinkDownIfIndex	LookupIfEntry	Espera un suceso de interfaz para ser identificado por el ifIndex si no se configura la interfaz `NmosEntityId`. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: – Dirección IP – Nombre de entidad – nombre de DNS – sysName – entityId • `LocalPriObj`, donde este campo incluye un valor `ifIndex` de la tabla `ifTable`, con el formato `ifEntry.`*`ifIndex`*, donde *ifIndex* es el valor de `ifIndex`; por ejemplo, `ifEntry.1`.
ItnmMonitorEventNoRca	LookupEntityId	Se utiliza para gestionar los sucesos generados por el motor de sondeo de Network Manager, ncp_poller, para el que no se debería realizar un análisis de causa raíz. Campos de entrada esperados: `NmosEntityId`, donde este campo incluye el entityId de NCIM para la entidad.
ItnmStatus	Ningún agrupador relacionado	Correlación de sucesos multiusos para sucesos de información de estado de Network Manager que no gestiona ninguna otra correlación de sucesos de forma explícita; por ejemplo, ItnmHealthCheck. No se realiza ninguna acción para estos sucesos. Para obtener más información sobre los sucesos de información de estado de Network Manager, consulte *IBM Tivoli Network Manager IP Edition: Guía de instalación y configuración*.

Tabla 89. Correlaciones de sucesos predeterminadas (continuación)

Correlación de sucesos	Agrupador llamado por la correlación de sucesos	Descripción de la correlación de sucesos
LinkDownIfDescr	LookupIfEntry	Espera un suceso de interfaz para ser identificado por el valor `ifDescr`. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: – Dirección IP – Nombre de entidad – nombre de DNS – sysName – entityId • `LocalPriObj`, donde este campo incluye un valor `ifDescr` de la tabla `ifTable`, con el formato `ifEntry.`*`ifDescr`*, donde *ifDescr* es el valor de `ifDescr`; por ejemplo, `ifEntry.FastEthernet0/1`.
LinkDownIfIndex	LookupIfEntry	Espera un suceso de interfaz para ser identificado por el valor `ifIndex`. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: – Dirección IP – Nombre de entidad – nombre de DNS – sysName – entityId • `LocalPriObj`, donde este campo incluye un valor `ifIndex` de la tabla `ifTable`, con el formato `ifEntry.`*`ifIndex`*, donde *ifIndex* es el valor de `ifIndex`; por ejemplo, `ifEntry.1`.

Tabla 89. Correlaciones de sucesos predeterminadas (continuación)

Correlación de sucesos	Agrupador llamado por la correlación de sucesos	Descripción de la correlación de sucesos
LinkDownIfName	LookupIfEntry	Espera un suceso de interfaz para ser identificado por el valor `ifName`. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: – Dirección IP – Nombre de entidad – nombre de DNS – sysName – entityId • `LocalPriObj`, donde este campo incluye un valor `ifName` de la tabla `ifTable`, con el formato `ifEntry.`*`ifName`*, donde *ifName* es el valor de `ifName`; por ejemplo, `ifEntry.Fa0/1`.
NbrFail	LookupNbrFailure	Gestiona OSPF, LDP y sucesos de cambio contiguos de BGP. Además, de realizar una búsqueda de requisitos, el agrupador LookupNbrFailure añade también un valor `RemoteNodeEntityId`, que utiliza el conector de RCA. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: – Dirección IP – Nombre de entidad – nombre de DNS – sysName – entityId • `RemoteNodeAlias`, donde este campo incluye la dirección IP de nodo contiguo o el nombre DNS. • `LocalPriObj`, donde este campo incluye un valor `ifDescr` con el formato `ifEntry.`*`ifDescr`*, donde *ifDescr* es el valor de `ifDescr`; por ejemplo, `ifEntry.ifFastEthernet0/1`.

Tabla 89. Correlaciones de sucesos predeterminadas (continuación)

Correlación de sucesos	Agrupador llamado por la correlación de sucesos	Descripción de la correlación de sucesos
OspfIfState	LookupOspfIfEntry	Gestiona sucesos de interfaz de OSPF. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo incluye la dirección IP de nodo (utilizada únicamente por las interfaces sin dirección). • `LocalPriObj`, donde este campo incluye un índice de la tabla `ospfIfTable`; por ejemplo: – `ospfIfEntry.0.0.0.0.66` para interfaces sin dirección (sin número de IP) – `ospfIfEntry.84.82.109.12.0` para interfaces de Ethernet o en serie
PollFailure	LookupIp	Abarca los sucesos generados para una dirección IP específica, como los sucesos del analizador de pings de Tivoli Netcool/OMNIbus. Campos de entrada esperados: `NmosEntityId`, donde este campo incluye el entityId de NCIM para la entidad.
PrecisionMonitorEvent	LookupEntityId	Se usa para gestionar sucesos generados por el sondeador de ITNM, para el que debe realizarse el análisis de causa raíz. Campos de entrada esperados: `NmosEntityId`, donde este campo incluye el entityId de NCIM para la entidad.
Reconfiguración	LookupMainNode	El conector Disco utiliza los sucesos asignados a esta correlación de sucesos para volver a descubrir el dispositivo que tienen asociado. De forma predeterminada, se asignan sucesos de rearranque (los sucesos con el ID NmosSnmpReboot) a esta correlación de sucesos, suponiendo que después de la reconfiguración de un dispositivo (por ejemplo, la adición de una nueva tarjeta), el dispositivo se reiniciará y deberá descubrirse de forma inmediata, para que los cambios en la configuración puedan almacenarse rápidamente en el modelo de topología. Campo de entrada esperado: `LocalNodeAlias`, donde este campo contiene una de las siguientes opciones: • Dirección IP • Nombre de entidad • nombre de DNS • sysName • entityId

Tabla 89. Correlaciones de sucesos predeterminadas (continuación)		
Correlación de sucesos	**Agrupador llamado por la correlación de sucesos**	**Descripción de la correlación de sucesos**
rttMonNotifications	LookupProbeSourceEntity	Fix Pack 4 Añade el nodo principal y el ID de análisis a las interrupcioens RTTMON entrantes. Campos de entrada esperados: • `LocalNodeAlias`, donde este campo incluye la dirección IP de nodo, el nombre de DNS, el sysName o el entityName del nodo. • `X733SpecificProb`, donde este campo identifica el tipo de excepción; por ejemplo, `rttMonNotification`. • `LocalPriObj`, donde este campo identifica el índice de interrupción. • `ExtendedAttr`, donde este campo almacena varios campos relacionados con RTT.

Correlaciones de sucesos heredadas

La tabla siguiente muestra las correlaciones de sucesos heredadas y la correlación de sucesos 3.9 a la que se delega cada una de estas correlaciones.

Tabla 90. Correlaciones de sucesos heredadas	
Correlación de sucesos heredada	**Gestionada por la siguiente correlación de sucesos 3.9**
EntityIfDescr	LinkDownIfDescr
NbrFailIfDescr	NbrFail
NcpHealthChk	ItnmHealthChk
OSPFIfStateChange	OspfIfState
OSPFIfStateChangeIP	OspfIfState

Cómo se delegan las correlaciones de sucesos heredadas a las correlaciones de sucesos 3.9

Este explica cómo la correlación de sucesos NbrFailIfDescr se delega a la correlación de sucesos 3.9 NbrFail.

1. Se recibe un suceso que tiene un eventId incluido en la tabla config.precedence, que se correlaciona con la correlación de sucesos NbrFailIfDescr.
2. La correlación de sucesos NbrFailIfDescr delega en la correlación NbrFail, mediante el campo HandledBy.
3. El suceso se considera como si se hubiera correlacionado con el eventMap NbrFail en primer lugar; es decir, se gestionará del siguiente modo:
   - Se llama al agrupador LookupNbrFailure. Este agrupador es referenciado en el campo `Stitcher` correspondiente a la entrada de correlación de sucesos NbrFail de la tabla config.eventMaps.
   - Los campos de la correlación de sucesos NbrFail (no la descripción NbrFailIfDescr con la que se correlacionó originalmente el suceso) se adjuntan al suceso antes de pasarlos a los conectores.
   - Los conectores que han registrado interés en el eventMap NbrFail (no el NbrFailIfDescr con el que se correlacionó originalmente el suceso) reciben el suceso.

En este ejemplo, la flexibilidad del lenguaje del agrupador permite gestionar los dos tipos de suceso de la misma forma. Si el eventMap heredado NbrFailIfDescr espera ifDescr, se extrae y se utiliza en el agrupador LookupNbrFailure.

Conceptos relacionados

Categorías de sucesos de Network Manager
Los sucesos que se generan mediante Network Manager están en dos categorías: sucesos acerca de la red que se supervisa y sucesos acerca de los procesos de Network Manager.

Agrupadores de la pasarela de sucesos

Los agrupadores de la Pasarela de sucesos emparejan sucesos con una entidad, ejecutan una búsqueda de topología y después utilizan los datos recuperados para enriquecer los datos del suceso.

Los agrupadores Pasarela de sucesos están almacenados en la siguiente ubicación: `$NCHOME/precision/eventGateway/stitchers/`.

Para obtener más información acerca del lenguaje de los agrupadores, consulte la publicación *Referencia de IBM Tivoli Network Manager*.

Existen cuatro tipos de agrupadores de Pasarela de sucesos:

- "Agrupadores de búsqueda de topologías" en la página 550
- "Agrupadores de extracción de datos" en la página 555
- "Agrupadores de recuperación de entidades" en la página 556
- "Agrupadores de enriquecimiento de sucesos" en la página 558

Además, se suministran varios agrupadores de Pasarela de sucesos que no se utilizan de forma predeterminada. Estos agrupadores se proporcionan como ejemplos de funcionalidad adicional que se pueden añadir a la Pasarela de sucesos mediante agrupadores. Para obtener más información, consulte "Agrupadores no utilizados de forma predeterminada" en la página 561.

Selección de agrupadores mediante correlaciones de sucesos

Utilice esta información para comprender cómo configurar la Pasarela de sucesos para habilitar correlaciones de sucesos para invocar determinados agrupadores de Pasarela de sucesos.

Configuración de correlaciones de sucesos para seleccionar agrupadores de Pasarela de sucesos específicos utilizando la tabla config.eventMaps de la Pasarela de sucesos. La tabla config.eventMaps se configura en el archivo de configuración EventGatewaySchema.cfg. Este archivo se encuentra ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

El siguiente ejemplo muestra cómo se configura parte de la tabla config.eventMaps en el archivo de configuración EventGatewaySchema.cfg. Esta inserción de ejemplo configura las correlaciones de sucesos incluidas en la siguiente tabla para invocar los agrupadores listados.

Tabla 91. Correlaciones de sucesos y agrupadores seleccionados

Correlación de sucesos	**Agrupador seleccionado**
PollFailure	LookupIp.stch
ItnmMonitorEventNoRca	LookupEntityId.stch
PrecisionMonitorEvent	LookupEntityId.stch
LinkDownIfIndex	LookupIfEntry.stch

La parte del código que es relevante para la configuración de las correlaciones de sucesos para seleccionar agrupadores de Pasarela de sucesos se incluye en las siguientes líneas del ejemplo. En la tabla siguientes se describen las líneas relevantes de este ejemplo. Este código se refiere a la tabla config.eventMaps.

Nota: El fragmento de código que se muestra a continuación puede intercalarse con otras inserciones en el código real.

Tabla 92. Líneas de código relevantes para el filtro de sucesos entrantes

Números de línea	Descripción
1-12	Configura la correlación de sucesos PollFailure para seleccionar el agrupador LookupIp.stch.
14-23	Configura la correlación de sucesos ItnmMonitorEventNoRca para seleccionar el agrupador LookupEntityId.stch.
25-34	Configura la correlación de sucesos PrecisionMonitorEvent para seleccionar el agrupador LookupEntityId.stch.
36-49	Configura la correlación de sucesos LinkDownIfIndex para seleccionar el agrupador LookupIfEntry.stch. Dado que se trata de un suceso de interrupción, es posible que el suceso fluctúe. Rodar es una condición donde un dispositivo o interfaz se conectan y desconectan de la red repetidamente en un corto espacio de tiempo. Esto provoca problemas y borra los sucesos a recibir uno después del otro para el mismo dispositivo o interfaz. La configuración del distintivo EventCanFlap en 1 informa al conector RCA de esta condición. El conector RCA comprueba si los sucesos con este distintivo establecido en 1 están fluctuando, es decir si el dispositivo o la interfaz se está conectando y desconectando continuamente, y si es así, RCA espera hasta que el suceso se haya solucionado. Los sucesos que pueden rodar se pasan de la Pasarela de sucesos con un valor `EventCanFlap = 1`. Estos sucesos se colocan en la base de datos mojo.events con `TimedEscalation = 1` y se dejan allí durante 30 segundos. Tras 30 segundos, el agrupador RCA de TimedEventSuppression procesará todos los sucesos que tengan al menos 30 segundos y que tengan el valor `TimedEscalation = 1`.

```
insert into config.eventMaps
(
    EventMapName,
    Stitcher
    IsPollingEvent
)
values
(
    "PollFailure",
    "LookupIp"
    1
);

insert into config.eventMaps
(
    EventMapName,
    Stitcher
)
values
(
    "ItnmMonitorEventNoRca",
    "LookupEntityId"
);

insert into config.eventMaps
(
    EventMapName,
    Stitcher
)
values
(
    "PrecisionMonitorEvent",
    "LookupEntityId"
);
```

```
insert into config.eventMaps
(
    EventMapName,
    Stitcher,
    IsPollingEvent
    EventCanFlap
)
values
(
    "LinkDownIfIndex",
    "LookupIfEntry",
    0
    1
);
```

Descripciones del agrupador de la Pasarela de sucesos

Los agrupadores de la Pasarela de sucesos se agrupan en cuatro categorías. Los agrupadores de cada categoría se encargan de distintos aspectos de la búsqueda de topologías y del enriquecimiento de sucesos.

Agrupadores de búsqueda de topologías

Estos son los agrupadores mostrados en las correlaciones de sucesos. Los agrupadores de búsqueda de topologías toman el suceso sin procesar, ejecutan una búsqueda de topologías y realizan un cierto enriquecimiento de sucesos. Con frecuencia utilizan otros agrupadores para realizar las tareas. Por ejemplo, puede utilizar agrupadores de extracción de datos para extraer información del suceso, agrupadores de recuperación de entidades para emparejar el suceso con una entidad de la caché de NCIM y agrupadores de enriquecimiento de sucesos para enriquecer el suceso.

Los agrupadores buscan la topología de la caché de NCIM que difunde el gestor de topología, ncp_model. Para obtener más información sobre la caché de NCIM y sobre el formato de los datos en la caché de NCIM, consulte *Referencia de IBM Tivoli Network Manager*.

Los agrupadores de búsqueda de topologías devuelven un valor booleano de 1 o 0. Estos valores de devolución tienen el siguiente significado:

Valor de devolución 1
: Pasa los datos de sucesos enriquecidos a los conectores de suscripción. Esto, por lo general, significa que la búsqueda de topologías tuvo éxito y que se ha encontrado una entidad en la caché de NCIM.

Valor de devolución 0
: No pasa los datos de suceso a ningún conector. Esto, por lo general, significa que la búsqueda de topologías no tuvo éxito y no se ha encontrado ninguna entidad en la caché de NCIM.

La siguiente tabla describe los agrupadores de búsqueda de topologías.

Tabla 93. Agrupadores de búsqueda de topologías

Agrupador	Descripción	Argumentos esperados	Devuelve
LookupEntityId.stch	Busca una entidad basada estrictamente en el valor del campo NmosEntityId del suceso. Este agrupador está indicado únicamente para su uso en los sucesos generados por: • El motor de sondeo, ncp_poller. • El gestor de topología, ncp_model. • Netcool Configuration Manager El agrupador lleva a cabo el enriquecimiento de sucesos predeterminado en función de los resultados de la búsqueda.	Ninguno. Se llama desde la correlación de sucesos.	Devuelve uno de los valores siguientes: • 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.
LookupEntPhysEntry	Busca una entidad en función de los datos entPhysicalIndex del MIB de Entidad del campo LocalPriObj. Lleva a cabo el enriquecimiento de sucesos predeterminado en función de los resultados de la búsqueda.	Ninguno. Se llama desde la correlación de sucesos.	Devuelve uno de los valores siguientes: • 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.
LookupIfEntry.stch	Busca la entrada de índice de una interfaz de un dispositivo en función de los valores de campo del suceso. Este agrupador lo utilizan los sucesos que se producen en interfaces. Lleva a cabo el enriquecimiento de sucesos predeterminado en función de los resultados de la búsqueda.	Ninguno. Se llama desde la correlación de sucesos.	Devuelve uno de los valores siguientes: • 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.

Tabla 93. Agrupadores de búsqueda de topologías (continuación)

Agrupador	Descripción	Argumentos esperados	Devuelve
LookupIp.stch	Busca una entidad que utilice una dirección IP o nombre DNS. Tenga en cuenta que la entidad que encuentre el agrupador puede ser una interfaz o un nodo principal. Lleva a cabo el enriquecimiento de sucesos predeterminado en función de los resultados de la búsqueda.	Ninguno. Se llama desde la correlación de sucesos.	Devuelve uno de los valores siguientes: • 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.
LookupMainNode.stch	Busca un dispositivo de nodo principal. Si existe un valor en el campo NmosEntityId del suceso, ese valor se utiliza para determinar el ID de entidad del nodo principal. En caso contrario, adopta el valor del campo LocalNodeAlias. Lleva a cabo el enriquecimiento de sucesos predeterminado en función de los resultados de la búsqueda.	Ninguno. Se llama desde la correlación de sucesos.	Devuelve uno de los valores siguientes: • 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.
LookupNbrFailure	Busca una entidad que utilice una dirección IP o nombre DNS, junto con una descripción de interfaz opcional. Este agrupador busca también el nodo remoto con el que se relaciona el suceso. Lleva a cabo el enriquecimiento de sucesos predeterminado en función de los resultados de la búsqueda.	Ninguno. Se llama desde la correlación de sucesos.	Devuelve uno de los valores siguientes: • 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.

Tabla 93. Agrupadores de búsqueda de topologías (continuación)

Agrupador	Descripción	Argumentos esperados	Devuelve
LookupOspfIfEntr	Busca una interfaz en función de los datos de ospfIfEntry. Lleva a cabo el enriquecimiento de sucesos predeterminado en función de los resultados de la búsqueda. Este agrupador comprueba los datos de OSPF en función de uno de los siguientes formatos: **ospfIfEntry.0.0.0.0.*ifIndex*** Un ejemplo de este formato es: `ospfIfEntry.0.0.0.0.66`. En este ejemplo, el valor de índice extraído es 66. Este formato se aplica a los sucesos de interfaz de interfaces sin dirección, también conocidas como interfaces sin números de IP. El formato lo utilizan las interfaces de puerto serie P2P. **ospfIfEntry.*ipV4Adress*.0** Un ejemplo de este formato es: `ospfIfEntry.84.82.109.12.0` En este ejemplo, el valor de índice de la interfaz extraído es la dirección IP 84.82.109.12. Este formato se aplica a los sucesos de interfaz OSPF en interfaces que tienen direcciones IP asignadas. El formato lo utilizan las interfaces Ethernet y en serie.	Ninguno. Se llama desde la correlación de sucesos.	Devuelve uno de los valores siguientes: • 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.
LookupProbeSourceEntity	Busca la entidad de origen de un análisis. Lo invoca la correlación de sucesos `rttMonNotifications`.	Ninguno. Se llama desde la correlación de sucesos.	• 1: Se ha encontrado una entidad en la caché de NCIM. Pasa los datos de sucesos enriquecidos a los conectores de suscripción. • 0: No se ha encontrado ninguna entidad en la caché de NCIM. No pasa los datos de sucesos enriquecidos a los conectores de suscripción.

Ejemplo: Agrupador LookupIp.stch
Utilice este tema para comprender el funcionamiento de los agrupadores de búsqueda de topologías.

El agrupador LookupIp.stch busca una entidad utilizando una dirección IP o un nombre DNS. La entidad que encuentre el agrupador puede ser una interfaz o un nodo principal. La tabla siguiente describe los elementos clave del agrupador.

Tabla 94. Descripción línea por línea del agrupador LookupIp.stch	
Números de línea	**Descripción**
3-7	No hay ningún activador para el agrupador. Las correlaciones de sucesos PollFailure y EntityFailure llaman de forma automática al activador. Al llamar al agrupador, estas correlaciones de sucesos proporcionan el suceso asociado como el registro dentro del ámbito.
11	Cree una entidad de registro con nombre para almacenar los datos de topología asociados con el suceso (el registro dentro del ámbito).
13	Acceda al campo NmosEntityId dentro del suceso y cargue el valor de este campo en la variable nmosEntityId.
14	Utilice la regla del agrupador GwEntityData() para buscar los detalles de entidad en la caché de NCIM, en función del valor de la variable nmosEntityId. Para obtener más información sobre la regla del agrupador GwEntityData(), y otras reglas de agrupador de la Pasarela de sucesos, consulte *Referencia de IBM Tivoli Network Manager*.
16-19	Si el campo NmosEntityId es NULL, significa que esta es la primera aparición de este suceso. Por lo tanto, el suceso no ha pasado por la Pasarela de sucesos y no se ha enriquecido nunca. Como alternativa a NmosEntityId, determine la identidad de la entidad afectada utilizando el campo LocalNodeAlias del registro del suceso. A continuación, utilice la regla del agrupador GwIpLookup() para buscar los detalles de entidad en la caché de NCIM, en función del valor de la variable nmosEntityId. Para obtener más información sobre la regla del agrupador GwIpLookup(), y otras reglas de agrupador de la Pasarela de sucesos, consulte *Referencia de IBM Tivoli Network Manager*.
21	Establezca el valor de devolución del agrupador utilizando la variable foundEntity. Establezca inicialmente el valor de esta variable en 0; se supone que no se ha encontrado ninguna entidad.
22-25	Si se ha encontrado una entidad, llame al agrupador StandardEventEnrichment.stch para realizar un enriquecimiento del suceso utilizando los datos de entidad recuperados en la búsqueda. Establezca el valor de devolución del agrupador en 1.
27	Pase el valor de devolución a la Pasarela de sucesos.

```
UserDefinedStitcher
{
    StitcherTrigger
    {
        // There is no trigger, as the eventMaps will automatically
        // call this with the event as the in-scope record
    }

    StitcherRules
    {
        Record entity;

        int nmosEntityId = eval(int, '&NmosEntityId');
        entity = GwEntityData( nmosEntityId );

        if ( entity == NULL )
        {
            entity = GwIpLookupUsing( "LocalNodeAlias" );
        }

        int foundEntity = 0;
        if ( entity <> NULL )
        {   ExecuteStitcher( "StandardEventEnrichment", entity );
            foundEntity = 1;
        }

        SetReturnValue( foundEntity );
```

```
    }
}
```

Agrupadores de extracción de datos
La única finalidad de estos agrupadores es tomar una sola cadena de datos en formato estándar y analizar la cadena para extraer un solo valor, que se devuelve.

La siguiente tabla describe los agrupadores de extracción de datos.

Tabla 95. Agrupadores de extracción de datos

Agrupador	**Descripción**	**Devuelve**
ExtractEntPhysIndex.stch	Intenta extraer un valor textual que representa un identificador de interfaz procedente de una cadena de datos de entrada con el formato "entPhysicalEntry.*identificador de cadena*". Por lo general, se utiliza para extraer el valor de un campo de suceso, como LocalPriObj o LocalRootObj.	Entero que representa un índice físico.
ExtractIfIndex.stch	Intenta extraer el valor de número entero que representa un identificador de interfaz procedente de una cadena de datos de entrada con el formato "ifEntry.*identificador numérico*". Por lo general, se utiliza para extraer el valor ifIndex de un campo de suceso, como LocalPriObj o LocalRootObj.	Índice de número entero
ExtractIfString.stch	Intenta extraer un valor textual que representa un identificador de interfaz procedente de una cadena de datos de entrada con el formato "ifEntry.*identificador de cadena*". Por lo general, se utiliza para extraer el valor ifIndex de un campo de suceso, como LocalPriObj o LocalRootObj.	Serie que representa la serie de interfaz, `ifString`.

Ejemplo: Agrupador ExtractIfString.stch
Utilice este tema para comprender el funcionamiento de los agrupadores de extracción.

El agrupador ExtractIfString.stch intenta extraer un identificador de interfaz textual de un argumento de entrada con el formato `ifEntry.`*`string_identifier`*, donde *string_identifier* es el identificador de interfaz textual. Este método se utiliza por lo general para extraer el valor ifIndex de un campo de suceso, como LocalPriObj o LocalRootObj.

Tabla 96. Descripción línea por línea del agrupador ExtractIfString.stch

Números de línea	**Descripción**
3-11	Este agrupador se invoca por otro agrupador, que es, por lo general, el agrupador de búsqueda de topologías.

Tabla 96. Descripción línea por línea del agrupador ExtractIfString.stch (continuación)	
Números de línea	**Descripción**
15	Inicialice la variable ifString como nula. La variable ifString almacenará los resultados de la operación de extracción de el identificador de interfaz textual.
17	Lea el argumento de entrada del agrupador que invoca y cárguelo en la variable ifInputStr.
19	Especifique una expresión regular para utilizarla como parte de la operación de coincidencia de patrón o de extracción de datos.
21-27	Realice la operación de coincidencia de patrón y de extracción de datos.
29	Pase la cadena extraída otra vez al agrupador que invoca.

```
UserDefinedStitcher
{
    StitcherTrigger
    {
        //
        // Called from another stitcher using the syntax:
        //
        // text ifString = "";
        // ifString = ExecuteStitcher( 'ExtractIfString', myStringField );
        //
    }

    StitcherRules
    {
        text ifString = "";

        text ifInputStr = eval(text, '$ARG_1');

        text stringMatch = "^ifEntry\.(\S+)";

        int stringMatchCount = MatchPattern( ifInputStr, stringMatch );

        // We only recognise a match if we matched once on the entire field
        if (stringMatchCount == 1 AND REGEX0 == ifInputStr )
        {
            ifString = eval(text, '$REGEX1');
        }

        SetReturnValue( ifString );
    }
}
```

Agrupadores de recuperación de entidades
Estos agrupadores toman datos predefinidos, por lo general extraídos del suceso, e intentan recuperar una entidad coincidente de la tabla entityData en la caché de NCIM. Los agrupadores devuelven el registro entityData recuperado, si se encuentra, o NULL en caso contrario.

La siguiente tabla describe los agrupadores de recuperación de entidades.

Tabla 97. Agrupadores de recuperación de entidades

Agrupador	Descripción	Devuelve
EntityFromEntPhysIndex.stch	Toma una entrada como nombre de nodo principal en formato de texto y un valor `entPhysicalIndex` con formato de número entero e intenta recuperar cualquier tipo de entidad que pueda tener un valor `entPhysicalIndex`, como proporcionado en el MIB de entidad.	Cualquier tipo de entidad que pueda tener un `entPhysicalIndex`, como proporcionado en el MIB ENTITY
EntityFromIfIndex.stch	Toma como entrada un nombre de nodo principal en formato de texto y un valor `ifIndex` con formato de número entero e intenta recuperar una interfaz del nodo principal proporcionado con el valor `ifIndex` proporcionado.	Un interfaz del nodo principal dado con el `ifIndex` proporcionado
EntityFromIfString.stch	Toma como entrada un nombre de nodo en formato de texto y un valor `ifDescr`, `ifName` o `ifAlias` con formato de número entero e intenta recuperar una interfaz del nodo principal proporcionado con un valor `ifDescr`, `ifName` o `ifAlias` coincidente con la cadena suministrada.	Una interfaz del nodo principal proporcionado con un valor `ifDescr` `ifName` o `ifAlias` coincidente con la cadena suministrada
EntityFromNsei.stch	Toma como entrada un nombre de nodo principal en formato de texto y un identificador de Punto final de entidad de servicio de red (NSEI) en formato de entero, e intenta recuperar la entidad de implementación (normalmente una interfaz o un chasis) para el NSEI.	La entidad de implementación (por lo general, una interfaz o un chasis) del Punto final de entidad de servicio de red (NSEI) identificado por el NSEI especificado en el nodo principal dado.
EntityIdFromProbeIdIndex	Toma como entrada la entidad de nodo principal y el ID de análisis, según su configuración en el dispositivo. Busca el ID de entidad de un análisis.	El entityId del análisis del dispositivo proporcionado con el ID de análisis suministrado o 0.

Ejemplo: EntityFromIfString.stch
Utilice este tema para comprender el funcionamiento de los agrupadores de recuperación.

El agrupador EntityFromIfString.stch busca una interfaz en función de un entityName de nodo principal y una cadena, que se espera que sea ifName, ifDescr o ifAlias de la interfaz. Esto devuelve la entidad de la interfaz, si se encuentra en la caché de NCIM.

Tabla 98. Descripción línea por línea del agrupador EntityFromIfString.stch

Números de línea	Descripción
3-7	Este agrupador se invoca por otro agrupador, que es, por lo general, el agrupador de búsqueda de topologías.
11-12	Lea los argumentos de entrada del agrupador que invoca.
16-27	Configure una consulta SQL para recuperar un registro de datos de entidad para una interfaz en función de un entityName de nodo principal y una cadena, que se espera que sea ifName, ifDescr o ifAlias de la interfaz.
30	Use la regla del agrupador RetrieveSingleOQL () para ejecutar la consulta y recuperar el registro de datos de entidad de la interfaz. Para obtener más información sobre la regla del agrupador RetrieveSingleOQL(), y otras reglas de agrupador de la Pasarela de sucesos, consulte *Referencia de IBM Tivoli Network Manager*.
32	Pase el resultado de la búsqueda de entidades otra vez al agrupador que invoca.

```
UserDefinedStitcher
{
    StitcherTrigger
    {
        // There is no trigger, as this is explicitly called from
        // other stitchers.
    }

    StitcherRules
    {
        text mainNodeEntityName = ARG_1;
        text ifString = ARG_2;

        Record entity;

        text ifStringQuery =
                "select * from ncimCache.entityData
                 where
                 ENTITYTYPE = 2
                 and
                 BASENAME = eval(text, '$mainNodeEntityName')
                 and
                 ( interface->IFNAME = eval(text, '$ifString')
                   or
                   interface->IFDESCR = eval(text, '$ifString')
                   or
                   interface->IFALIAS = eval(text, '$ifString') );";


        entity = RetrieveSingleOQL( ifStringQuery );

        SetReturnValue( entity );
    }
}
```

Agrupadores de enriquecimiento de sucesos
Estos agrupadores enriquecen el suceso con los datos de topología recuperados por otros agrupadores.

La siguiente tabla describe los agrupadores de enriquecimiento de sucesos.

Tabla 99. Agrupadores de enriquecimiento de sucesos

Agrupador	Descripción	Argumentos esperados	Devuelve
EntityNotFound.stch	De forma predeterminada, los campos establecidos por la Pasarela de sucesos son los siguientes: • NmosObjInst • NmosSerial • NmosCauseType Este agrupador restablece campos básicos si el suceso se asignó anteriormente a este dominio, pero no se ha encontrado ninguna entidad coincidente.	Ninguno.	Ningún valor de devolución.
ProbeSrcEndPtFromProbe	Recupera información sobre los puntos finales del análisis proporcionado.	El ID de entidad del análisis.	Un registro de datos sobre el origen asociado y los puntos finales de análisis de destino (si se descubren).
IPSLAEventEnrichment	Enriquece el suceso actual mediante GwEnrichEvent () utilizando los datos suministrados.	El registro de entidad de análisis según se ha adquirido de GwEntity Data() para el ID de entidad de análisis, los datos de punto final de análisis adquiridos de ProbeSrc EndPt From Probe.stch.	Ningún valor de devolución.

Tabla 99. Agrupadores de enriquecimiento de sucesos (continuación)			
Agrupador	**Descripción**	**Argumentos esperados**	**Devuelve**
StandardEventEnrichment.stch	Lleva a cabo el enriquecimiento de sucesos predeterminado rellenando los campos de suceso que algunos conectores esperan utilizar, así como los campos que vuelven a rellenarse para actualizar el suceso en el ObjectServer.	La entidad que se ha emparejado con el suceso dentro del ámbito de nivel superior.	Ningún valor de devolución.

Ejemplo: StandardEventEnrichment.stch
Utilice este tema para comprender el funcionamiento de los agrupadores de enriquecimiento de sucesos.

El agrupador StandardEventEnrichment.stch ejecuta el enriquecimiento de sucesos estándar. Rellena los campos de suceso que los conectores esperan poder utilizar (por ejemplo, entityType), así como los campos que vuelve a rellenar directamente La Pasarela de sucesos para actualizar el suceso en el ObjectServer. Los únicos campos que tienen permiso para actualizar la tabla ObjectServer alerts.status son aquellos que están incluidos en el filtro de campos salientes, tal y como se define en la sección FieldFilter de la tabla nco2ncp en el archivo de configuración EventGatewaySchema.cfg. Por ejemplo, los campos entityType y entityName se añaden al suceso para que los utilicen los conectores, pero no enriquecen realmente el suceso en el ObjectServer, porque estos campos no pasan el filtro de campos salientes.

Tabla 100. Descripción línea por línea del agrupador StandardEventEnrichment.stch	
Números de línea	**Descripción**
3-8	Este agrupador se invoca por otro agrupador, que es, por lo general, el agrupador de búsqueda de topologías.
12	Lea en el registro de datos de la entidad de una operación de búsqueda de topologías.
13	Declare un registro para almacenar los campos que se utilizan para enriquecer el suceso.
15-19	Inicialice variables con valores recuperados de la operación de búsqueda de topologías.
19	Utilice la regla del agrupador GwManagedStatus() para recuperar el estado gestionado de la entidad. Para obtener más información sobre la regla del agrupador GwManagedStatus(), y otras reglas de agrupador de la Pasarela de sucesos, consulte *Referencia de IBM Tivoli Network Manager*.
21-26	Establezca los valores de campo del registro que se utilizarán para enriquecer el suceso.

Tabla 100. Descripción línea por línea del agrupador StandardEventEnrichment.stch (continuación)	
Números de línea	**Descripción**
28	Utilice la regla del agrupador GwEnrichEvent() para actualizar los campos del suceso. Para obtener más información sobre la regla del agrupador GwEnrichEvent(), y otras reglas de agrupador de la Pasarela de sucesos, consulte *Referencia de IBM Tivoli Network Manager*.

```
UserDefinedStitcher
{
    StitcherTrigger
    {
        // There is no trigger. This is called from other stitchers
        // with the event as the in-scope record, and the entity as
        // the single argument.
    }

    StitcherRules
    {
        Record entity = ARG_1;
        Record enrichedFields;

        int entityType = @entity.entityData.ENTITYTYPE;
        text entityName = @entity.entityData.ENTITYNAME;
        int entityId = @entity.entityData.ENTITYID;
        int mainNodeId = @entity.entityData.MAINNODEENTITYID;
        int managedStatus = GwManagedStatus( entityId );

        @enrichedFields.EntityType = entityType;
        @enrichedFields.EntityName = entityName;
        @enrichedFields.NmosDomainName = eval(text, '$DOMAIN_NAME');
        @enrichedFields.NmosEntityId = entityId;
        @enrichedFields.NmosManagedStatus = managedStatus;
        @enrichedFields.NmosObjInst = mainNodeId;

        GwEnrichEvent( enrichedFields );
    }
}
```

Tareas relacionadas

Ejemplo: Enriquecimiento de un suceso con la ubicación del dispositivo de nodo principal
Puede configurar el enriquecimiento de suceso para que la ubicación del dispositivo de nodo principal asociado con el suceso se añada a un campo del suceso.

Ejemplo: Enriquecimiento de un suceso con un nombre de interfaz
Puede configurar el enriquecimiento de sucesos para que todos los sucesos de interfaz, el nombre de la interfaz en la que se produce el suceso se añadan a un campo del suceso.

Agrupadores no utilizados de forma predeterminada
Estos agrupadores se proporcionan como ejemplos de funcionalidad adicional que se pueden añadir a la Pasarela de sucesos mediante agrupadores. Estos agrupadores se pueden ejecutar desde otros agrupadores.

En la tabla siguiente se describen los agrupadores de la Pasarela de sucesos que no se utilizan de forma predeterminada.

Tabla 101. Agrupadores no utilizados de forma predeterminada

Agrupador	Descripción	Argumentos esperados	Devuelve
EntityFromAtmIfDescr.stch	Este agrupador muestra cómo se pueden manipular los datos extraídos de un suceso (por lo general, mediante el agrupador ExtractIfString) antes de buscar la topología relacionada en la caché de NCIM. En este ejemplo, los sucesos se generan con una descripción de interfaz breve, que no tiene un sufijo estándar. Este sufijo se añade antes de buscar la topología.	Nombre de nodo principal (texto) `ifDecr` (texto) sin un sufijo `-atm subif`	Una interfaz del nodo principal proporcionado con un `ifDescr` que coincide con la descripción de la interfaz de sucesos, concatenada con la cadena `-atm subif` predefinida.
RetrieveAlertDetails.stch	Busca en la tabla alert.details del servidor de objetos los datos relacionados con el suceso actual dentro del ámbito, y añade cualquier datos encontrado en el suceso dentro del ámbito. Observe que en este ejemplo, esto se realiza de forma indiscriminada y no se ejecuta ningún filtrado de datos. También ofrece un ejemplo de plantilla de cómo consultar datos adicionales al servidor de objetos.	Ninguno	Sin valor de devolución

Ejemplo: Enriquecimiento predeterminado de un suceso de interrupción de Tivoli Netcool/OMNIbus

Utilice esta información para comprender cómo se procesa un suceso de Tivoli Netcool/OMNIbus y pasa a través de la Pasarela de sucesos.

La Pasarela de sucesos recibe un suceso de interrupción de enlace inactivo de Tivoli Netcool/OMNIbus del ObjectServer. Este suceso se origina desde un analizador de interrupciones de Tivoli Netcool/OMNIbus. Este suceso, por lo tanto, se origina desde el exterior de Network Manager. Este ejemplo muestra cómo se procesa el suceso y pasa a través de la Pasarela de sucesos.

Los pasos de este proceso son los siguientes.

1. El analizador SNMP (mttrapd) recibe una interrupción de Enlace inactivo de un dispositivo.
2. Las reglas de analizador procesan la interrupción y crean una alerta de Tivoli Netcool/OMNIbus con el ID de suceso SNMPTRAP-LinkDown. El archivo de reglas snmptrap.rules (procedente de Netcool/OMNIbus Knowledge Library versión 4.4.3 y posteriores) asigna al suceso un valor de LinkDownIfIndex.910 para el campo NmosEventMap, según lo determinado por las reglas del analizador. El valor LinkDownIfIndex especifica que es necesario utilizar el correlacionador de sucesos LinkDownIfIndex para procesar este suceso. El valor .910 añadido al valor indica que el suceso tiene una precedencia de 910. Los sucesos con una alta precedencia suprimen los sucesos con una precedencia más baja durante RCA. El analizador SNMP envía la alerta al ObjectServer.
3. La Pasarela de sucesos recibe el suceso del ObjectServer.
4. El filtro de sucesos entrantes se aplica al suceso.

   Este filtro comprueba el campo LocalNodeAlias del suceso. El campo LocalNodeAlias no está vacío y, por lo tanto, el suceso pasa el filtro y avanza al paso siguiente.
5. La Pasarela de sucesos asigna un estado al suceso en función de los campos Severity, Tally y Type del suceso. El suceso de interrupción de enlace inactivo tiene la siguiente información en los campos Severity y Tally:
   - El valor de Severity es distinto de cero.
   - El valor de Tally es 1
   - El tipo es Problem

   En base a esta información, la Pasarela de sucesos asigna el estado Occurred a este suceso. Se trata de un suceso de problema y es idóneo para RCA.
6. El filtro de sucesos entrantes predeterminado se aplica al suceso. Este filtro de campos filtra los campos de alerts.status que no participan en el proceso de la Pasarela de sucesos y solo permite los siguientes campos:
   - Acknowledged
   - AlertGroup
   - EventId
   - FirstOccurrence
   - LastOccurrence
   - LocalNodeAlias
   - LocalPriObj
   - LocalRootObj
   - Manager
   - NmosCauseType
   - NmosDomainName
   - NmosEntityId
   - NmosEventMap
   - NmosManagedStatus
   - NmosObjInst
   - NmosSerial
   - Nodo
   - RemoteNodeAlias
   - EventId
   - Serial
   - ServerName
   - Gravedad

- Resumen
- SuppressEscl
- Cuadrar
- Tipo

7. La Pasarela de sucesos determina cómo tratar este suceso, determinando qué correlación de suceso se utilizará. Las correlaciones de sucesos definen cómo tratar un suceso. Las reglas del analizador de interrupciones pueden asociar un valor de precedencia numérica con el suceso.

   El suceso de este ejemplo tiene un valor NmosEventMap de `LinkDownIfIndex.910`. La pasarela de sucesos, por lo tanto procesa el suceso utilizando la correlación de sucesos LinkDownIfIndex. Esta correlación de sucesos abarca los sucesos de enlaces activos e inactivos procedentes del analizador Tivoli Netcool/OMNIbus de SNMP. Todos estos sucesos utilizan el valor ifIndex incluido en el campo LocalPriObj de alerts.status para identificar la interfaz desde la que se originó esta interrupción. El conector RCA se suscribe a los sucesos gestionados por la correlación de sucesos LinkDownIfIndex. En consecuencia, este suceso se pasará al conector del RCA. Cuando el suceso se envía para RCA, se utiliza un valor de precedencia de 910 para el suceso.

   Nota: El archivo NcoGateInserts para definir la correlación de sucesos y la precedencia se ha dejado de utilizar a partir de la V4.4.3 de Netcool/OMNIbus Knowledge Library.

8. La Pasarela de sucesos llama el agrupador LookupIfEntry designado en el eventMap para emparejar el suceso con una entidad.

   La correlación de sucesos seleccionada es LinkDownIfIndex. En el archivo de configuración EventGatewaySchema.cfg, el siguiente inserto se asocia con esta correlación de sucesos:

   ```
   insert into config.eventMaps
   (
       EventMapName,
       Stitcher,
       EventCanFlap
   )
   values
   (
       "LinkDownIfIndex",
       "LookupIfEntry",
       1
   );
   ```

   Esta inserción indica a la Pasarela de sucesos que lleve a cabo las siguientes acciones:

   - Utilice el agrupador LookupIfEntry para realizar la búsqueda de topología.

     El agrupador LookupIfEntry busca la entrada de índice de una interfaz de un dispositivo en función de los valores de campo del suceso. En función del valor del índice de interfaz extraído de los campos del suceso, el agrupador recupera una fila de la caché de NCIM que consta de los datos de interfaz y de entidad. Se llama a otro agrupador para que realice el enriquecimiento de sucesos.
   - Establezca el distintivo EventCanFlap en 1 para informar al conector RCA que el dispositivo o la interfaz relacionados pueden continuar conectándose y desconectándose.

9. Si la Pasarela de sucesos encuentra una entidad coincidente en la topología de red, los datos de suceso enriquecidos se filtran mediante el filtro de campo saliente y se sitúan en la cola de la Pasarela de sucesos. El suceso también se pasa a los conectores que han registrado interés.
10. Puesto que el conector de RCA ha registrado interés, recibe el suceso para procesarlo y realiza la RCA utilizando la precedencia de 910 procedente del campo NmosEventMap.
11. El suceso se enriquece con los resultados del RCA y se sitúan en la cola de la Pasarela de sucesos.

Conceptos relacionados

Referencia rápida de enriquecimiento de sucesos

Utilice esta información para comprender cómo se procesan los sucesos y se pasan a través de la Pasarela de sucesos.

Conector de Análisis de causa raíz (RCA)

El conector de análisis de causa raíz (RCA) recibe un conjunto de sucesos enriquecidos de la Pasarela de sucesos y determina qué sucesos son causa raíz y qué sucesos son síntomas. RCA sólo recibe los sucesos que afectan el direccionamiento del tráfico a través de la red.

Una situación de error en la red suele generar varias alertas, porque la condición de fallo de un dispositivo puede hacer que no se pueda acceder a otros dispositivos. Las alertas generadas indican que todos los dispositivos son inaccesibles. Network Manager realiza un análisis de causa raíz mediante la correlación de la información del suceso con la información de la topología, lo que le permite determinar a qué dispositivos no se puede acceder temporalmente debido a otros errores de red. Se suprimen las alertas de dispositivos a los que no se puede acceder temporalmente, esto es, se muestran como síntomas de la alerta de la causa raíz. Las alertas de causa raíz se muestran en las listas de alerta y mapas de tipología; si se ha creado y habilitado la automatización ObjectServer `severity_from_causetype`, estas alertas de causa raíz tendrán el nivel de gravedad más alto para que los operadores puedan identificarlos con facilidad.

Conceptos relacionados

Conectores de la Pasarela de sucesos
Los conectores de la Pasarela de sucesos son módulos de la Pasarela de sucesos que reciben sucesos enriquecidos de ella y los enriquecen aún más o llevan a cabo otras acciones en ellos.

Referencia rápida de RCA

Utilice esta información para comprender cómo se procesan los sucesos y se pasan a través del conector RCA.

La finalidad del conector RCA es determinar, en función de los datos del suceso y de las reglas codificadas en los agrupadores de RCA, qué sucesos están causados por otros o causan otros sucesos. Los pasos están descritos en la tabla siguiente.

Tabla 102. Referencia rápida de RCA

Acción	Información adicional
1. Se recibe un suceso de la Pasarela de sucesos. El conector RCA comprueba que este suceso coincida con sus correlaciones de sucesos y cumpla con los requisitos de suscripción a estados de suceso. En términos de RCA, esto se conoce como *suceso activador* porque inicia una actividad del conector RCA.	*Conector de Análisis de causa raíz (RCA)* en el *IBM Tivoli Network Manager IP Edition Administration Guide* *Conectores de la Pasarela de sucesos* en *IBM Tivoli Network Manager IP Edition Administration Guide*
2. El suceso se inserta en la base de datos mojo.events del conector RCA y los agrupadores de RCA pueden recuperarla para su proceso.	*tabla de base de datos de sucesos mojo.events* en *IBM Tivoli Network Manager IP Edition Administration Guide*
3. El suceso se pasa al ProcessEvent.stch, para el proceso de análisis de causa raíz por parte de los agrupadores de RCA.	

Tareas relacionadas

Modificación de las suscripciones de mapas de sucesos

Puede cambiar los mapas de sucesos que se suscriben a un plug-in. Por ejemplo, si añade un mapa de sucesos nuevo y quiere que el sistema realice RCA en los sucesos gestionados por ese mapa de sucesos, debe añadir el mapa de sucesos a la lista de subscripciones para el plug-in RCA.

Prioridad de valor

Al tiempo que se selecciona una correlación de sucesos para gestionar el suceso, se asocia un valor de precedencia numérica con el suceso. El conector RCA utiliza el valor de precedencia en los casos en los que hay varios sucesos en la misma entidad. El suceso con el valor de precedencia más alto de la entidad se utiliza para suprimir otros sucesos.

Los valores de precedencia se configuran para un ID de suceso mediante la tabla config.precedence de la Pasarela de sucesos. La tabla config.precedence se configura en el archivo de configuración EventGatewaySchema.cfg. Este archivo se encuentra ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

A continuación, figura un ejemplo de cómo configurar la tabla config.precedence en el archivo de configuración EventGatewaySchema.cfg.

La sección de código relevante para la configuración de un valor de precedencia se muestra en las siguientes líneas del ejemplo. Esta inserción de ejemplo configura la Pasarela de sucesos para asignar un valor de precedencia de 910 a todos los sucesos que tengan el campo EventId establecido en SNMPTRAP-LinkDown. Se trata de sucesos de interrupción que se originan desde un analizador de Tivoli Netcool/OMNIbus. El código contiene un inserción en la tabla config.precedence.

La tabla siguiente describe las líneas relevantes de este ejemplo:

Tabla 103. Líneas de código relevantes para el filtro de sucesos entrantes

Números de línea	Descripción
1	Configure el filtro entrante realizando una inserción en la tabla config.precedence.
3	Especifique una inserción en el campo Precedence de la tabla config.precedence.
10	Establezca el campo Precedence en el valor 910.

```
insert into config.precedence
(
    Precedence,
    EventMapName,
    NcoEventId
)
values
(
    910,
    "LinkDownIfIndex",
    "SNMPTRAP-LinkDown"
);
```

Valores de precedencia predeterminados

Por convención, la Pasarela de sucesos asigna valores de umbral predefinidos que tienen un significado especial en el conector RCA.

Puede especificar sus propios valores de precedencia al configurar la Pasarela de sucesos.

Debe especificar un valor de precedencia más alto para los sucesos que cumplan alguna de estas circunstancias:

- Los sucesos de entidades que están por debajo de la pila de protocolos. Por ejemplo, la confirmación de que ha fallado un puerto físico tendría un valor de precedencia que un problema de capa de IP en esa interfaz.

- Los sucesos que son un indicio más seguro de un problema. Por ejemplo, el contraste entre estos dos sucesos; un suceso de error de ping y un suceso de enlace inactivo. El suceso menos cierto es el error de ping. Esto puede deberse a que el paquete ICMP no ha podido llegar a la interfaz. Eso, a su vez, podría deberse a un problema de red entre la estación de sondeo y la interfaz. El suceso más cierto es una interrupción de SNMP que afirma de forma explícita que un enlace ha pasado a estar inactivo, debido a que es una confirmación más positiva de un problema en la propia interfaz, o en su vecino directamente conectado.

La siguiente tabla muestra los valores de precedencia que la Pasarela de sucesos asigna de forma predeterminada.

Tabla 104. Valores de precedencia predeterminados

Valor	Significado	Ejemplos de sucesos
0	Asignado a los sucesos que no pueden causar otros problemas. Durante el RCA, el suceso no puede suprimir otros sucesos, pero sí puede ser suprimido.	SYSLOG-cisco-ios-SYS-CPUHOG SYSLOG-cisco-ios-BGP-NOTIFICATION
300	Reservado para sucesos no autoritativos que sugieren, pero no indican necesariamente, un error del dispositivo. Por ejemplo, el hecho de que no se pueda alcanzar un dispositivo no indica necesariamente un problema en ese dispositivo; este error puede estar causado por un problema entre la estación de sondeo y el dispositivo.	probeping-icmptimeout SNMPTRAP-IETF-OSPF-TRAP-MIB-ospfIfStateChange
600	Destinado a errores de protocolo. Los errores identificados por debajo de la pila de protocolos deben tener un valor de precedencia mayor. Por ejemplo, a medida que OSPF se ejecuta a través de IP, se espera que un error de OSPF tenga un valor de precedencia más bajo que un error de IP.	SNMPTRAP-IETF-OSPF-TRAP-MIB-ospfIfConfigError
900	Se asigna a los errores físicos confirmados que implican indirectamente un enlace inactivo o un error de ping (y la mayoría de los demás sucesos).	SNMPTRAP-cisco-CISCO-WIRELESS-IF-MIB-cwrTrapLinkQuality
910	Se asigna a los errores físicos confirmados que indican de forma directa un enlace inactivo o un error de ping.	SNMPTRAP-linkDown SYSLOG-smc-switch-linkDown
10 000	Se asigna a los sucesos que no pueden estar causados por otros problemas. Durante el RCA, el suceso no puede ser eliminado por otros sucesos, pero puede convertirse en causa raíz, y suprimir otros sucesos.	SYSLOG-cisco-ios-CI-SHUTDOWN SNMPTRAP-riverstone-RIVERSTONE-NOTIFICATIONS-MIB-rsEnvirHotSwapOut

Entidad de sondeador

Utilice esta información para comprender qué es la entidad de sondeador y cómo configurarla.

La entidad de sondeador también conocida como estación de sondeo, es el servidor desde el que Network Manager sondea dispositivos. Si la estación de sondeo, por lo general el servidor Network Manager, no se encuentra dentro del ámbito del dominio de red, para habilitar el conector RCA para realizar la supresión aislada, es necesario especificar la dirección IP o el nombre del DNS de la interfaz de ingreso como entidad de sondeo. Esta es la interfaz dentro del alcance del descubrimiento desde la que se transmiten los paquetes de red a y desde la estación de sondeo.

La entidad de sondeo es el nombre de un servidor que se utilizará para representar el servidor local de Network Manager y se almacenará en la tabla config.defaults en el campo NcpServerEntity. Se requiere un valor en el campo NcpServerEntity si el servidor de Network Manager no está en el ámbito del descubrimiento.

El campo NcpServerEntity debe configurarse del siguiente modo:

Tabla 105. Valores de configuración del campo NcpServerEntity

¿El servidor de Network Manager está en el ámbito de descubrimiento?	**Valor del campo NcpServerEntity**
Sí	Serie vacía
No	Dirección IP o nombre DNS de la interfaz de ingreso

El siguiente diagrama muestra la interfaz de ingreso (en un círculo) cuando el servidor de Network Manager está fuera del ámbito del descubrimiento.

Nota: Debe ejecutar como mínimo un descubrimiento para que la Pasarela de sucesos encuentre la entidad de sondeador en la base de datos NCIM.

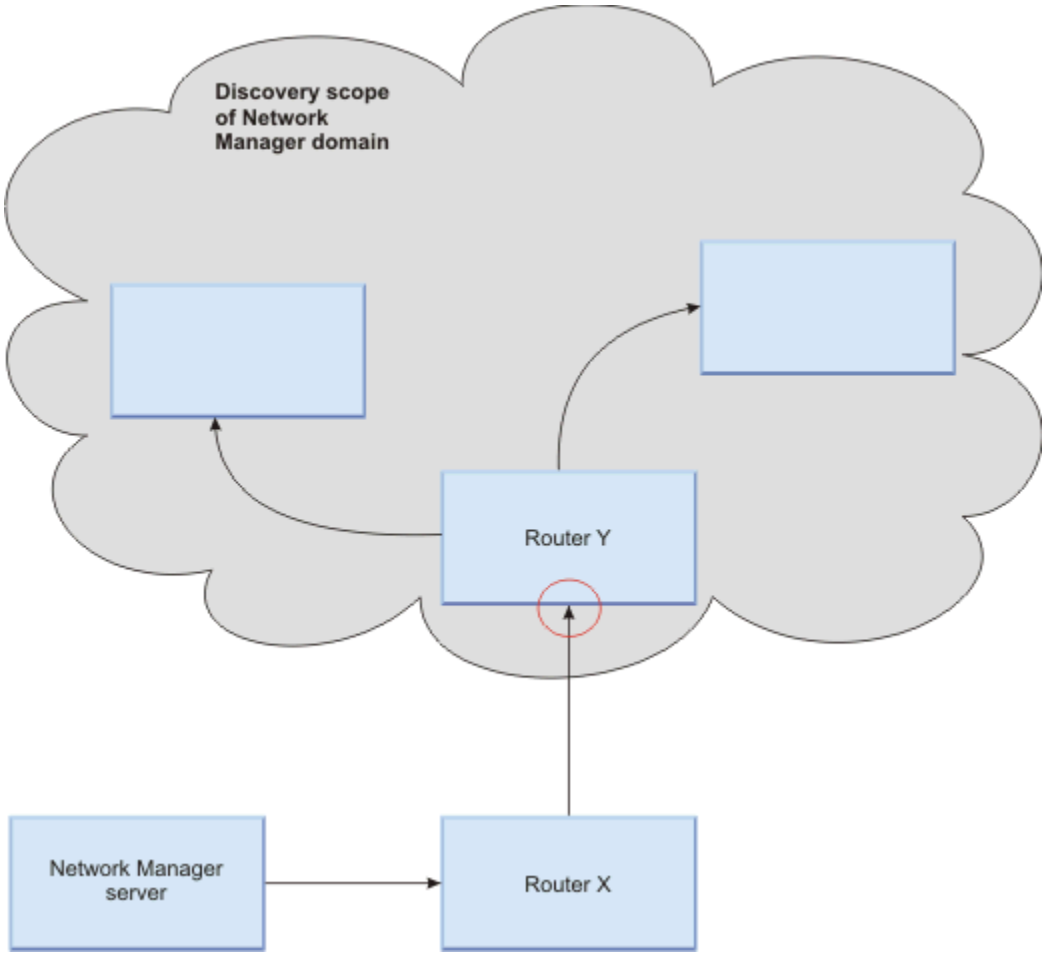


Figura 10. Interfaz de ingreso

Tareas relacionadas

Configuración de la entidad del sondeador
Cuando el servidor de Network Manager no está en el ámbito del dominio de red, o si tiene varios dominios, especifique la dirección IP o el nombre DNS de la entidad del sondeador.

RCA y estado sin gestionar

Utilice esta información para conocer cómo el conector RCA gestiona los sucesos procedentes de dispositivos que están en un estado sin gestionar, también conocido como estado de mantenimiento.

El método utilizado por el conector RCA para gestionar sucesos procedentes de dispositivos que están en un estado no gestionado se rige por el valor establecido para `HonourManagedStatus` en el archivo de configuración del conector `$NCHOME/etc/precision/RCASchema.cfg`. Este campo puede tomar los siguientes valores.

- 1 (valor predeterminado): indica al conector RCA que ratifique el estado gestionado de los sucesos. Todos los sucesos de los dispositivos no gestionados se colocan en mojo.events pero después se ignoran en términos de procesamiento de RCA.
- 0: indica al conector RCA que procese los sucesos procedentes de dispositivos sin gestionar como sucesos normales.

El plug-in RCA determina si el dispositivo no está gestionado analizando el campo NmosManagedStatus del suceso.

Suponiendo que el conector RCA se configura para ratificar el estado gestionado de los sucesos (`HonourManagedStatus` = 1), un suceso de un dispositivo sin gestionar no puede ser la causa raíz y no se puede suprimir.

Si el suceso tiene un estado de Sucedido de nuevo y apariciones anteriores de este mismo suceso indicaban que el dispositivo estaba gestionado con anterioridad, el registro de suceso de la base de datos mojo.events se actualiza y sus campos `NmosCauseType`, `NmosSerial` y `SuppressionState` se restablecerán a 0, lo que indica, de hecho, al conector RCA que no tenga en cuenta este suceso. El estado gestionado de los sucesos que reaparecen puede cambiar debido a que el siguiente estado gestionado es una propiedad de una entidad; por ejemplo, una interfaz. El estado gestionado de la entidad se almacena en un campo del registro de entidad. Además, los sucesos generados en una entidad también incluyen un campo denominado `NmosManagedStatus` que registra el estado gestionado de la entidad *en el momento en que se generó el suceso*. Por lo tanto, es posible que un suceso se produzca cuando se esté gestionando una entidad, pero posteriormente el mismo suceso puede volver a producirse cuando la entidad no esté gestionada, es decir, después de que la entidad haya cambiado su estado de gestionado a sin gestionar.

Los siguientes casos de ejemplo explican cómo el conector RCA gestiona sucesos cuyo estado gestionado cambia en las apariciones posteriores.

Cambios de suceso de gestionado a sin gestionar

La secuencia es la siguiente:

1. El suceso que se produce inicialmente (por ejemplo, un suceso de error del ping) se procesa como normal por parte del RCA, puesto que el suceso tenía un estado `NmosManagedStatus` de 0, lo que significa que la entidad estaba gestionada cuando el suceso se produjo por primera vez.
2. Un tiempo después, la entidad de interfaz se establece como sin gestionar; es decir, el valor de `ManagedStatus` para la interfaz pasa a ser 1.
3. El suceso de la interfaz se vuelve a producir.
4. El suceso de error del ping sucedido de nuevo ahora contiene el valor de campo `NmosManagedStatus` = 1, pero la aparición anterior de este suceso, todavía en la base de datos mojo.events, tenía el valor de campo `NmosManagedStatus` = 0.
5. El plug-in RCA detecta que el valor del campo `NmosManagedStatus` ha cambiado de 0 a 1, para el suceso Sucedido (o Actualizado).
6. El plug-in RCA actualiza el registro de sucesos en la base de datos mojo.events y, a partir de ese momento, gestiona el suceso como si se hubiera eliminado; es decir, vuelve a procesar todas las eliminaciones del suceso porque ya no se permite a este suceso suprimir sucesos.

Cambios de suceso de sin gestionar a gestionado

La secuencia es la siguiente:

1. El suceso que se produce inicialmente (por ejemplo, un suceso de error del ping) llega con un `NmosManagedStatus` de 1, lo cual significa que la entidad estaba sin gestionar cuando el suceso se produjo por primera vez. Por lo tanto, el suceso se procesa como si fuera un suceso eliminado y no tiene permitido suprimir sucesos.
2. Un tiempo después, la entidad de interfaz se establece como gestionada; es decir, el valor de `ManagedStatus` para la interfaz pasa a ser 0.
3. El suceso de la interfaz se vuelve a producir.
4. El suceso de error del ping sucedido de nuevo ahora contiene el valor de campo `NmosManagedStatus` = 0, pero la aparición anterior de este suceso, todavía en la base de datos mojo.events, tenía el valor de campo `NmosManagedStatus` = 1.
5. El conector RCA detecta que el valor del campo `NmosManagedStatus` ha cambiado de 1 a 0, para el suceso con el estado Sucedido de nuevo (o Actualizado).
6. El conector RCA actualiza el registro de suceso en la base de datos mojo.events y a partir de ese momento gestiona ese suceso como un suceso normal; este suceso no tiene permitido suprimir otros sucesos.

Agrupadores de análisis de causa raíz

Los agrupadores de análisis de causa raíz procesan un suceso desencadenante cuando pasa por el conector RCA.

Los agrupadores del conector RCA están almacenados en la siguiente ubicación: `$NCHOME/precision/eventGateway/stitchers/RCA`.

Para obtener más información acerca del lenguaje de los agrupadores, consulte la publicación *Referencia de IBM Tivoli Network Manager*.

Secuencia del agrupador de análisis de causa raíz

Los agrupadores invocados por el plugin RCA y la secuencia en la que aquéllos se ejecutan para determinar la causa raíz.

1. Cuando Event Gateway pasa un suceso al plugin RCA, se invoca el agrupador `ProcessEvent.stch` para gestionar el suceso. Este suceso se denomina suceso desencadenante.
2. El agrupador `ProcessEvent.stch` determina qué agrupador invocar, según el estado de suceso para el suceso desencadenante, según se describe en la tabla siguiente:

Estado de suceso del suceso desencadenante	**Agrupador que se invoca**
Sucedido Reactivado, Resucedido Resincronizado Actualizado	`ProcessProblemEvent.stch`
Borrado Eliminado	El agrupador `ProcessResolutionEvent.stch` ha procesado los sucesos de borrado y supresión. Fix Pack 3 El agrupador `TimedClearEventProcessing.stch` vuelve a procesar los sucesos que se han eliminado con los sucesos de borrado y supresión. Este agrupador incorpora un retraso de 30 segundos para evitar problemas causados por los eventos que llegan muy cerca unos de otros.

3. El agrupador `ProcessProblemEvent.stch` invoca dos desencadenantes para intentar suprimir el suceso desencadenante. Estos desencadenantes son según se indica a continuación:
   - El agrupador `SuppressTrigger.stch` determina si el suceso desencadenante se puede suprimir mediante un suceso existente.
   - Para sucesos OSPF o BGP, el agrupador `PeerEntitySuppression.stch` determina si el suceso desencadenante se puede suprimir mediante otro sucesos en la entidad homóloga.

   Si los agrupadores `SuppressTrigger.stch` o `PeerEntitySuppression.stch` no pueden suprimir el suceso desencadenante, éste pasa a ser la causa raíz.
4. El plugin de RCA comprueba si el suceso desencadenante ha sido suprimido por otro suceso en la misma identidad. Esto es, la comprobación evalúa si el suceso desencadenante no es el suceso maestro para la entidad. Si el suceso desencadenante no es el suceso maestro, se impide la supresión de otros sucesos, ya que el suceso maestro para la entidad realiza la supresión de suceso. En los pasos posteriores, `ProcessProblemEvent.stch` invoca otras agrupaciones, que intentan utilizar el suceso desencadenante para suprimir otros sucesos. En correspondencia, se ejecuta cada uno de los agrupadores.
5. El agrupador `EntitySuppression.stch` utiliza el suceso desencadenante para suprimir otros sucesos en la misma entidad. El suceso con la prioridad más alta en la entidad suprime el resto de sucesos en dicha entidad.
6. El agrupador `ContainedEntitySuppression.stch` utiliza el suceso desencadenante para intentar suprimir otros sucesos mediante los principios de entidad contenidos. El suceso de la entidad contenedora suprime los sucesos de todas las entidades contenidas.
7. El agrupador `IsolatedEntitySuppression.stch` utiliza el suceso desencadenante para intentar suprimir otros sucesos mediante los principios de entidad en sentido descendente.
8. El agrupador `ConnectedEntitySuppression.stch` utiliza el suceso desencadenante para intentar suprimir otros sucesos mediante los principios de entidad conectados. Por ejemplo, cuando dos interfaces están conectadas y hay un suceso en ambas, el suceso de una de las interfaces suprime el suceso de la otra interfaz.

Conceptos relacionados

Estados de suceso

La Pasarela de sucesos asigna un estado al suceso en función del tipo de suceso y de los campos Severity y Tally del suceso. El estado del suceso es uno de los parámetros utilizados por los conectores de suceso al suscribirse a sucesos.

Constantes predefinidas en agrupadores RCA

Network Manager proporciona constantes predefinidas para el tipo de supresión RCA y el tipo de causa RCA. Al codificar nuevos agrupadores RCA o al modificar agrupadores RCA existentes, puede almacenar estas constantes predefinidas en una variable de entero.

Las constantes predefinidas para el tipo de supresión son las siguientes:

$RCA_NO_SUPPRESSION
No suprimida. Un suceso de causa raíz toma este estado.

$RCA_ENTITY_SUPPRESSION
Suprimida por otro suceso en la misma entidad.

$RCA_CONTAINED_SUPPRESSION
Suprimida contenida; por ejemplo, los fallos en interfaces que están dentro de un dispositivo de chasis se suprimen por un fallo en ese dispositivo de chasis.

$RCA_ISOLATED_SUPPRESSION
Suprimida aislada; los fallos en dispositivos en sentido descendente y aislados por un único dispositivo de chasis se suprimen por un fallo en ese dispositivo de chasis aislado.

$RCA_CONNECTED_SUPPRESSION
Suprimida por un suceso en una entidad conectada.

$RCA_PEER_SUPPRESSION
Supresión de entidad de igual.

Las constantes predefinidas por tipo de causa son las siguientes:

$RCA_UNKNOWN_CAUSE
La causa del suceso es desconocida

$RCA_ROOT_CAUSE
Suceso de causa raíz.

$RCA_SUPPRESSED
Suceso suprimido.

Nota: No utilice nunca un código de agrupador para configurar la variable causeType como $RCA_SUPPRESSED. Esto sólo se debe hacer por medio del código RCA subyacente.

Descripciones del agrupador de RCA

Utilice esta información para comprender qué es lo que realiza el agrupador de RCA.

La siguiente tabla describe los agrupadores de RCA.

Tabla 106. Agrupadores de análisis de causa raíz

Agrupador	Descripción
ConnectedEntitySuppression.stch	Utiliza el suceso desencadenante para intentar suprimir otros sucesos utilizando los principios de entidad conectada. Por ejemplo, cuando dos interfaces conectadas tienen un suceso, el suceso de una de las interfaces suprime el suceso de la otra.
ContainedEntitySuppression.stch	Utiliza el suceso desencadenante para intentar suprimir otros sucesos utilizando los principios de entidad contenida. El suceso de la entidad contenedora suprime los sucesos de todas las entidades contenidas.
EntitySuppression.stch	Utiliza el suceso desencadenante para intentar suprimir otros sucesos utilizando los mismos principios de supresión de entidad. El suceso con la precedencia más alta de la misma entidad suprime el resto de sucesos de esa entidad.
IsolatedEntitySuppression.stch	Utiliza el suceso desencadenante para intentar suprimir otros sucesos utilizando los principios de entidad en sentido descendente.
PeerEntitySuppression.stch	Determina si el suceso desencadenante se puede suprimir mediante un suceso OSPF o BGP existente.
ProcessEvent.stch	Se llama a este agrupador cada vez que se pasa un suceso desencadenante al conector RCA. El agrupador `ProcessEvent.stch` determina a qué agrupador se llamará en función del estado del suceso desencadenante: • Se llama a ProcessProblemEvent.stch para gestionar sucesos con los estados `Occurred`, `ReAwakened`, `ReOccurred`, `Resync` y `Updated`. • Se llama a ProcessResolutionEvent para gestionar sucesos con los estados `Cleared` y `Deleted`.

Tabla 106. Agrupadores de análisis de causa raíz (continuación)

Agrupador	Descripción
ProcessProblemEvent.stch	Gestiona sucesos de problema, es decir, sucesos con los estados `Occurred`, `ReAwakened`, `ReOccurred`, `Resync` y `Updated`. Este agrupador llama a los agrupadores `SuppressTrigger` y `PeerEntitySuppression` para intentar suprimir el suceso desencadenante utilizando otros sucesos. A continuación, llama a los agrupadores `EntitySuppression`, `ContainedEntitySuppression`, `ConnectedEntitySuppression` y `cIsolatedEntitySuppression`, en ese orden, para intentar suprimir otros sucesos mediante el suceso desencadenante. A partir de la versión 4.2, los sucesos no se devuelven a ObjectServer si no hay cambios en el estado RCA.
ProcessResolutionEvent.stch	Gestiona sucesos de resolución, es decir, sucesos con el estado `Cleared` y `Deleted`.
SuppressTrigger.stch	Determina si el suceso desencadenador se puede suprimir mediante un suceso existente.
TimedClearEventProcessing.stch	Fix Pack 3 Un agrupador temporizado que se ejecuta cada 30 segundos. Este intervalo se define mediante la propiedad `m_IntervalSeconds` en el agrupador. Llama al agrupador `AmosTimedClearEventProcessing()` , que vuelve a procesar los sucesos que se han suprimido por un suceso de borrado. El agrupador `AmosTimedClearEventProcessing()` solo procesa los sucesos suprimidos si el suceso de borrado se ha producido hace más de 30 segundos. Este umbral de tiempo se define por la propiedad `Age` en el agrupador.

Tabla 106. Agrupadores de análisis de causa raíz (continuación)	
Agrupador	**Descripción**
TimedEventSuppression.stch	La finalidad de este agrupador es evitar que el conector RCA procese sucesos fluctuantes. Los sucesos que pueden rodar se pasan de la Pasarela de sucesos con un valor `EventCanFlap = 1`. Estos sucesos se colocan en la base de datos mojo.events con `TimedEscalation = 1` y se dejan allí durante 30 segundos. Tras 30 segundos, el agrupador RCA de TimedEventSuppression procesará todos los sucesos que tengan al menos 30 segundos y que tengan el valor `TimedEscalation = 1`. **Nota:** Al esperar 30 segundos para procesar el suceso, el sistema garantiza que la entidad que generó el suceso no fluctúa. Una entidad fluctuante, por ejemplo, una interfaz que genera una corriente continua de sucesos de enlace activo e inactivo, podría generar estos sucesos cada dos segundos. A medida que el suceso de enlace activo pase por el conector RCA, el agrupador ProcessResolutionEvent eliminará el suceso de enlace inactivo . Ningún suceso fluctuante es procesado por TimedEventSuppression porque ya se han suprimido durante el intervalo de espera de 30 segundos. Tras el proceso, todos los sucesos con el valor `TimedEscalation = 1` tendrán el campo `TimedEscalation` establecido en 2 para evitar procesos posteriores.

Conceptos relacionados

Estados de suceso

La Pasarela de sucesos asigna un estado al suceso en función del tipo de suceso y de los campos Severity y Tally del suceso. El estado del suceso es uno de los parámetros utilizados por los conectores de suceso al suscribirse a sucesos.

Ejemplos de análisis de causa raíz

Estos ejemplos muestran cómo el proceso de RCA realiza un análisis de causa raíz basado en la consideración de los distintos tipos de dispositivos de red e interfaces. Los ejemplos tienen únicamente un carácter ilustrativo y están pensados para mostrar los principios que el RCA utiliza. El RCA en redes más grandes es más complejo.

El sistema de análisis de causa raíz suprime sucesos en entidades basadas en la siguiente jerarquía de supresión:

1. La misma supresión de entidad.
2. Supresión contenida
3. Supresión aislada
4. Supresión conectada

Por ejemplo, si un suceso suprime otro suceso en la misma entidad, ese suceso no puede estar contenido suprimido, aislado suprimido o conectado suprimido. De forma parecida, si un suceso en el dispositivo que lo contiene suprime un suceso en una interfaz, ese suceso no puede ser aislado suprimido o conectado suprimido.

Los colores que se muestran en los diagramas coinciden los colores de suceso de la **Visor de sucesos**:

- Rojo: suceso de causa raíz.
- Púrpura: suceso de síntoma (eliminado).

Para obtener más información sobre la identificación e investigación de sucesos causa raíz en **Visor de sucesos**, consulte *Guía del usuario de IBM Tivoli Network Manager*.

Referencia relacionada

Consideraciones de RCA en una red de dominios cruzados

En un entorno de dominios cruzados, el proceso **ncp_g_event** de cada dominio de descubrimiento ejecuta RCA en los dispositivos en el mismo dominio de descubrimiento. En cada dominio, RCA opera de la misma forma que cuando sólo hay un único dominio. También puede analizarse la causa raíz en varios dominios cuando se visualizan conjuntamente utilizando un descubrimiento de dominios cruzados.

Definición de sentido ascendente y del sentido descendente en RCA

Utilice esta información para entender cómo se aplican los términos en sentido ascendente y en sentido descendente dentro del plug-in RCA.

Definición de términos

Los términos en sentido ascendente y en sentido descendente se utilizan con referencia a la entidad de sondeador.

En sentido descendente
: Especifica una ubicación en la red topológicamente más distante de la estación de sondeo pero en la misma vía de acceso física que la segunda ubicación.

En sentido ascendente
: Especifica una ubicación en la red topológicamente más cercana a la estación de sondeo pero en la misma vía de acceso física que la segunda ubicación.

En redes complejas, la distancia de los dispositivos de la estación de sondeo cambia cuando se desactivan los dispositivos. Este cambio en la distancia tiene un impacto sobre los dispositivos que están en sentido ascendente y los que están en sentido descendente.

Ejemplo

La figura que aparece a continuación muestra un ejemplo de ubicaciones en sentido ascendente y descendente. En este ejemplo, el dispositivo B está en sentido descendente a A; por lo tanto, el dispositivo A está en sentido descendente al dispositivo B.

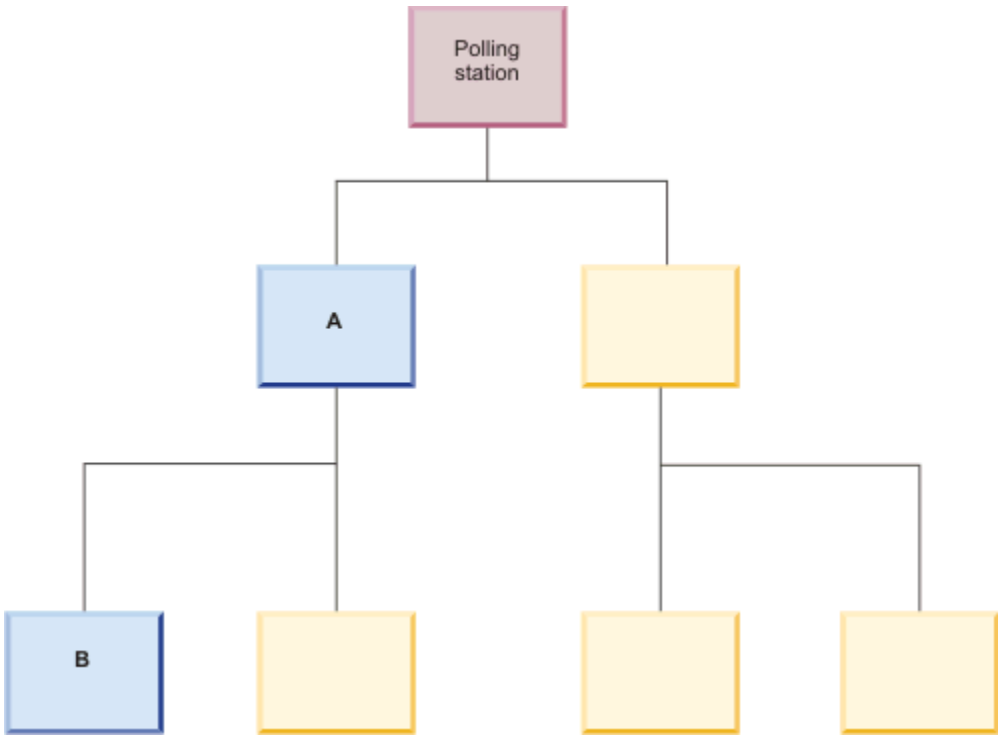


Figura 11. Dispositivos en sentido ascendente y descendente

Referencia relacionada

Supresión aislada de los dispositivos de chasis
Una anomalía en un dispositivo de chasis suprime anomalías en todos los dispositivos de chasis aislados por el dispositivo de chasis donde se produjo la anomalía. Este es un ejemplo de *supresión aislada*.

Supresión aislada para dispositivos al límite de la red
Una anomalía en una interfaz física o lógica que es la única conexión entre otras entidades y la red suprime anomalías en las entidades en sentido descendente. Este es un ejemplo de *supresión aislada*.

Dispositivos de chasis e interfaces de bucle de retorno

En la mayoría de los casos, el proceso de RCA supone que si falla un chasis, entonces la causa raíz para otras anomalías se origina en el chasis. Las anomalías de chasis suprimen anomalías en las interfaces contenidas, interfaces conectadas y dispositivos de chasis en sentido descendente.

La interfaz de bucle de retorno tiene una función especial dentro de un dispositivo de chasis, si es direccionador o conmutador. Una interfaz de bucle de retorno siempre tiene una dirección IP, que corresponde a la dirección IP del dispositivo de chasis. Network Manager asocia la interfaz de bucle de retorno con el chasis durante el descubrimiento. La interfaz de bucle de retorno representa el chasis completo y se le puede realizar el sondeo de forma individual. Las anomalías en la interfaz de bucle de retorno suprimen anomalías en entidades conectadas y contenidas de exactamente la misma forma que las anomalías en los dispositivos de chasis.

Sólo los sucesos de los dispositivos de chasis, interfaces, módulos y tarjetas tienen permiso para conectar o suprimir otros sucesos. Sin embargo, un chasis no conectará-suprimirá otro chasis (o tarjeta hija).

Interfaces contenidas

Una anomalía del chasis suprime todas las anomalías en las interfaces contenidas dentro de ese chasis.

En la figura siguiente, una anomalía en el dispositivo A del chasis suprime anomalías de las interfaces b, c y d. Las interfaces b, c y d están contenidas dentro del dispositivo A del chasis.

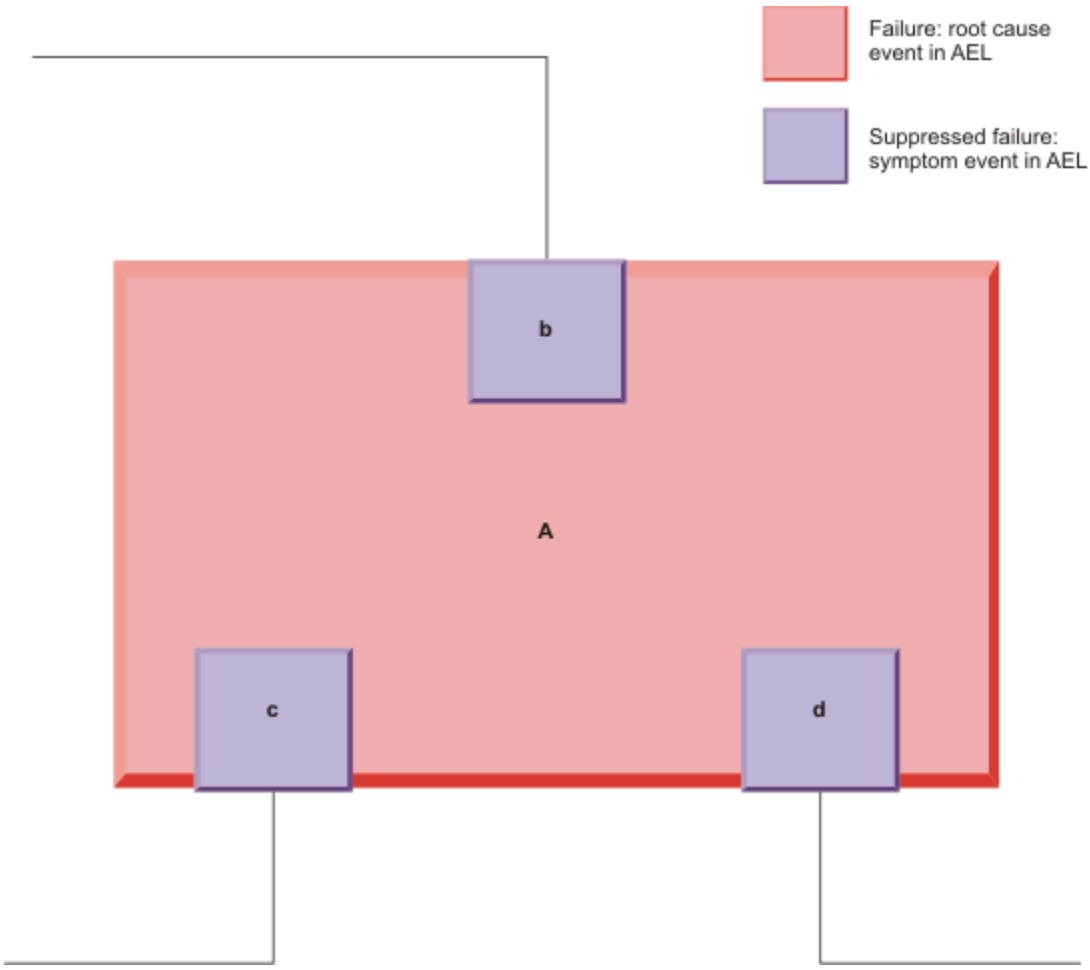


Figura 12. La anomalía del chasis suprime las anomalías en interfaces contenidas

Interfaces conectadas

Una anomalía de chasis suprime todas las anomalías en las interfaces conectadas a ese dispositivo de chasis. Las anomalías se suprimen en las interfaces en sentido ascendente y en sentido descendente.

En la figura que aparece a continuación, el dispositivo A suprime las anomalías en las interfaces b, c y d.

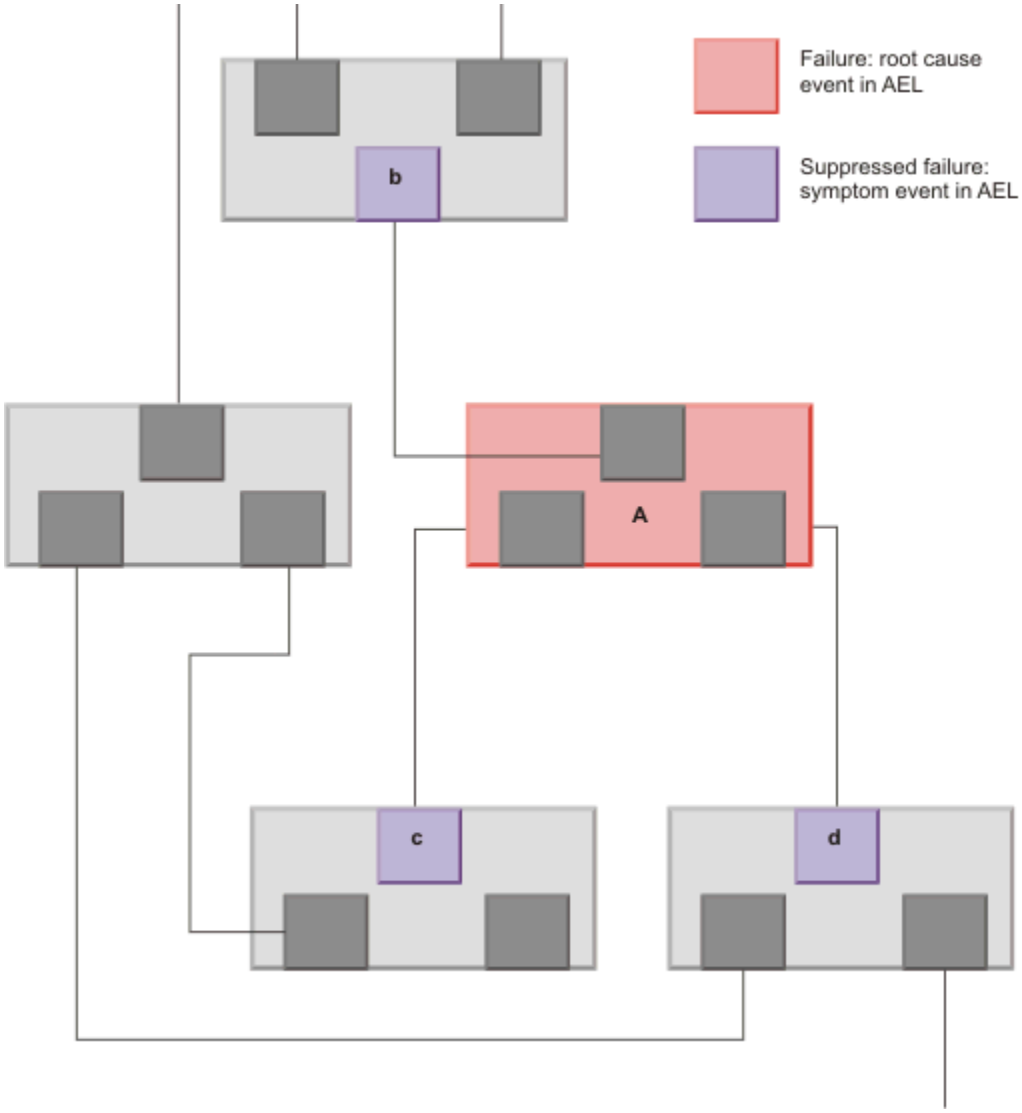


Figura 13. La anomalía de chasis suprime anomalías en las interfaces conectadas

Entidades conectadas a una entidad contenida

Un dispositivo de chasis puede contener una o más entidades. Ejemplos de entidades que se pueden contener dentro de un dispositivo de chasis son VLAN, tarjetas y direccionadores virtuales. Una entidad contenida, como una tarjeta puede tener más de una interfaz.

Una anomalía en un dispositivo de chasis suprime las anomalías en entidades directamente conectada a cualquiera de las entidades contenidas en ese dispositivo de chasis. En la figura que aparece a continuación, la entidad B se contiene en el dispositivo de chasis A. Una anomalía en el dispositivo de chasis A suprime una anomalía en la interfaz d del dispositivo D y la interfaz e en el dispositivo E. Ambas interfaces d y e está directamente conectadas a la entidad B.

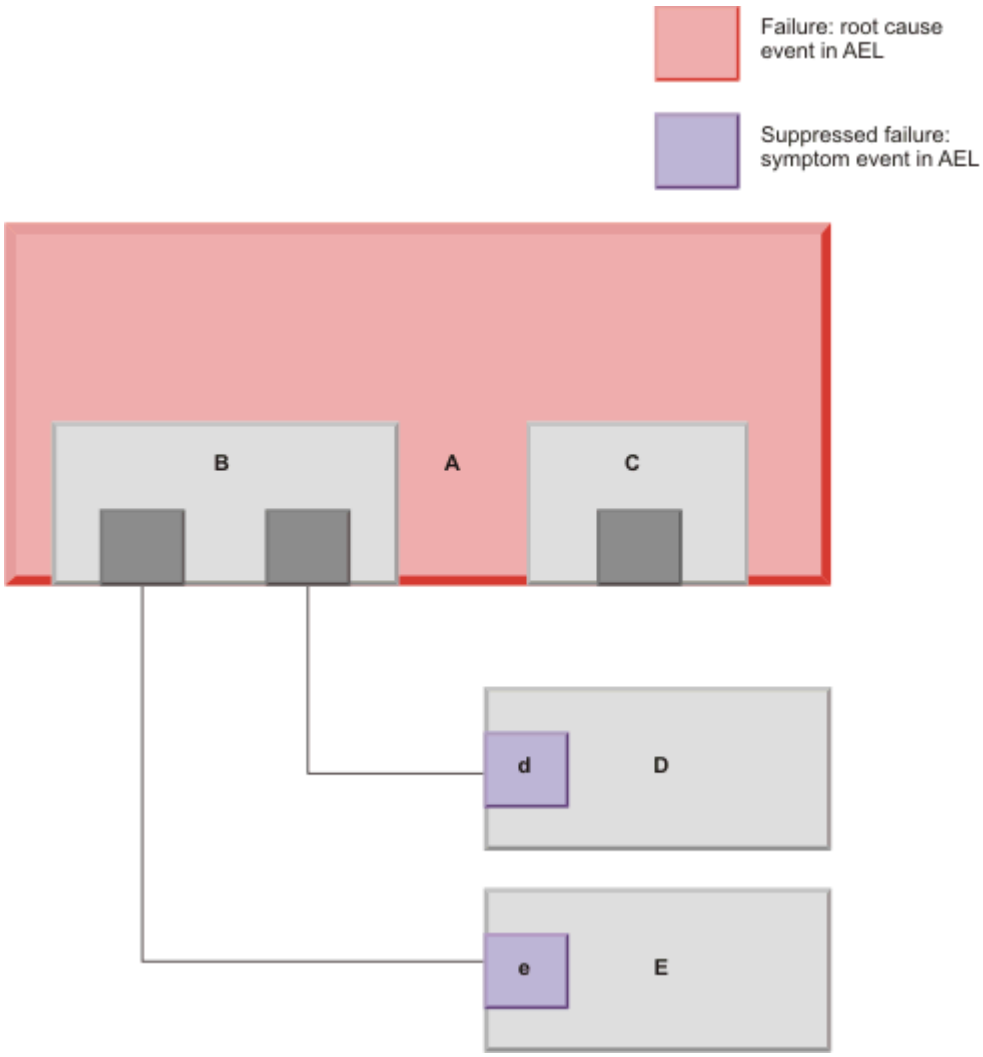


Figura 14. Una anomalía de chasis suprime anomalías en dispositivos conectados a entidades contenidas

Supresión aislada de los dispositivos de chasis

Una anomalía en un dispositivo de chasis suprime anomalías en todos los dispositivos de chasis aislados por el dispositivo de chasis donde se produjo la anomalía. Este es un ejemplo de *supresión aislada*.

En la figura que aparece a continuación, una anomalía en el dispositivo A del chasis suprime anomalías en los dispositivos de chasis B, C y D. Los dispositivos de chasis B, C y D están todos aislados por el dispositivo de chasis A.

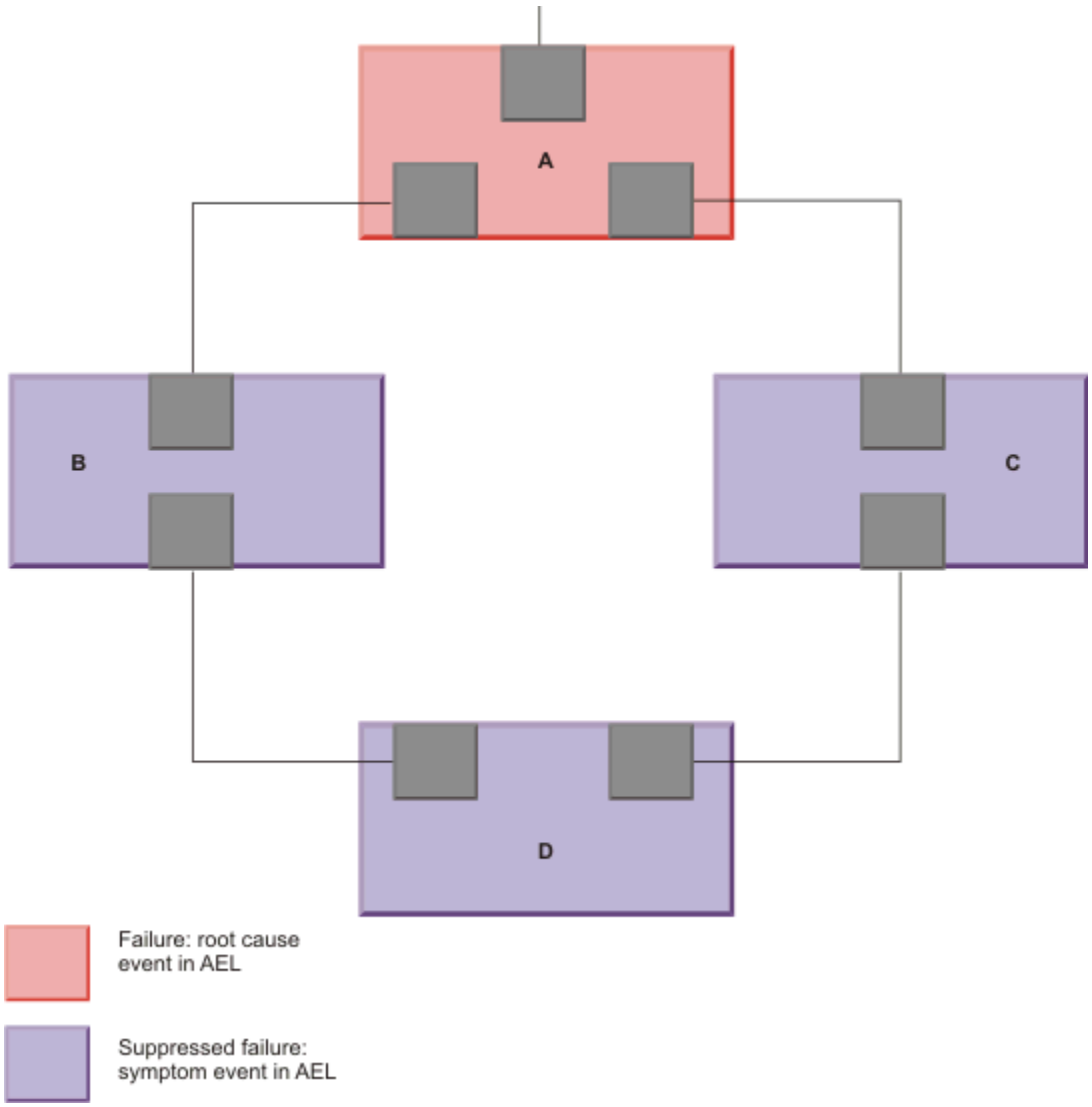


Figura 15. La anomalía de chasis suprime anomalías en entidades en sentido descendente

Referencia relacionada

Definición de sentido ascendente y del sentido descendente en RCA
Utilice esta información para entender cómo se aplican los términos en sentido ascendente y en sentido descendente dentro del plug-in RCA.

Interfaces

Si una interfaz está aislando anomalías en sentido descendente, entonces la anomalía de interfaz puede suprimir las anomalías en sentido descendente.

Interfaces conectadas

Una anomalía A en la interfaz suprime una anomalía B en la interfaz siguiente si las dos interfaces están conectadas directamente. La interfaz cuya regla de supresión se activa en primer lugar, suprime la otra interfaz. La supresión de una anomalía B en la interfaz por una anomalía A anterior en una interfaz conectada sólo puede producirse si existen las siguientes condiciones:

- La anomalía de la interfaz B ya no está contenida suprimida.
- La anomalía de la interfaz A ya no está contenida aislada.
- La anomalía de la interfaz A ya no está suprimida conectada.

- El chasis que contiene la interfaz A no está suprimido aislado.
- El chasis que contiene la interfaz A no está suprimido conectado.

Además, si la anomalía B en la interfaz fue primero una anomalía A en la interfaz conectar suprimir y, después el estado de topología cambió para que en lugar de A sea ahora B aislada, la supresión conectada de A por B se debe eliminar y A será B aislada suprimida.

Interfaces físicas y lógicas

Una interfaz física puede contener varias interfaces lógicas. Una anomalía en una interfaz física puede suprimir anomalías en sus interfaces lógicas relacionadas. La interfaz física puede suprimir su interfaz lógica relacionada aunque haya conectividad entre la interfaz lógica y un vecino externo. Incluso los sucesos en una interfaz física suprimida pueden contener sucesos que contienen supresión en sus interfaces lógicas asociadas.

Interfaz conectada directamente

Una anomalía de la interfaz física estándar suprime una segunda anomalía de interfaz física si las dos interfaces están conectadas directamente.

En general, una interfaz suprimida puede suprimir interfaces conectadas. Sin embargo, tenga en cuenta las siguientes restricciones relacionadas con la supresión de interfaces conectadas directamente:

- Una entidad no puede suprimir una interfaz contenida suprimida a la que está conectada.
- Una interfaz contenida suprimida no puede suprimir una entidad a la que está conectada.
- Una interfaz suprimida aislada no puede suprimir una entidad a la que está conectada.

En la figura que hay a continuación, la anomalía en la interfaz suprime la anomalía más reciente en una interfaz b conectada directamente.

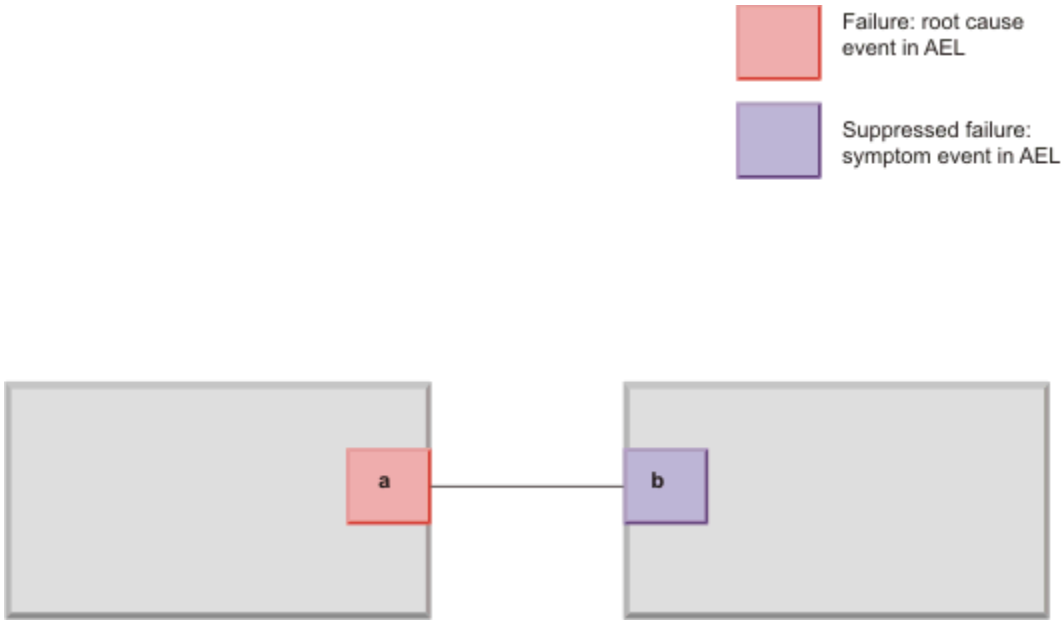


Figura 16. La anomalía de interfaz suprime una anomalía más reciente en una interfaz vecina conectada directamente

Interfaz lógica relacionada

Una anomalía en una interfaz física suprime las anomalías en las interfaces lógicas relacionadas.

En la figura siguiente, la anomalía en una interfaz física suprime anomalías en las interfaces lógicas contenidas b y c.

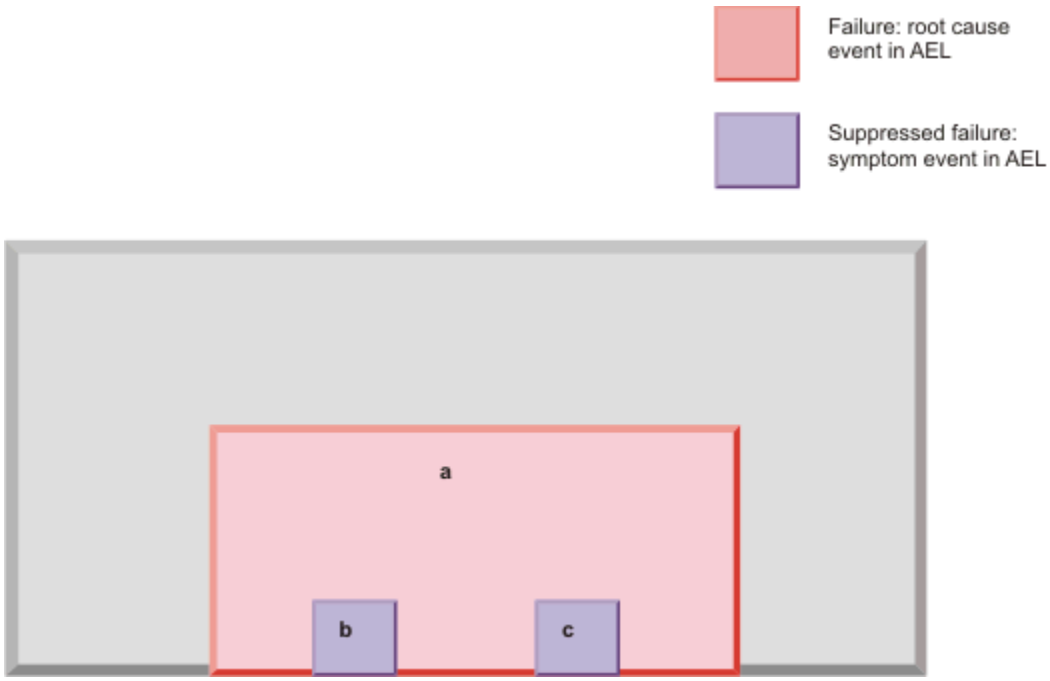


Figura 17. La anomalía de la interfaz física suprime anomalías en interfaces lógicas contenidas

Supresión aislada para dispositivos al límite de la red

Una anomalía en una interfaz física o lógica que es la única conexión entre otras entidades y la red suprime anomalías en las entidades en sentido descendente. Este es un ejemplo de *supresión aislada*.

En la figura siguiente, la anomalía de la interfaz d en el dispositivo A suprime anomalías en los dispositivos B, C y D y sus interfaces.

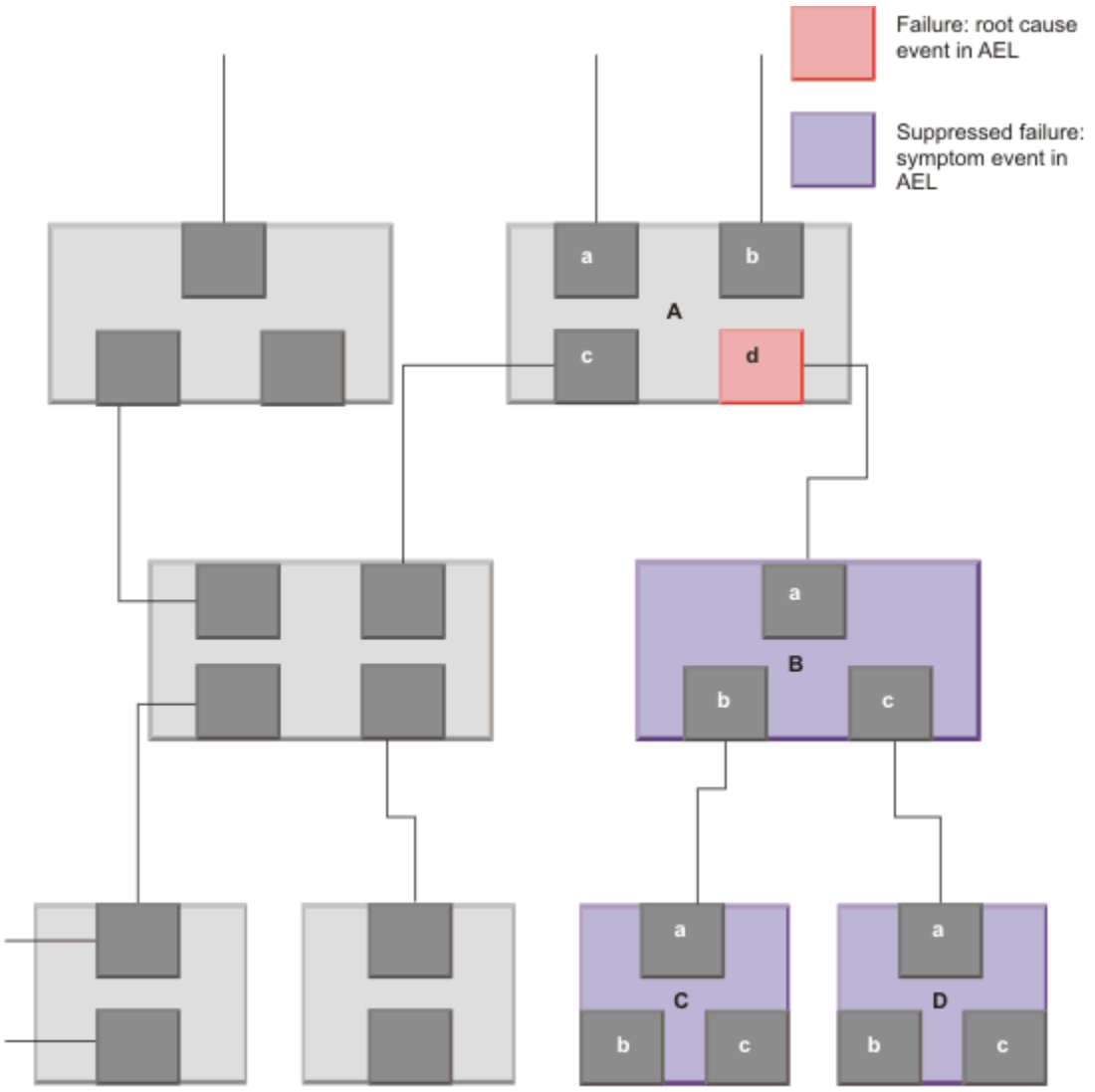


Figura 18. La anomalía de interfaz suprime una anomalía más reciente en una interfaz vecina conectada directamente

Referencia relacionada

Definición de sentido ascendente y del sentido descendente en RCA
Utilice esta información para entender cómo se aplican los términos en sentido ascendente y en sentido descendente dentro del plug-in RCA.

Consideraciones de RCA en una red de dominios cruzados

En un entorno de dominios cruzados, el proceso **ncp_g_event** de cada dominio de descubrimiento ejecuta RCA en los dispositivos en el mismo dominio de descubrimiento. En cada dominio, RCA opera de la misma forma que cuando sólo hay un único dominio. También puede analizarse la causa raíz en varios dominios cuando se visualizan conjuntamente utilizando un descubrimiento de dominios cruzados.

Supresión contenida

Como las interfaces están en el mismo dominio que el chasis que las contiene, el RCA contenido no se ve afectado por un entorno de dominios cruzados.

Interfaces conectadas

En un entorno de dominios cruzados, la mayoría de las conexiones se realizan entre dos interfaces en el mismo dominio y la supresión conectada funciona según lo esperado. Si las interfaces están en dominios diferentes, la supresión conectada no asocia los sucesos en cada extremo del enlace.

Supresión aislada

Los dispositivos en el límite de la red, que tienen menos conexiones, puede quedar inaccesibles (aislados) desde la entidad de sondeador si falla un dispositivo entre ellos y la entidad de sondeador. Los sucesos en estos dispositivos aislados se suprimen, siempre que todos los dispositivos aislados estén en el mismo dominio. Cuando particione la red, asegúrese de que los grupos de dispositivos que estén aislados se mantengan en el mismo dominio.

SAE RCA

Si un servicio, por ejemplo, una VPN está formada por dispositivos en dos dominios, pueden crearse dos sucesos SAE para la misma VPN, uno en cada dominio.

Conceptos relacionados

Acerca del descubrimiento de dominios cruzados
El descubrimiento de dominios cruzados puede configurarse para unir dos o más dominios descubiertos.

Tareas relacionadas

Configuración de descubrimientos de dominios cruzados
Para habilitar enlaces entre dispositivos en diferentes dominios para mostrar en las vistas de red y de topología, debe configurar y ejecutar descubrimientos de dominios cruzados en los distintos dominios.

Configuración de la entidad del sondeador
Cuando el servidor de Network Manager no está en el ámbito del dominio de red, o si tiene varios dominios, especifique la dirección IP o el nombre DNS de la entidad del sondeador.

Referencia relacionada

Ejemplos de análisis de causa raíz
Estos ejemplos muestran cómo el proceso de RCA realiza un análisis de causa raíz basado en la consideración de los distintos tipos de dispositivos de red e interfaces. Los ejemplos tienen únicamente un carácter ilustrativo y están pensados para mostrar los principios que el RCA utiliza. El RCA en redes más grandes es más complejo.

Comprobación de las vías de acceso de topología utilizadas por RCA

Utilice la herramienta de vía de acceso RCA para comprobar si hay disponible una vía de acceso lógica entre los dispositivos de red para fines de correlación topológica.

Acerca de la herramienta de vía de acceso RCA

La herramienta de vía de acceso RCA proporciona una ayuda de depuración para situaciones de análisis de causa raíz que implican una supresión aislada.

La herramienta de vía de acceso RCA le indica la vía de acceso más corta de A a Z, donde A y Z son dos nodos (por ejemplo, dispositivos) en la topología. Utilice la herramienta de vía de acceso RCA para determinar qué vías de acceso existen en la topología y para determinar dónde hay desconexiones inesperadas o vías de acceso adicionales inesperadas, las cuales afectarán al análisis de causa raíz de la sección de topología correspondiente en el entorno de producción.

La herramienta de vía de acceso RCA puede mostrar los siguientes tipos de vías de acceso entre entidades especificadas:

- **Vía de acceso completa**: muestra la vía de acceso más corta entre las entidades de origen y de destino, independientemente del estado actual de la red. La vía de acceso no cambia cuando los sucesos se colocan en nodos en esa vía de acceso. Por ejemplo, si hay un suceso, como una alerta PingFail en uno o varios dispositivos intermedios junto con la vía de acceso, este suceso se ignora. En consultas de la

herramienta de vía de acceso RCA, el valor de vía de acceso completa se indica por medio de la notación `atoz.full`.

Nota: Para alterar la vía de acceso completa, debe eliminar entidades de la topología. Es un gran cambio; sin embargo, puede ser necesario en alguna ocasión para una investigación en profundidad.

- **Vía de acceso actual**: también conocida como vía de acceso activa, esta vía de acceso muestra la vía de acceso más corta entre las entidades de origen y de destino, teniendo en cuenta el estado actual de la red. Por ejemplo, si hay un suceso, como una alerta PingFail en uno o varios dispositivos intermedios junto con la vía de acceso más corta a la entidad de destino, esta vía de acceso a la entidad de destino se interrumpe y la herramienta de vía de acceso RCA no la devuelve. Si hay una vía de acceso alternativa, se devuelve, aunque sea una vía de acceso más larga a la entidad de destino. En consultas de la herramienta de vías de acceso RCA, el valor de vía de acceso actual se indica por medio de la notación `atoz.current`.

Nota: No hay ninguna base de datos `atoz`, ni hay tablas `atoz.full` y `atoz.current`. Esta base de datos hipotética y sus tablas forman parte del mecanismo de selección OQL utilizado para comunicarse con el plug-in RCA para obtener información sobre su gráfico de topología

La manera más efectiva de utilizar la herramienta de vía de acceso RCA para llevar a cabo la depuración es cargar la topología desde la memoria caché y, a continuación, realizar las siguientes actividades de investigación en esta topología de memoria caché:

1. Determine la vía de acceso existente (vía de acceso actual) en la topología entre los dos nodos de interés, A y Z.
2. Inyecte sucesos en los nodos especificados entre A y Z junto a la vía de acceso de interés:
   a. ¿Existe una vía de acceso actual alternativa entre A y Z?
   b. ¿Ya no hay una vía de acceso? Si no existe una vía de acceso actual, los sucesos aportados se aislarán suprimidos por un suceso en A o Z. Si es A o Z depende de la ubicación de la entidad del sondeador. Suponiendo que es A, un suceso en A es candidato para ser el supresor de causa raíz de los sucesos en la vía de acceso entre A y Z.

Para aportar sucesos en dispositivos de la memoria caché de topología, utilice el script inject_fake_events.pl Perl. Para obtener más información sobre el script de Perl inject_fake_events.pl Perl, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Nota: No confunda la herramienta de vía de acceso RCA con la herramienta de vistas de vía de acceso disponible en la GUI. La herramienta de vía de acceso RCA es una herramienta de línea de mandatos y se utiliza principalmente para la resolución de problemas de análisis de causa raíz; por el contrario, la herramienta de vistas de vía de acceso basada en la GUI proporciona vistas gráficas a operadores de dispositivos y enlaces que componen una vía de acceso de red entre dos dispositivos seleccionados.

Uso de la herramienta de vía de acceso RCA

Utilice estos ejemplos para entender cómo se puede utilizar la herramienta de vía de acceso RCA para mostrar vías de acceso entre las entidades de origen y de destino especificadas en la red.

Ejemplo de uso

La herramienta de vía de acceso RCA utiliza el Proveedor de servicios de OQL, ncp_oql, para ejecutar consultas. Para obtener más información sobre el Proveedor de servicios de OQL, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

El siguiente mandato de ejemplo consulta la vía de acceso completa entre un dispositivo de origen con un valor de campo entityId de 6 y un dispositivo de destino con un valor de campo entityId de 137.

```
ncp_oql -domain NCOMS -service Events -query "select * from atoz.full
where a = 6 and z = 137;"
```

El resultado de la consulta puede parecerse a este:

```
{
   ENTITYID=6;
   ENTITYNAME='router4';
}

{
   ENTITYID=385;
   ENTITYNAME='VLAN_OBJECT_router4_VLAN_37';
}

{  ENTITYID=137;
   ENTITYNAME='router4[ Fa0/3/3 ]';
}

( 3 record(s) :   Transaction complete )
```

Ejemplo de consultas

Puede hacer un seguimiento de las vías de acceso desde una entidad de origen específica, u opcionalmente, desde cualquier sitio contenido dentro de esa entidad de origen. Además, las consultas de la herramienta de vía de acceso RCA deben especificar siempre dos entidades, una entidad de origen a la que se hace referencia como "a" y una entidad de destino, a la que se hace referencia como "z", y estas dos entidades representan el origen y destino de la vía de acceso. Las entidades de origen y de destino se pueden proporcionar como cualquier combinación de lo siguiente:

- ID de entidad
- Nombre de entidad
- Direcciones IP

Las consultas pueden seleccionarse adicionalmente para permitir que se haga seguimiento a una vía de acceso desde cualquier entidad contenida en el origen. Esto puede resultar útil al tratar con VLAN, donde es posible que no exista una vía de acceso directa desde el chasis que la contiene a una interfaz.

Nota: Las consultas se registran en el archivo de rastreo para el proceso de Pasarela de sucesos, ncp_g_event, en el nivel de depuración 1; por ejemplo, el archivo de registro de consulta se puede llamar ncp_g_event.NCOMS.trace.

Las siguientes consultas proporcionan ejemplos de cómo puede utilizar la herramienta de vía de acceso RCA.

1. Muestra la vía de acceso completa desde entityId 102 a entityId 105.

   ```
   ncp_oql -domain NCOMS -service Events -query "select * from atoz.full
   where a = 102 and z = 105;"
   ```

2. Muestra la vía de acceso completa desde la entidad denominada 'rod' a la entidad denominada 'freddy.

   ```
   ncp_oql -domain NCOMS -service Events -query "select * from atoz.full
   where a = 'rod' and z = 'freddy';"
   ```

3. Muestra la vía de acceso actual desde entityId 102 a la entidad con la dirección IP 172.21.226.3.

   ```
   ncp_oql -domain NCOMS -service Events -query "select * from atoz.current
   where a = 102 and z = '172.21.226.3';"
   ```

4. Muestra la vía de acceso actual desde la interfaz denominada 'rod[0 [1]]' a entityId 105.

   ```
   ncp_oql -domain NCOMS -service Events -query "select * from atoz.current
   where a = 'rod[ 0 [ 1 ] ]' and z = 105;"
   ```

5. Muestra la vía de acceso completa desde entityId 102 a la entidad con la dirección IP 172.21.226.3. Si no se encuentra la vía de acceso intente encontrar una vía de acceso desde cualquier sitio contenido por el contenedor de entityId 102. En otras palabras, suba un nivel en la jerarquía del contenedor para obtener el identificador del contenedor y, a continuación, intente construir la vía de acceso al usar como entidad de origen cada una de las entidades contenidas en ese contenedor.

```
ncp_oql -domain NCOMS -service Events -query "select * from atoz.full
where a = 102 and z = '172.21.226.3' and fromContained = 1;"
```

6. Cuando no hay vía de acceso, esto lo indicará claramente la salida.

```
ncp_oql -domain NCOMS -service Events -query "select * from atoz.full
where a = 6 and z = 97;"
```

Si no hay vía de acceso, la salida se parecerá a lo siguiente:

```
{
    EntityId=0;
    EntityName='No path found from A to Z';
}
( 1 record(s) : Transaction complete )
```

Tareas relacionadas

Consultas de bases de datos de gestión desde la línea de mandatos
Utilice el Proveedor de servicios OQL para realizar consultas en bases de datos de componentes de Network Manager.

Ejemplo: Determinación de las posibles causas raíz junto a una vía de acceso

Puede utilizar la herramienta de vía de acceso RCA para simular un error junto a una vía de acceso de la red. Si no hay vía de acceso alternativa a la entidad de destino, la vía de acceso a dispositivos en sentido descendente del error no se interrumpirá. En el entorno de producción, el dispositivo correspondiente al dispositivo con error se convierte en causa raíz.

Este ejemplo considera los dispositivos A, B, C y D conectados en una fila. Para mantener las cosas sencillas, no se muestran las interfaces:

```
A ------------ B ------------- C ------------- D
```

Network Manager sondea el dispositivo D de la entidad de sondeador. En el siguiente diagrama, la entidad de sondeador se muestra como entidad X.

```
X
\
 \
  \
   \
    A ------------ B ------------- C ------------- D
```

Si se aporta una alerta PingFail en el dispositivo B, esta alerta hace que el nodo B pase a inactivo e interrumpe la vía de acceso desde A a D y hace que la herramienta de vía de acceso devuelva los siguientes resultados:

- **Vía de acceso completa (atoz.full)**: muestra la vía de acceso más corta entre los nodos A y D, independientemente del estado actual de la red. En consecuencia, atoz.full muestra la vía de acceso desde A hasta D.
- **Vía de acceso actual (atoz.current)**: muestra la vía de acceso más corta entre los nodos A y D, teniendo en cuenta el estado actual de la red. Como el nodo B está inactivo, no hay vía de acceso desde A a D, por lo tanto, no se devuelve vía de acceso.

En el entorno de producción correspondiente, si se va a producir una alerta PingFail en el nodo D, esta alerta se suprimirá, y la alerta en el nodo B se resaltará como la causa raíz.

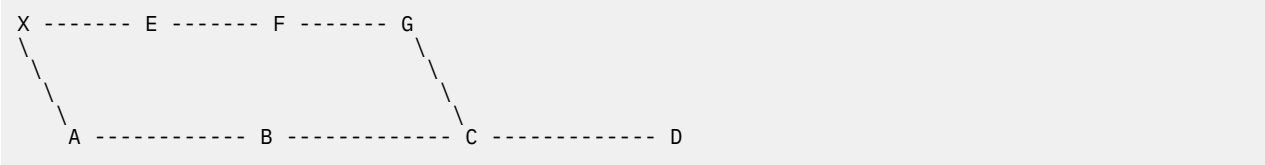
Conceptos relacionados

Entidad de sondeador
Utilice esta información para comprender qué es la entidad de sondeador y cómo configurarla.

Ejemplo: Determinación de vías de acceso alternativas

Puede utilizar la herramienta de vía de acceso RCA para determinas vías de acceso alternativas en caso de un error de dispositivo. Si hay una vía de acceso alternativa a la entidad de destino, a continuación, en el entorno de producción, el dispositivo correspondiente para el dispositivo con error no se convierte en causa raíz porque hay una vía de acceso alternativa para la entidad de destino.

Este ejemplo tiene en cuenta una sección de la red que incluye dos vías de acceso al nodo D, conectadas en una fila. Network Manager sondea al dispositivo D desde la entidad sondeadora. En el siguiente diagrama, la entidad de sondeador se muestra como entidad X. To mantener cosas sencillas, no se muestran las interfaces.



Si se aporta una alerta PingFail en el dispositivo B, esta alerta hace que el nodo B pase a inactivo e interrumpe la vía de acceso desde X a D a través de A. Sin embargo, hay una vía de acceso alternativa desde X a D, a través de E, y esto hace que la herramienta de vía de acceso RCA devuelva los siguientes resultados:

- **Vía de acceso completa (atoz.full)**: muestra la vía de acceso más corta entre los nodos X y D, independientemente del estado actual de la red. En consecuencia, esto muestra la vía de acceso desde X a D, a través de A, ya que es la vía de acceso más corta.
- **Vía de acceso actual (atoz.current)**: muestra la vía de acceso más corta entre los nodos X y D, teniendo en cuenta el estado actual de la red. En consecuencia, esto muestra la vía de acceso desde X a D, a través de E, ya que es la vía de acceso actual. El nodo B está inactivo, por lo que la vía de acceso de X a D, a través de A está interrumpida.

En el entorno de producción correspondiente, si se va a producir una alerta PingFail en el nodo D, esta alerta no se suprimirá; y la alerta en el nodo B no se mostrará como la causa raíz.

Conceptos relacionados

Entidad de sondeador
Utilice esta información para comprender qué es la entidad de sondeador y cómo configurarla.

Suscripciones de plug-ins de RCA

Utilice esta información para comprender a qué correlaciones de sucesos y estados de suceso se suscribe el plug-in de RCA.

Suscripciones de correlaciones de sucesos

El conector RCA se suscribe a las siguientes correlaciones de sucesos:

1. ChassisFailure
2. EMSNonPollingEvent
3. EMSPollingEvent
4. EntityFailure
5. EntityIfDescr
6. EntityMibTrap
7. ItnmLinkDownIfIndex
8. LinkDownIfDescr
9. LinkDownIfIndex
10. LinkDownIfName

11. NbrFail
12. NbrFailIfDescr
13. OSPFIfStateChange
14. OSPFIfStateChangeIP
15. PollFailure
16. PrecisionMonitorEvent

El conector RCA se suscribe a los siguientes estados de suceso:

1. Borrado
2. Suprimido
3. Sucedido
4. Reactivado
5. Sucedido de nuevo
6. Resincronizado
7. Actualizado

Conectores de la Pasarela de sucesos

Los conectores de la Pasarela de sucesos son módulos de la Pasarela de sucesos que reciben sucesos enriquecidos de ella y los enriquecen aún más o llevan a cabo otras acciones en ellos.

Nota: El conector RCA es considerablemente más complejo que los demás conectores de la Pasarela de sucesos y está documentado en la sección Conector RCA.

Los siguientes conectores están habilitados de forma predeterminada:

- Sondeo adaptativo
- Comprobación de la compatibilidad
- Disco
- Migración tras error
- PostNcimProcessing
- RCA
- Todos los conectores de suceso afectados por el servicio (SAE)

La siguiente tabla describe los conectores de la Pasarela de sucesos. Cada uno de estos conectores recibe sucesos enriquecidos de la Pasarela de sucesos y realiza un posterior enriquecimiento del suceso o lleva a cabo alguna otra acción.

Tabla 107. conectores de la Pasarela de sucesos

Plug-in	**Descripción**
Sondeo adaptativo	Graba un subconjunto de datos de suceso y de entidad relacionados en la tabla ncmonitor.activeEvent. Esto permite crear vistas de red en función de los datos de suceso (vistas de alerta). El ámbito de las políticas de sondeo se determina en función de las vistas de red y, por lo tanto, los sondeos se pueden definir en función de las alertas de red. Se conocen como sondeos adaptativos porque el sondeo se inicia en función de las condiciones del problema de red.
Comprobación de la compatibilidad	Intenta actualizar las tablas ObjectServer con cualquiera de los valores necesarios para Network Manager.

Tabla 107. conectores de la Pasarela de sucesos (continuación)	
Plug-in	**Descripción**
Disco	Recibe sucesos de arranque de la Pasarela de sucesos e inicia el descubrimiento parcial en función de estos sucesos. De forma predeterminada, este conector solo se interesa por sucesos que indican que se ha producido un rearranque.
Migración tras error	Recibe sucesos de comprobación de estado (ItnmHealthChk) de Network Manager de la Pasarela de sucesos y pasa estos sucesos al proceso de Dominio virtual, que decide si iniciar o no la migración tras error según el suceso.
PostNcimProcessing	Desencadena la agrupación de varios dominios en un único dominio de agregación cuando se recibe un suceso de actualización de topología. Para ello, ejecuta los agrupadores que sean necesarios una vez actualizada la base de datos NCIM.
Análisis de causa principal (RCA)	En función de los datos del suceso y de la topología descubierta, las reglas codificadas en los agrupadores de RCA intentan identificar sucesos que están causados por otros sucesos o que causan ellos.
Enlace agregado SAE	Genera un suceso afectado por servicios (SAE) si alguno de los puertos que participan en un enlace agregado tiene una alerta de gravedad 5 o superior. Estos puertos son del tipo de entidad de colección 170, `aggregatedLink`.
Vía de acceso de IP SAE	Genera un servicio afectado por sucesos para vías de acceso de IP.
Servicio de ITNM SAE	Servicio genérico de Network Manager: se puede configurar para generar sucesos sintéticos cuando se produce un suceso en un dispositivo asociado con un servicio personalizado.
VPN de MPLS SAE	Genera sucesos afectados por servicios para VPN de MPLS.
zNetView	Rellena campos adicionales personalizados de alerts.status que utiliza IBM Tivoli NetView para z/OS. **Nota:** En primer lugar, debe añadir los siguientes campos personalizados a la tabla alerts.status: • NmosClassName • NmosEntityType

Los temas individuales en cada plugin describen la operación de cada plugin con más detalle. Para comprobar qué correlaciones de sucesos están registradas con cada plugin, ejecute el siguiente mandato:

```
$NCHOME/precision/scripts/perl/scripts/ncp_gwplugins.pl
-domain DOMAIN -plugin Plugin name
```

Conceptos relacionados

Conector de Análisis de causa raíz (RCA)

El conector de análisis de causa raíz (RCA) recibe un conjunto de sucesos enriquecidos de la Pasarela de sucesos y determina qué sucesos son causa raíz y qué sucesos son síntomas. RCA sólo recibe los sucesos que afectan el direccionamiento del tráfico a través de la red.

Plug-in de sondeo adaptativo

Utilice esta información para comprender los requisitos previos del conector, la forma en que el conector de sondeo adaptativo rellena campos en la tabla activeEvent, así como los detalles de configuración asociados con el conector. La tabla activeEvent se encuentra en el esquema NCMONITOR.

El conector de sondeo adaptativo elimina filas de la tabla activeEvent cuando se elimina o borra un suceso del ObjectServer.

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- Acknowledged
- AlertGroup
- EventId
- FirstOccurrence
- LastOccurrence
- LocalPriObj
- NmosCauseType
- NmosSerial
- NmosEntityId
- Serial
- Gravedad
- SuppressEscl
- Cuadrar

Suscripciones de correlaciones de sucesos

El conector de sondeo adaptativo se suscribe a las siguientes correlaciones de sucesos:

1. ChassisFailure
2. EMSNonPollingEvent
3. EMSPollingEvent
4. EntityFailure
5. EntityIfDescr
6. EntityMibTrap
7. genericip-event
8. ItnmLinkDownIfIndex
9. ItnmMonitorEventNoRca
10. LinkDownIfDescr
11. LinkDownIfIndex
12. LinkDownIfName
13. NbrFail
14. NbrFailIfDescr
15. OSPFIfState
16. OSPFIfStateChange
17. OSPFIfStateChangeIP
18. PollFailure

19. PrecisionMonitorEvent
20. Reconfiguración

El conector de sondeo adaptativo se suscribe a los siguientes estados de suceso:

1. Borrado
2. Suprimido
3. Sucedido
4. Reactivado
5. Sucedido de nuevo
6. Resincronizado
7. Actualizado

Sucesos de la tabla activeEvent

La tabla activeEvent incluye solo sucesos de problemas activos que han coincidido con una entidad de la topología y que cumplen las siguientes condiciones:

- El suceso está activo. Esto significa que el suceso no se ha borrado y se expresa en términos de campo por la relación `Severity > 0`.
- El suceso es un suceso de problema. El tipo de campo alerts.status tiene el valor `Problem`, `More Severe` o `Less Severe`.
- El suceso ha coincidido con una entidad. La Pasarela de sucesos ha identificado el nodo principal. Esto se expresa en términos de campo por la relación `NmosObjInst > 0`.

Campos de la tabla activeEvent

La siguiente tabla muestra los campos de la tabla activeEvent que rellena el conector de sondeo adapativo. Para obtener un ejemplo de la creación de una vista de alerta, que utiliza estos campos consulte *Guía del usuario de IBM Tivoli Network Manager*.

Tabla 108. Campos de la tabla activeEvent rellenados por el conector de sondeo adaptativo

Plug-in	Descripción
Acknowledged	Indica si el suceso ha sido reconocido por el operador.
AlertGroup	Identifica el originador del suceso.
domainMgrId	Número entero exclusivo que identifica el dominio al que pertenece el dispositivo afectado.
entityId	El NmosEntityId del suceso. Este campo se denomina entityId en esta tabla por motivos de coherencia con otras tablas de base de datos de topología de NCIM y, por lo tanto, facilitan la funcionalidad de la GUI.
EventId	El nombre del tipo de suceso. En base a este campo, se pueden iniciar sondeos secundarios en función de determinados tipos de error.
FirstOccurrence	El tiempo en segundos (desde las 12 de la noche del 1 de enero de 1970) cuando se creó este suceso o se inició el sondeo.
LastOccurrence	La hora de la última actualización de este suceso.
LocalPriObj	El objeto principal referenciado por el suceso. Para uso en la identificación de instancias de objetos gestionados.
NmosCauseType	Almacena los resultados de los análisis de causa raíz y permite identificar los sucesos de causa raíz.
NmosSerial	Si el suceso se ha suprimido durante el análisis de causa raíz, este campo indica el valor del campo Serial del suceso de eliminación.

Tabla 108. Campos de la tabla activeEvent rellenados por el conector de sondeo adaptativo (continuación)	
Plug-in	**Descripción**
Serial	Identificador exclusivo del suceso, dentro del contexto de un único ObjectServer. Este campo se almacena en la tabla para permitir generar una clave para la tabla.
Gravedad	Gravedad del suceso. **Nota:** No se incluyen los sucesos de gravedad cero, dado que estos sucesos indican que la alerta se ha resuelto y, por lo tanto, no se requieren en vistas de alertas o políticas de sondeo que utilizan vistas de alertas como ámbito.
SuppressEscl	Se utiliza para suprimir o escalar la alerta. El nivel de supresión se selecciona manualmente mediante operadores de **Visor de sucesos**.
Cuadrar	Un recuento del número de apariciones del suceso. Esto permite filtrar sucesos esporádicos, como los errores de ping excepcionales.

Configuración del conector

Durante el inicio, o en el momento de resincronización de la Pasarela de sucesos (un SIGHUP, una migración tras error o un restablecimiento), este conector rellenará también las tablas alertColors y alertConversions en función de los valores de las tablas alerts.colors y alerts.conversions del servidor de objetos.

Los parámetros de configuración de plugin siguientes se pueden establecer opcionalmente mediante el script `ncp_gwplugins.pl`.

Tabla 109. Configuración opcional del conector de sondeo adaptativo			
Nombre del parámetro	**Valor**	**Finalidad**	**Predeterminado**
CopyAlertTablesAtStartup	Indica si deben rellenarse las tablas alertColors y alertConversions. Los valores posibles son: • Verdadero • Falso	Esto permite que un solo dominio pueda rellenar estas tablas si se producen problemas cuando se ejecutan varios dominios.	Verdadero
ActiveEventUpdateInterval	Intervalo, en segundos, de actualización de la tabla activeEvent.	Se realizan actualizaciones de la tabla en las transacciones para intentar minimizar la carga en el servidor de base de datos. Este intervalo identifica el período en el que se confirman estas transacciones.	5

Tareas relacionadas

Establecimiento de los parámetros de configuración de plug-in
Puede establecer parámetros de configuración opcionales para los plug-ins de la pasarela de sucesos utilizando el script `ncp_gwplugins.pl` .

Gestión del sondeo adaptativo
Los sondeos adaptativos reaccionan de forma dinámica a los sucesos en la red. Puede crear sondeos adaptativos que gestionen una amplia gama de situaciones de problemas de red.

Información relacionada

Documentación de Tivoli Netcool/OMNIbusEn IBM Knowledge Center para Tivoli Netcool/OMNIbus, Consulte el tema *'Especificación del puerto IDUC '*. De forma predeterminada, cuando se inicia un ObjectServer, se elige un número de puerto disponible para la conexión IDUC. También puede especificar el puerto IDUC a utilizar. Debe especificar el puerto IDUC al acceder a un ObjectServer protegido por un firewall.

Plugin de comprobación de compatibilidad

El plugin de comprobación de compatibilidad añade automáticamente campos y valores necesarios para Network Manager a las bases de datos relevantes en Tivoli Netcool/OMNIbus.

El plugin intenta realizar los cambios necesarios en la base de datos. Si no se pueden hacer los cambios, el plugin genera un suceso de tipo ItnmConfiguration que explica el cambio que se ha intentado.

Campos requeridos

Este plugin no tiene los campos obligatorios. El plugin se ejecuta cuando Network Manager se conecta a un Tivoli Netcool/OMNIbus ObjectServer.

Suscripciones de correlaciones de sucesos

El plugin de comprobación de compatibilidad no se suscribe a ninguna correlación de sucesos.

Configuración del conector

No necesita configurar el plugin para el funcionamiento normal. Todos los parámetros necesarios se configuran de forma predeterminada.

Tabla 110. Configuración obligatoria del plugin de comprobación de compatibilidad

Nombre del parámetro	Descripción	Valor predeterminado	Finalidad
StartupStitcher	Nombre del agrupador del directorio StitcherSubDir para que se ejecute cuando se inicie el plugin.	StartupCheck	Si se proporciona un nombre de agrupador de inicio, este agrupador se ejecutará sin argumentos durante el inicio, tras SIGHUP o tras una migración tras error o restablecimiento.
StitcherSubDir	Nombre del subdirectorio dentro del directorio `$NCHOME/precision/eventGateway/stitchers/` que contiene los agrupadores de este conector.	CompatibilityCheck	La especificación del nombre de este directorio solo permite a este plugin analizar sus agrupadores.

Los parámetros de configuración de plugin siguientes se pueden establecer opcionalmente mediante el script `ncp_gwplugins.pl`.

Tabla 111. Configuración opcional del plugin de comprobación de compatibilidad			
Nombre del parámetro	**Valor**	**Finalidad**	**Predeterminado**
SchemaFile	Nombre de un archivo de esquema en `$NCHOME/etc/precision/` para analizar durante la inicialización.	Si se proporciona un nombre de esquema, este archivo se analizará durante el inicio, tras SIGHUP o tras una migración tras error o un restablecimiento, antes de que se ejecute el agrupador de inicio.	Ninguno

conector de Disco

Utilice esta información para comprender cierta información básica de cómo funciona este conector, sus requisitos previos y detalles de configuración asociados con el conector.

Funcionamiento del conector

El conector Disco se suscribe a la correlación de sucesos de reconfiguración. De forma predeterminada, la correlación de sucesos de reconfiguración solo maneja los sucesos con el ID de suceso NmosSnmpReboot. Estos sucesos se basan en la política de sondeo rebootDetection e indican que se ha rearrancado un dispositivo. Para configurar el conector Disco para gestionar otros sucesos, configure el suceso relacionado para que lo maneje la correlación de sucesos de reconfiguración.

Importante: La política de sondeo rebootDetection no está habilitada de forma predeterminada. Debe habilitar esta política de sondeo para poder generar los sondeos basándose en un arranque de dispositivo.

El diagrama siguiente proporciona un breve resumen del funcionamiento del conector Disco.

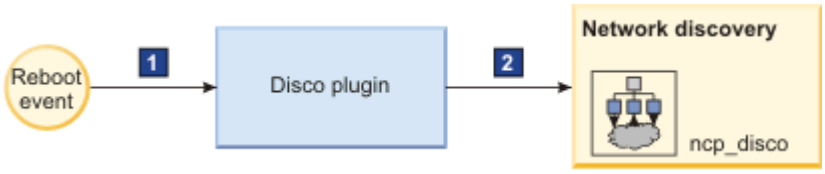


Figura 19. Operación del conector de Disco

1 Se recibe el suceso de rearranque
Se pasa un suceso de rearranque desde la Pasarela de sucesos al conector Disco

2 Se activa un redescubrimiento parcial
El plugin Disco activa un redescubrimiento parcial del dispositivo que se ha reiniciado.

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- NmosObjInst

Suscripciones de correlaciones de sucesos

El conector Disco se suscribe a la correlación de sucesos de reconfiguración.

Configuración del conector

Los parámetros de configuración de plugin siguientes se pueden establecer opcionalmente mediante el script `ncp_gwplugins.pl`.

Tabla 112. Configuración opcional del conector Disco

Nombre del parámetro	Valor	Finalidad	Predeterminado
SchemaFile	Nombre de un archivo de esquema en `$NCHOME/etc/precision/` para analizar durante la inicialización.	Si se proporciona un nombre de esquema, este archivo se analizará durante el inicio, tras SIGHUP o tras una migración tras error o un restablecimiento, antes de que se ejecute el agrupador de inicio.	
StartupStitcher	Nombre de un agrupador en el subdirectorio dentro de `$NCHOME/precision/eventGateway/stitchers/`, para ejecutar durante la inicialización.	Si se proporciona un nombre de agrupador de inicio, este agrupador se ejecutará sin argumentos durante el inicio, tras SIGHUP o tras una migración tras error o restablecimiento.	Ninguno
StitcherSubDir	Nombre del subdirectorio dentro del directorio `$NCHOME/precision/eventGateway/stitchers/` que contiene los agrupadores de este conector.	La especificación del nombre de este directorio solo permite al conector Disco analizar estos agrupadores.	`Disco`

Tareas relacionadas

Establecimiento de los parámetros de configuración de plug-in
Puede establecer parámetros de configuración opcionales para los plug-ins de la pasarela de sucesos utilizando el script `ncp_gwplugins.pl` .

Habilitación e inhabilitación de sondeos
Para activar el sondeo de Network Manager, deberá habilitar las políticas de sondeo.

Configuración del conector Disco
De forma predeterminada, el plugin Disco activa el redescubrimiento de dispositivos asociados con los sucesos de rearranque desde el ObjectServer de Tivoli Netcool/OMNIbus. Puede configurar el conector Disco para desencadenar el descubrimiento basándose en la recepción de un suceso.

Información relacionada

Documentación de Tivoli Netcool/OMNIbusEn IBM Knowledge Center para Tivoli Netcool/OMNIbus, Consulte el tema *'Especificación del puerto IDUC '*. De forma predeterminada, cuando se inicia un ObjectServer, se elige un número de puerto disponible para la conexión IDUC. También puede especificar el puerto IDUC a utilizar. Debe especificar el puerto IDUC al acceder a un ObjectServer protegido por un firewall.

Conector de migración tras error

Utilice esta información para comprender el funcionamiento del conector así como los detalles de configuración asociados con el conector.

Funcionamiento del conector

No hay ninguna información de configuración asociada con este conector.El diagrama siguiente proporciona un breve resumen del funcionamiento del Conector de migración tras error.

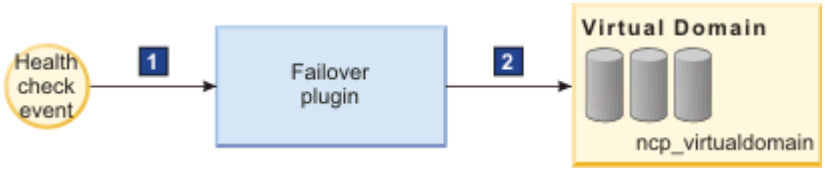


Figura 20. Operación del conector de migración tras error

1 Network Manager se recibió el suceso de la comprobación de estado
Se pasa un suceso de comprobación de estado de Network Manager desde la Pasarela de sucesos hasta el Conector de migración tras error

2 Se genera la solicitud de migración tras error
El conector de migración tras error convierte el suceso de comprobación de estado de Network Manager en una sentencia de OQL adecuada para el Dominio virtual, ncp_virtualdomain, la tabla state.domains.

3 Solicitud de migración tras error enviada al Dominio virtual, ncp_virtualdomain
La sentencia OQL se ejecutará y ello inicia la migración tras error o la conmutación por recuperación.

Campos requeridos

Este conector espera que los sucesos facilitados por la Pasarela de sucesos tenga el campo Nodo relleno con el nombre del dominio de Network Manager afectado.

Suscripciones de correlaciones de sucesos

Este conector se suscribe a la correlación de sucesos de ItnmHealthChk.

El conector de migración tras error se suscribe a los siguientes estados de suceso:

1. Borrado
2. Sucedido
3. Reactivado
4. Borrado nuevamente
5. Sucedido de nuevo
6. Resolución
7. Resincronizado

Este conector se suscribe a los siguientes estados de suceso:

1. Información
2. Sucedido

Tareas relacionadas

Establecimiento de los parámetros de configuración de plug-in
Puede establecer parámetros de configuración opcionales para los plug-ins de la pasarela de sucesos utilizando el script `ncp_gwplugins.pl` .

Información relacionada

Documentación de Tivoli Netcool/OMNIbusEn IBM Knowledge Center para Tivoli Netcool/OMNIbus, Consulte el tema *'Especificación del puerto IDUC '*. De forma predeterminada, cuando se inicia un ObjectServer, se elige un número de puerto disponible para la conexión IDUC. También puede especificar el puerto IDUC a utilizar. Debe especificar el puerto IDUC al acceder a un ObjectServer protegido por un firewall.

Conector PostNCIMProcessing

El conector PostNCIMProcessing ejecuta los agrupadores que sean necesarios una vez actualizada la base de datos NCIM. De forma predeterminada, el conector desencadena la agrupación de varios dominios en un único dominio de agregación cuando se recibe un suceso de actualización de topología.

Funcionamiento del conector

El conector PostNCIMProcessing se suscribe a la correlación de sucesos de ItnmStatus. El flujo de proceso del conector se describe en los pasos siguientes:

1. La pasarela de sucesos recibe un suceso ItnmStatus.
2. La pasarela de sucesos invoca el conector PostNCIMProcessing.
3. El conector PostNCIMProcessing ejecuta el agrupador PostNcimProcessing, que comprueba el tipo de suceso.
4. Si el suceso es del tipo ItnmTopologyUpdate, y si la agrupación de dominios cruzados está habilitada, el agrupador PostNCIMProcessing ejecuta el agrupador AggregationDomain.
5. El agrupador AggregationDomain comprueba que no haya un descubrimiento en curso y, a continuación, ejecuta los otros agrupadores de dominio de agregación, que agrupan los dominios descubiertos en un único dominio de agregación.

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- NmosObjInst

Suscripciones de correlaciones de sucesos

El conector PostNcimProcessing se suscribe a la correlación de sucesos de ItnmStatus.

El conector PostNcimProcessing se suscribe a los siguientes estados de suceso:

1. Información
2. Sucedido

Configuración del conector

El parámetro siguiente se establece de forma predeterminada y debe estar presente en la tabla ncmonitor.gwPluginConf.

Tabla 113. Configuración opcional del conector PostNCIMProcessing

Nombre del parámetro	Valor	Finalidad	Predeterminado
StitcherSubDir	Nombre del subdirectorio dentro del directorio `$NCHOME/precision/eventGateway/stitchers/` que contiene los agrupadores de este conector.	La especificación del nombre de este directorio solo permite al conector PostNCIMProcessing analizar sus agrupadores.	`PostNcimProcessing`

Los parámetros de configuración de plugin siguientes se pueden establecer opcionalmente mediante el script `ncp_gwplugins.pl`.

Tabla 114. Configuración opcional del conector PostNCIMProcessing			
Nombre del parámetro	**Valor**	**Finalidad**	**Predeterminado**
StartupStitcher	Nombre de un agrupador en el subdirectorio dentro de `$NCHOME/precision/eventGateway/stitchers/`, para ejecutar durante la inicialización.	Si se proporciona un nombre de agrupador de inicio, este agrupador se ejecutará sin argumentos durante el inicio, tras SIGHUP o tras una migración tras error o restablecimiento.	Ninguno
SchemaFile	Nombre de un archivo de esquema en `$NCHOME/etc/precision/` para analizar durante la inicialización.	Si se proporciona un nombre de esquema, este archivo se analizará durante el inicio, tras SIGHUP o tras una migración tras error o un restablecimiento, antes de que se ejecute el agrupador de inicio.	Ninguno

Tareas relacionadas

Establecimiento de los parámetros de configuración de plug-in

Puede establecer parámetros de configuración opcionales para los plug-ins de la pasarela de sucesos utilizando el script `ncp_gwplugins.pl` .

Conector de Enlace agregado SAE

El plug-in de Enlace agregado SAE genera sucesos afectados por servicios para grupos de agregación de enlaces (LAGs).

Este plug-in genera un suceso afectado por servicio (SAE) si alguno de los puertos que participan en un LAG tiene una alerta de gravedad 5 o tiene una alerta que es una alerta de síntoma o de causa raíz (indicado por un NmosCauseType mayor de 0). Las entidades de enlace agregado son del tipo de entidad Colección 170, aggregatedLink.

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- NmosEntityId
- Gravedad
- NmosCauseType
- NmosDomainName

Conector de Vía de acceso de IP SAE

El conector de vía de acceso de IP SAE genera sucesos afectados por servicios para dispositivos en Vías de acceso de IP.

Un suceso sintético se genera cuando se produce un suceso en un dispositivo en cualquiera de las rutas IP creadas utilizando la GUI de rutas de red. El SAE generado se asocia con el ID de entidad que se corresponde a la ruta IP que contiene el dispositivo en el que se produjo el suceso.

Nota: Como con todos los plug-ins SAE, este plug-in genera un Suceso afectado por el servicio (SAE) solo si las alertas subyacentes tienen una gravedad de 5 o son las alertas de síntoma o causa raíz (indicado por un NmosCauseType mayor de 0).

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- NmosEntityId
- Gravedad
- NmosCauseType
- NmosDomainName

Suscripciones de correlaciones de sucesos

Este conector se suscribe al siguiente estado de suceso: Resincronizado

Conector de Servicio de ITNM SAE

El conector de Servicio de ITNM SAE le permite ampliar la funcionalidad de SAE creando sucesos para el servicio.

Configuración de un servicio personalizado

El conector de Servicio de ITNM SAE se puede configurar para generar sucesos sintéticos generados cuando se produce un suceso en un dispositivo asociado con un servicio personalizado. Para ejecutar esta configuración, debe realizar las siguientes tareas:

1. Configure el motor de descubrimiento, `ncp_disco`, para recopilar datos del servicio personalizado. Ejecute esta configuración escribiendo un agrupador personalizado que defina en el servicio personalizado y asegúrese de que el agrupador de Network Manager estándar correspondiente invoque este agrupador.

   Nota: Para obtener ayuda sobre cómo escribir agrupadores personalizados, póngase en contacto con el soporte de IBM.
2. Actualice la memoria caché de NCIM para almacenar datos en el servicio personalizado en la tabla de base de datos NCIM `itnmService`.
3. Actualice la tabla de base de datos del conector SAE `config.serviceTypes` para almacenar datos en el nuevo servicio personalizado.

Para obtener más información sobre `ncp_disco` y la tabla de base de datos NCIM `itnmService`, consulte la publicación *IBM Tivoli Network Manager IP Edition Administration Guide*.

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- NmosEntityId
- Gravedad
- NmosCauseType
- NmosDomainName

Suscripciones de correlaciones de sucesos

Este conector se suscribe al siguiente estado de suceso: Resincronizado.

Conector VPN de MPLS SAE

El conector VPN de MPLS SAE crea sucesos afectados por servicios para las VPN de MPLS.

Suceso sintético que se genera cuando se produce un suceso de error de Gravedad 5 (crítico), un suceso de error de causa raíz o un suceso de error de síntoma en el direccionador de proveedor (PE) o de cliente

(CE) o en cualquiera de las interfaces PE que señalan a un direccionador CE en cualquiera de las VPN MPLS descubiertas. El SAE generado se asocia con el ID de la entidad lógica del descubrimiento que representa la recopilación de dispositivos de VPN MPLS en los que se han producido los sucesos de error.

Todas las interfaces PE a CE se agregan a una lista de miembros y un suceso en cualquiera de las interfaces de esta lista de miembros hace que el sistema genere un SAE de VPN de MPLS sintético.

Puede habilitar la generación de sucesos SAE en función de las dependencias de interfaces más profundas de la red principal si habilita el agente de descubrimiento BGPPeerNextHopInterface como parte del descubrimiento de red. Este agente llama al agrupador AddLayer3VPNInterfaceDependency.stch.

Para obtener más información sobre el agente de descubrimiento BGPPeerNextHopInterface y el agrupador AddLayer3VPNInterfaceDependency.stch, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*

Este agrupador determina a todas las interfaces de las PE hasta las de direccionador de proveedor principal (P) y las interfaces P hasta las PE implicadas en una VPN. Estas interfaces PE -> P y P ->PE se agregan a una lista de dependencia. Un suceso de cualquiera de las interfaces de esta lista de dependencia hace que el sistema genere un SAE de VPN de MPLS sintético. Si ya se ha generado un SAE de VPN de MPLS según un suceso en cualquiera de las interfaces de la lista de miembros, cualquier suceso de las interfaces de la lista de dependencia se agregará como suceso relacionado con el SAE de VPN de MPLS ya generado.

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- NmosEntityId
- Gravedad
- NmosCauseType
- NmosDomainName

Suscripciones de correlaciones de sucesos

El conector MPLS VPN SAE se suscribe al siguiente estado de suceso: Resincronizado.

Conector zNetView

Utilice esta información para conocer los requisitos previos del conector, así como los detalles de configuración asociados con el conector.

Campos requeridos

Este conector espera sucesos proporcionados por la Pasarela de sucesos para rellenarlos con los siguientes campos:

- Acknowledged

El conector exigen que existan los siguientes campos personalizados en la tabla alerts.status.

Tabla 115. Configuración opcional del conector de sondeo adaptativo

Nombre del campo	Tipo	Descripción
NmosClassName	cadena de 64 caracteres	Clase del dispositivo en relación con la cual se generó el suceso. Este valor se recupera de la tabla de chasis de la base de datos de topología de NCIM.
NmosEntityType	Entero de 32 bits	Tipo de entidad en relación con el cual se generó el suceso. Este valor se especifica en el campo NmosEntityId.

Suscripciones de correlaciones de sucesos

El conector zNetView se suscribe a las siguientes correlaciones de sucesos:

1. ChassisFailure
2. EntityIfDescr
3. EntityFailure
4. EntityMibTrap
5. genericip-event
6. ItnmLinkDownIfIndex
7. ItnmMonitorEventNoRca
8. LinkDownIfIndex
9. LinkDownIfDescr
10. LinkDownIfName
11. NbrFailIfDescr
12. NbrFail
13. OspfIfState
14. OSPFIfStateChange
15. OSPFIfStateChangeIP
16. PollFailure
17. PrecisionMonitorEvent
18. Reconfiguración

El conector zNetView se suscribe a los siguientes estados de suceso:

1. Información
2. Sucedido
3. Reactivado
4. Sucedido de nuevo
5. Resolución
6. Resincronizado
7. Actualizado

Configuración del conector

Los parámetros de configuración de plugin siguientes se pueden establecer opcionalmente mediante el script `ncp_gwplugins.pl`.

Tabla 116. Configuración opcional del conector de sondeo adaptativo

Nombre del parámetro	Valor	Finalidad	Predeterminado
SchemaFile	Nombre de un archivo de esquema en `$NCHOME/etc/precision/` para analizar durante la inicialización.	Si se proporciona un nombre de esquema, este archivo se analizará durante el inicio, tras SIGHUP o tras una migración tras error o un restablecimiento, antes de que se ejecute el agrupador de inicio.	Ninguno

Tabla 116. Configuración opcional del conector de sondeo adaptativo (continuación)			
Nombre del parámetro	**Valor**	**Finalidad**	**Predeterminado**
StartupStitcher	Nombre de un agrupador en el subdirectorio dentro de `$NCHOME/precision/eventGateway/stitchers/`, para ejecutar durante la inicialización.	Si se proporciona un nombre de agrupador de inicio, este agrupador se ejecutará sin argumentos durante el inicio, tras SIGHUP o tras una migración tras error o restablecimiento.	CheckAdditionalFields
StitcherSubDir	Nombre del subdirectorio dentro del directorio `$NCHOME/precision/eventGateway/stitchers/` que contiene los agrupadores de este conector.	La especificación del nombre de este directorio solo permite al conector zNetView analizar estos agrupadores.	`zNetView`

Tareas relacionadas

Establecimiento de los parámetros de configuración de plug-in
Puede establecer parámetros de configuración opcionales para los plug-ins de la pasarela de sucesos utilizando el script `ncp_gwplugins.pl` .

Información relacionada

Documentación de Tivoli Netcool/OMNIbusEn IBM Knowledge Center para Tivoli Netcool/OMNIbus, Consulte el tema *'Especificación del puerto IDUC '*. De forma predeterminada, cuando se inicia un ObjectServer, se elige un número de puerto disponible para la conexión IDUC. También puede especificar el puerto IDUC a utilizar. Debe especificar el puerto IDUC al acceder a un ObjectServer protegido por un firewall.

Capítulo 29. Configuración del enriquecimiento de sucesos

Puede configurar la forma en la que se procesa un suceso cuando pasa a través de la Pasarela de sucesos.

Configuración de enriquecimiento de suceso extra

Puede configurar la pasarela de sucesos para llevar a cabo un enriquecimiento de suceso extra. Los ejemplos siguientes ilustran los tipos de información que se pueden añadir a un suceso utilizando el enriquecimiento de suceso.

Acerca de esta tarea

Puede configurar la pasarela de sucesos para llenar cualquier campo de la tabla alerts.status de ObjectServer. Puede llenar un campo existente o un campo personalizado.

Nota: La pasarela de sucesos no altera la tabla alerts.status. Si quiere crear un campo nuevo en la tabla alerts.status y hacer que la pasarela de sucesos llene este nuevo campo, primero debe alterar la tabla alerts.status de ObjectServer para añadir el campo nuevo.

Modificaciones de la tabla alerts.status de ObjectServer

La Pasarela de sucesos no crea nuevos campos en la tabla alerts.status. Si va a configurar un enriquecimiento de sucesos adicional, es posible que necesite configurar el ObjectServer para añadir nuevos campos a la tabla alerts.status.

En los siguientes ejemplos se describe un enriquecimiento de sucesos personalizado típico. Cada ejemplo especifica si se requiere configurar alguna tabla alerts.status antes de configurar el enriquecimiento de suceso personalizado.

Enriquecimiento de un campo de sucesos predeterminado que no está enriquecido actualmente
Un ejemplo de esto sería un caso en el que deseara enriquecer el campo PhysicalPort alerts.status. Este es un campo que existe de forma predeterminada en la tabla alerts.status y, por lo tanto, no hay necesidad de modificar el ObjectServer.

Enriquecimiento de un campo personalizado que se ha añadido con anterioridad con otro fin
Un ejemplo sería un caso en el que ya disponga de un campo relleno por uno o varios analizadores y desea rellenarlo para todos los sucesos. En este ejemplo, algunos sucesos que llegan a través del analizador de supervisión, desde el sondeador, pueden tener relleno el campo EXTRAINFO_sysLocation en los datos de caché de NCIM. Ha añadido un campo NmosLocation al ObjectServer y este campo se rellena desde el analizador de supervisión en todos los casos posibles. Ahora se puede rellenar para todos los sucesos. En este caso, no es necesario modificar el ObjectServer.

Ejecución de un enriquecimiento de topología desde la base de datos de topología de NCIM
En este caso, es posible que desee enriquecer el suceso con los datos procedentes de NCIM. En primer lugar, debe modificar el ObjectServer para agregar el nuevo campo o campos a la tabla alerts.status.

Ejemplo: Enriquecimiento de un suceso con la ubicación del dispositivo de nodo principal

Puede configurar el enriquecimiento de suceso para que la ubicación del dispositivo de nodo principal asociado con el suceso se añada a un campo del suceso.

Antes de empezar

Tenga en cuenta qué campo llenar en ObjectServer. Ya existen un campo de ubicación predeterminado en la tabla alerts.status. Este ejemplo presupone que quiere llenar este campo, a menos que ya esté lleno. Si tiene una razón para crear un campo independiente personalizado para almacenar el valor de ubicación enriquecido, puede añadir un campo a la tabla alerts.status para almacenar la ubicación de dispositivo de nodo principal; por ejemplo, NmosLocation. Para obtener información sobre cómo añadir un campo personalizado a una tabla de ObjectServer, consulte *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Acerca de esta tarea

La ubicación del dispositivo de nodo principal asociado con un suceso está disponible en la tabla de chasis de la base de datos de topología de NCIM. Se puede acceder a este campo utilizando la memoria caché de NCIM, contenida en la tabla ncimCache.entityData.

Para obtener más información sobre la estructura de los campos y tablas de memoria caché de NCIM, consulte *Referencia de IBM Tivoli Network Manager*.

Los pasos siguientes explican cómo configurar este enriquecimiento de suceso extra.

Procedimiento

1. Edite el archivo de esquema de la pasarela de sucesos, `$NCHOME/etc/precision/EventGatewaySchema.cfg`, para permitir que la pasarela de sucesos actualice el nuevo campo. Para ello, añada el texto en negrita al filtro de sucesos de salida. Recuerde añadir una coma al final de la línea que contiene el campo `NmosSerial`, antes de la línea que contiene el nuevo campo `Location`.

```
insert into config.ncp2nco
(
    FieldFilter
)
values
(
    [
        "NmosCauseType",
        "NmosDomainName",
        "NmosEntityId",
        "NmosManagedStatus",
        "NmosObjInst",
        "NmosSerial",
        "Location"
    ]
);
```

   Nota: Los campos que se añaden al filtro de sucesos de salida se añaden automáticamente al filtro de campos de entrada, config.nco2ncp, asegurando que se recupera el valor actual del campo. Esto permite al agrupador StandardEventEnrichment en el siguiente paso comprobar el valor del campo InterfaceName antes de actualizarlo. Esta técnica garantiza que la pasarela de sucesos no sigue actualizando el mismo valor.

2. Edite los agrupadores de la pasarela de sucesos para recuperar la información de ubicación de la base de datos de topología y llenar el campo de ubicación.

   Una manera de hacer esto es añadir el código siguiente al agrupador StandardEventEnrichment. Añadir este código garantiza que se realiza este procedimiento para todos los sucesos de topología que coinciden con una entidad. Añada este código al agrupador inmediatamente antes de la línea final, la llamada a `GwEnrichEvent( enrichedFields )`. Para obtener más información sobre la regla del agrupador `GwEnrichEvent()`, consulte *Referencia de IBM Tivoli Network Manager*.

Tabla 117. Líneas de código relevante para el ejemplo de ubicación del dispositivo de nodo principal	
Números de línea	**Descripción**
1	Llame a la regla `GwMainNodeLookupUsing()` para asegurarse de que los datos del chasis están disponibles para el suceso actual. Es posible que el suceso haya surgido en una interfaz, en cuyo caso los datos del chasis normalmente no estarían disponibles en este punto. Para obtener más información sobre la regla del agrupador `GwMainNodeLookupUsing()`, consulte*Referencia de IBM Tivoli Network Manager*.
5	Recupera los datos de sysLocation de la tabla del chasis. **Nota:** Cada vez que recupere datos de la caché NCIM, es necesario especificar el campo de los datos de entidad en mayúsculas; por ejemplo, `@mainNode.chassis.SYSLOCATION`.
7 - 9	Si el campo de ubicación ya no está configurado, añada los datos de sysLocation a los otros datos que se van a enriquecer.

```
Record mainNode = GwMainNodeLookupUsing( "LocalNodeAlias" );

if ( mainNode <> NULL )
{
      text sysLocation = @mainNode.snmpSystem.SYSLOCATION;

      if ( sysLocation <> eval(text, '&Location') )
      {
           @enrichedFields.Location = sysLocation;
      }
}
```

Conceptos relacionados

Filtro de campos salientes
El filtro de campos salientes define el conjunto de campos de ObjectServer que puede actualizar la Pasarela de sucesos.

Referencia relacionada

Ejemplo: StandardEventEnrichment.stch
Utilice este tema para comprender el funcionamiento de los agrupadores de enriquecimiento de sucesos.

Ejemplo: Enriquecimiento de un suceso con un nombre de interfaz

Puede configurar el enriquecimiento de sucesos para que todos los sucesos de interfaz, el nombre de la interfaz en la que se produce el suceso se añadan a un campo del suceso.

Antes de empezar

Debe crear un nuevo campo personalizado en la tabla alerts.status de ObjectServer para almacenar el valor de nombre de interfaz enriquecido. En este ejemplo, se presupone que se ha creado un nuevo campo personalizado llamado InterfaceName en la tabla alerts.status. Para obtener información sobre cómo añadir un campo personalizado a una tabla de ObjectServer, consulte *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Acerca de esta tarea

El nombre de la interfaz está disponible en la tabla de interfaz de la base de datos de topología de NCIM. Se puede acceder a este campo utilizando la memoria caché de NCIM, contenida en la tabla ncimCache.entityData.

Para obtener más información sobre la estructura de los campos y tablas de memoria caché de NCIM, consulte *Referencia de IBM Tivoli Network Manager*.

Los pasos siguientes explican cómo configurar este enriquecimiento de suceso extra.

Procedimiento

1. Edite el archivo de esquema de la pasarela de sucesos, `$NCHOME/etc/precision/EventGatewaySchema.cfg`, para permitir que la pasarela de sucesos actualice el nuevo campo. Para ello, añada el texto en negrita al filtro de sucesos de salida. Recuerde añadir una coma al final de la línea que contiene el campo `NmosSerial`, antes de la línea que contiene el nuevo campo `InterfaceName`.

```
insert into config.ncp2nco
(
    FieldFilter
)
values
(
    [
        "NmosCauseType",
        "NmosDomainName",
        "NmosEntityId",
        "NmosManagedStatus",
        "NmosObjInst",
        "NmosSerial",
        "InterfaceName"
    ]
);
```

   Nota: Los campos que se añaden al filtro de sucesos de salida se añaden automáticamente al filtro de campos de entrada, config.nco2ncp, asegurando que se recupera el valor actual del campo. Esto permite al agrupador StandardEventEnrichment en el siguiente paso comprobar el valor del campo InterfaceName antes de actualizarlo. Esta técnica garantiza que la pasarela de sucesos no sigue actualizando el mismo valor.

2. Edite los agrupadores de la pasarela de sucesos para recuperar la información de nombre de interfaz de la base de datos de topología y llenar el campo InterfaceName.

   Una manera de hacer esto es añadir el código siguiente al agrupador StandardEventEnrichment. Añadir este código garantiza que se realiza este procedimiento para todos los sucesos de topología que coinciden con una entidad. Añada este código al agrupador inmediatamente antes de la línea final, la llamada a `GwEnrichEvent( enrichedFields )` y después de determinar el valor entityType. Para obtener más información sobre la regla del agrupador `GwEnrichEvent()`, consulte *Referencia de IBM Tivoli Network Manager*.

Tabla 118. Líneas de código relevantes para el ejemplo de nombre de interfaz

Números de línea	Descripción
1	Este enriquecimiento de suceso sólo es relevante para los sucesos de interfaz. Compruebe que este suceso se relaciona con una interfaz garantizando que el valor entityType es 2, y si es así, continúe el proceso.
3	Recupera los datos ifName de la tabla de interfaz. **Nota:** Cada vez que recupere datos de la caché NCIM, es necesario especificar el campo de los datos de entidad en mayúsculas; por ejemplo, `@mainNode.chassis.SYSLOCATION`.
5 - 8	Únicamente llena el campo `InterfaceName` si el valor del nombre de interfaz no está presente en el suceso dentro del alcance.

```
if ( entityType == 2 )
{
    text interfaceName = @entity.networkInterface.IFNAME;

    if ( interfaceName <> eval(text, '&InterfaceName') )
    {
```

```
            @enrichedFields.InterfaceName = interfaceName;
    }
}
```

Conceptos relacionados

Filtro de campos salientes
El filtro de campos salientes define el conjunto de campos de ObjectServer que puede actualizar la Pasarela de sucesos.

Referencia relacionada

Ejemplo: StandardEventEnrichment.stch
Utilice este tema para comprender el funcionamiento de los agrupadores de enriquecimiento de sucesos.

Configuración del campo de intervalo de actualización de ObjectServer

Puede configurar el intervalo que utiliza la pasarela de sucesos para poner en cola las actualizaciones de enriquecimiento de sucesos para ObjectServer.

Acerca de esta tarea

El valor predeterminado para el intervalo de actualización de ObjectServer es de 5 segundos. Es posible que desee alterar este valor para que coincida con los datos que fluyen en el sistema.

- Aumente el valor para agrupar más actualizaciones de enriquecimiento de sucesos en una única actualización de ObjectServer. Esto desciende la carga de ObjectServer pero aumenta la demora de las actualizaciones del enriquecimiento de sucesos en ObjectServer
- Disminuya el valor para acelerar las actualizaciones de enriquecimiento de sucesos para ObjectServer. Esto aumenta la carga en ObjectServer, ya que tendrá que gestionar más actualizaciones de enriquecimiento de sucesos.

El archivo de configuración para la pasarela de sucesos es el archivo de configuración EventGatewaySchema.cfg. Este archivo está ubicado en: `$NCHOME/etc/precision/EventGatewaySchema.cfg`. El intervalo de actualización de ObjectServer está almacenado en la tabla config.defaults, en el campo ObjectServerUpdateInterval.

Procedimiento

1. Abra el archivo de configuración EventGatewaySchema.cfg.
2. Identifique la sentencia de inserción en la tabla config.defaults.
   De forma predeterminada, esta sentencia de inserción tiene la forma siguiente:

```
insert into config.defaults
(
    IDUCFlushTime,
    ObjectServerUpdateInterval,
    NcpServerEntity
)
values
(
    5,
    5,
    ""
);
```

   De forma predeterminada el campo ObjectServerUpdateInterval está establecido en 5 segundos.
3. Modifique el valor del campo ObjectServerUpdateInterval al valor deseado, en segundos.

Conceptos relacionados

Cola de pasarela de sucesos salientes
La cola de la pasarela de sucesos de salida recibe sucesos enriquecidos de los agrupadores de la pasarela de sucesos (enriquecimiento de sucesos principal) y de los plug-ins. Con el fin de minimizar el número de actualizaciones y, por lo tanto, minimizar la carga del ObjectServer, las actualizaciones de este se colocan

en una cola, se agregan y se envían al ObjectServer en un período de tiempo especificado. El valor predeterminado es de 5 segundos.

Capítulo 30. Uso del proveedor de servicios OQL para iniciar sesión en las bases de datos de la Pasarela de sucesos

Debe iniciar sesión en las bases de datos utilizando el proveedor de servicios OQL (lenguaje de consulta de objetos) y el nombre de servicio EventGateway para consultar las bases de datos de la pasarela.

El ejemplo de la línea de mandatos inferior inicia sesión en el servicio NcoGate para la Pasarela de sucesos, que se está ejecutando en el dominio NCOMS.

```
ncp_oql -domain NCOMS -service EventGateway
```

La autenticación de usuario para el proveedor de servicios OQL está desactivada de forma predeterminada. Si se ha activado la autenticación, escriba un nombre de usuario y una contraseña válidos cuando se le solicite.

Consulta de ObjectServer

Puede utilizar el proveedor de servicios OQL para consultar ObjectServer.

El ejemplo de línea de mandatos del proveedor de servicios OQL que aparece a continuación inicia sesión en el servicio ObjectServer, que se está ejecutando en el dominio NCOMS en un ObjectServer denominado NCOMS.

```
ncp_oql -domain NCOMS -service ObjectServer -server NCOMS -username root
```

La autenticación de usuario para el proveedor de servicios OQL está desactivada de forma predeterminada. Si se ha activado la autenticación, escriba un nombre de usuario y una contraseña válidos cuando se le solicite.

Nota: El argumento `-server` es opcional. Si no se especifica este argumento, se utiliza el servidor configurado en el archivo `$NCHOME/etc/precision/ConfigItnm.cfg`.

Consulta a la base de datos de NCIM

Puede utilizar el proveedor de servicios OQL para consultar la base de datos de NCIM.

El ejemplo de línea de mandatos del proveedor de servicios OQL que aparece a continuación inicia sesión en el esquema NCMONITOR dentro del servicio de NCIM, que se está ejecutando en el dominio NCOMS. Esto resulta útil si desea acceder a la tabla del esquema NCMONITOR; por ejemplo, la tabla activeEvent.

```
ncp_oql -domain NCOMS -service Ncim -dbId NCMONITOR
```

La autenticación de usuario para el proveedor de servicios OQL está desactivada de forma predeterminada. Si se ha activado la autenticación, escriba un nombre de usuario y una contraseña válidos cuando se le solicite.

Nota: El argumento `-dbId` es opcional.

Capítulo 31. Resincronización de sucesos con ObjectServer

Emita el mandato SIGHUP a la pasarela de sucesos para cambiar la configuración de la pasarela de sucesos.

Escriba este mandato: `kill -HUP` *`PID`*, donde *`PID`* es el ID de proceso de la pasarela de sucesos.

La pasarela de sucesos comprueba la indicación de fecha y hora en el archivo de configuración. Si el archivos de configuración se modifica, la pasarela de sucesos lee este archivo de nuevo para procesar cualquier cambio en la configuración.

Nota: Este mandato también vuelve a sincronizar todos los sucesos con la pasarela de sucesos.

Pasos de procesamiento para el mandato SIGHUP

El procesamiento del mandato SIGHUP se describe en los pasos siguientes:

1. La pasarela de sucesos recibe un mandato HUP.
2. La pasarela de sucesos deja de escuchar sucesos en el canal IDUC de ObjectServer.
3. La pasarela de sucesos vacía su memoria caché de sucesos actual. Esta memoria caché se utiliza para determinar el estado del suceso.
4. La pasarela de sucesos envía a todos los plug-ins un sucesos de inicio de resincronización sintético
5. El pluing RCA vuelve a leer el archivo de configuración RCASchema`.cfg` si el archivo se ha modificado desde la última vez que se leyó al inicio.
6. El plug-in RCA borra la tabla de base de datos mojo.events y vuelve a dibujar el gráfico basándose en los datos de la memoria caché de NCIM.

   Nota: El plugin RCA no relee los agrupadores RCA en este punto.
7. La pasarela de sucesos recupera todos los sucesos del servidor de objetos, de la misma forma que lo haría en el inicio.
8. La pasarela de sucesos procesa todos los sucesos de la misma forma que haría al inicio y pasa cualquier suceso relevante a los plug-in.
9. La pasarela de sucesos envía un suceso final de resincronización a sus plug-in.
10. La pasarela de sucesos reanuda la escucha para sucesos en el canal IDUC de ObjectServer.

Tareas relacionadas

Configuración del análisis de causa raíz
Puede configurar el plug-in RCA.

Capítulo 32. Configuración de propiedades comunes de Event Gateway (Pasarela de sucesos)

Puede configurar las propiedades comunes de Event Gateway editando el archivo `NCP_G_EVENT.props`.

Antes de empezar

Las pasarelas de Tivoli Netcool/OMNIbus tiene una serie de propiedades comunes y opciones de línea de mandatos asociadas. Las propiedades definen valores para las funciones genéricas, como el registro de mensajes, para comunicaciones entre procesos (IPC), y para valores comunes de pasarela, como el establecimiento del periodo de tiempo que el cliente espera para la respuesta del servidor.

La Event Gateway de Network Manager utiliza los valores predeterminados para las propiedades comunes de la pasarela de Tivoli Netcool/OMNIbus. Puede configurar las propiedades comunes de pasarela de Tivoli Netcool/OMNIbus en otros valores, editando el archivo de propiedades `NCP_G_EVENT.props`, que se instala en el directorio `$NCHOME/etc/precision`. Por ejemplo, para evitar que se cumplan los tiempos de espera, puede especificar un valor distinto al predeterminado (60 segundos) para la propiedad común `Ipc.Timeout`, y ajustarlo a un corte rápido en la conexión al ObjectServer primario, si no se detecta actividad.

Nota: El archivo `NCP_G_EVENT.props` puede ser específico del dominio.

Acerca de esta tarea

Para configurar las propiedades comunes, complete los pasos siguientes:

Procedimiento

1. Haga copia de seguridad del archivo de propiedades `NCP_G_EVENT.props` instalado en el directorio `$NCHOME/etc/precision`.
2. Abra el archivo de propiedades `NCP_G_EVENT.props` en un editor de texto.
3. Localice, elimine el comentario y actualice la propiedad que desea cambiar.

   Puede editar las siguientes propiedades:

   Ipc.Timeout
   La propiedad `Ipc.Timeout` especifica el periodo de tiempo (en segundos) que el cliente espera a que el servidor responda. Si se sobrepasa este tiempo, se registra un error. El valor predeterminado es `60` segundos.

   Fix Pack 4 **SSLCommonNames**
   Si se está conectando a un ObjectServer remoto que es parte de un par de migración tras error utilizando SSL, debe configurar los nombres de los ObjectServers primario y de copia de seguridad. Si no configura este valor correctamente, la Pasarela de sucesos no se conecta al par de migración tras error de ObjectServer.
4. Guarde el archivo de propiedades `NCP_G_EVENT.props`.

Ejemplo

El ejemplo siguiente configura un tiempo de espera de 20 segundo y especifica los nombres del los ObjectServer primario y de copia de seguridad.

```
# INTEGER (IPC Session timeout), default 60 seconds
Ipc.Timeout: 20
# STRING (Comma separated list of common names),
used only if connecting to remote object servers
with SSL and failover configuration.
SSLCommonNames: 'NCOMS_Primary,NCOMS_Backup'
```

Capítulo 33. Categorías de sucesos de Network Manager

Los sucesos que se generan mediante Network Manager están en dos categorías: sucesos acerca de la red que se supervisa y sucesos acerca de los procesos de Network Manager.

Estos sucesos se almacenan en el ObjectServer de Tivoli Netcool/OMNIbus. La Sonda para Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) se utiliza para procesar y reenviar los datos de los sucesos a la tabla alerts.status en ObjectServer.

La figura siguiente muestra el flujo de sucesos desde Network Manager al ObjectServer.

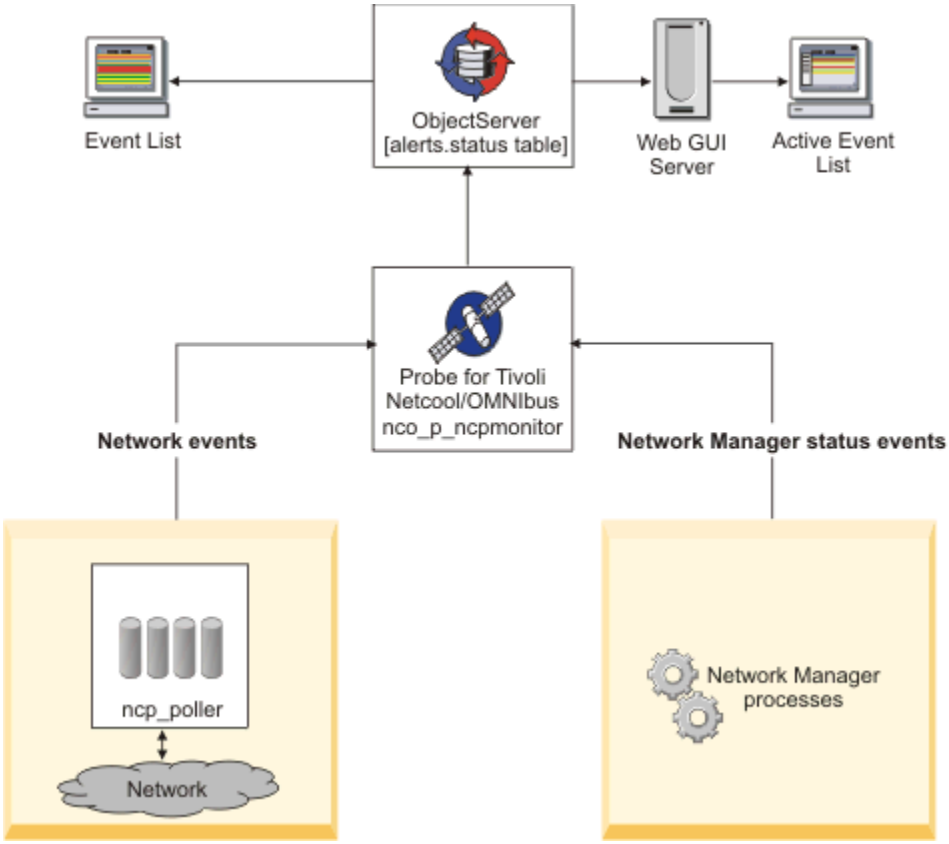


Figura 21. El flujo de sucesos desde Network Manager a Tivoli Netcool/OMNIbus

Referencia relacionada

Correlaciones de sucesos predeterminadas
Network Manager proporciona una configuración predeterminada de estas correlaciones de sucesos. Utilice esta información para conocer las correlaciones de sucesos disponibles y qué realiza cada una de ellas y para comprender cómo las correlaciones de sucesos delegadas se delegan en las correlaciones de sucesos actuales.

Sucesos de red de Network Manager

El Motor de sondeo, **ncp_poller**, genera sucesos acerca del estado de la red. Dichos sucesos se pueden utilizar para identificar problemas de red y son configurables utilizando la **GUI de sondeo de red** (vaya a **Administración** > **Red** > **Sondeo de red**). Estos sucesos se conocen como sucesos de red y tienen el valor de campo de AlertGroup de alerts.status de `ITNM Monitor`.

Cada suceso de red se genera en una entidad única, tal como una interfaz o un chasis, y los datos del suceso dependen del tipo de sondeo. Cuando los sucesos de red se reenvían al ObjectServer para su inserción en la tabla alerts.status, se les asigna un valor de AlertGroup de `ITNM Monitor`.

Está disponible un conjunto ilimitado de identificadores de sucesos para los sucesos de red. A los sucesos que se generen cuando falle un sondeo de SNMP se les asigna específicamente un valor de EventID de `NmosSnmpPollFail` en la tabla de alerts.status.

Los sucesos de red de ObjectServer se repliegan en Network Manager a través de la Pasarela de sucesos para realizar el enriquecimiento de sucesos, incluido el análisis de la causa raíz.

Sucesos de estado de Network Manager

Network Manager puede generar sucesos que muestren el estado de varios procesos de Network Manager. Estos sucesos se conocen como sucesos de estado de Network Manager y tienen el valor del campo de AlertGroup de alerts.status de `Estado ITNM`.

Cuando estos sucesos de estado se envían a ObjectServer para su inserción en la tabla alerts.status, se les asigna un valor AlertGroup de `ITNM Status`.

Tipos de suceso de estado

Se utiliza un conjunto de identificadores de sucesos para identificar sucesos de estado de Network Manager por tipo. La siguiente lista identifica los valores EventId que se insertan en la tabla alerts.status y describe cómo se genera cada suceso de estado asociado.

ItnmConfiguration
Este tipo de suceso se genera para indicar un error de configuración. El campo Resumen describe el problema.

ItnmDatabaseConnection
Este tipo de suceso se genera para indicar la pérdida de conexión a NCIM. Este suceso se genera mediante la hebra de sondeo de estado gestionada en el proceso **`ncp_model`**. La generación de este suceso depende del periodo de tiempo configurado en el intervalo de sondeo de estado gestionado en el modelo. Se generará un suceso de problema si la conexión se pierde, y se generará un suceso de resolución correspondiente si la conexión se restaura, o en el inicio para borrar cualquier fallo de una operación anterior. Este tipo de suceso permite al dominio de la copia de seguridad tomar posesión cuando se configura la migración tras error. El proceso de dominio virtual reacciona ante este suceso como se define en el filtro para NCIM en el archivo `NCHOME/etc/precision/VirtualDomainSchema.cfg`.

ItnmDiscoAgentStatus
`Ncp_disco` genera este tipo de suceso cuando un agente de descubrimiento pasa a un nuevo estado. Al finalizar un descubrimiento, se envía un suceso de información a ObjectServer, para cada agente que se ha utilizado durante el descubrimiento.

Puede utilizar esta información para identificar el estado de cada agente. En la tabla alerts.status, se utiliza el campo LocalPriObj para almacenar el nombre del agente.

Los sucesos del agente de descubrimiento en ObjectServer se sobrescriben cuando se ejecuta un descubrimiento posterior.

La generación de este tipo de suceso se puede inhabilitar modificando el valor del campo m_CreateStchrEvents de la tabla disco.config.

ItnmDiscoFinderStatus
`Ncp_disco` genera este tipo de suceso cuando un buscador de descubrimiento pasa a un nuevo estado. Al finalizar un descubrimiento, se envía un suceso de información a ObjectServer, para cada buscador que se ha utilizado durante el descubrimiento.

Puede utilizar esta información para identificar qué buscadores se están ejecutando y su estado. En la tabla alerts.status, se utiliza el campo LocalPriObj para almacenar el nombre del buscador.

Los sucesos del buscador de descubrimiento en ObjectServer se sobrescriben cuando se ejecuta un descubrimiento posterior.

La generación de este tipo de suceso se puede inhabilitar modificando el valor del campo m_CreateStchrEvents de la tabla disco.config.

ItnmDiscoPhase

Ncp_disco genera este tipo de suceso cuando el proceso de descubrimiento pasa a una nueva fase. Al finalizar el descubrimiento, deben estar presentes cinco sucesos de información en ObjectServer, para mostrar las transiciones en bucle desde la fase 0 (standby) a las fases 1, 2 y 3 (recopilación de datos) a la fase -1 (proceso de datos). Se genera un suceso para cada uno de los cambios de fase siguientes en un único descubrimiento:

- 0 a 1
- 1 a 2
- 2 a 3
- 3 a -1
- -1 a 0

Puede utilizar esta información para determinar la longitud de cada fase. En la tabla alerts.status, el campo LocalPriObj se utiliza para almacenar la fase a la que está pasando el descubrimiento y el campo LocalSecObj almacena la fase anterior del descubrimiento.

Consejo: Los valores de cadena para las fases también se muestran en el archivo de registro del descubrimiento cuando el proceso **ncp_disco** se ejecuta en modalidad de depuración.

Los sucesos de fase de descubrimiento en ObjectServer se sobrescriben cuando se ejecuta un descubrimiento posterior.

ItnmDiscoStitcherStatus

El proceso de descubrimiento se compone de una fase de recopilación de datos y de una fase de procesamiento de datos, durante las cuales se crea la topología. Los sucesos de ItnmDiscoStitcherStatus se generan mediante el Motor de descubrimiento, **ncp_disco**, cuando se alcanza una fase grave en la fase del proceso de datos. Al final del descubrimiento, se reenviará un suceso de información a ObjectServer, para cada agrupador de descubrimiento mayor que se utilizara durante el descubrimiento.

Puede utilizar esta información para identificar en qué fase de las del proceso de datos está el descubrimiento. En la tabla alerts.status, el campo LocalPriObj se utiliza para almacenar el nombre del agrupador correspondiente a esta fase.

Los sucesos de ItnmDiscoStitcherStatus se generan cuando se ejecutan los siguientes agrupadores:

- BuildFinalEntityTable
- BuildContainment
- BuildLayers
- MergeLayers
- PostLayerProcessing

Posteriormente, los sucesos se generan durante la fase de creación de la topología cuando se ejecutan los agrupadores siguientes.

- Si ncp_disco está utilizando la base de datos dNCIM:
  - PopulateDNCIM

Los sucesos del agrupador de descubrimiento en ObjectServer se sobrescriben cuando se ejecuta un descubrimiento posterior.

La generación de este tipo de suceso se puede inhabilitar modificando el valor del campo m_CreateStchrEvents de la tabla disco.config.

ItnmEntityCreation

Si está configurado en el archivo $NCHOME/etc/precision/ModelSchema.cfg, **ncp_model** genera este tipo de suceso de información, para cada chasis nuevo o entidad de interfaz de IP (EntityType = 1) que está insertado en la base de datos NCIM.

Puede configurar ModelSchema.cfg definiendo el valor de las columnas ChassisCreationEvents e IpInterfaceCreationEvents en 1 en la sentencia INSERT para la tabla model.config. Por ejemplo:

```
insert into model.config
(
    LingerTime,
    ChassisCreationEvents,
    IpInterfaceCreationEvents,
    MaintenanceStateEvents,
    ManagedStatusUpdateInterval,
    DeleteRenamedDevices,
    KeepOldEntityDetails
)
values
(
    3,
    1,  // If set to 1, generates ItnmEntityCreation and ItnmEntityDeletion events
when a chassis entity is created.
    1,  // If set to 1, generates ItnmEntityCreation and ItnmEntityDeletion events
when an interface with its own IP address is created.
    0,
    30,
    1,
    0
);
```

Nota: Para que se puedan aplicar los cambios de configuración y habilitar los sucesos, se debe reiniciar el proceso **ncp_model**. El proceso lee los valores de configuración durante el inicio.

ItnmEntityDeletion

Si está configurado en el archivo $NCHOME/etc/precision/ModelSchema.cfg, **ncp_model** genera este tipo de suceso de información, para cada chasis o entidad de interfaz de IP (EntityType = 1) que se suprime de la base de datos NCIM.

Puede configurar ModelSchema.cfg definiendo el valor de la columna RaiseEntityEvent en 1 en la sentencia INSERT para la tabla model.config, tal como se muestra en la descripción precedente para el EventId de ItnmEntityCreation.

ItnmFailover

Ncp_virtualdomain genera este tipo de suceso cuando un dominio de Network Manager en un par de migración tras error migra tras error o se conmuta por recuperación.

Un suceso de problema se genera cuando tiene lugar una migración tras error y un suceso de resolución se genera durante la conmutación por recuperación.

En la tabla alerts.status, la descripción del campo Resumen indica si el dominio es el primario o la copia de seguridad y si se encuentra en un modo activo o en espera.

ItnmFailoverConnection

Ncp_virtualdomain genera este tipo de suceso para indicar cuando el dominio de copia de seguridad en par de migración tras error se conecta a o se desconecta del dominio primario.

Cuando Network Manager se ejecuta en modalidad de migración tras error, se genera un suceso de resolución cuando el dominio primario y el de copia de seguridad configuran su conexión de socket TCP. Esta conexión de socket es necesaria para transferir las actualizaciones de topología del dominio primario porque el proceso de descubrimiento (**ncp_disco**) no se ejecuta en el dominio de copia de seguridad. Si posteriormente se pierde la conexión, se genera un suceso de problema.

Nota: El estado de la conexión no determina si se ha desencadenado la migración tras error. La migración tras error se desencadena solo cuando los sucesos de comprobación de estado se transfieren (a través de ObjectServer) por los dominios y se proporciona una conexión de socket que se ha establecido en un determinado momento.

ItnmGwPluginInitialization
Este suceso de tipo identifica si se ha inicializado correctamente cada plugin de la pasarela de sucesos habilitado. Si se trata de un suceso de problema, consulte el archivo de registro de la pasarela de sucesos (`ncp_g_event.`*`nombre_dominio`*`.log`) para obtener más detalles.

ItnmHealthChk
Los sucesos de comprobación de estado gobiernan la migración tras error de Network Manager. Cada dominio en el par de migración tras error genera sucesos de resolución de comprobación de estado mientras ese dominio está sano.

Los sucesos de problema de comprobación de estado para un dominio se pueden generar de dos maneras:

- Mediante el dominio local: El dominio local detecta un fallo en uno de sus procesos, tal como está configurado en el archivo `$NCHOME/etc/precision/VirtualDomainSchema.cfg`.
- Mediante el dominio remoto: Un dominio detecta que el otro dominio no generó un suceso de resolución de comprobación de estado en la cantidad de tiempo configurada, y genera un suceso de problema de comprobación de estado sintético en nombre del dominio remoto.

Cuando se genera un suceso de problema de comprobación de estado para el dominio primario, se inicia la migración tras error y el dominio de copia de seguridad se vuelve activo.

A los sucesos de comprobación de estado se les ha asignado anteriormente un valor EventID de NcpHealthChk. Para la compatibilidad con versiones anteriores de Network Manager, puede sustituir NcpHealthChk en lugar de ItnmHealthChk en el archivo de reglas de sonda.

Nota: La pasarela de sucesos de Network Manager maneja los sucesos de comprobación de estado, que exigen que el valor Nodo sea el dominio al que se refiere el suceso. No tiene por qué ser el dominio que genera el suceso, ya que un dominio puede generar sucesos de error en nombre de otro.

ItnmMaintenanceState
Si está configurado en el archivo `$NCHOME/etc/precision/ModelSchema.cfg`, este tipo de suceso se genera mediante el Gestor de topología, **ncp_model**, para los cambios del estado de mantenimiento en un chasis o en una interfaz IP.

Puede configurar `ModelSchema.cfg` estableciendo el valor de la columna RaiseEntityEvent en 1 en la sentencia INSERT para la tabla model.config, como se muestra en la descripción anterior para el suceso ItnmEntityCreation.

Se genera un suceso de problema cuando el chasis o la entidad de interfaz de IP se encuentra en mantenimiento y se genera un suceso de resolución cuando la entidad está fuera de mantenimiento.

Nota: Solo se envía un suceso de interfaz individual si el cambio no se aplica a nivel del chasis; cuando cambia un dispositivo, un suceso de chasis y una serie de sucesos de interfaz no se generan de forma colectiva.

ItnmServiceState
Este tipo de suceso se genera cuando se inicia o finaliza un proceso y significa que si un proceso no se ha podido iniciar o se ha detenido durante el tiempo de ejecución. (Tenga en cuenta que los sucesos de estado de proceso no se generan cuando se detienen los procesos durante el apagado del sistema).

Se genera un suceso de resolución cuando **ncp_ctrl** inicia un proceso. Si no se puede iniciar un proceso o si se detiene durante el tiempo de ejecución, se genera un suceso de problema.

En la tabla alerts.status, la descripción del campo Resumen incluye el nombre de proceso, el PID y una indicación de si el proceso se ha:

- Iniciado (e iniciado satisfactoriamente)
- Detenido (es decir, se ha suprimido de la tabla de la base de datos **ncp_ctrl** denominada services.inTray)
- Terminado (es decir, se ha detenido, pero **ncp_ctrl** lo reiniciará)
- No se ha podido iniciar

- Ha fallado y no se reiniciará (es decir, se ha detenido y se ha excedido el número de reintentos configurados para el proceso)

ItnmTopologyUpdated

Ncp_model genera este tipo de suceso de información cuando la actualización de la base de datos de topología NCIM finaliza al final de un ciclo de descubrimiento. Esta información es útil si intenta programar scripts o procedimientos que se vayan a ejecutar después de actualizar la base de datos NCIM. Este evento contiene el siguiente parámetro: DISCOMODE, para el cual 0 indica que la topología se actualizó porque terminó un ciclo de descubrimiento completo y 1 un ciclo de descubrimiento parcial.

Nota: Si está activada la opción de retroalimentación o se hace ping en subredes mayores, puede haber varios ciclos de descubrimiento y, de esta manera, varios sucesos de este tipo, un suceso por cada ciclo de descubrimiento. Para determinar si el descubrimiento ha finalizado, se puede realizar la siguiente consulta OQL al servicio del buscador de pings:

```
select * from pingFinder.status where m_Completed <> 1;
```

Esta consulta busca las subredes a las que el buscador de pings está haciendo ping todavía. Si no hay barridos de ping pendientes y el descubrimiento están en fase 0, esto significa que el descubrimiento ha finalizado.

Tareas relacionadas

Supervisión de mensajes de estado de proceso
Puede ver mensajes de estado en Network Manager para comprender el estado del producto.

Capítulo 34. Configuración de plug-ins de la Pasarela de sucesos

Puede configurar los plug-ins de la Pasarela de sucesos. Puede visualizar plug-ins habilitados actualmente.

Habilitación e inhabilitación de conectores

Puede habilitar e inhabilitar conectores.

Acerca de esta tarea

Utilice el script `ncp_gwplugins.pl` para habilitar e inhabilitar los conectores. El script está ubicado en `$NCHOME/precision/scripts/perl/scripts/ncp_gwplugins.pl`.

Para ejecutar el script para habilitar las suscripciones al mapa de sucesos, emita un mandato similar al siguiente. Este ejemplo habilita el conector zNetView en todos los dominios.

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ncp_gwplugins.pl -domain NCOMS -plugin zNetView -enable -global
```

Opciones de línea de mandatos

La tabla siguiente describe las opciones de la línea de mandatos para el script `ncp_gwplugins.pl` utilizado en este ejemplo. Para obtener ayuda, ejecute el script como sigue:

- Para obtener una breve lista de las opciones disponibles, ejecute el mandato sin ninguna opción.
- Para obtener un conjunto completo de opciones de línea de mandatos, ejecute el script con la opción `-help`.

Tabla 119. Opciones de línea de mandatos de ncp_gwplugins.pl

Opción de línea de mandatos	Descripción
`-domain` *DomainName*	Obligatorio; el nombre de un dominio relacionado con el conector. Este dominio se utiliza para habilitar el script para leer el archivo DbLogins.cfg relevante para conectar y actualizar las bases de datos de conector de Pasarela de sucesos relevantes. Debe especificar un dominio, incluso si quiere cambiar un valor para los plugins de todos los dominios.

Tabla 119. Opciones de línea de mandatos de ncp_gwplugins.pl (continuación)	
Opción de línea de mandatos	**Descripción**
`-plugin` *NombreConector*	Nombre del conector. **Nota:** Sólo puede ejecutar el script para un conector a la vez. Los nombres de conector que se utilizan en esta opción de línea de mandatos son los siguientes. Si el nombre del conector está formado por más de una palabra, el nombre debe ponerse entre comillas dobles; por ejemplo: "Sondeo adaptativo". • Sondeo adaptativo • Comprobación de la compatibilidad • Disco • Migración tras error • PostNcimProcessing • RCA • Enlace agregado SAE • Vía de acceso de IP SAE • Servicio de ITNM SAE • VPN de MPLS SAE • zNetView
`-disable`	Inhabilita el conector especificado.
`-enable`	Habilita el conector especificado.
`-global`	Habilita conectores en todos los dominios. Si no se especifica esto, los conectores se habilitarán únicamente en el dominio especificado utilizando el parámetro `-domain`.

Listado de información sobre plug-ins

Puede listar información sobre los plug-ins de la pasarela de sucesos. Por ejemplo, puede listar los mapas de sucesos y los estados de sucesos a los que se subscriben los plug-ins.

Acerca de esta tarea

Utilice el script `ncp_gwplugins.pl` para listar la información sobre plug-in. El script está ubicado en `$NCHOME/precision/scripts/perl/scripts/ncp_gwplugins.pl`.

Para ejecutar el script para listar las subscripciones al mapa de sucesos, emita un mandato similar al siguiente. Este ejemplo lista todos los mapas de sucesos y estados de sucesos subscritos por el plug-in Disco.

```
$NCHOME/precision/bin/ncp_perl
$NCHOME/precision/scripts/perl/scripts/ncp_gwplugins.pl -domain NCOMS -plugin Disco
```

Opciones de línea de mandatos

La tabla siguiente describe las opciones de la línea de mandatos para el script `ncp_gwplugins.pl` utilizado en este ejemplo. Para obtener ayuda, ejecute el script como sigue:

- Para obtener una breve lista de las opciones disponibles, ejecute el mandato sin ninguna opción.
- Para obtener un conjunto completo de opciones de línea de mandatos, ejecute el script con la opción `-help`.

Tabla 120. Opciones de línea de mandatos de ncp_gwplugins.pl

Opción de línea de mandatos	Descripción
`-domain` *DomainName*	Obligatorio; el nombre de un dominio relacionado con el conector. Este dominio se utiliza para habilitar el script para leer el archivo DbLogins.cfg relevante para conectar y actualizar las bases de datos de conector de Pasarela de sucesos relevantes. Debe especificar un dominio, incluso si quiere cambiar un valor para los plugins de todos los dominios.
`-plugin` *NombreConector*	Nombre del conector. **Nota:** Sólo puede ejecutar el script para un conector a la vez. Los nombres de conector que se utilizan en esta opción de línea de mandatos son los siguientes. Si el nombre del conector está formado por más de una palabra, el nombre debe ponerse entre comillas dobles; por ejemplo: "Sondeo adaptativo". • Sondeo adaptativo • Comprobación de la compatibilidad • Disco • Migración tras error • PostNcimProcessing • RCA • Enlace agregado SAE • Vía de acceso de IP SAE • Servicio de ITNM SAE • VPN de MPLS SAE • zNetView

Modificación de las suscripciones de mapas de sucesos

Puede cambiar los mapas de sucesos que se suscriben a un plug-in. Por ejemplo, si añade un mapa de sucesos nuevo y quiere que el sistema realice RCA en los sucesos gestionados por ese mapa de sucesos, debe añadir el mapa de sucesos a la lista de subscripciones para el plug-in RCA.

Acerca de esta tarea

Utilice el script `ncp_gwplugins.pl` para modificar las subscripciones del mapa de sucesos. El script está ubicado en `$NCHOME/precision/scripts/perl/scripts/ncp_gwplugins.pl`.

Para ejecutar el script para modificar las subscripciones del mapa de sucesos, emita un mandato similar al siguiente. En este ejemplo, el mapa de sucesos `PnniIfState` se añade a la lista de subscripciones para el plug-in RCA.

```
$NCHOME/precision/perl/bin/ncp_perl $NCHOME/precision/scripts/
perl/scripts/ncp_gwplugins.pl -domain NCOMS -plugin RCA -add -eventMap PnniIfState
```

Opciones de línea de mandatos

La tabla siguiente describe las opciones de la línea de mandatos para el script `ncp_gwplugins.pl` utilizado en este ejemplo. Para obtener ayuda, ejecute el script como sigue:

- Para obtener una breve lista de las opciones disponibles, ejecute el mandato sin ninguna opción.
- Para obtener un conjunto completo de opciones de línea de mandatos, ejecute el script con la opción `-help`.

Tabla 121. Opciones de línea de mandatos de ncp_gwplugins.pl

Opción de línea de mandatos	Descripción
`-domain` *DomainName*	Obligatorio; el nombre de un dominio relacionado con el conector. Este dominio se utiliza para habilitar el script para leer el archivo DbLogins.cfg relevante para conectar y actualizar las bases de datos de conector de Pasarela de sucesos relevantes. Debe especificar un dominio, incluso si quiere cambiar un valor para los plugins de todos los dominios.
`-plugin` *NombreConector*	Nombre del conector. **Nota:** Sólo puede ejecutar el script para un conector a la vez. Los nombres de conector que se utilizan en esta opción de línea de mandatos son los siguientes. Si el nombre del conector está formado por más de una palabra, el nombre debe ponerse entre comillas dobles; por ejemplo: "Sondeo adaptativo". • Sondeo adaptativo • Comprobación de la compatibilidad • Disco • Migración tras error • PostNcimProcessing • RCA • Enlace agregado SAE • Vía de acceso de IP SAE • Servicio de ITNM SAE • VPN de MPLS SAE • zNetView
`-add`	Para obtener un plug-in o plug-ins específicos, aumente el interés en el mapa de sucesos especificado. Se deben especificar las opciones `-plugin` y `-eventMap`.
`-drop`	Para obtener un plug-in o plug-ins específicos, disminuya el interés en el mapa de sucesos especificado.
`-eventMap` *EventMapName*	Mapa de sucesos para el que se a aumentado o suprimido el interés.

Conceptos relacionados

Referencia rápida de enriquecimiento de sucesos
Utilice esta información para comprender cómo se procesan los sucesos y se pasan a través de la Pasarela de sucesos.

Referencia rápida de RCA
Utilice esta información para comprender cómo se procesan los sucesos y se pasan a través del conector RCA.

Cola de pasarela de sucesos salientes
La cola de la pasarela de sucesos de salida recibe sucesos enriquecidos de los agrupadores de la pasarela de sucesos (enriquecimiento de sucesos principal) y de los plug-ins. Con el fin de minimizar el número de actualizaciones y, por lo tanto, minimizar la carga del ObjectServer, las actualizaciones de este se colocan en una cola, se agregan y se envían al ObjectServer en un período de tiempo especificado. El valor predeterminado es de 5 segundos.

Establecimiento de los parámetros de configuración de plug-in

Puede establecer parámetros de configuración opcionales para los plug-ins de la pasarela de sucesos utilizando el script `ncp_gwplugins.pl` .

Acerca de esta tarea

Utilice el script `ncp_gwplugins.pl` para establecer parámetros de configuración opcionales. El script está ubicado en `$NCHOME/precision/scripts/perl/scripts/ncp_gwplugins.pl`.

Para ejecutar el script para establecer parámetros de configuración, emita un mandato similar al siguiente. Este ejemplo establece el intervalo de actualización para la tabla ncmonitor.activeEvent en 10 segundos. El valor predeterminado es de 5 segundos.

```
$NCHOME/precision/perl/bin/ncp_perl
$NCHOME/precision/scripts/perl/scripts/ncp_gwplugins.pl -domain NCOMS [ -global ]
-plugin "Adaptive Polling" -set -name ActiveEventUpdateInterval -value 10
```

Opciones de línea de mandatos

La tabla siguiente describe las opciones de la línea de mandatos para el script `ncp_gwplugins.pl` utilizado en este ejemplo. Para obtener ayuda, ejecute el script como sigue:

- Para obtener una breve lista de las opciones disponibles, ejecute el mandato sin ninguna opción.
- Para obtener un conjunto completo de opciones de línea de mandatos, ejecute el script con la opción `-help`.

Tabla 122. Opciones de línea de mandatos de ncp_gwplugins.pl

Opción de línea de mandatos	Descripción
`-domain` *DomainName*	Obligatorio; el nombre de un dominio relacionado con el conector. Este dominio se utiliza para habilitar el script para leer el archivo DbLogins.cfg relevante para conectar y actualizar las bases de datos de conector de Pasarela de sucesos relevantes. Debe especificar un dominio, incluso si quiere cambiar un valor para los plugins de todos los dominios.
`-global`	Opcional. Establece el parámetro para este plugin en todos los dominios. Si no incluye el parámetro -global, se establece para el plugin sólo en el dominio especificado.

Tabla 122. Opciones de línea de mandatos de ncp_gwplugins.pl (continuación)	
Opción de línea de mandatos	**Descripción**
`-name`*ParameterName*	Nombre del parámetro a establecer.
`-plugin` *NombreConector*	Nombre del conector. **Nota:** Sólo puede ejecutar el script para un conector a la vez. Los nombres de conector que se utilizan en esta opción de línea de mandatos son los siguientes. Si el nombre del conector está formado por más de una palabra, el nombre debe ponerse entre comillas dobles; por ejemplo: "Sondeo adaptativo". • Sondeo adaptativo • Comprobación de la compatibilidad • Disco • Migración tras error • PostNcimProcessing • RCA • Enlace agregado SAE • Vía de acceso de IP SAE • Servicio de ITNM SAE • VPN de MPLS SAE • zNetView
`-set`	Indica que se va a establecer una variable.
`-value`*Parametervalue*	Valor a establecer para este parámetro.

Conceptos relacionados

Plug-in de sondeo adaptativo
Utilice esta información para comprender los requisitos previos del conector, la forma en que el conector de sondeo adaptativo rellena campos en la tabla activeEvent, así como los detalles de configuración asociados con el conector. La tabla activeEvent se encuentra en el esquema NCMONITOR.

conector de Disco
Utilice esta información para comprender cierta información básica de cómo funciona este conector, sus requisitos previos y detalles de configuración asociados con el conector.

Conector de migración tras error
Utilice esta información para comprender el funcionamiento del conector así como los detalles de configuración asociados con el conector.

Conector PostNCIMProcessing
El conector PostNCIMProcessing ejecuta los agrupadores que sean necesarios una vez actualizada la base de datos NCIM. De forma predeterminada, el conector desencadena la agrupación de varios dominios en un único dominio de agregación cuando se recibe un suceso de actualización de topología.

Conector zNetView
Utilice esta información para conocer los requisitos previos del conector, así como los detalles de configuración asociados con el conector.

Configuración del plug-in SAE

Utilice esta información para entender cómo configurar el plug-in SAE.

Configuración de la información de campo de resumen en sucesos afectados por el servicio

Para hacer que los sucesos afectados por el servicio sean más significativos para los operadores, puede configurar el plug-in SAE para insertar información relacionada con el cliente en el campo resumen de un suceso afectado por el servicio.

Acerca de esta tarea

Los archivos de configuración del plug-in SAE donde hace este cambio son los siguientes:

- SaeIpPath.cfg para el servicio de vía de acceso IP, ubicado en $NCHOME/etc/precision/SaeIpPath.cfg
- SaeMplsVpn.cfg ara el servicio de VPN de MPLS, ubicado en$NCHOME/etc/precision/SaeMplsVpn.cfg
- SaeItnmService.cfg para servicios personalizados, ubicado en $NCHOME/etc/precision/SaeItnmService.cfg

El campo utilizado en cada uno de estos archivos para configurar información extra que se inserta en el campo resumen de SAE se denomina CustomerNameField. El siguiente ejemplo muestra cómo configurar este campo en el archivo SaeMplsVpn.cfg.

Procedimiento

1. Abra el archivo de configuración SaeMplsVpn.cfg.
2. Modifique la sentencia de inserción añadiendo el texto en negrita para insertar datos desde un campo relevante en el registro de servicio en la memoria caché de NCIM en el campo CustomerNameField. Por ejemplo, la siguiente sentencia insertará el contenido del campo entityData->DESCRIPTION (si existe este campo) en CustomerNameField, y en el campo Resumen de cualquier SAE de servicio límite de VPN de MPLS generado.

   Nota: Al añadir un campo a la inserción, debe añadir una coma a la línea precedente.

```
insert into config.serviceTypes
(
    ServiceTypeName,
    CollectionEntityType,
    ConstraintFilter,
    CustomerNameField
)
values
(
    "MPLSVPNEdgeService",
    17 -- "networkVpn",
    "networkVpn->VPNTYPE <> 'MPLS Core'",
    "entityData->DESCRIPTION"
```

Adición de tipos SAE al plug-in SAE

Puede configurar el conector SAE para generar más tipos SAE de los proporcionados de forma predeterminada. Por ejemplo, puede configurar el plug-in para crear sucesos SAE para entidades de límite VPN de MPLS (un tipo de SAE) y para entidades de núcleo VPN de MPLS (otro tipo de SAE).

Ejemplo

En este ejemplo el archivo de configuración existente SaeMplsVpn.cfg está personalizado para añadir un tipo de servicio SAE de VPN de MPLS extra a la tabla config.serviceTypes. El nuevo tipo de servicio se denomina MPLS VPN Core Service, y genera SAE cuando se produce un suceso de anomalía Gravedad 5 (critico) en cualquier direccionador de la red principal. También puede crear nuevos tipos de servicios SAE creando un archivo de configuración nuevo y especificando las inserciones relevantes.

El archivo de configuración para los tipos de servicios SAE de VPN de MPLS en el plug-in SAE es el archivo de configuración SAEMplsVpn.cfg. Este archivo está ubicado en: $NCHOME/etc/precision/SAEMplsVpn.cfg.

1. Abra el archivo de configuración SAEMplsVpn.cfg.
2. La inserción predeterminada crea un MPLS VPN Edge Service y se lee de la siguiente manera:

```
insert into config.serviceTypes
(
    ServiceTypeName,
    CollectionEntityType,
    ConstraintFilter
)
values
(
    "MPLS VPN Edge Service",
    17,   -- networkVpn
    "networkVpn->VPNTYPE <> 'MPLS Core'"
);
```

3. Añada una nueva inserción después de la inserción existente. La nueva inserción debe leerse de la siguiente manera:

```
insert into config.serviceTypes
(
    ServiceTypeName,
    CollectionEntityType,
    ConstraintFilter
)
values
(
    "MPLS VPN Core Service",
    17,   -- networkVpn
    "networkVpn->VPNTYPE = 'MPLS Core'"
);
```

Nota: Puede tener dos o más tipos de servicio SAE para una tabla determinada como networkVpn (17), como se describe en este ejemplo. En este caso, los tipos de servicio SAE deben ser conjuntos mutuamente excluyente, de lo contrario ninguno ganará sobre el otro donde se superponen. Por ejemplo, los tipos de servicio descritos en este ejemplo no se superponen porque tienen valores `ConstraintFilter` complementarios de la siguiente manera:

- `networkVpn->VPNTYPE <> 'MPLS Core'`
- `networkVpn->VPNTYPE = 'MPLS Core'`

Configuración del conector Disco

De forma predeterminada, el plugin Disco activa el redescubrimiento de dispositivos asociados con los sucesos de rearranque desde el ObjectServer de Tivoli Netcool/OMNIbus. Puede configurar el conector Disco para desencadenar el descubrimiento basándose en la recepción de un suceso.

Acerca de esta tarea

De forma predeterminada, sólo se pasan sucesos de rearranque (sucesos con un campo `eventId` establecido en `NmosSnmpReboot`) al conector Disco. Para poder pasar sucesos con un valor de campo `eventId` diferente al conector Disco, puede utilizarse uno de los métodos siguientes:

- Asigne un `eventId` diferente a la correlación de sucesos de reconfiguración existente utilizando uno de los siguientes métodos de selección de sucesos:
  - Configure los archivos de reglas de analizador de IBM Tivoli Netcool/OMNIbus correspondientes.
  - Rellene la tabla config.precedence de la pasarela de sucesos utilizando la inserción correspondiente.

  Esto se puede hacer si el `LocalNodeAlias` del suceso identifica el chasis o si se establece `NmosEntityId`.

Nota: De forma predeterminada, la correlación de sucesos de reconfiguración no pasa los sucesos al conector RCA para el análisis de causa raíz. No utilice este método si los sucesos que se van a pasar al conector Disco también deben tenerse en cuenta para el análisis de causa raíz (RCA).

- Registre una correlación de sucesos existente con el conector Disco, utilizando el script `ncp_gwplugins.pl`.

  Nota: Todos los sucesos que utilizan esta correlación de sucesos existentes se pasarán al conector Disco. No utilice este método si hay sucesos que utilizan la correlación existente que no deben desencadenar el redescubrimiento.
- Cree una nueva correlación de sucesos, asígnele los sucesos con un determinado valor de campo `eventId` y registre la nueva correlación de sucesos con el conector Disco, mediante el script `ncp_gwplugins.pl`. Este es el método que se presenta en el ejemplo siguiente.

Configuración del conector Disco para responder a un suceso

En este ejemplo se supone que existe un tipo de suceso, es decir, un grupo de sucesos con el mismo valor de campo `eventId`, que contiene una dirección IP en el campo LocalNodeAlias. Existe el requisito de considerar este tipo de suceso para el RCA y también para volver a descubrir las entidades asociadas con los sucesos de este tipo de suceso.

1. Añada una nueva correlación de sucesos al archivo EventGatewaySchema.cfg, con el agrupador de búsqueda correspondiente. El agrupador LookupMainNode existente seleccionará un chasis en un IP. En este ejemplo se supone que el nombre de la nueva correlación de sucesos es `NewEventMap`.

   Nota: El archivo EventGatewaySchema.cfg se encuentra en: `$NCHOME /etc/precision/EventGatewaySchema.cfg`.

   ```
   insert into config.eventMaps
   (
       EventMapName,
       Stitcher
   )
   values
   (
       "NewEventMap",
       "LookupMainNode"
   );
   ```

2. Asocie el tipo de suceso con la nueva correlación de sucesos configurando el archivo de reglas del analizador correspondiente para rellenar el campo NmosEventMap con el nombre de la nueva correlación de sucesos, `NewEventMap`.

   Nota: La configuración del archivo de reglas del analizador es la forma preferida de asociar el suceso con la nueva correlación de sucesos, ya que este método actualiza el suceso en el origen y, por lo tanto, un cambio en la correlación de sucesos se detecta automáticamente en Netcool/OMNIbus Knowledge Library y en todas las instalaciones de Network Manager que se conectan al ObjectServer de Tivoli Netcool/OMNIbus al que está conectado el analizador. Donde *EventId* es el identificador de suceso del tipo de suceso que va a manejar la nueva correlación de sucesos.

   a. En el servidor donde está instalado Netcool/OMNIbus Knowledge Library, localice el archivo de reglas que corresponde al ID de suceso del tipo de sucesos que desea personalizar. Para reglas específicas de proveedor, los archivos de reglas se colocan bajo el directorio de proveedor, por ejemplo, `include-snmptrap/cisco`.

   b. Localice el archivo de reglas apropiado con el sufijo `user.include.rules`. Por ejemplo `/include-snmptrap/adtran/adtran-ADTRAN-ACTDAXL3-MIB.user.include.snmptrap.rules`. Si las personalizaciones se ponen en un archivo independiente, es más fácil identificarlas y realizar copias de seguridad de las mismas más adelante.

   c. Edite el archivo y localice la sección que corresponde al tipo de interrupción que desea personalizar.

d. Establezca el campo @NmosEventMap utilizando el formato siguiente: *nombre_correlación_sucesos.valor_prioridad*. Por ejemplo:

```
@NmosEventMap = "NewEventMap.0"
```

3. Asimismo, si no puede realizar cambios en el archivo de reglas del analizador, puede asociar el suceso con la nueva correlación de sucesos al añadir una inserción config.precedence al archivo EventGatewaySchema.cfg, como en el siguiente ejemplo:

```
# Precedence of 0 implies this event cannot suppress others
# 'MyEventId' should be the EventId field of the event in the Omnibus
alerts.status table
insert into config.precedence
(
    Precedence,
    EventMapName,
    NcoEventId
)
values
(
    0,
    "NewEventMap",
    "EventId"
);
```

4. Configure los conectores RCA y Disco para que se suscriban a la nueva correlación de sucesos, ejecutando los siguientes mandatos. Esto garantiza que el tipo de suceso que desee se considere candidato para la supresión en el análisis de causa raíz y se utilice para desencadenar el redescubrimiento de la entidad asociada con el suceso.

```
ncp_gwplugins.pl -domain domain -plugin Disco -add -eventMap NewEventMap
ncp_gwplugins.pl -domain domain -plugin RCA -add -eventMap NewEventMap
```

Donde *domain* es el dominio actual.

5. Realice una de las siguientes operaciones de verificación:

- Compruebe la configuración del conector al ejecutar los mandatos siguientes:

```
ncp_gwplugins.pl -domain domain -plugin Disco
ncp_gwplugins.pl -domain domain -plugin RCA
```

Las respuestas a cada uno de estos mandatos deben mostrar que el conector se suscribe a la nueva correlación de sucesos NewEventMap.

- Compruebe la configuración de la correlación de sucesos al ejecutar el siguiente mandato:

```
ncp_gwplugins.pl -domain domain -eventMap NewEventMap
```

Las respuestas a estos mandatos deben mostrar que los conectores RCA y Disco se han suscrito a la correlación de sucesos NewEventMap.

Conceptos relacionados

conector de Disco

Utilice esta información para comprender cierta información básica de cómo funciona este conector, sus requisitos previos y detalles de configuración asociados con el conector.

Métodos de selección de correlaciones de sucesos

La correlación de sucesos y la prioridad pueden asignarse directamente desde el archivo de reglas del analizador de Tivoli Netcool/OMNIbus o en el archivo de configuración de la pasarela de sucesos.

Tareas relacionadas

Modificación de las suscripciones de mapas de sucesos

Puede cambiar los mapas de sucesos que se suscriben a un plug-in. Por ejemplo, si añade un mapa de sucesos nuevo y quiere que el sistema realice RCA en los sucesos gestionados por ese mapa de sucesos, debe añadir el mapa de sucesos a la lista de subscripciones para el plug-in RCA.

Capítulo 35. Configuración del análisis de causa raíz

Puede configurar el plug-in RCA.

Referencia relacionada

Resincronización de sucesos con ObjectServer

Emita el mandato SIGHUP a la pasarela de sucesos para cambiar la configuración de la pasarela de sucesos.

Configuración de la entidad del sondeador

Cuando el servidor de Network Manager no está en el ámbito del dominio de red, o si tiene varios dominios, especifique la dirección IP o el nombre DNS de la entidad del sondeador.

Acerca de esta tarea

La entidad del sondeador es un nodo designado en la topología desde el que se calcula el RCA. De forma predeterminada, la entidad del sondeador es la misma que la del servidor donde se han instalado los componentes principales de Network Manager.

Defina una entidad de sondeador para cada dominio de descubrimiento. La entidad de sondeador debe existir en la topología de red descubierta para el dominio donde se ha definido. Si el servidor donde se ha instalado Network Manager no está en la topología, establezca la entidad del sondeador en el nodo más próximo dentro de la topología.

Para garantizar una supresión aislada y en sentido descendente, establezca la entidad del sondeador en el servidor desde donde se sondea la red o lo más próximo posible al servidor.

El archivo de configuración de la pasarela de sucesos es el archivo de configuración EventGatewaySchema.*DOMINIO*.cfg, donde *DOMINIO* es el nombre del dominio donde se ejecuta la pasarela de sucesos. Este archivo está ubicado en: `NCHOME/etc/precision/`. El valor de entidad del sondeador está almacenado en la tabla config.defaults, en el campo NcpServerEntity.

Procedimiento

1. Abra el archivo de configuración EventGatewaySchema.*DOMAIN*.cfg.
2. Identifique la sentencia de inserción en la tabla config.defaults.
   De forma predeterminada, esta sentencia de inserción tiene la forma siguiente:

```
insert into config.defaults
(
    IDUCFlushTime,
    ObjectServerUpdateInterval,
    NcimHandleCount,
    NcpServerEntity
)
values
(
    5,
    5,
    1
    ""
);
```

   De forma predeterminada, el campo NcpServerEntity está vacío. En este caso, la pasarela de sucesos busca la topología utilizando la dirección o direcciones IP del host local en el que se está ejecutando.
3. Modifique esta sentencia para establecer el campo NcpServerEntity al valor de la dirección IP o nombre DNS de la interfaz de ingreso, por ejemplo:

```
insert into config.defaults
(
    IDUCFlushTime,
    ObjectServerUpdateInterval,
```

```
    NcimHandleCount,
    NcpServerEntity
)
values
(
    5,
    5,
    1
    "switch108-abc.example.co.uk"
);
```

4. Si utiliza RCA en varios dominios, repita estos pasos para cada dominio, utilizando un sondeador diferente para cada dominio.

Conceptos relacionados

Entidad de sondeador
Utilice esta información para comprender qué es la entidad de sondeador y cómo configurarla.

Referencia relacionada

Consideraciones de RCA en una red de dominios cruzados
En un entorno de dominios cruzados, el proceso **ncp_g_event** de cada dominio de descubrimiento ejecuta RCA en los dispositivos en el mismo dominio de descubrimiento. En cada dominio, RCA opera de la misma forma que cuando sólo hay un único dominio. También puede analizarse la causa raíz en varios dominios cuando se visualizan conjuntamente utilizando un descubrimiento de dominios cruzados.

Configuración de la diferencia de edad máxima para sucesos

De manera predeterminada, los sucesos pueden suprimirse unos a otros independientemente de la antigüedad de los sucesos. Un suceso recibido hoy puede suprimir un suceso recibido ayer. Puede cambiar esto especificando una diferencia de edad máxima entre sucesos que pasan a través del plug-in RCA. Los sucesos que tienen una diferencia de edad mayor que este valor especificado no pueden suprimirse unos a otros.

Acerca de esta tarea

El archivo de configuración para el plug-in RCA es el archivo de configuración `RCASchema.cfg`. Este archivo está ubicado en: `$NCHOME/etc/precision/RCASchema.cfg`. El valor para la diferencia de antigüedad máxima entre suceso se almacena en la tabla `config.defaults`, en el campo `MaxAgeDifference`.

Procedimiento

1. Abra el archivo de configuración `RCASchema.cfg`.
2. Identifique la sentencia de inserción en la tabla `config.defaults`.
   De forma predeterminada, esta sentencia de inserción tiene la forma siguiente:

```
//  MaxAgeDifference is in minutes
insert into config.defaults
(
    RequeueableEventIds,
    MaxAgeDifference,
    HonourManagedStatus,
    TopologyChangesThreshold,
    GraphTopologyNames
)
values
(
    [
        'NmosPingFail',
        'NmosSnmpPollFail'
    ],
        0,
        1,
        100,
    [

        'Layer2Topology',
        'LocalVlanTopology'
```

```
    ]
);
```

De manera predeterminada, el valor de `MaxAgeDifference` es 0. Esto significa que la función está desactivada.

3. Modifique esta sentencia para establecer el campo `MaxAgeDifference` a un valor deseado en minutos.

   Consejo: Por ejemplo, establezca el campo `MaxAgeDifference` a un valor de 15 para configurar el sistema así los sucesos de la misma entidad que tengan una diferencia de antigüedad de más de quince minutos no se podrán suprimir unos a otros.

Capítulo 36. Configuración de la Sonda para Tivoli Netcool/OMNIbus

La Sonda para Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) adquiere y procesa los sucesos que generan los sondeos y los procesos de Network Manager, y reenvía estos sucesos al ObjectServer.

La Sonda para Tivoli Netcool/OMNIbus se instala en el directorio $NCHOME/probes/*arch*, donde *arch* representa un directorio del sistema operativo. Puede configurar la sonda utilizando sus archivos de configuración, que son los siguientes:

- Archivo de propiedades: nco_p_ncpmonitor.props
- Archivo de reglas: nco_p_ncpmonitor.rules

Nota: El archivo ejecutable (o mandato **nco_p_ncpmonitor**) para la sonda también se instala en el directorio $NCHOME/probes/*arch*. La sonda se configura, sin embargo, para ejecutarse bajo el controlador de proceso del dominio CTRL, de forma predeterminada, y el mandato **nco_p_ncpmonitor** debería ejecutarse manualmente únicamente para fines de resolución de problemas.

Los sucesos generados en Network Manager son específicos del dominio. Cuando Network Manager se ejecuta en modalidad de migración tras error, la sonda utiliza el nombre del dominio virtual de forma predeterminada, suponiendo que el nombre esté configurado en el archivo $NCHOME/etc/precision/ConfigItnm.cfg.

Para obtener más información acerca de los conceptos de la sonda, consulte la publicación *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* de la información de Tivoli Netcool/OMNIbus en http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Acerca del archivo nco_p_ncpmonitor.props

El archivo $NCHOME/probes/*arch*/nco_p_ncpmonitor.props define el entorno en el que se ejecuta la Sonda para Tivoli Netcool/OMNIbus.

El archivo de propiedades se forma de pares de nombre-valor que están separados por dos puntos. El archivo de propiedades predeterminado lista una subred de las propiedades que soporta la sonda; a estas propiedades se les quita el comentario con un signo de número (#) al inicio de la línea. El conjunto estándar de propiedades de sonda comunes, que son aplicables para la versión de Tivoli Netcool/OMNIbus en ejecución, se puede especificar para la Sonda para Tivoli Netcool/OMNIbus, donde sea relevante.

Una práctica sugerida para cambiar los valores predeterminados de las propiedades es que agregue una línea de nombre-valor para cada propiedad requerida al final del archivo. Para especificar una propiedad, asegúrese de que la línea no está comentada y, a continuación, modifique el valor como sea necesario. Los valores de cadena deben encerrarse en comillas; otros valores no requieren comillas. Por ejemplo:

```
Buffering         :    1
BufferSize        :    15
```

Para fines de resolución de problemas, puede configurar de forma alternativa las propiedades de la sonda para la línea de mandatos ejecutando el mandato **nco_p_ncpmonitor** con las opciones relevantes de la línea de mandatos.

Nota: Las propiedades siguientes tienen valores predeterminados estándar:

Servidor
Toma como valor predeterminado el ObjectServer identificado en el esquema ConfigItnm, lo que garantiza la coherencia con la pasarela de Network Manager.

PropsFile
Toma como valor predeterminado $NCHOME/probes/*platform*/nco_p_ncpmonitor.props.

RulesFile
Toma como valor predeterminado $NCHOME/probes/*platform*/nco_p_ncpmonitor.rules.

MessageLog
Toma como valor predeterminado $NCHOME/log/precision/nco_p_ncpmonitor.*domain_name*.log.

RawCaptureFile
Toma como valor predeterminado $NCHOME/var/precision/nco_p_ncpmonitor.*domain_name*.cap.

Para obtener más información acerca de las propiedades comunes a las sondas, consulte la publicación *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* en el centro de información de Tivoli Netcool/OMNIbus en http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Referencia de configuración de nco_p_ncpmonitor.rules

El archivo $NCHOME/probes/*arch*/nco_p_ncpmonitor.rules define cómo Sonda para Tivoli Netcool/OMNIbus debe procesar los datos de sucesos de Network Manager para crear un suceso significativo de Tivoli Netcool/OMNIbus.

En la práctica, el archivo de reglas correlaciona los datos de sucesos de Network Manager en los campos de ObjectServer, y se puede utilizar para personalizar el comportamiento del analizador. Es necesario conocer la sintaxis de las reglas del analizador de Tivoli Netcool/OMNIbus para configurar el archivo de reglas.

La sonda utiliza señales y elementos, y aplica reglas, para transformar los datos del origen de sucesos de Network Manager en un formato que el ObjectServer pueda reconocer. Los datos del origen de sucesos sin formato se convierten a señales, que se analizarán en elementos. El archivo de reglas se utilizará para realizar el proceso condicional de los elementos, y para correlacionarlos en los campos de alerts.status de ObjectServer. En el archivo de reglas, los elementos se identifican mediante el símbolo $ y los campos de alerts.status se identifican mediante el símbolo @. La configuración del archivo de reglas correlaciona elementos en campos, como se muestra en el siguiente código de ejemplo:

```
@Summary=$Description
```

En este ejemplo, @Summary identifica el campo alerts.status, y $Description identifica el campo de entrada de Network Manager.

Donde el campo ExtraInfo de Network Manager se utiliza con campos anidados para almacenar datos adicionales en entidades (por ejemplo, ExtraInfo->ifIndex), estos campos estarán disponibles en el formato siguiente del archivo de reglas:

```
$ExtraInfo_variable
```

Donde *variable* representa una variable de la MIB (base de información de gestión) (por ejemplo, ifIndex), u otros datos (por ejemplo, nombres de la columna en las tablas de NCIM). Las variables de MIB están especificadas en caracteres en mayúscula y minúscula mezcladas, y otros datos, en caracteres en mayúscula. Por ejemplo:

```
$ExtraInfo_ifIndex
$ExtraInfo_MONITOREDENTITYID
```

Para configurar el archivo de reglas para la Sonda para Tivoli Netcool/OMNIbus, es necesario comprender lo siguiente:

- Los datos de origen de sucesos de Network Manager que están disponibles para su uso en el archivo de reglas de la sonda
- El conjunto de campos de alerts.status que se pueden rellenar con datos de sucesos desde Network Manager
- La correlación de datos entre los campos de Network Manager y de alerts.status

Para obtener más información acerca de la sintaxis utilizada en los archivos de reglas de la sonda, consulte la publicación *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* en el centro de información de Tivoli Netcool/OMNIbus en http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Ejemplo de proceso de archivos de reglas

Este ejemplo muestra cómo procesa el archivo de reglas los datos de origen de Network Manager para generar los datos de salida que se insertarán en la tabla `alerts.status`.

El código de ejemplo siguiente muestra un registro de datos de sucesos de Network Manager que se pasa a la Sonda para Tivoli Netcool/OMNIbus para su proceso. En este registro, se creó un suceso de resolución cuando **`ncp_ctrl`** inició el proceso **`ncp_store`**.

```
{
    EventName='ItnmServiceState';
    Severity=1;
    EntityName='BACKUP';
    Description='ncp_store process [15299] has started';
    ExtraInfo={
        EVENTTYPE=2;
        SOURCE='ncp_ctrl';
        ALERTGROUP='ITNM Status';
        EVENTMAP='ItnmStatus';
        SERVICE='ncp_store';
        PID=15299;
        };
}
```

El siguiente extracto del archivo de reglas de la sonda muestra la sintaxis utilizada para procesar y correlacionar estos campos de entrada en los campos de alerts.status:

```
...
    #
    # populate some standard fields
    #
    @Severity = $Severity
    @Summary = $Description
    @EventId = $EventName
    @Type = $ExtraInfo_EVENTTYPE
    @AlertGroup = $ExtraInfo_ALERTGROUP
    @NmosEventMap = $ExtraInfo_EVENTMAP
    @Agent = $ExtraInfo_SOURCE

    if (exists($ExtraInfo_ACCESSIPADDRESS))
    {
        @Node = $ExtraInfo_ACCESSIPADDRESS
    }
    else
    {
        @Node = $EntityName
    }

    #
    # Stamp the event with the name of its originating domain
    #
    @NmosDomainName = $Domain
    @Manager = "ITNM"
    @Class = 8000

    #
    # populate fields for RCA
    #
    @LocalNodeAlias = @Node

...

    #
    # Now set the AlertKey and Identifier
    #
    if (match(@AlertGroup, "ITNM Status"))
    {
        switch ($EventName)
        {
            case ...
```

```
...
            case "ItnmServiceState":
                @LocalPriObj = $ExtraInfo_SERVICE
...
            case ...
....
        }
    }

    #
    # Both the Identifier and the AlertKey contain the domain name. This ensures
    # that in a multi-domain setup, events are handled on a per-domain basis
    #

    #
    # Include the LocalPriObj in the AlertKey or the link-downs on
    # all interfaces will cleared by a link-up on any interface
    #
    @AlertKey = $EntityName + @LocalPriObj + "->" + $EventName + @NmosDomainName

    #
    # Set up deduplication identifier and include the LocalPriObj
    # so we can correctly handle de-duplication of events raised on interfaces
    #
    @Identifier = $EntityName + @LocalPriObj + "->" + $EventName + @Type + @NmosDomainName
}
```

Cuando el proceso del archivo de reglas se complete, los datos de salida que se reenvían al ObjectServer toman la forma siguiente:

```
CMonitorProbeApp::ProcessStatusEvent
{
    AlertGroup='ITNM Status';
    EventId='ItnmServiceState';
    Type=2;
    Severity=1;
    Summary='ncp_store process [15299] has started';
    Node='BACKUP';
    NmosDomainName='PRIMARY';
    LocalNodeAlias='BACKUP';
    LocalPriObj='ncp_store';
    LocalRootObj='';
    RemoteNodeAlias='';
    AlertKey='BACKUPncp_store->ItnmServiceStateVIRTUAL';
    Identifier='BACKUPncp_store->ItnmServiceState2VIRTUAL';
    Class=8000;
    Agent='ncp_ctrl';
    LastOccurrence=1267122089;
}
```

Según el proceso del archivo de reglas de este ejemplo, se puede ver que los campos de entrada de Network Manager se correlacionan con los campos alerts.status como sigue:

campo Network Manager	**campo alerts.status**
EventName	EventId
Gravedad	Gravedad
EntityName	Nodo
Descripción	Resumen
ExtraInfo->EVENTTYPE	Tipo
ExtraInfo->SOURCE	Agente
ExtraInfo->ALERTGROUP	AlertGroup
ExtraInfo->EVENTMAP	NmosEventMap
ExtraInfo->SERVICE	LocalPriObj

Nota: A continuación, se pueden ver la entrada y salida completas de las reglas del analizador en el archivo de rastreo del analizador. Establezca el rastreo en depuración 4. El archivo de rastreo del

analizador se puede encontrar en: $NCHOME/log/precision. Para obtener más información sobre el establecimiento de niveles de registro, consulte *IBM Tivoli Network Manager IP Edition Administration Guide*.

Campos de los datos de sucesos de Network Manager

Cuando se generen los sucesos en Network Manager, los datos de sucesos se insertarán en un número de campos (o columnas) de las tablas de Network Manager. Aunque cada suceso utiliza únicamente un subconjunto de los posibles campos, son comunes un número de campos para todos los tipos de sucesos.

La tabla siguiente lista todos los nombres de campos de Network Manager que están disponibles para su uso en el archivo de reglas de sonda, y describe los datos de sucesos almacenados en cada campo. La tabla identifica igualmente cual de los campos de Network Manager son comunes para todos los sucesos y, por lo tanto, siempre estarán disponibles en el archivo de reglas.

Tabla 123. Campos de Network Manager que rellenan los sucesos

Nombre del campo de Network Manager	Contenido del campo	¿Disponible en todo momento?
Descripción	Una descripción breve del suceso.	Sí
Dominio	El dominio actual. Si Network Manager está configurado para la modalidad de migración tras error, éste será el dominio principal.	Sí (suponiendo que el archivo de correlación no esté modificado)
EntityName	Para sucesos de red, este es el campo de entityName desde la tabla de entityData de NCIM para la entidad en la que el suceso se genera. Para sucesos de estado, este es siempre el nombre del dominio sobre el que se genera el suceso.	Sí
EventName	El identificador del suceso. Por ejemplo, ItnmDiscoPhase.	Sí
ExtraInfo_ACCESSIPADDRESS	Si el nodo principal o la entidad de la interfaz identificada por el campo de entrada de EntityName tiene una dirección IP accesible de forma directa (el campo accessIPAddress desde la interfaz de NCIM o las tablas de chasis), se facilitará aquí. Aplicable únicamente a sucesos de red.	No
ExtraInfo_AGENT	El agente responsable de un suceso del agente de descubrimiento (ItnmDiscoAgentStatus).	Sí (para sucesos de ItnmDiscoAgentStatus)
ExtraInfo_ALERTGROUP	El grupo de alerta del suceso. Para los sucesos de estado de Network Manager, el grupo de alerta es `ITNM Status` y, para los sucesos de red, el valor es `ITNM Monitor`.	Sí

Tabla 123. Campos de Network Manager que rellenan los sucesos (continuación)

Nombre del campo de Network Manager	Contenido del campo	¿Disponible en todo momento?
ExtraInfo_ENTITYCLASS	El nombre de la clase asignada a la entidad, como se identifica en las tablas entityClass y classMembers de NCIM.	Sí (para sucesos de red y de ItnmEntityCreation)
ExtraInfo_ENTITYTYPE	El tipo de la entidad, como se define en la tabla entityType de NCIM.	Sí (para sucesos de red)
ExtraInfo_LocalPriObj	Proporciona un valor para el campo LocalPriObj en el registro alerts.status. Este campo tiene el mismo valor que el campo en desuso ExtraInfo_EventSnmpIndex, a excepción de que tiene el prefijo de un identificador para la entidad de MIB que se sondeará; por ejemplo ifEntry, bgpPeerEntry.	Sí (para sucesos de red)
ExtraInfo_EVENTTYPE	El tipo de suceso generado por Network Manager. Los valores son los siguientes: • 1: Problema • 2: Resolución • 13: Información	Sí
ExtraInfo_FINDER	El buscador responsable de un suceso de buscador de descubrimiento (ItnmDiscoFinderStatus).	Sí (para sucesos de ItnmDiscoFinderStatus)
ExtraInfo_ifIndex	Para sucesos generados en una interfaz con un valor de ifIndex en la tabla de la interfaz de NCIM, dicho valor se otorga aquí. Aplicable únicamente a sucesos de red en interfaces.	No
ExtraInfo_IFALIAS	Para sucesos generados en interfaces, este campo contiene el valor ifAlias, si se conoce. Aplicable únicamente a sondeos de interfaz de red.	No
ExtraInfo_IFDESCR	Para sucesos generados en interfaces, este campo contiene el valor ifDescr, si se conoce. Aplicable únicamente a sondeos de interfaz de red.	No
ExtraInfo_IFNAME	Para sucesos generados en interfaces, este campo contiene el valor ifName, si se conoce. Aplicable únicamente a sondeos de interfaz de red.	No
ExtraInfo_IFTYPESTRING	Para sucesos generados en interfaces, este campo contiene la representación de cadenas del valor ifType. Aplicable únicamente a sondeos de interfaz de red.	No

Tabla 123. Campos de Network Manager que rellenan los sucesos (continuación)

Nombre del campo de Network Manager	Contenido del campo	¿Disponible en todo momento?
ExtraInfo_MAINNODEADDRESS	La interfaz de gestión del nodo principal que contiene la entidad, como se identifica mediante el campo accessIPAddress de la tabla de chasis de NCIM. Aplicable únicamente a sucesos de red y de ItnmEntityCreation.	Sí (para sucesos de red)
ExtraInfo_MAINNODEENTITYID	El campo entityId de la tabla entityData de NCIM para el nodo principal, como se identifica mediante el campo accessIPAddress de la tabla de chasis de NCIM. Aplicable únicamente a sucesos de red.	Sí (para sucesos de red)
ExtraInfo_MAINNODEENTITYNAME	El campo entityName de la tabla entityData de NCIM para el nodo principal, como se identificó en NCIM. Aplicable únicamente a sucesos de red.	Sí (para sucesos de red)
ExtraInfo_MONITOREDENTITYID	El campo de entityId de la tabla entityData de NCIM para la entidad en la que se genera el suceso. Aplicable únicamente a sucesos de red y de ItnmEntityCreation.	No
ExtraInfo_MONITOREDINSTID	Un registro en la tabla ncpolldata.monitoredInstance.	No
ExtraInfo_NEWPHASE	La fase de descubrimiento que se ha iniciado. Aplicable únicamente a los sucesos de la fase de descubrimiento (ItnmDiscoPhase).	Sí (para sucesos de la fase de descubrimiento)
ExtraInfo_OLDPHASE	La fase de descubrimiento que ha finalizado. Aplicable únicamente a los sucesos de la fase de descubrimiento (ItnmDiscoPhase).	Sí (para sucesos de la fase de descubrimiento)
ExtraInfo_POLICYNAME	El nombre de la política de sondeo que dio lugar al suceso.	Sí (para sucesos de red)
ExtraInfo_PID	El ID de proceso del servicio de Network Manager afectado. Aplicable únicamente para los sucesos de ItnmServiceState.	Sí (para sucesos del estado de servicio)
ExtraInfo_REMOTEDOMAIN	El nombre del dominio remoto. Aplicable únicamente para sucesos de ItnmFailoverConnection.	Sí (para sucesos de conexión de migración tras error)
ExtraInfo_sysContact	Si está disponible, el valor sysContact se otorga únicamente para los sucesos de ItnmEntityCreation.	No
ExtraInfo_sysLocation	Si está disponible, el valor sysLocation se otorga únicamente para los sucesos de ItnmEntityCreation	No

Tabla 123. Campos de Network Manager que rellenan los sucesos (continuación)		
Nombre del campo de Network Manager	**Contenido del campo**	**¿Disponible en todo momento?**
ExtraInfo_sysObjectId	Si está disponible, el valor sysObjectId se otorga únicamente para sucesos de ItnmEntityCreation	No
ExtraInfo_SERVICE	El nombre del servicio de Network Manager afectado. Aplicable únicamente para los sucesos de ItnmServiceState.	Sí (para sucesos del estado de servicio)
ExtraInfo_SNMPSTATUS	Un código de estado de SNMP numérico.	Sí (para sucesos de NmosSnmpPollFail)
ExtraInfo_SNMPSTATUSSTRING	Una indicación legible por humanos del estado de fallo de SNMP.	Sí (para sucesos de NmosSnmpPollFail)
ExtraInfo_SOURCE	El nombre del proceso desde el que se originó el suceso.	Sí
ExtraInfo_STITCHER	El agrupador responsable de un suceso de agrupador de descubrimiento (ItnmDiscoStitcherStatus).	Sí (para sucesos de ItnmDiscoStitcherStatus)
Gravedad	El nivel de gravedad del suceso. La gravedad es un valor distinto a cero.	Sí

campos alerts.status utilizados por Network Manager

La tabla alerts.status en ObjectServer contiene información de estado sobre problemas que han detectado las sondas.

Un subconjunto de campos `alerts.status` estándar se llena con datos de sucesos de Network Manager. De forma adicional, se reserva un conjunto de campos dedicados `alerts.status` para retener datos que son específicos para Network Manager. Los nombres de campo `alerts.status` dedicados son identificables por el prefijo `Nmos`.

La siguiente tabla describe los campos `alerts.status` que llenan los campos de Network Manager. A algunos de estos campos `alerts.status` se les asignan valores predeterminados desde dentro del archivo de reglas de sonda. (Intente no modificar estos valores predeterminados.)

Tabla 124. campos alerts.status utilizados por Network Manager			
campo alerts.status	**Tipo de datos**	**Descripción**	**Nombre/valor predeterminado de campo de Network Manager en el archivo de reglas**
Agente	varchar(64)	Nombre del proceso que ha generado el suceso. Puede utilizar este campo para filtrar el **Visor de sucesos** para mostrar solo los sucesos de un tipo específico; por ejemplo, solo sucesos de descubrimiento (con un valor de ncp_disco).	ExtraInfo_SOURCE

Tabla 124. campos alerts.status utilizados por Network Manager (continuación)

campo alerts.status	Tipo de datos	Descripción	Nombre/valor predeterminado de campo de Network Manager en el archivo de reglas
AlertGroup	varchar(255)	Utilizado para agrupar sucesos por tipo. Los valores proporcionados de forma predeterminada desde los sucesos de Network Manager son `ITNM Monitor` para sucesos de red o `ITNM Status` para sucesos de estado.	ExtraInfo_ALERTGROUP
AlertKey	varchar(255)	Una cadena de texto que concatena diferentes elementos relacionados con el suceso. Los elementos pueden incluir el ID de suceso, dominio, fase y nombre de proceso. Permite que los sucesos de problemas y de resolución sean coincidentes.	Este valor es generado desde la entrada para asegurar una coincidencia apropiada de los sucesos de problemas y de resolución en ObjectServer.
Clase	integer	La clase de alerta asignada a la Sonda para Tivoli Netcool/OMNIbus.	Se reserva un valor de `8000` para los sucesos generados por Network Manager.
EventId	varchar(255)	El tipo de suceso (por ejemplo, SNMPTRAP-linkDown). La pasarela de sucesos utiliza este valor para buscar la correlación de sucesos y para determinar la precedencia de los sucesos.	EventName
ExpireTime	integer	La fecha de caducidad del suceso en la base de datos. Network Manager, no lo utiliza actualmente.	
FirstOccurrence	time	Una indicación de fecha que señala cuando tuvo lugar por primera vez.	
Identificador	varchar(255)	Un valor exclusivo para cada tipo de suceso en una entidad determinada (por ejemplo, un suceso LinkDown en una interfaz de dispositivo específico). Este identificador controla la optimización del almacenamiento.	Este valor se genera desde la entrada para asegurar una optimización del almacenamiento de los sucesos apropiada en ObjectServer. En el archivo de reglas, el identificador se construye como una concatenación de valores de campo.
LastOccurrence	time	Una indicación de fecha que señala cuando tuvo lugar por última vez.	

Tabla 124. campos alerts.status utilizados por Network Manager (continuación)

campo alerts.status	Tipo de datos	Descripción	Nombre/valor predeterminado de campo de Network Manager en el archivo de reglas
LocalNodeAlias	varchar(64)	La dirección IP o DNS del dispositivo. Este valor se refiere normalmente al chasis, pero solo para pingFails, puede corresponderse con la interfaz.	Para sucesos de red, este campo se establece en el mismo valor que el campo Nodo. No se define ningún valor para sucesos de estado, para asegurarse de que no se retroalimentan en Network Manager mediante la pasarela de sucesos.
LocalPriObj	varchar(255)	La entidad específica para la cual se genera el suceso; por ejemplo, el valor de campo ifIndex, ifDescr o ifPhysAddress.	ExtraInfo_AGENT o ExtraInfo_FINDER o ExtraInfo_ifIndex o ExtraInfo_NEWPHASE o ExtraInfo_SERVICE o ExtraInfo_STITCHER El valor ExtraInfo_ifIndex se muestra utilizando la sintaxis `ifEntry.<ifIndex>`. Por ejemplo, `ifEntry.12`.
LocalRootObj	varchar(255)	El contenedor de la entidad referenciada en el campo LocalPriObj. No tiene por qué ser el chasis, pero podría ser, por ejemplo, la ranura en un chasis. El chasis todavía se puede identificar utilizando LocalNodeAlias.	
LocalSecObj	varchar(255)	El objeto secundario referenciado por el suceso.	ExtraInfo_OLDPHASE
Manager	varchar(64)	Un nombre descriptivo que identifica el sistema que enviaba los sucesos.	Un valor de `ITNM` se utiliza para los sucesos generados por Network Manager V3.8 o posterior. Un valor de `Omnibus` se utiliza en versiones anteriores.
NmosCauseType	integer	El estado de suceso. Rellenado por la pasarela NMOS. Los posibles valores son los siguientes: • 0: Desconocido • 1: Causa principal • 2: Síntoma	

Tabla 124. campos alerts.status utilizados por Network Manager (continuación)

campo alerts.status	Tipo de datos	Descripción	Nombre/valor predeterminado de campo de Network Manager en el archivo de reglas
NmosDomainName	varchar(64)	El nombre del dominio de red de Network Manager que ha generado el suceso. El nombre del dominio primario se utiliza en modalidad de migración tras error. De forma predeterminada, se rellena este campo solo para sucesos generados por Network Manager. Para rellenar este campo para otros orígenes de sucesos, como las de otras sondas, debe modificar los archivos de reglas para esas sondas. La pasarela de sucesos rellena este campo si un suceso es coincidente con una entidad en un dominio.	Dominio
NmosEntityId	integer	El ID de objeto exclusivo que identifica la entidad de topología con la que el suceso está asociada. Este campo es similar al campo NmosObjInst pero contiene información más detallada. Por ejemplo, este campo puede incluir el ID de una interfaz dentro de un dispositivo. El campo NmosEntityId se rellena en el archivo de reglas de la sonda. Para los demás sucesos, la pasarela rellena este campo cuando se identifica la entidad.	ExtraInfo_MONITOREDENTITYID
NmosEventMap	varchar(64)	El nombre de correlación del suceso y la precedencia opcional para el suceso, que indica cómo Network Manager debe procesar el suceso; por ejemplo, PrecisionMonitorEvent.910. El número de precedencia opcional se puede concatenar al final del valor, después de un punto (.) Si no se proporciona la precedencia, se define en 0. **Nota:** Este valor se puede sustituir por una inserción explícita en la tabla config.precedence de la pasarela de sucesos, que proporciona los mismos datos.	

Tabla 124. campos alerts.status utilizados por Network Manager (continuación)

campo alerts.status	Tipo de datos	Descripción	Nombre/valor predeterminado de campo de Network Manager en el archivo de reglas
NmosManagedStatus	integer	El estado gestionado de la entidad de red para el que el suceso se ha generado. Cuando una entidad de red no está gestionada, se suspenden los sondeos de Network Manager y los sucesos de otros orígenes se marcan como no gestionados. Este campo le permite filtrar sucesos desde entidades no gestionadas. Los posibles valores para este campo son los siguientes: • 0: Managed • 1: Operador no gestionado • 2: Sistema no gestionado • 3: Fuera de ámbito	
NmosObjInst	integer	El ID de objeto exclusivo que identifica la entidad de chasis de topología contenida con la que el suceso está asociado. Rellenado por la pasarela NMOS. **Consejo:** Este campo se puede utilizar para detectar si el suceso se ha pasado para el enriquecimiento de sucesos.	
NmosSerial	integer	El número de serie del suceso que suprime el suceso actual. Rellenado por la pasarela NMOS.	
Nodo	varchar(64)	El dispositivo a partir del cual se ha originado el suceso. Si se origina un suceso en un entidad con una dirección IP accesible, se utiliza esta dirección IP. En caso contrario, se utiliza el valor entityName de NCIM. De forma predeterminada, Nodo tiene el mismo valor que LocalNodeAlias.	ExtraInfo_ACCESSIPADDRESS o EntityName El valor EntityName se correlaciona con el campo Nodo solo si el campo de entrada ExtraInfo_ACCESSIPADDRESS está vacío.
NodeAlias	varchar(64)	La dirección IP del nodo principal, si está disponible.	ExtraInfo_MAINNODEADDRESS

Tabla 124. campos alerts.status utilizados por Network Manager (continuación)

campo alerts.status	Tipo de datos	Descripción	Nombre/valor predeterminado de campo de Network Manager en el archivo de reglas
RemoteNodeAlias	varchar(64)	La dirección de red de un nodo remoto, donde sea relevante. Por ejemplo: • Un valor en blanco (cuando una interfaz deja de funcionar) • Una dirección cercana (en la que una interfaz conectada ha dejado de funcionar) • La estación de sondeo (para un suceso de error de ping)	
Serial	incr	Un ID exclusivo por suceso y por instancia de ObjectServer. En donde se configuran ObjectServers primarios y de respaldo, ObjectServers tendrá números de serie diferentes para el mismo suceso.	
ServerName	varchar(64)	El nombre del ObjectServer originario.	
ServerSerial	integer	El número de serie del suceso en el ObjectServer originario. En donde se configuran ObjectServers primarios y de respaldo, ObjectServers tendrá números de serie diferentes para el mismo suceso. Si el suceso se ha originado en el ObjectServer actual, el valor ServerSerial es el mismo que el valor de serie.	
Gravedad	integer	El nivel de gravedad del suceso almacenado en ObjectServer. Los valores predeterminados son los siguientes: • 0: Despejado (VERDE) • 1: Indeterminado (PÚRPURA) • 2: Aviso (AZUL) • 3: Menor (AMARILLO) • 4: Grave (NARANJA) • 5: Crítico (ROJO)	Gravedad

Tabla 124. campos alerts.status utilizados por Network Manager (continuación)			
campo alerts.status	**Tipo de datos**	**Descripción**	**Nombre/valor predeterminado de campo de Network Manager en el archivo de reglas**
StateChange	time	Una indicación de fecha que señala cuando se ha modificado por última vez el suceso. Este campo se puede utilizar para determinar si un proceso está modificando un suceso después de que se haya agregado a ObjectServer.	
Resumen	varchar(255)	Una descripción textual del suceso.	Descripción
Cuadrar	integer	Un recuento del número de veces que un suceso ha tenido lugar. Este valor se muestra en la columna Recuento en la lista de sucesos o el **Visor de sucesos**, y en la columna Producidos en la tabla `mojo.events`.	
Tipo	integer	El tipo de alerta. Los valores de relevancia particular para Network Manager son • 1: Problema • 2: Resolución • 13: Información	ExtraInfo_EVENTTYPE

Para obtener más información sobre la tabla `alerts.status`, consulte la publicación *IBM Tivoli Netcool/OMNIbus Administration Guide* del centro de información de Tivoli Netcool/OMNIbus en IBM Tivoli Netcool/OMNIbus - Información sobre el producto.

Avisos

Esta información se aplica al conjunto de documentación en PDF para IBM Tivoli Network Manager IP Edition.

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

IBM puede no ofrecer los productos, servicios o características tratados en esta documentación en otros países. Consulte con el representante local de IBM para obtener información acerca de los productos y servicios que actualmente están disponibles en su localidad. Las referencias hechas a productos, programas o servicios de IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios de IBM. Puede utilizarse en su lugar cualquier otro producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del cliente evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran alguno de los temas tratados en esta documentación. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar sus consultas sobre licencias por escrito a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunos países no permiten la renuncia a garantías explícitas o implícitas en determinadas transacciones, por lo que puede que esta declaración no sea aplicable en su caso.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. En cualquier momento y sin previo aviso, IBM puede hacer mejoras y/o cambios en los productos y/o programas descritos en esta publicación.

Cualquier referencia incluida en esta información a sitios web que no sean de IBM sólo se proporciona para su comodidad y en ningún modo constituye una aprobación de dichos sitios web. Los materiales de estos sitios Web no forman parte de los materiales destinados a este producto de IBM, y el usuario será responsable del uso que se haga de estos sitios Web.

IBM puede utilizar o distribuir cualquier información que se le proporcione en la forma que considere adecuada, sin incurrir en ninguna obligación para con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deberían ponerse en contacto con:

IBM Corporation
958/NH04
IBM Centre, St Leonards
601 Pacific Hwy
St Leonards, NSW, 2069
Australia

IBM Corporation
896471/H128B
76 Upper Ground
Londres
SE1 9PZ
Reino Unido

IBM Corporation
JBF1/SOM1 294
Route 100
Somers, NY, 10589-0100
Estados Unidos de América

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluido, en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en esta documentación, así como todo el material bajo licencia disponible, según los términos del Acuerdo de Cliente de IBM, del Acuerdo Internacional de Programas bajo Licencia de IBM o cualquier acuerdo equivalente entre nosotros.

Los datos de rendimiento incluidos aquí se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Pueden haberse realizado algunas mediciones en sistemas a nivel de desarrollo y no existe ninguna garantía de que estas mediciones vayan a ser equivalentes en sistemas disponibles generalmente. Además, es posible que algunas mediciones se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha comprobado dichos productos y no puede afirmar la exactitud en cuanto a rendimiento, compatibilidad u otras características relativas a productos no IBM. Las consultas acerca de las posibilidades de los productos no IBM deben dirigirse a los proveedores de los mismos.

Este documento contiene ejemplos de datos e informes que se utilizan diariamente en la actividad de la empresa. Para que parezcan verídicos, los ejemplos incluyen nombres de personas, compañías, marcas y productos. Todos los nombres son ficticios y cualquier parecido con nombres y direcciones utilizados por una empresa real son simple coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en el lenguaje de origen, que muestran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo en cualquier formato sin abonar ninguna cantidad a IBM, con intención de desarrollar, utilizar, comercializar o distribuir programas de aplicación que estén en conformidad con la interfaz de programación de aplicación de la plataforma operativa para la que están escritos los programas de ejemplo. Los ejemplos no se han probado minuciosamente bajo todas las condiciones. Por

lo tanto, IBM no puede garantizar ni dar por sentada la fiabilidad, la facilidad de mantenimiento ni el funcionamiento de los programas.

Marcas registradas

Los términos de la Tabla 125 en la página 653 son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

Tabla 125. Marcas registradas de IBM

AIX	Informix	PR/SM
BNT	iSeries	System p
ClearQuest	Jazz	System z
Cognos	Lotus	Tivoli
Db2	Netcool	WebSphere
Db2 Universal Database	NetView	z/OS
developerWorks	OMEGAMON	z/VM
DS8000	Passport Advantage	zSeries
Servidor de almacenamiento empresarial	PowerPC	
IBM	PowerVM	

Adobe, Acrobat, Portable Document Format (PDF), PostScript y todas las marcas registradas de Adobe son marcas registradas de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Intel, logotipo de Intel, Intel Inside, logotipo de Intel Inside, Intel Centrino, logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas de Intel Corporation o de sus filiales en Estados Unidos y en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o de sus filiales.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

UNIX es una marca comercial registrada de The Open Group en los Estados Unidos y otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Consideraciones sobre política de privacidad

Los productos de IBM Software, incluidas las soluciones de software como servicio, ("Software Offerings") pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, para ayudar a mejorar la experiencia del usuario final, para adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las ofertas de software no recopilan información de identificación personal. Algunas Ofertas de software pueden ayudarle a recopilar información identificable personalmente. Si esta oferta de software utiliza cookies para recopilar información de identificación personal, la información específica sobre el uso de cookies de esta oferta se expone a continuación.

Esta oferta de software puede recopilar direcciones IP, nombres de usuario y contraseñas con el objetivo de ejecutar el descubrimiento de red. Si no habilita la recopilación de esta información, probablemente se eliminarán funciones importantes proporcionadas por la oferta de software. Como cliente, debe buscar asesoría legal sobre la legislación aplicable a este tipo de recopilación de datos, incluidos los requisitos de avisos y consentimiento.

Para obtener más información sobre el uso de distintas tecnologías, incluidas las cookies, a estos efectos, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración Online Privacy Statement de IBM en http://www.ibm.com/privacy/details, y las secciones tituladas "Cookies, Web Beacons and Other Technologies" y "IBM Software Products and Software-as-a-Service Privacy Statement" en http://www.ibm.com/privacy.

Número Pieza:

Printed in the Republic of Ireland

(1P) P/N:

2021-4212-01