Network Manager IP Edition
4.2

Guide d'installation et de configuration

2021-4212-01

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 229.

Cette édition s'applique à la version 4.2 de IBM Tivoli Network Manager IP Edition (référence 5724-S45) et à toutes les éditions et modifications ultérieures, sauf indication contraire dans les nouvelles éditions.

Table des matières

A propos de cette publication..... vii
Publications..... vii
Accessibilité..... viii
Formation technique Tivoli..... x
Informations sur le support et la communauté.....x

Chapitre 1. Téléchargement Network Manager..... 1

Chapitre 2. Planification de l'installation..... 3
Déploiement de Network Manager.....3
Scénarios de déploiement.....3
Remarques relatives au déploiement.....14
Exemples de déploiements.....17
Vérification des prérequis du système.....22
Domaines réseau..... 23
Collecte des événements à l'aide de plusieurs domaines par ObjectServer..... 23
Exemple d'affichage d'une topologie depuis plusieurs domaines.....24
Configuration matérielle requise.....25
Directives pour le choix des processeurs..... 26
Configuration requise pour l'exécution du programme d'installation..... 26
Exigences relatives aux composants centraux.....27
Configuration requise pour les composants de l'interface graphique.....28
Configuration requise pour le serveur de base de données topologiques..... 29
Espace disque pour les événements et les interfaces..... 29
Spécifications d'espace de permutation (UNIX)..... 29
Exigences en mémoire de la reconnaissance.....30
Configuration logicielle..... 30
Exigences de compatibilité pour d'autres produits.....30
Bases de données topologiques prises en charge..... 32
Systèmes d'exploitation pris en charge.....33
Navigateurs pris en charge pour les applications Web..... 34
Outils de système d'exploitation.....35
Exigences relatives à l'utilisateur sous UNIX..... 35
Exigences relatives au répertoire d'installation..... 35
Exigences relatives au descripteur de fichier.....36
Exigences relatives aux mots de passe..... 37
Configuration requise du réseau..... 37
Liste des ports utilisés par le produit..... 37
Exigences DNS.....38
Exigences en bande passante de la reconnaissance..... 39
A propos de DNCIM..... 39
Installations FIPS 140-2..... 40

Chapitre 3. Préparation à l'installation..... 41
Exécution des procédures d'installation et de maintenance en tant que superutilisateur ou non superutilisateur.....41
Configuration de Red Hat Linux Enterprise Edition.....41
Tâches de pré-installation sous AIX.....41
Configuration de SSH..... 42
Installation d'un utilitaire `zip`..... 42

Vérification des paramètres de port d'achèvement d'E-S (IOCP)....42

Chapitre 4. Installation de Network Manager et des produits connexes.... 45
Liste de contrôle de l'installation.... 45
Installation et configuration d'IBM Installation Manager....48
Installation d'IBM Installation Manager en téléchargeant les fichiers du produit....48
Installation d'IBM Installation Manager via une connexion directe à Passport Advantage.... 49
Installation et configuration d'une base de données topologiques.... 51
Installation et exécution des scripts de la base de données Network Manager....52
Configuration des bases de données DB2 existantes sous UNIX....53
Installation et configuration de bases de données Oracle sous UNIX.... 54
Paramétrer NCIM pour l'utilisation de caractères Multibyte.... 56
Installation et configuration d'Tivoli Netcool/OMNIbus....57
Options de ligne de commande ConfigOMNI.... 58
Installation des composants de base de Network Manager.... 59
Installation de WebSphere Application Server....64
Installation de Dashboard Application Services Hub.... 65
Installation de Tivoli Netcool/OMNIbus Web GUI.... 68
Installation des composants principaux de l'interface graphique de Network Manager....69
Installation et configuration d'Cognos Analytics.... 71
Installation des rapports Network Manager....73
Installation du **Tableau de bord d'état du réseau** (clients Netcool Operations Insight uniquement).. 75
Installation et désinstallation de groupes de correctifs....76
Tâches de post-installation.... 76

Chapitre 5. Désinstallation de Network Manager.... 79
Applications de l'interface graphique.... 79
Rapports....80
Composants principaux deNetwork Manager et de Tivoli Netcool/OMNIbus.... 81
WebSphere Application Server....82

Chapitre 6. Installation et désinstallation de groupes de correctifs.... 83
Installation de groupes de correctifs.... 83
Application de mises à jour de schéma.... 85
Vérification des mises à jour de schéma.... 86
Désinstallation de groupes de correctifs.... 87

Chapitre 7. Intégration.... 89
Tivoli Netcool/OMNIbus.... 90
Configuration d'un serveur ObjectServer à utiliser avec les processus centraux Network Manager....90
Configuration du référentiel d'utilisateurs....91
Configuration du nom de la source de données Tivoli Netcool/OMNIbus Web GUI....92
Configuration des types d'événement de topologie....93
Installation et configuration d'analyses.... 93
Installation de Knowledge Library....94
Référence d'intégration Tivoli Netcool/OMNIbus.... 94
Netcool Configuration Manager....109
CCMDB, TADDM et TBSM....109
Eléments prérequis....109
Configuration de l'adaptateur de bibliothèque de reconnaissance....110
Création d'un manuel de la bibliothèque de reconnaissance....117
Optimisation de l'exportation de données.... 118
Chargement des manuels de bibliothèque de reconnaissance et activation du lancement bidirectionnel.... 123
Configuration de TADDM pour démarrer Network Manager.... 124
Configuration de Network Manager pour démarrer TADDM.... 125

Importation d'identificateurs globaux uniques TADDM dans la base de données NCIM..... 126
Intégration à TBSM..... 127
Configuration de Dashboard Application Services Hub 128
IBM Tivoli Monitoring..... 128
IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition..... 128
Installation et configuration..... 129
Accès aux données de reconnaissance à partir de dNCIM..... 137

Chapitre 8. Mise à niveau et migration..... 139
A propos de la mise à niveau..... 139
Chemins de mise à niveau et limitations..... 139
Emplacements par défaut des différentes versions de produit..... 140
Données faisant l'objet d'une migration..... 141
Mise à niveau de Network Manager..... 142
Préparation de la mise à niveau..... 142
Mise à jour de la base de données..... 143
Migration des composants principaux..... 144
Migration des composants de l'interface graphique..... 149
Migration de la topologie de réseau..... 153

Chapitre 9. Configuration..... 159
Configuration des propriétés de connexion NCIM..... 159
Configuration de la longueur et du type de chiffrement..... 159
Configuration de Network Manager pour les systèmes d'exploitation UNIX..... 161
Configuration des autorisations de superutilisateur/non superutilisateur..... 161
Chargement des informations MIB mises à jour..... 164
Configuration de Cognos Analytics..... 165
Configuration de rapports pour des installations existantes..... 165
Activation de l'interrogation historique..... 165
Activation de la reprise en ligne..... 166
A propos de la reprise en ligne..... 166
A propos de la haute disponibilité de la base de données topologiques NCIM..... 166
Architectures de reprise en ligne..... 168
Opérations de reprise en ligne..... 177
Restrictions de la reprise en ligne..... 184
Configuration de la reprise en ligne..... 185
Traitement des incidents de reprise en ligne..... 204
Configuration de la sécurité..... 209
Configuration des cookies..... 209
Protection contre le détournement de clic..... 209
Changement de l'adresse IP et du nom d'hôte de l'installation Network Manager..... 210
Pour Network Manager..... 210
Sur le serveur OMNIbus..... 210
Mise à jour de Network Manager avec une adresse IP OMNIbus modifiée..... 211
Mise à jour de DASH avec une adresse IP OMNIbus modifiée..... 212
Sur le serveur DASH..... 212
Mise à jour de Network Manager avec le nom d'hôte modifié de DASH..... 213
Configuration de Network Manager pour une adresse IP modifiée du serveur NCIM DB2..... 213
Configuration des variables d'environnement..... 214
Structure de répertoire par défaut..... 215
Configuration de périphériques Juniper PE..... 218
Configuration de domaines..... 219
Ajout de domaines réseau..... 219
Liaison d'un domaine à un contrôleur d'interface réseau (NIC)..... 221
Configuration d'une base de données dNCIM sous Linux on IBM z Systems..... 222
Configuration de l'auxiliaire SNMP..... 223
Configuration de la régulation de l'auxiliaire SNMP..... 223

Configuration de la prise en charge de GetBulk pour SNMP v2 et v3.....224
Configuration de l'authentification.....226
Modification de la méthode d'authentification des utilisateurs.....227
Configuration de l'authentification du fournisseur de services OQL.....227
IBM Support Assistant (ISA).....228
Installation du collecteur IBM Support Assistant Lite.....228

Remarques.....229
Marques.....231

A propos de cette publication

Le manuel *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*décrit comment installer Network Manager. Elle décrit également les tâches de configuration post-installation facultatives et obligatoires. Elle est destinée aux administrateurs qui doivent installer et paramétrer Network Manager.

Publications

Cette section liste les publications dans la bibliothèque de documents Network Manager et les documents associés. Elle explique également comment accéder aux publications IBM en ligne et commander des publications.

Votre bibliothèque Network Manager

Les documents suivants sont disponibles dans la bibliothèque Network Manager :

- *IBM Tivoli Network Manager IP Edition - Notes sur l'édition* donne des informations importantes et actualisées à propos de Network Manager. Cette publication s'adresse aux chargés du déploiement et aux administrateurs et doit être lue en premier lieu.
- Le manuel *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*décrit comment installer Network Manager. Elle décrit également les tâches de configuration post-installation facultatives et obligatoires. Elle est destinée aux administrateurs qui doivent installer et paramétrer Network Manager.
- *IBM Tivoli Network Manager IP Edition - Guide d'administration* décrit les tâches administratives telles que la façon de démarrer et arrêter le produit, reconnaitre le réseau, interroger le réseau, gérer les événements, adminstrer les processus et les requêtes aux bases de données.. Elle est destinée aux administrateurs chargés de la maintenance et de la disponibilité d'Network Manager.
- *IBM Tivoli Network Manager Reference* contient les informations de référence incluant le language système, les bases de données, et API Perl utilisées par Network Manager. Elle est destinée aux utilisateurs avancés qui doivent personnaliser le fonctionnement d'Network Manager.

Publications prérequises

Pour utiliser correctement les informations de la présente publication, vous devez posséder certaines connaissances prérequises, que vous pouvez obtenir dans les publications suivantes :

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

  Inclut les procédures d'installation et de mise à niveau et décrit comment configurer la sécurité et les communications des composants. Cette publication comprend également des exemples d'architectures Tivoli Netcool/OMNIbus et décrit leur implémentation.
- *IBM Tivoli Netcool/OMNIbus User's Guide*

  Fournit un résumé des outils du bureau et décrit les tâches de l'opérateur liées à la gestion des événements, effectuées à l'aide des outils de bureau.
- *IBM Tivoli Netcool/OMNIbus Administration Guide*

  Décrit comment effectuer des tâches d'administration à l'aide de l'interface graphique d'administration, des outils de ligne de commande et de la commande de processus Tivoli Netcool/OMNIbus. Cette publication contient également des descriptions et des exemples de la syntaxe SQL ObjectServer et des automatisations.
- *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*

  Contient des informations de présentation et de référence sur l'analyse et les passerelles, notamment la syntaxe du fichier de règles d'analyse et les commandes de passerelles.

- *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*

  Décrit comment exécuter des tâches d'administration et de visualisation d'événement à l'aide de Tivoli Netcool/OMNIbus Web GUI.

Accès en ligne à la terminologie

Le site Web de terminologie IBM regroupe la terminologie des bibliothèques de produits IBM dans un emplacement unique et pratique. Vous pouvez y accéder à l'adresse suivante :

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

Accès en ligne aux publications

IBM publie des publications sur ce produit et tous les autres produits lorsqu'ils sont disponibles et à chaque mise à jour, sur le site Web IBM Knowledge Center à l'adresse suivante :

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

Network Manager documentation sous le nœud **Cloud & Smarter Infrastructure** sur ce site Web.

Remarque : Si vous imprimez des documents PDF sur du papier autre qu'au format lettre, définissez l'option qui permet à votre application de lecture de PDF d'imprimer des pages au format lettre sur votre papier local dans la fenêtre **Fichier** > **Imprimer**.

Commande de publications

Vous pouvez commander de nombreuses publications IBM en ligne sur le site Web suivant :

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

Vous pouvez également passer votre commande par téléphone en composant l'un des numéros suivants :

- Au États-Unis : 800-879-2755
- Au Canada : 800-426-4968

Dans les autres pays, contactez votre représentant de compte logiciel pour commander des publications IBM. Pour connaître le numéro de téléphone de votre représentant local, procédez comme suit :

1. Accédez au site Web suivant :

   http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss
2. Sélectionnez votre pays dans la liste et cliquez sur **Go**. La page de **bienvenue d'IBM Publications Center** est affichée pour votre pays.
3. Dans la partie gauche de la page, cliquez sur **A propos de ce site** pour afficher la page d'informations qui comporte le numéro de téléphone de votre représentant local.

Accessibilité

Les fonctions d'accessibilité aident les utilisateurs ayant un handicap physique, comme les personnes à mobilité réduite ou à vue limitée, à utiliser les logiciels.

Fonctions d'accessibilité

Network Manager inclut les fonctions d'accessibilité majeures suivantes :

- Opérations qui utilisent un lecteur d'écran.

Network Manager utilise IBM Installation Manager pour installer le produit. Des informations relatives aux fonctions d'accessibilité d'IBM Installation Manager figurent à l'adresse https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Network Manager utilise la norme W3C la plus récente, http://www.w3.org/TR/wai-aria/, pour assurer la conformité avec http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-

the-section-508-standards/section-508-standards et http://www.w3.org/TR/WCAG20/. Pour tirer parti des fonctions d'accessibilité, utilisez la dernière version de votre lecteur d'écran de pair avec le navigateur Web le plus récent pris en charge par ce produit.

La documentation en ligne du produit Network Manager dans IBM Knowledge Center prend en charge les fonctions d'accessibilité. Les fonctions d'accessibilité d'IBM Knowledge Center sont décrites à la page https://www.ibm.com/support/knowledgecenter/v1/content/about/releasenotes.html#accessibility.

Navigation à l'aide du clavier

Ce produit utilise les touches de navigation standard.

Informations sur l'interface

Network Manager inclut les fonctions suivantes pour les utilisateurs malvoyants :

- Tout le contenu autre que textuel de l'interface graphique comporte un texte descriptif associé.
- Les utilisateurs malvoyants peuvent régler les paramètres d'affichage du système, notamment le mode de contraste élevé, et peuvent contrôler les tailles de police dans les paramètres de navigateur.
- La couleur n'est pas le seul moyen visuel de véhiculer les informations qui indiquent une action, demandent une réponse ou différencient un élément visuel.

Network Manager inclut les fonctions suivantes pour les utilisateurs atteints d'épilepsie photosensible :

- Les interfaces utilisateur de Network Manager ne contiennent pas d'animation qui clignote à une fréquence supérieure à deux fois par seconde.

L'interface utilisateur Web de Network Manager contient des repères de navigation WAI-ARIA dont vous pouvez vous servir pour naviguer rapidement jusqu'aux zones fonctionnelles de l'application.

Etapes supplémentaires permettant de configurer les fonctions d'accessibilité d'Internet Explorer

Si vous utilisez Internet Explorer comme navigateur Web, il se peut que vous deviez effectuer des étapes de configuration supplémentaires pour activer les fonctions d'accessibilité.

Pour activer le contraste élevé, procédez comme suit :

1. Cliquez sur **Outils** > **Options Internet** > **Accessibilité**.
2. Cochez toutes les case de la section Mise en forme.

Si vous ne parvenez pas à accroître la taille de la police lorsque vous cliquez sur **Affichage** > **Taille du texte** > **La plus grande**, cliquez sur **Ctrl +** et **Ctrl -**.

Autres informations sur l'accessibilité

Outre le centre d'assistance IBM standard et les sites Web de support, IBM a mis en place un service de téléscripteur permettant aux clients sourds ou malentendants d'accéder aux services commerciaux et de support :

Service TTY
800-IBM-3383 (800-426-3383)
(en Amérique du Nord)

IBM et l'accessibilité

Pour plus d'informations sur l'engagement d'IBM en matière d'accessibilité, voir https://www.ibm.com/able.

Formation technique Tivoli

Pour plus d'informations sur la formation technique Tivoli, visitez le site Web IBM Tivoli suivant :

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

Informations sur le support et la communauté

Les groupes d'utilisateurs Support IBM, SMC (Service Management Connect) et Tivoli vous permettent de contacter IBM pour obtenir l'aide et l'information dont vous avez besoin.

Support IBM

Si vous avez un problème avec votre logiciel IBM, vous voulez le résoudre rapidement. IBM founit les possibilités suivantes pour obtenir le soutient dont vous avez besoin :

En ligne
Accédez au site Service de support IBM à l'adresse https://www.ibm.com/support/home/ et suivez les instructions.

IBM Support Assistant
IBM Support Assistant (ISA) est un plan de travail de serviçabilité des logiciels local gratuit qui vous permet d'obtenir des réponses à vos questions et des solutions aux problèmes liés aux logiciels IBM. ISA offre un accès rapide aux informations de support et outils de serviçabilité pour l'identification des problèmes. Pour installer le logiciel ISA, accédez à https://www.ibm.com/support/knowledgecenter/SSLLVC/welcome/isa_welcome.html.

Service Management Connect

Accédez à Service Management Connect sur https://www.ibm.com/developerworks/community/groups/service/html/communitystart?communityUuid=cdd16df5-7bb8-4ef1-bcb9-cefb1dd40581. Utilisez Service Management Connect des manières suivantes :

- Impliquez-vous dans le développement transparent et ouvert de produits Tivoli avec d'autres utilisateurs et développeurs IBM. Vous pouvez accéder à des conceptions exclusives, des démonstrations de sprint, des feuilles de route de produits et un code de version préliminaire.
- Communiquez en tête-à-tête avec les experts pour collaborer et échanger à propos de Tivoli et de la communauté.
- Lisez des blogs pour tirer parti de l'expérience et de l'expertise des autres.
- Utilisez les wikis et les forums pour collaborer avec la communauté utilisateur.

Chapitre 1. Téléchargement Network Manager

La procédure pour le téléchargement du produit diffère pour des sorties General Availability (GA) et les correctifs fix packs.

Avant de commencer

Remarque : Si vous utilisez Network Manager comme partie d'une solution, vous devez aussi contrôler la compatibilité des versions de tous les produits composants dans la documentation de la solution. Par exemple, si vous utilisez Netcool Operations Insight, contrôlez la matrice de version de produit et composant de pour votre version de Netcool Operations Insight à https://www.ibm.com/support/knowledgecenter/en/SSTPTP.

Pourquoi et quand exécuter cette tâche

Pour télécharger le produit, repérez votre version dans le tableau suivant :

Tableau 1. Emplacement de téléchargement

Version de produit	Emplacement de téléchargement	Informations complémentaires
Version 4.2 groupe de correctifs 12 :	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm16364949
Version 4.2 groupe de correctifs 11	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm16257035
Version 4.2 groupe de correctifs 10	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm16233900
Version 4.2 groupe de correctifs 9 :	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm12984181
Version 4.2 groupe de correctifs 8 :	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm11099863
Version 4.2 groupe de correctifs 7 :	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=ibm10886151
Version 4.2 groupe de correctifs 6 :	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=ibm10794123

Tableau 1. Emplacement de téléchargement (suite)		
Version de produit	**Emplacement de téléchargement**	**Informations complémentaires**
Version 4.2 groupe de correctifs 5 :	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=swg24044739
Version 4.2 groupe de correctifs 4 :	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=swg24044399
Version 4.2 groupe de correctifs 3 :	Passport Advantage http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm	http://www.ibm.com/support/docview.wss?uid=swg24043360
Version 4.2 groupe de correctifs 2 :	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=swg24042981
Version 4.2 groupe de correctifs 1 :	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=swg24042425
4.2	Passport Advantage http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm	http://www.ibm.com/support/docview.wss?uid=swg24041283

Chapitre 2. Planification de l'installation

Consultez les remarques sur le déploiement et les exigences système relatives à Network Manager.

Avant de commencer

Vérifiez la documentation de planification de tous les autres produits que vous souhaitez intégrer à Network Manager. Par exemple, si vous installez IBM Tivoli Netcool Configuration Manager, consultez le manuel *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Remarque : Si vous utilisez Network Manager comme partie d'une solution, vous devez aussi contrôler la compatibilité des versions de tous les produits composants dans la documentation de la solution. Par exemple, si vous utilisez Netcool Operations Insight, contrôlez la matrice de version de produit et composant de pour votre version de Netcool Operations Insight à https://www.ibm.com/support/knowledgecenter/en/SSTPTP.

Déploiement de Network Manager

Ces informations sont utiles pour la configuration du déploiement physique de votre installation Network Manager.

Scénarios de déploiement

Le mode de déploiement de Network Manager dépend de votre environnement, et notamment de facteurs tels que la taille et la complexité de votre réseau et le nombre d'opérations nécessitant un accès système.

Vous trouverez ci-dessous des scénarios de déploiement de Network Manager standard :

- Déploiement de système éducatif ou de démonstration de petite taille
- Réseau client de petite taille
- Réseau client de taille moyenne
- Réseau client de grande taille
- Réseau client de très grande taille

Un scénario de déploiment ultérieur est le suivant : Réseau de fournisseur de services ou d'entreprise de télécommunications

Remarque : La reprise en ligne peut ensuite être appliquée à chacun de ces déploiements Network Manager.

Cette section vous aide lors de la prise de décision en matière de mode de déploiement de Network Manager. Pour obtenir des informations plus détaillées, voir les documents *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration* et *IBM Tivoli Network Manager IP Edition - Notes sur l'édition*.

Comparaisons de réseau et de déploiement

Ces informations permettent de comparer les réseaux client exemple et de comparer les déploiements Network Manager pour chaque réseau client exemple.

Comparaison des réseaux client

Utilisez ces informations pour comparer les exemples de réseaux client et identifier celui qui correspond le mieux à votre réseau.

Le tableau suivant répertorie les fonctions standard pour chacun des exemples de réseaux client. Ces valeurs sont fournies à titre d'exemple uniquement. Elles peuvent être différentes de celles de votre réseau. Vous devez en particulier noter les éléments suivants :

- En ce qui concerne les valeurs indiquées pour *Nombre moyen d'interfaces par périphérique* dans ce tableau, le nombre réel d'interfaces peut varier considérablement par rapport au nombre moyen spécifié. Un exemple est disponible dans les réseaux MPLS, où le nombre d'interfaces par périphérique est très élevé dans le réseau principal, mais peut ne pas être supérieur à deux ou trois interfaces par périphérique dans les périphériques extérieurs.
- En ce qui concerne le nombre de périphériques dans une entreprise de télécommunications, la valeur spécifiée (15 000) est une valeur moyenne. Une entreprise de télécommunications au niveau national comporte un nombre de périphériques bien plus élevé et une petite entreprise locale en aura beaucoup moins.

Tableau 2. Exemples de comparaison de réseaux client

Fonction	**Démonstration**	**Entreprise**				**Telco**
		Petite	**Moyenne**	**Grande**	**Très grande**	
Nombre de périphériques	25	150 à 300	250 à 5 000	5 000 à 15 000	15 000 à 30 000	15 000
Nombre moyen d'interfaces par périphérique	1-2	Entre 3 et 5	20-30	30 ou plus	30 ou plus	1 200
Emplacements réseau	Emplacement unique	Emplacement unique	Répartis	Réseau global	Réseau global, gestion répartie	Un ou plusieurs emplacements
Architecture de réseau	Non hiérarchique	Non hiérarchique	Non hiérarchique	Complexe	Complexe	Complexe
Nombre de clients d'interface graphique actifs	1 à 3	3	5 à 20	5 à 20	5 à 20	5 à 20
Exemples d'interrogation ping de boîtier	Valeurs définies à des fins de démonstration	Intervalles de 2 minutes	Entre 2 et 5 minutes	Entre 2 et 5 minutes	Entre 2 et 5 minutes	Entre 2 et 5 minutes
Exemples d'interrogation SNMP	Valeurs définies à des fins de démonstration	3 à 6 valeurs à des intervalles de 30 minutes	Intervalles de 5 à 15 minutes	Intervalles de 10 à 15 minute.	Intervalles de 15 minutes ou plus	5 valeurs à des intervalles de 5 minutes
	Interrogation SNMP v1, 2c ou 3 dans n'importe lequel des environnements répertoriés Interrogations de périphérique et d'interface dans l'un des environnements répertoriés.					
Intégrations de produits Tivoli	Aucun	Aucun	Aucun	Netcool Operations Insight TADDM	Netcool Operations Insight TADDM	Netcool Operations Insight TADDM

Comparaison des événements Network Manager

Utilisez ces informations pour comparer les déploiements Network Manager pour chacun des réseaux client exemples.

Le tableau suivant répertorie les paramètres requis pour les déploiements Network Manager pour chacun des réseaux client exemple. Ces valeurs sont fournies à titre d'exemple uniquement. Elles peuvent être différentes de celles adaptées à votre déploiement spécifique.

Remarque : Les valeurs indiquées pour *Déploiement* dans cette table ne prennent pas en compte les serveurs de reprise en ligne.

Tableau 3. Comparaison d'exemples de déploiement Network Manager

Paramètres	**Démonstration**	**Entreprise**				**Telco**
		Petite	**Moyenne**	**Grande**	**Très grande**	
Plateforme	Linux® x86	N'importe quelle plateforme prise en charge	N'importe quelle plateforme prise en charge	Linux	Linux	N'importe quelle plateforme prise en charge
Déploiement	Serveur unique	Serveur unique	1 à 2 serveurs	3 à 4 serveurs	4 serveurs ou plus	3 serveurs
Système client	Processeur unique 2 Go de mémoire DRAM minimum ou 4 Go de mémoire DRAM pour les réseaux étendus Environnement JRE et navigateur Internet pris en charge					
Base de données topologiques	Base de données par défaut	Base de données par défaut	DB2 ou SGBDR Oracle	DB2 ou SGBDR Oracle	DB2 ou SGBDR Oracle	DB2 ou SGBDR Oracle
Nombre de domaines réseau	1	1	1 - 2	2 ou plus	2 ou plus	1 - 2
Nombre de moteurs d'interrogation dépendant de la taille du réseau	1	1	Envisagez l'utilisation de plusieurs interrogateurs	Envisagez l'utilisation de plusieurs interrogateurs	Envisagez l'utilisation de plusieurs interrogateurs	Envisagez l'utilisation de plusieurs interrogateurs

Raisons pour lesquelles il existe plusieurs domaines

Il existe plusieurs raisons pour lesquelles il peut être nécessaire de partitionner votre réseau en plusieurs domaines.

Il peut être nécessaire de partitionner votre réseau en plusieurs domaines pour une des raisons suivantes :

- Votre réseau dépasse une certaine taille définie. Voir la section *Instructions relatives au nombre de domaines réseau* afin de déterminer si votre réseau requiert plusieurs domaines.
- La reconnaissance est un processus très long. Vous pouvez réduire cette durée en partitionnant votre réseau en plusieurs domaines.
- Les limites de fonctionnement imposent le besoin de plusieurs domaines. Les limites géographiques et de sécurité sont des limites de fonctionnement.
- Votre réseau contient des adresses IP se chevauchant.

Conseil :

Si vous avez l'intention d'exécuter des reconnaissances interdomaines pour visualiser les liens entre les différents domaines, vous devez étudier la manière dont les limites entre les domaines affectent les liens interdomaine. En particulier, veillez à bien choisir des limites de domaine avec un minimum de liens interdomaine.

Instructions relatives au nombre de domaines réseau

Si votre réseau dépasse une certaine taille, il peut être nécessaire de fractionner le réseau en plusieurs domaines. Ces informations permettent de définir le nombre de domaines réseau requis pour votre déploiement.

Suivant le système d'exploitation, un même domaine Network Manager peut prendre en charge environ 1 000 000 entités réseau créées lors d'une opération de reconnaissance. Les entités réseau comprennent les ports, les interfaces (y compris les éléments d'interface logique), les cartes, les emplacements et les boîtiers. Il est théoriquement possible d'inclure plus d'entités réseau dans un même domaine, mais la reconnaissance peut être assez longue.

Sous Linux 64 bits, la quantité maximale de mémoire autorisée pour un processus Network Manager n'est pas limitée de manière arbitraire, mais elle dépend de la quantité de mémoire installée sur le serveur.

En général, le processus de reconnaissance (ncp_disco) et le processus de modèle de topologie (ncp_model) utilisent la plupart de la mémoire.

Le nombre d'entités réseau créées par une opération de reconnaissance dépend du nombre de facteurs qui peuvent nécessiter que vous créiez et configuriez des domaines réseau supplémentaires. Ces facteurs comprennent les éléments suivants :

- Types de périphérique — Par exemple, un routeur Cisco NEXUS ou Juniper avec des instances de routeur virtuelles peut fournir des centaines de milliers d'entités réseau (ports, interfaces, cartes, emplacements, etc.) par boîtier.
- Type de réseau — Par exemple, une opération de reconnaissance effectuée sur un réseau local fournit généralement davantage d'entités réseau qu'un réseau étendu de taille semblable.
- Types d'agent de reconnaissance activé — Par exemple, les agents de reconnaissance Entity et JuniperBoxAnatomy sont des agents de reconnaissance basés sur des inventaires qui créent généralement des entités réseau supplémentaires que les autres agents ne créent pas.
- Réseau acheminé ou commuté — Par exemple, les réseaux commutés ont tendance à générer davantage d'entités réseau que les réseaux acheminés car ils contiennent des réseaux locaux virtuels, qui contiennent plusieurs entités.

La taille d'un domaine Network Manager peut dépendre des besoins métier. Par exemple, un client peut avoir besoin qu'une reconnaissance réseau soit effectuée à l'intérieur de périodes de maintenance quotidienne définies. Dans ce scénario, bien qu'un seul domaine Network Manager s'exécutant sur les systèmes UNIX puisse prendre en charge environ 400 000 entités réseau, la durée nécessaire à une reconnaissance de cette taille risque d’excéder la période de maintenance quotidienne. Il faut alors définir deux domaines sectorisés, prenant en charge chacun environ 200 000 entités de réseau, pour répondre à ce besoin métier.

La procédure suivante permet de déterminer le nombre de domaines requis. Pour obtenir des informations sur le mode de création et de configuration de domaines réseau supplémentaires, voir le document *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Remarque : Les calculs présentés ici incluent uniquement des chiffres approximatifs. Le nombre réel de domaines requis varie en fonction de divers facteurs et notamment des facteurs décrits précédemment.

1. Rassemblez les données suivantes :
   - Nombre de périphériques dans le réseau
   - Nombre moyen d'interfaces par périphérique

     Remarque : Le nombre réel d'interface sur un périphérique donné peut être très éloigné du nombre moyen d'interfaces. Un exemple est disponible dans les réseaux MPLS, où le nombre d'interfaces par périphérique est très élevé dans le réseau principal, mais peut ne pas être supérieur à deux ou trois interfaces par périphérique dans les périphériques extérieurs.

2. Appliquez l'équation suivante pour déterminer un nombre approximatif d'entités réseau :

   Nombre d'entités réseau = Nombre de périphériques * nombre d'interfaces moyen * *multiplicateur*

   Où :

   - *multiplicateur* = 2 pour un réseau acheminé
   - *multiplicateur* = 3,5 pour un réseau commuté

   Remarque : Les réseaux commutés ont tendance à générer plus d'entités réseau car ils contiennent des réseaux virtuels locaux qui contiennent plusieurs entités.
3. Appliquez l'équation suivante pour déterminer le nombre suggéré de domaines réseau :

   Nombre de domaines requis = (Nombre d'entités réseau) / 1000,000

   Remarque : Le nombre maximal d'entités réseau indiqué ne constitue qu'une estimation approximative de la taille des domaines. Le nombre réel d'entités réseau par domaine varie en fonction de divers facteurs et notamment des facteurs décrits précédemment.

Client de type routeur

Les données de ce client sont les suivantes :

- Nombre de périphériques dans le réseau 60.000
- Nombre moyen d'interfaces par périphérique 20

Ce réseau client génère approximativement 400000 entités réseau :

Nombre d'entités réseau = 60 000 x 20 x 2 = 2 400 000

Selon le calcul suivant, ce réseau requiert *trois* domaines réseau :

Nombre de domaines requis = 2,400 000 / 1 000 000 > 2

Client de type commutateur

Les données de ce client sont les suivantes :

- Nombre de périphériques dans le réseau 1.000
- Nombre moyen d'interfaces par périphérique 24

Le réseau de ce client produira aproximativement 84 000 entités réseau :
Nombre d'entités réseau = 1 000 * 24 * 3,5 = 84 000

Sur la base du calcul suivant, ce réseau nécessite *un* domaine réseau :
Nombre de domaines requis = 84 000 / 1 000 000 < 1

Concepts associés

Domaines réseau
Avant l'installation, vous devez déterminer si vous souhaitez partitionner votre réseau en domaines ou si vous souhaitez conserver un domaine unique pour l'ensemble de votre réseau. Un domaine réseau est une collection d'entités réseau définie pour être reconnue et gérée.

Déploiement de système éducatif ou de démonstration

Il s'agit d'une petite installation à utiliser en tant que système de démonstration ou à des fins éducatives ou de formation.

Les sections suivantes décrivent ce réseau de manière détaillée et incluent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

Cet environnement se compose d'environ 25 périphériques réseau et de serveurs de clés. Tous les périphériques se trouvent à un emplacement, sur le même sous-réseau que les périphériques à gérer. Il

existe une session client d'interface graphique locale prise en charge par la machine qui héberge les composants du produit Network Manager. Il peut exister une ou deux sessions client d'interface graphique sur d'autres machines. Les périphériques réseau proviennent de plusieurs fournisseurs. L'architecture réseau n'est pas hiérarchique. Tous les périphériques sont connectés à un réseau local et ont des connexions Fast Ethernet. A des fins de démonstration uniquement, plusieurs périphériques réseau disposent de SNMPv3 et plusieurs postes de travail d'IPv6.

Dans l'environnement, les conditions suivantes s'appliquent :

- 1 à 3 clients d'interface graphique actifs.
- L'interrogation ping de boîtier et des activités d'interrogation SNMP sont requises.
- Aucun produit Tivoli principal n'est intégré au système, autre que le produit Tivoli Netcool/OMNIbus requis.
- Des rapports de performances sont requis pour de courtes périodes de collecte de données (généralement, 1 à 5 jours) en fonction de la durée de la formation.

Déploiement de Network Manager

Un déploiement de serveur unique est suffisant pour ce type d'environnement. En plus de la description du déploiement à serveur unique disponible ici, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Le système est une machine de classe de poste de travail d'entrée, avec 8 Go de mémoire, de préférence un processeur double coeur mais un processeur comportant un seul coeur est admis, une vitesse de processeur en cours raisonnable et une fonction Fast Ethernet.
- Base de données par défaut utilisée pour la base de données NCIM.
- Système client : processeur unique, 4 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau client de petite taille

Ce client est une entreprise avec un réseau se composant d'environ 150-300 périphériques réseau et de serveurs principaux. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs.

Les sections suivantes décrivent ce réseau de manière détaillée et incluent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

Les principaux utilisateurs du produit sont les membres de l'équipe de gestion du réseau. Tous les périphériques se trouvent à un seul emplacement et sont gérés par une équipe comportant peu de membres. Les périphériques réseau proviennent de plusieurs fournisseurs. Un mélange de périphériques réseau de couche 2 et 3 sont présents. 20 à 30 réseaux VLAN sont définis. L'architecture réseau est relativement simple. Tous les périphériques à gérer se trouvent dans le même réseau que le système Network Manager et ont des connexions Fast Ethernet. Les connexions Internet transitent via un pare-feu et l'accès aux systèmes dans le réseau protégé est disponible via un réseau VPN d'entreprise. L'équipe de gestion du réseau assure la connexion des clients via un des moyens suivants : réseau local, connexions WiFi ou via un réseau VPN établi par un fournisseur de services de télécommunication. Les modifications réseau ont lieu une fois par mois et une nouvelle reconnaissance est alors anticipée.

Dans l'environnement, les conditions suivantes s'appliquent :

- 3 clients d'interface graphique actifs.
- Interrogation ping de boîtier à des intervalles de deux minutes. Interrogation SNMP à des intervalles de 30 minutes. Généralement, l'interrogation est requise pour trois à six valeurs MIB SNMP.
- Aucun produit Tivoli principal n'est intégré au système, autre que le produit Tivoli Netcool/OMNIbus requis.

Déploiement de Network Manager

Un déploiement de serveur unique est suffisant pour ce type d'environnement. En plus de la description du déploiement à serveur unique disponible ici, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Un domaine réseau unique est suffisant pour un réseau de cette taille.
- Le système peut être une des plateformes prises en charge. Le système requiert 16 Go de mémoire, un processeur quadricoeur et plusieurs disques physiques dans une configuration RAID 5.
- Système client : processeur unique, 4 Go de mémoire, navigateur Internet et JRE pris en charge
- Base de données par défaut utilisée pour la base de données NCIM.
- Un moteur d'interrogation ncp_poller unique est suffisant pour cet environnement.
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau client de taille moyenne

Ce client est une entreprise avec un centre de données central principal et des connexions à différents sites distants. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs.

Les sections suivantes décrivent ce réseau de manière détaillée et incluent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

Ce réseau contient entre 250 et 5000 périphériques réseau et serveurs principaux importants. Les postes de travail ne sont pas gérés lorsque leur nombre est supérieur à 1 000. Les périphériques réseau proviennent de plusieurs fournisseurs. Tous les périphériques de l'emplacement central ont des connexions Fast Ethernet ou Gigabit Ethernet. Les sites distants sont connectés via des liaisons WAN. Les périphériques et les serveurs à gérer sont répartis entre le site central et les sites distants.

Dans l'environnement, les conditions suivantes s'appliquent :

- Il existe 5 à 20 clients d'interface graphique actifs.
- Interrogation ping de boîtier à des intervalles de deux à cinq minutes. Interrogation SNMP à des intervalles de 5 à 15 minutes.
- Autres principaux produits Tivoli intégrés au système, autres que le produit Tivoli Netcool/OMNIbus requis.

Déploiement de Network Manager

Chaque environnement client avec ce type de réseau est différent. La clé du succès est une mémoire appropriée et une connaissance approfondie des cibles d'interrogation, des taux d'interrogation combinés et des taux d'événement. Les paramètres de déploiement suivants sont appropriés pour ce type d'environnement.

- Un ou plusieurs domaines réseau sont requis, en fonction de la taille du réseau.
- Déploiement à un seul serveur (jusqu'à 250 périphériques réseau et 5 à 10 utilisateurs simultanés)

  Quatre processeurs.
  Jusqu'à 32 Go de mémoire.
  Plusieurs disques physiques dans une configuration RAID 5.
- Déploiement à deux serveurs (jusqu'à 5000 périphériques réseau et 1 à 20 utilisateurs simultanés).

  Quatre processeurs pour le système avec Network Manager.
  Quatre processeurs pour le système avec Tivoli Netcool/OMNIbus et Dashboard Application Services Hub.
  Jusqu'à 32 Go de mémoire pour chaque serveur.
  Plusieurs disques physiques dans une configuration RAID 5.

- Le système peut être une des plateformes prises en charge.
- Système client : processeur unique, 4 Go de mémoire, navigateur Internet et JRE pris en charge
- DB2 ou SGBDR Oracle utilisé pour la base de données NCIM sur le serveur avec 4 processeurs et 32 Go de mémoire RAM.
- Nombre de moteurs d'interrogation :

  Déploiement sur un serveur unique 1
  Déploiement sur deux serveurs Un interrogateur pour les opérations ping de châssis, un ou plusieurs interrogateurs pour les interrogations SNMP.
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau client de grande taille

Ce client est une entreprise de grande taille avec un réseau globalement déployé. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs et de prendre en charge les périphériques et l'architecture réseau les plus récents.

Les sections suivantes décrivent ce réseau de manière détaillée et incluent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

L'architecture du réseau est complexe et contient la technologie la plus récente. Par exemple, le réseau contient des réseaux centraux MPLS. Le nombre de périphériques réseau est compris entre 5 000 et 15 000. La présence d'au moins 30 ports par périphérique indique qu'il s'agit d'un réseau complexe. Les opérations réseau sont effectuées à partir d'un emplacement central avec une équipe surveillant en permanence le réseau central. Les périphériques réseau proviennent de plusieurs fournisseurs.

Dans l'environnement, les conditions suivantes s'appliquent :

- Il existe généralement 5 à 20 clients d'interface graphique actifs simultanément.
- Interrogation :

  Interrogation ping de boîtier à des intervalles de deux à cinq minutes.
  Interrogation SNMP à des intervalles de 10-15 minutes.
  Interrogation SNMPv3 des périphériques réseau principaux
  Interrogation SNMPv1 pour le traçage de graphique en temps réel ainsi que pour le stockage des rapports de performances.
- Autres principaux produits Tivoli intégrés au système, autres que le produit Tivoli Netcool/OMNIbus requis :

  IBM® Tivoli Business Service Manager (TBSM)
  IBM Tivoli Application Dependency Discovery Manager (TADDM)

Déploiement de Network Manager

Les choix de déploiement varient en fonction de la taille du réseau. Pour le réseau à 5000 périphériques de cette plage de clients, le déploiement peut comporter un seul serveur ou deux serveurs. Les facteurs clé pour la réussite incluent le temps de réponse réseau pour les cibles (à condition qu'il s'agisse d'une distribution pays ou globale des périphériques cible), la disponibilité de la mémoire sur les serveurs de prise en charge, l'interrogation sélectionnée et la fréquence d'interrogation.

Pour la partie supérieure du réseau (15 000 périphériques environ), un déploiement distribué comportant plusieurs domaines est requis. En plus de la description du déploiement à plusieurs serveurs disponible à un autre emplacement, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Déploiement de deux domaines.
- Déploiement d'un serveur de base de données dédié.
- Chaque serveur requiert les éléments suivants :

8 processeurs.
Jusqu'à 128 Go de mémoire.
3 disques, grappe de disques multiple RAID 5

- Pour les systèmes utilisés, effectuez le déploiement de la manière suivante :

  Serveur 1 : Network Manager avec 36 Go de mémoire.
  Serveur 2 : Tivoli Netcool/OMNIbus et Dashboard Application Services Hub avec jusqu'à 12 Go de mémoire.
  Serveur 3 : SGBDR sélectionné par le client (DB2 ou Oracle) avec jusqu'à 84 Go de mémoire.
- Systèmes à déployer sur la plateforme Linux ou UNIX.
- DB2 ou SGBDR Oracle utilisé pour la base de données NCIM.
- Deux moteurs d'interrogation :

  Utilisez le processus ncp_poller par défaut pour l'interrogation ping de boîtier.
  Créez un élément ncp_poller séparé pour les interrogations SNMP.
- Système client : processeur unique, 4 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau client de très grande taille

Ce client est une entreprise globale de très grande taille avec une architecture réseau simple mais un grand nombre de périphériques. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs et de prendre en charge la planification de capacité à court terme.

Les sections suivantes décrivent ce réseau de manière détaillée et incluent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

La gestion réseau est effectuée à partir d'un emplacement central et à partir d'emplacements régionaux. Le réseau est très grand et contient plus de 15 000 périphériques réseau et serveurs importants Les périphériques réseau proviennent de plusieurs fournisseurs. Les périphériques sont rassemblés en deux catégories :

- Infrastructure de périphériques réseau avec un nombre d'interfaces supérieur ou égal à 30 par périphérique.
- Périphériques gérés avec 1 à 2 interfaces par périphérique.

La plupart des périphériques se trouvent dans la deuxième catégorie (périphériques gérés). Pour gérer un réseau de cette taille, le réseau est partitionné pour la gestion sur une base géographique.

Dans cet environnement, les conditions suivantes s'appliquent :

- Il existe 5 à 20 clients d'interface graphique actifs.
- Interrogation :

  Interrogation ping de boîtier à des intervalles de deux à cinq minutes.
  Interrogation SNMP à des intervalles égaux ou supérieurs à 15 minutes.
  Collecte de données SNMPv1
- Autres principaux produits Tivoli à intégrer au système, autres que le produit Tivoli Netcool/OMNIbus requis :

  IBM Tivoli Business Service Manager
  IBM Tivoli Application Dependency Discovery Manager

Déploiement de Network Manager

Une assistance d'un groupe de services IBM expérimentés ou d'un partenaire métier IBM qualifié est hautement recommandée pour que le déploiement puisse aboutir. Plusieurs domaines sont requis, pris en charge par une collecte de serveurs individuels ou s'exécutant sur un système de très grande taille. Après avoir effectué une enquête du réseau à gérer, fractionnez le réseau en sections facilement gérables, puis définissez chacune de ces sections comme étant un domaine. En plus de la description du déploiement à plusieurs serveurs disponible à un autre emplacement, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Plusieurs domaines réseau.
- Sélection de plateforme : Linux et UNIX
- Les systèmes de grande taille (grand nombre de processeurs et quantité de mémoire importante) peuvent héberger plusieurs domaines tant que les allocations de mémoire et le nombre de processeurs sont acceptables.

  Mémoire 32 à 64 Go par domaine
  Processeurs : 4 à 8 par domaine en fonction des charges de travail
- DB2 ou SGBDR Oracle utilisé pour la base de données NCIM.
- Deux moteurs d'interrogation pour chaque domaine :

  Utilisez le processus ncp_poller par défaut pour l'interrogation ping de boîtier.
  Créez un élément ncp_poller séparé pour les interrogations SNMP.
- Les limitations de mémoire de processus individuel constituent un facteur dans cet environnement. Si vous utilisez AIX, activez un accès étendu à la mémoire.
- Système client : processeur unique, 4 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau d'entreprise de télécommunications

Ce client est une société de télécommunications et un fournisseur de services Internet. L'objectif de cette installation est de gérer ce réseau client en signalant 24 heures sur 24 et 7 jours sur 7 à l'équipe de production les principales erreurs.

Les sections suivantes décrivent ce réseau de manière détaillée et incluent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

Le réseau à gérer contient environ 600 périphériques réseau avec un nombre moyen d'interfaces par périphérique égal à 500. Il s'agit d'un réseau MPLS. Par conséquent, le nombre d'interfaces des périphériques réseau est élevé et les périphériques réseau sont complexes. Les périphériques réseau proviennent de plusieurs fournisseurs. Tous les périphériques se trouvent à un seul emplacement ou à plusieurs emplacements et sont gérées par une équipe comportant peu de membres. Tous les périphériques à gérer sont connectés via Fast Ethernet ou Gigabit Ethernet.

Dans l'environnement, les conditions suivantes s'appliquent :

- Nombre de clients simultanément actifs : 11 à 12
- Exigences d'interrogation : interrogation ping de boîtier à des intervalles de 2 à 5 minutes ; interrogation SNMP de cinq valeurs à des intervalles de 5 minutes.
- Certaines interrogations SNMPv3 sont en place.
- Autres principaux produits Tivoli intégrés au système, autres que le produit Tivoli Netcool/OMNIbus requis :

  IBM Tivoli Business Service Manager (TBSM)
  IBM Tivoli Application Dependency Discovery Manager (TADDM)

- Rapports de performances effectués une fois par jour pour les principaux périphériques, utilisés pour la création des rapports de capacité hebdomadaires.

Déploiement de Network Manager

Un déploiement à trois serveurs est requis pour ce type d'environnement. En plus de la description du déploiement à plusieurs serveurs disponible à un autre emplacement, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Un ou deux domaines.
- Un déploiement à trois serveurs est recommandé.
- Spécifications du système

  Système 1 (sur lequel Network Manager est installé) : quatre processeurs, 32 à 64 Go de mémoire, deux disques ou plus. Notez qu'au delà de quatre processeurs ou coeurs de processeur, la vitesse d'horloge des coeurs et la mémoire cache intégrée peuvent s'avérer plus importantes que des coeurs supplémentaires. La règle générale est la suivante : sélectionnez les 4 coeurs les plus rapides avant les autres coeurs.
  Système 2 : (où Dashboard Application Services Hub et Tivoli Netcool/OMNIbus sont installés) quatre processeurs, 16 Go de mémoire, deux disques ou plus
  Système 3 : serveur de base de données, quatre processeurs, 16 Go de mémoire
- DB2 ou SGBDR Oracle utilisé pour la base de données NCIM.
- Deux moteurs d'interrogation :

  Utilisez le processus ncp_poller par défaut pour l'interrogation ping de boîtier.
  Créez un élément ncp_poller séparé pour les interrogations SNMP.
- Système client : processeur unique, 4 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau d'entreprise de télécommunications sans fil LTE 4G

Ce client est une importante société de télécommunications sans fil offrant des services de téléphonie sans fil 4G à l'aide de leur infrastructure LTE (Long term Evolution). L'objectif de cette installation est de gérer ce réseau client en signalant 24 heures sur 24 et 7 jours sur 7 à l'équipe de production les principales erreurs.

Les sections ci-après offrent des recommandations afin qu'un déploiement de Network Manager répondent aux besoins de ce réseau.

Description

Le réseau à géré contient environ 5000 périphériques eNodeB, avec 3000 autres périphériques qui se trouvent dans le réseau EPC (Evolved Packet Core) associé ou qui servent de routeurs de raccordement mobiles. Le nombre d'entités Network Manager reconnues pour ce réseau est généralement le suivant :

- Pour les périphériques eNodeB : environ 20 à 25 entités par périphérique eNodeB.
- Pour les périphériques de raccordement et réseau EPC : environ 10 à 15 entités par périphérique.

Le périphérique eNodeB LTE et le matériel associé sont fournis par plusieurs fournisseurs dont la complexité et l'échelle peuvent varier. Ces périphériques sont distribués dans de nombreux endroits, ce qui est normal pour un réseau mobile 4G. Tous les périphériques à gérer sont connectés à l'aide de Fast Ethernet ou Gigabit Ethernet. Les données d'inventaire réseau et topologiques reconnues par Network Manager proviennent de systèmes EMS spécifiques aux fournisseurs et sont traitées par les collecteurs Network Manager spécifiques aux fournisseurs correspondants.

Dans cet environnement, les conditions suivantes s'appliquent généralement :

- Nombre de clients GUI simultanément actifs : 5 à 20

- Exigences d'interrogation : aucune car les données topologiques sont reçues du système EMS et par conséquent, les périphériques ne sont pas interrogés.

Déploiement de Network Manager

Un déploiement à trois composants est requis pour ce type d'environnement.

1. Composants centraux de Network Manager.
2. Dashboard Application Services Hub et Cognos Analytics.
3. Base de données topologiques NCIM.

Ces trois composants peuvent être déployés sur des serveurs (un ou plusieurs) ou des machines virtuelles (une ou plusieurs). Un seul domaine est suffisant pour ce type d'environnement. De plus, les paramètres de déploiement suivants sont appropriés :

- Composants principaux de Network Manager
  - 4 à 6 processeurs.
  - Environ 20 Go de mémoire.
  - 50 Go d'espace disque.
- Dashboard Application Services Hub et Cognos Analytics
  - 4 à 6 processeurs.
  - 6 à 8 Go de mémoire.
  - 20 Go d'espace disque.
- Base de données topologiques NCIM
  - Quatre processeurs.
  - 10 Go de mémoire.
  - Au moins 50 Go d'espace disque configurés dans une configuration RAID appropriée, pour fournir le niveau requis de tolérance aux pannes, de fiabilité et de performances.
  - DB2 ou toute autre plateforme de base de données prise en charge.

En outre, le système de client d'interface graphique utilisateur suivant est approprié :

- Un seul processeur.
- 3 Go de mémoire.
- Environnement JRE et navigateur Internet pris en charge.

Remarques relatives au déploiement

Vous pouvez déployer l'ensemble de l'installation Network Manager sur un serveur unique ou dans une installation répartie.

Au cours d'une installation de Network Manager, vous installez un certain nombre de composants Network Manager et notamment les suivants :

Composants principaux de Network Manager
Ce composant est constitué des processus Network Manager centraux suivants : reconnaissance de réseau, interrogation, analyse de la cause première et enrichissement des événements.

base de données NCIM
Cette base de données stocke les données de topologie.

Tivoli Netcool/OMNIbus
Ce composant est constitué du logiciel de gestion des événements Tivoli Netcool/OMNIbus. Un grand nombre de clients optent pour un système de génération de ticket d'incident intégré à Tivoli Netcool/OMNIbus.

Composants d'interface graphique de Network Manager
Ce composant inclut l'infrastructure d'interface graphique de Dashboard Application Services Hub, les composants Interface graphique Web, Jazz for Service Management et Java™.

Autres composants
Les autres composants incluent les Cognos Analytics et les rapports Network Manager.

L'installation a pour objet de placer ces composants sur un ou plusieurs serveurs.

Restriction : Vous devez utiliser ensemble différentes versions des mêmes produits ou composants, à moins que vous ayez été avisé d'agir autrement selon des instructions dans IBM Knowledge Center ou par IBM Support. Si vous avez besoin de plusieurs instances d'un produit ou composant, vous devez les installer ou mettre à niveau la version et les correctifs. Vous devez également veiller à ce que le même ensemble de correctifs de test soit installé le cas échéant. Par exemple, si vous avez besoin de plusieurs instances de Network Manager GUI Components dans un déploiement, veillez à ce qu'elles mettent en œuvre la même version, le même correctif, et les même correctifs de test.

Les configurations de déploiement standard de Network Manager sont les suivantes :

- Déploiement sur un serveur unique
- Déploiement réparti : deux serveurs ou plus

Les facteurs qui exigent un nombre croissant de serveurs dans un déploiement réparti incluent les suivants :

- Débits d'événements actifs
- Quantité et débit des données d'interrogation stockées
- Début d'interrogation du statut d'unité et nombre de cibles d'interrogation
- Temps de réponse du réseau pour les cibles interrogées
- Fréquence de reconnaissance et
- Taille du réseau à reconnaître (pour chaque domaine comportant plusieurs domaines)

Remarque : Ces configurations de déploiement ne prennent pas en compte les exigences d'intégrations d'autres produits.

De plus, vous devez prendre en compte le déploiement des systèmes appropriés pour prendre en charge les sessions client d'interface graphique.

Par ailleurs, le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Déploiement sur un serveur unique

Les déploiements sur un serveur unique sont adaptés aux systèmes de démonstration ou de formation de petite taille et pour les systèmes devant prendre en charge des réseaux client de petite ou de moyenne taille.

Restriction : La limitation d'un déploiement sur un serveur unique contraint à mettre à niveau Tivoli Netcool/OMNIbus et Network Manager en même temps. Toutes les mises à niveau vers des éditions majeures doivent être effectuées simultanément afin d'éviter les problèmes de compatibilité. Une édition majeure est une édition possédant sa propre documentation, par exemple Tivoli Netcool/OMNIbus V8.1.0. Les fixpacks peuvent être appliqués à des moments différents.

Déploiement réparti : deux serveurs ou plus

Dans les déploiements répartis, les composants Network Manager sont répartis sur plusieurs serveurs, c'est-à-dire sur deux serveurs ou plus. Voici quelques instructions concernant les déploiements répartis :

- Les déploiements sur deux serveurs concernent la gamme supérieure de la famille de réseaux client de taille moyenne.

- Les déploiements peuvent exiger trois serveurs ou plus dans les situations où il existe plusieurs domaines réseau.
- Les déploiements sur trois serveurs peuvent également être appliqués dans le cas où un serveur séparé est requis pour prendre en charge un produit de base de données relationnelle qui fournit un stockage des données de topologie. De plus, un serveur de base de données séparé autorise la base de données relationnelle à prendre en charge plusieurs applications, en plus de Network Manager.

Déploiement sur deux serveurs

Un exemple de déploiement sur deux serveurs est constitué de l'allocation suivante de postes de travail hôte :

- *Serveur 1* : Composants centraux Network Manager, Tivoli Netcool/OMNIbus, et base de données NCIM. Les composants centraux sont les composants de reconnaissance de réseau, d'interrogation, d'analyse de la cause première et d'enrichissement des événements.
- *Serveur 2* : Dashboard Application Services Hub avec applications Web Network Manager associées.

Déploiement sur trois serveurs

Un exemple de déploiement sur trois serveurs est constitué de l'allocation suivante de postes de travail hôte :

- *Serveur 1* : Composants centraux Network Manager.
- *Serveur 2* : Tivoli Netcool/OMNIbus
- *Serveur 3* : Dashboard Application Services Hub avec les applications web Network Manager associées, ainsi que la base de données NCIM.

Systèmes client

Vous devez prendre en compte le déploiement de systèmes appropriés pour prendre en charge les sessions client d'interface graphique.

La spécification système suivante permet de prendre en charge une gamme plus large d'activités d'utilisateur final dans les sessions client d'interface graphique :

- Ecran plus large permettant un affichage plus confortable avec une résolution plus élevée (par exemple, 1280x1024)
- Processeur à un ou deux coeurs à la vitesse en cours
- 3 Go de mémoire
- Environnement JRE et navigateur Internet pris en charge
- Fast Ethernet.
- Spécification du processeur :

  Pour les affichages de topologie normaux ou les affichages d'événements
  Processeur unique avec les vitesses suivantes : 1 GHz ou supérieur, comme sur de nombreux ordinateurs portables, 2,4 GHz comme sur de nombreux postes de travail

  Durée supérieure pour l'affichage de mappes de topologie plus complexes et de plus grande taille et l'affichage avancé de graphiques MIB
  Processeur de dernière génération (3,0 GHz ou supérieur) généralement disponible sur les systèmes de classe de poste de travail les plus récents.

Exemples de déploiements

Utilisez ces exemples de Network Manager pour planifier votre architecture de déploiement.

Exemple d'architecture de déploiement simple

Cet exemple vous permet de vous familiariser avec l'architecture d'un déploiement simple de Network Manager.

Composants

Cet exemple de déploiement simple comporte les composants suivants :

- Une paire virtuelle ObjectServer.
- Un serveur Dashboard Application Services Hub.
- Une installation Network Manager exécutant un domaine avec reprise en ligne.
- Une instance de la base de données topologiques NCIM.

La figure suivante présente l'architecture pour ce déploiement.

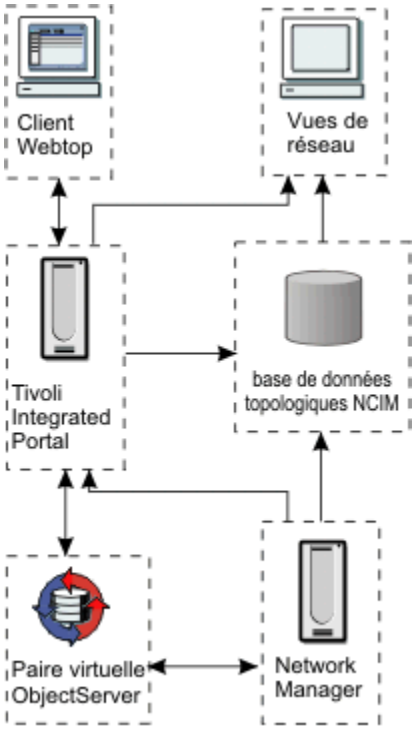

Figure 1. Architecture de déploiement simple

Allocation des postes de travail hôte

La figure suivante illustre l'allocation des postes de travail hôtes pour ce déploiement.

Remarque : Si votre topologie est très importante, vous pouvez installer la base de données topologiques sur un serveur distinct. Ce choix dépend des spécifications de vos machines et de la répartition de la charge souhaitée.

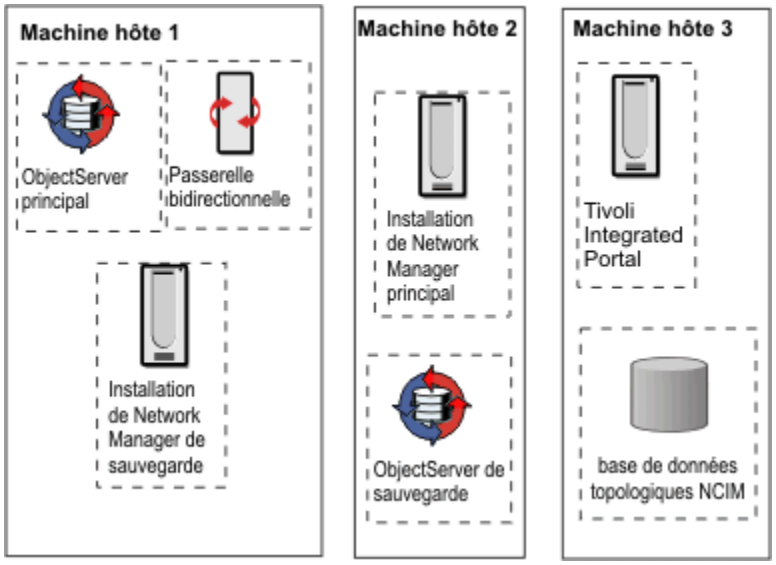

Figure 2. Allocation de machine hôte de déploiement simple

Etapes d'installation d'un déploiement simple

Les étapes ci-après présentent les tâches requises pour ce déploiement et permettent de planifier un déploiement similaire. .

Pour installer le déploiement décrit ci-dessus, procédez comme suit :

1. Installez la base de données topologiques sur la machine hôte 3, créez les tables nécessaires et lancez la base de données.

   Remarque : La base de données topologiques doit être installée et démarrée avant le démarrage des composants centraux de Network Manager afin de pouvoir sauvegarder les données de reconnaissance.
2. Installez les composants ObjectServer et les composants liés suivants :
   a. Installez le serveur ObjectServer principal et la passerelle bidirectionnelle sur la machine hôte 1.
   b. Installez l'ObjectServer de sauvegarde sur la machine hôte 2.
3. Configurez et exécutez les serveurs ObjectServer.

   Remarque : Ces derniers doivent être en cours d'exécution avant le démarrage des composants centraux de Network Manager.
4. Installez les composants centraux du Network Manager principal sur la machine hôte 2.
5. Installez les composants centraux du Network Manager de sauvegarde sur la machine hôte 1.
6. Installez l'environnement GUI Network Manager sur la machine hôte 3. L'environnement GUI inclut les logiciels suivants :
   - WebSphere Application Server
   - Dashboard Application Services Hub
   - Composants d'interface graphique de Network Manager
   - Tivoli Netcool/OMNIbus Web GUI
   - Cognos Analytics

   Conseil : Les performances de la machine sont meilleures si vous installez Dashboard Application Services Hub sur une machine où aucun autre produit n'est installé.

   Remarque : Les composants centraux de Network Manager doivent être installés avant l'infrastructure d'interface graphique de Network Manager.
7. Configurez le Network Manager principal pour la reprise en ligne et démarrez-le.

8. Configurez le Network Manager de sauvegarde pour la reprise en ligne et démarrez-le.

Exemple d'architecture de déploiement de grande taille

Utilisez cet exemple pour vous familiariser avec l'architecture d'un déploiement Network Manager de grande taille.

Composants

Ce déploiement exemple comprend :

- Un serveur d'objets et une installation Network Manager à Londres. Le domaine de Londres envoie des événements et la topologie à San Francisco.
- Un serveur d'objets et une installation Network Manager à New York. Le domaine de New York envoie également des événements et une topologie à San Francisco.
- Un serveur d'objets et une installation Dashboard Application Services Hub à San Francisco. Le serveur d'objets de San Francisco consolide les événements issus de Londres et New York. Le serveur Dashboard Application Services Hub de San Francisco peut accéder à la topologie depuis Londres et New York, mais ne consolide pas les topologies. Les clients répartis dans le monde entier peuvent se connecter au serveur Dashboard Application Services Hub et afficher la topologie depuis Londres et New York.

La figure suivante présente l'architecture pour ce déploiement.

Remarque : Pour un déploiement important de ce type, le temps d'attente du réseau étendu doit être pris en compte. Cela est particulièrement important si le programme d'interrogation doit stocker une grande quantité de données historiques

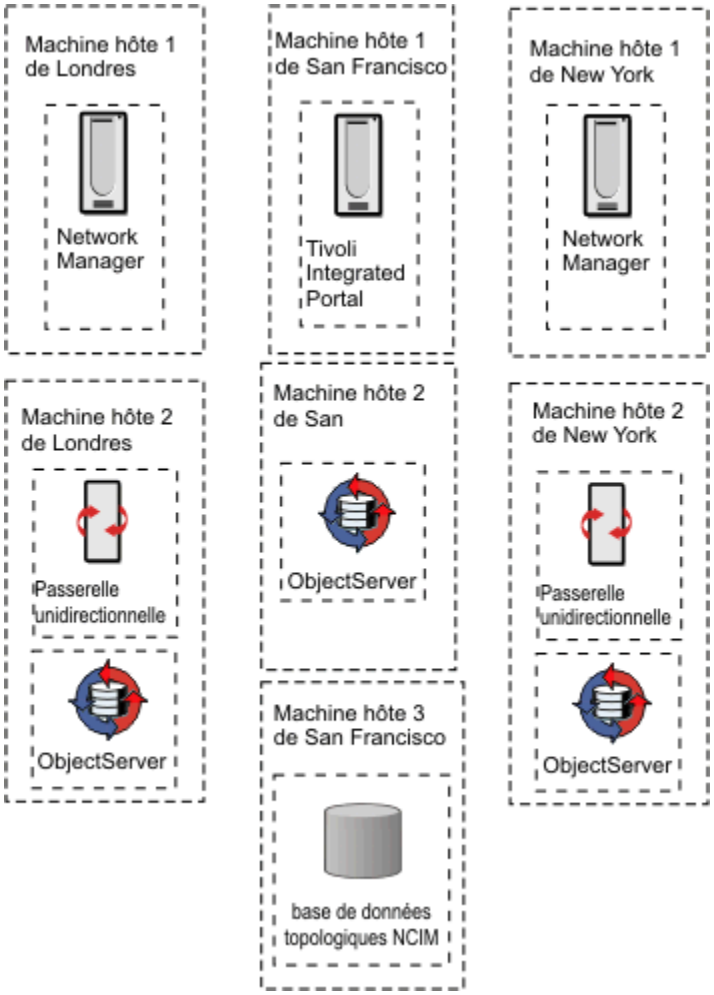

Figure 3. Architecture de déploiement large

Allocation des postes de travail hôte

La figure suivante présente un exemple d'allocation de serveurs pour ce déploiement.

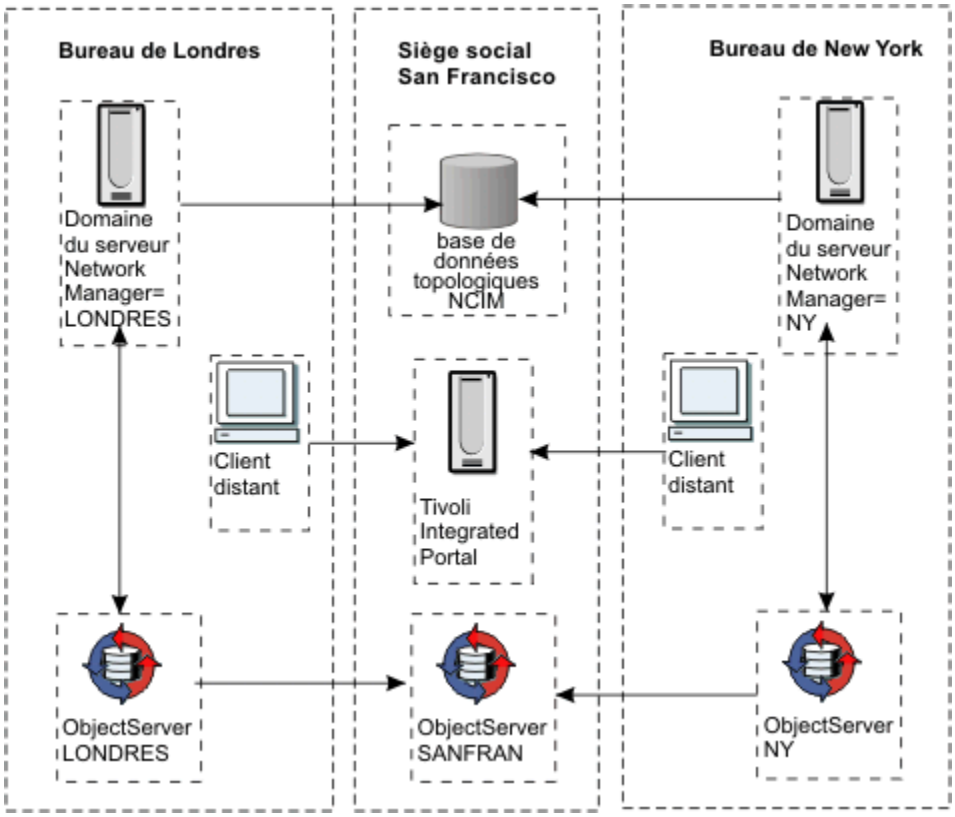

Figure 4. Allocation de machine hôte de déploiement large

Etapes d'installation d'un déploiement de grande taille

Les étapes ci-après présentent les tâches requises pour ce déploiement et permettent de planifier un déploiement similaire. .

Remarque : Si vous installez des serveurs d'applications Web et de composants de base Network Manager distribués dont les fuseaux horaires sont différents, vous devez définir le même fuseau horaire sur tous les serveurs et notamment sur le serveur de base de données, les serveurs de base et les serveurs d'interface graphique. Ainsi, Network Manager pourra effectuer des comparaisons d'horodatages précises pour des processus se trouvant sur différents serveurs. Vous devez aussi avertir les utilisateurs, comme les opérateurs réseau, que le système peut afficher des heures différentes de celle du lieu où ils se trouvent.

Pour installer ce déploiement, accomplissez les étapes suivantes :

1. Installez la base de données topologiques sur la machine hôte 3 de San Francisco et créez les tables de base de données nécessaires.

   Remarque : La base de données topologiques doit être installée et démarrée avant le démarrage des composants centraux de Network Manager afin de pouvoir sauvegarder les données de reconnaissance.
2. Installez les composants ObjectServer et les composants liés suivants :
   - Installez ObjectServer sur la machine hôte 2 de San Francisco.
   - Installez le serveur ObjectServer et la passerelle unidirectionnelle sur la machine hôte 2 de Londres.
   - Installez le serveur ObjectServer et la passerelle unidirectionnelle sur la machine hôte 2 de New York.
3. Configurez et exécutez les serveurs ObjectServer.

   Remarque : Ces derniers doivent être en cours d'exécution avant le démarrage des composants centraux de Network Manager.

4. Installez les composants principaux de Network Manager sur la machine hôte 1 de Londres.

   Remarque : Les composants centraux de Network Manager doivent être installés avant les applications Web.
5. Installez les composants principaux de Network Manager sur la machine hôte 1 de New York.
6. Installez l'environnement GUI Network Manager sur la machine hôte 3. L'environnement GUI inclut les logiciels suivants :
   - WebSphere Application Server
   - Dashboard Application Services Hub
   - Composants d'interface graphique de Network Manager
   - Tivoli Netcool/OMNIbus Web GUI
   - Cognos Analytics

   Conseil : Les performances de la machine sont meilleures si vous installez Dashboard Application Services Hub sur une machine où aucun autre produit n'est installé.

   Remarque : Les composants centraux de Network Manager doivent être installés avant l'infrastructure d'interface graphique de Network Manager.

Vérification des prérequis du système

Vous devez vérifier les prérequis du système avant d'essayer d'installer Network Manager ou des produits connexes.

Pourquoi et quand exécuter cette tâche

Vous pouvez effectuer une vérification préliminaire de l'environnement matériel et logiciel sur le serveur sur lequel vous souhaitez installer Network Manager ou des produits connexes sans télécharger ces produits. Pour faire cette vérification, vous pouvez utiliser IBM Prerequisite Scanner, qui est un logiciel distinct. Cette vérification préliminaire vous permet de savoir si vous devez mettre à niveau le matériel ou configurer le système d'exploitation avant d'installer vos produits.

En plus des vérifications effectuées par IBM Prerequisite Scanner, le programme d'installation Network Manager exécute ses propres vérifications lorsque vous tentez d'installer vos produits. IBM Prerequisite Scanner Peut vérifier les prérequis de nombreux produits. Le programme d'installation de Network Manager vérifie uniquement les prérequis des produits que vous avez choisi d'installer.

Important : Les vérifications automatiques ne peuvent pas se substituer à une bonne compréhension du matériel, du logiciel et des autres prérequis décrits dans la documentation. Certains prérequis dépendent de votre réseau ou du déploiement et ne peuvent pas être automatisés.

Pour vérifier la configuration système requise pour les composants principaux et des composants d'interface graphique de Network Manager 4.2, vous devez télécharger le scanner et les fichiers de configuration mis à jour. Consultez les instructions à l'emplacement suivant : https://www.ibm.com/support/pages/node/727673

Pour savoir comment utiliser IBM Prerequisite Scanner avec d'autres produits, reportez-vous à la documentation d'installation de ces produits.

Résultats

Les résultats de la vérification s'affichent, indiquant si le serveur est adapté à l'installation des composants de votre choix.

Domaines réseau

Avant l'installation, vous devez déterminer si vous souhaitez partitionner votre réseau en domaines ou si vous souhaitez conserver un domaine unique pour l'ensemble de votre réseau. Un domaine réseau est une collection d'entités réseau définie pour être reconnue et gérée.

Restriction : Utilisez uniquement des caractères alphanumériques et des traits de soulignement (_) pour les noms de domaine. Tous les autres caractères, notamment le trait d'union le (-), ne sont pas autorisés.

Raisons pour lesquelles partitionner un réseau en plusieurs domaines

Le partitionnement de votre réseau en plusieurs domaines vous permet de reconnaître votre réseau par section. Voici les raisons possibles du partitionnement de votre réseau.

- Scalabilité : Votre réseau peut être trop grand pour être reconnu en une fois.
- Géographie : Vous pouvez éventuellement vouloir diviser votre réseau en régions géographiques, chacune correspond alors à un domaine.
- Bordures logiques de réseau : Vous pouvez éventuellement vouloir reconnaître et gérer le réseau selon des bordures réseau particulières.

Les domaines reconnus peuvent être contrôlés indépendamment.

Vous pouvez exécuter plusieurs domaines afin d'effectuer plusieurs reconnaissances de réseau. De plus, plusieurs processus Network Manager peuvent fonctionner indépendamment sur le même serveur s'ils appartiennent à différentes domaines.

Identification du domaine d'un événement

L'identification du domaine des événements permet aux vues réseau et de tronçon de générer la mappe topologique correcte pour cet événement.

Le domaine dans lequel un événement se produit peut être identifié des manières suivantes :

- En utilisant un domaine par ObjectServer et le nom du serveur ObjectServer pour identifier le domaine dans lequel l'événement s'est produit.
- Si vous utilisez plusieurs domaines par ObjectServer, les sondes de chaque domaine doivent être configurées pour permettre à l'événement lui-même de comporter des informations qui identifient le domaine. Cette approche permet à plusieurs domaines Network Manager d'être connectés à un seul ObjectServer.

Concepts associés

Instructions relatives au nombre de domaines réseau
Si votre réseau dépasse une certaine taille, il peut être nécessaire de fractionner le réseau en plusieurs domaines. Ces informations permettent de définir le nombre de domaines réseau requis pour votre déploiement.

Tâches associées

Création et configuration de domaines réseau supplémentaires
Pour ajouter des domaines réseau supplémentaires, configurez le contrôle de processus des domaines et enregistrez ces derniers avec la base de données topologiques NCIM. Les configurations et les interrogations peuvent être copiées depuis des domaines existants. Configurez ou reconfigurez les vues de réseau pour afficher les périphériques dans les nouveaux domaines.

Collecte des événements à l'aide de plusieurs domaines par ObjectServer

Vous pouvez connecter plusieurs domaines Network Manager à un même serveur ObjectServer.

Dans cette configuration, les sondes Tivoli Netcool/OMNIbus collectent les informations relatives au nom du domaine lorsqu'un événement est généré et renseignent la zone NmosDomainName afin de conserver ce nom de domaine.

Pour implémenter cette configuration, vous devez d'abord modifier tous les fichiers de règles d'analyse de Tivoli Netcool/OMNIbus pour garantir que chaque événement contienne une zone `NmosDomainName`. Cette zone est utilisée pour stocker le nom de domaine associé à l'événement. Ceci garantit aussi que l'événement est traité par la passerelle d'événements.

Remarque : Par défaut, le filtre d'événement entrant dans la passerelle d'événements gère aussi bien les systèmes à domaine unique que ceux à domaines multiples. Pour plus d'informations, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Remarque : Cette approche est plus économique car elle ne nécessite qu'un seul ObjectServer. L'évolutivité peut être un problème car chaque nouveau domaine nécessite la configuration d'une sonde supplémentaire.

La figure suivante illustre un exemple d'architecture utilisant plusieurs domaines par ObjectServer.

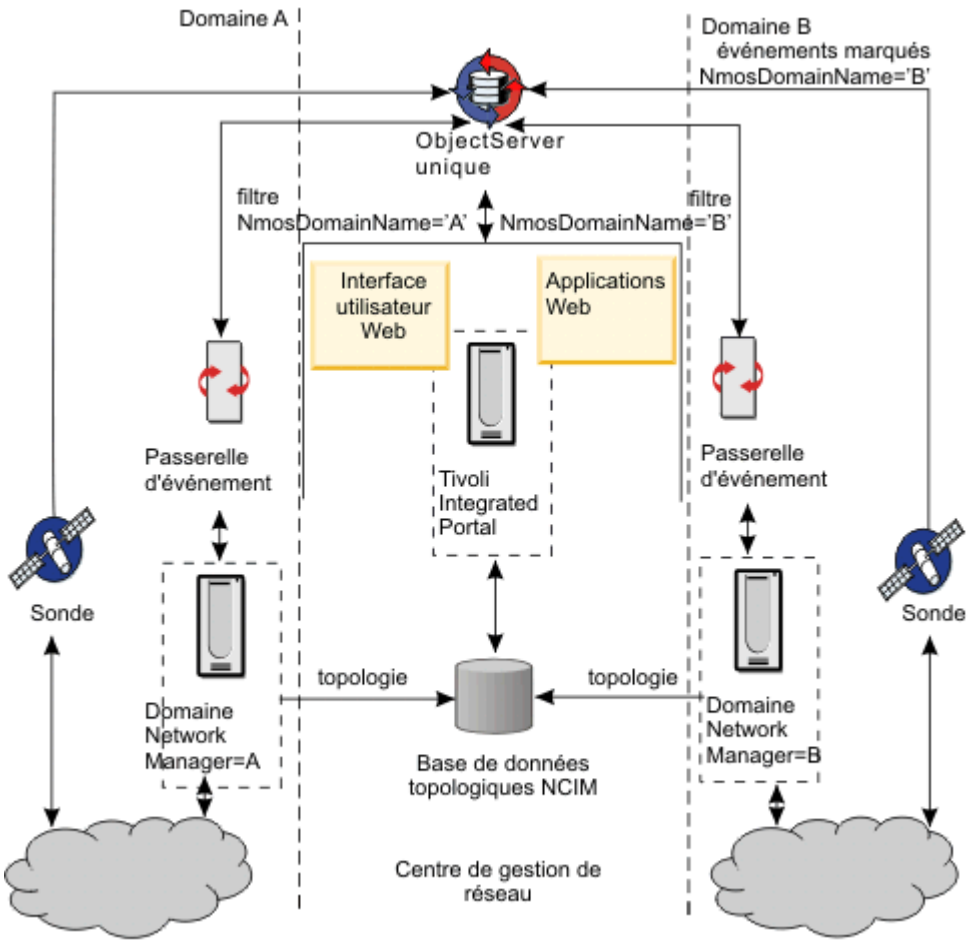

Figure 5. Gestion de la propriété d'événement : architecture pour un serveur d'objet de domaine unique

Exemple d'affichage d'une topologie depuis plusieurs domaines

Les clients Web utilisant un Dashboard Application Services Hub unique peuvent afficher la topologie depuis plusieurs domaines Network Manager.

Domaines multiples contenus dans une seule base de données topologiques

Pour activer la visualisation de topologie de plusieurs domaines, chaque domaine Network Manager transmet les informations de topologie à la base de données topologiques NCIM (Network Connectivity and Inventory Model). Lorsque vous disposez de plusieurs domaines, la topologie de chaque domaine est stockée dans la base de données NCIM.

Lien des domaines reconnus

Vous pouvez trouver des liens entre les périphériques dans différents domaines, en configurant et exécutant une reconnaissance interdomaine.

La figure suivante montre un exemple de trois domaines de reconnaissance fournissant des données à une seule base de données topologiques NCIM. Tous les clients Web connectés à Dashboard Application Services Hub peuvent afficher les mappes topologiques dans n'importe lequel des domaines en choisissant un seul domaine dans le menu du domaine.

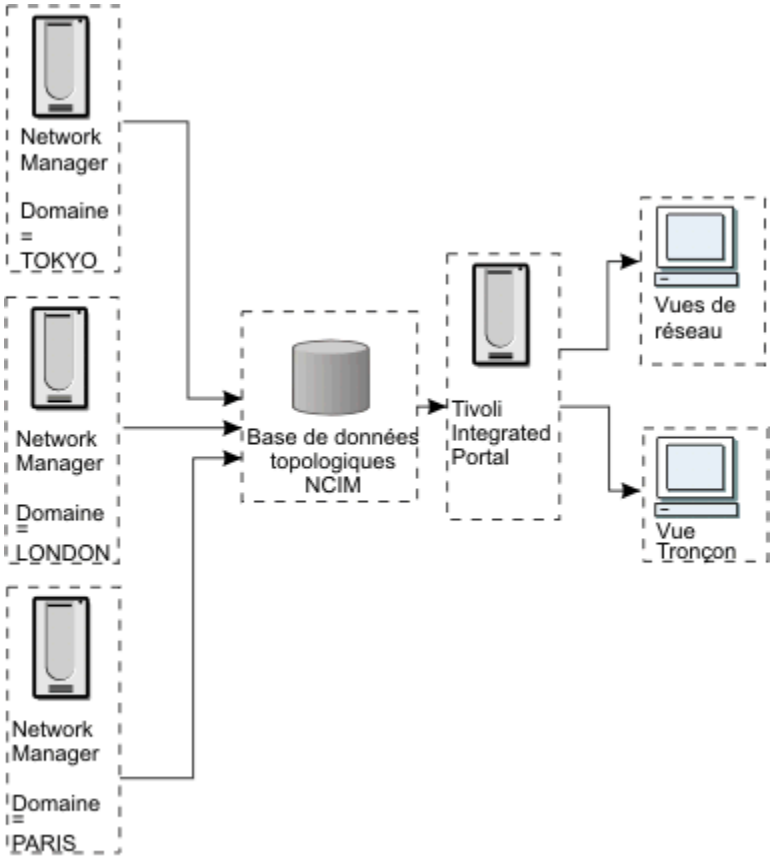

Figure 6. Affichage de la topologie depuis plusieurs domaines

Si les reconnaissances interdomaines ont été exécutées, un domaine agrégé est créé dans la base de données de topologie, qui comprend des collections de périphérique de tous les domaines reconnus. Tous les clients Web connectés à Dashboard Application Services Hub peuvent afficher les mappes topologiques dans tous les domaines en choisissant le domaine AGGREGATION dans le menu du domaine.

Pour plus d'informations sur l'affichage de la topologie, consultez le guide *Network Manager Topology Visualization Guide*.

Configuration matérielle requise

La configuration matérielle requise varie suivant la taille et la composition de votre réseau ainsi que les fonctions de Network Manager que vous souhaitez utiliser.

Vérifiez que vos serveurs disposent de la configuration matérielle requise avant d'installer Network Manager.

Important : N'exécutez aucune autre application nécessitant beaucoup de ressources pendant l'installation de Network Manager.

Directives pour le choix des processeurs

Lisez les directives pour le choix des processeurs avant de sélectionner le serveur approprié pour y installer Network Manager.

Les directives présentées ici concernent les serveurs destinés seulement à prendre en charge des composants Network Manager. Les directives supposent que d'autres produits Tivoli, notamment IBM Tivoli Monitoring, et IBM Tivoli Business Service Manager, sont déployés sur d'autres serveurs. Pour combiner le déploiement de plusieurs produits majeurs sur un même serveur, additionnez les spécifications minimales pour chaque produit (consultez la documentation de chacun des produits pour plus d'informations).

Pour les petits réseaux et les déploiements de démonstration ou de formation, utilisez deux processeurs au moins sur toutes les plateformes. Les déploiements de réseaux de taille moyenne ou grande requièrent quatre processeurs ou plus.

Remarque : Pour les processeurs multicoeurs, la vitesse individuelle des coeurs peut être plus importante que le nombre de coeurs. Si des processeurs de n'importe quelle vitesse peuvent être utilisés, le choix de la vitesse de coeur la plus rapide et de la mémoire cache intégrée la plus grande apporte une différence significative quant à la taille du réseau à reconnaître et à interroger.

Pour les paramètres virtualisés (pris en charge par des partitions logiques (LPAR) AIX, VMWare ESX, etc.), utilisez des ressources processeur et mémoire fixes pour un système virtuel prenant en charge Network Manager.

Pour les paramètres Linux on IBM z Systems, utilisez l'allocation de processeur équivalente à celle de deux processeurs modernes, depuis n'importe quelle plateforme UNIX ou Windows native prise en charge par Network Manager.

Pour plus d'informations sur le choix des processeurs et sur les autres considérations en matière de déploiement, voir «Déploiement de Network Manager», à la page 3.

Configuration requise pour l'exécution du programme d'installation

Pour permettre l'installation de composants de l'interface graphique de Network Manager, votre serveur doit être conforme à la configuration matérielle requise pour IBM Installation Manager.

En plus de ces prérequis, consultez les prérequis de votre version d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Espace requis pour l'installation en tant que superutilisateur

Certains répertoires doivent disposer d'un certain espace libre afin d'exécuter le programme d'installation, quels que soient les composants installés. Si vous installez Network Manager en tant que superutilisateur, vous devez respecter les exigences suivantes :

- Au moins 1 Go d'espace dans le répertoire `/tmp` sur le serveur des composants de l'interface graphique.
- Au moins 1 Go d'espace dans le répertoire `/var`.
- Si vous installez Network Manager dans un autre emplacement que `/opt`, vous devez disposer d'au moins 50 Mo d'espace dans le répertoire `/opt`.
- Au moins 10 Go d'espace dans l'emplacement de données d'IBM Installation Manager. Vous choisissez l'emplacement des données pendant l'installation d'IBM Installation Manager. Cet emplacement est celui où les packages sont décompressés pendant l'installation et où ils sont stockés pour l'annulation.

Espace requis pour l'installation en tant qu'utilisateur non superutilisateur

Si vous installez Network Manager en tant que superutilisateur, vous devez respecter les exigences suivantes :

- Au moins 1 Go d'espace dans le répertoire `/tmp` sur le serveur des composants de l'interface graphique.
- Au moins 350 Mo d'espace dans le répertoire de base.
- Au moins 10 Go d'espace dans l'emplacement de données d'IBM Installation Manager. Vous choisissez l'emplacement des données pendant l'installation d'IBM Installation Manager. Cet emplacement est celui où les packages sont décompressés pendant l'installation et où ils sont stockés pour l'annulation.

Exigences relatives aux composants centraux

Pour installer et exécuter les composants centraux de Network Manager vos serveurs doivent disposer de la configuration matérielle minimale.

Exigences relatives à la mémoire

Vérifiez que les serveurs sur lesquels vous souhaitez exécuter Network Manager répondent aux exigences suivantes concernant la mémoire.

- Pour un déploiement sur un seul serveur, sur lequel les composants centraux, les applications Web, la base de données topologiques Network Manager et Tivoli Netcool/OMNIbus se trouvent sur le même serveur, vous avez besoin d'au moins 16 Go de mémoire vive dynamique.
- Pour un déploiement distribué où seuls les composants principaux de Network Manager sont installés sur le serveur, vous avez besoin d'un minimum de 8 Go de mémoire DRAM.

Il s'agit d'exigences minimales, la quantité de mémoire requise pouvant varier selon la taille du réseau à gérer et la manière de déployer Network Manager. Pour plus d'informations, voir «Déploiement de Network Manager», à la page 3.

Espace disque requis

Vérifiez que le serveur sur lequel vous souhaitez installer Network Manager dispose de l'espace disque requis.

- 5 Go d'espace disque pour stocker le logiciel
- 4 Go d'espace disque par domaine pour stocker le cache
- Comme estimation de référence pour les fichiers journaux, si l'on considère que chaque fichier journal a une taille d'1 Go et que le niveau de débogage complet est défini pour six processus, 24 Go d'espace disque sont nécessaires. (6 processus x 4 fichiers journaux ou de trace chacun = 24 fichiers journaux ou de trace X 1 Go = 24 Go).
- 50 Go d'espace disque libre pour exécuter Network Manager.

Il s'agit de valeurs minimales données à titre indicatif, la quantité d'espace disque requise pouvant varier selon la taille du réseau à gérer et la manière de déployer Network Manager. Pour plus d'informations, voir «Déploiement de Network Manager», à la page 3.

Remarque :

Pour un système de production que vous prévoyez d'utiliser sur le long terme, vous devez disposer de suffisamment d'espace disque supplémentaire pour stocker les fichiers générés par l'exploitation des produits, par exemple les fichiers d'annulation. Si vous installez les composants principaux de Network Manager et Tivoli Netcool/OMNIbus, vous avez besoin d'au moins 400 Go d'espace sur la partition où les produits sont installés.

Exigences relatives à la bande passante

Le serveur Network Manager nécessite une connexion Fast Ethernet bidirectionnelle de 100 Mbps (ou équivalent) avec le serveur DNS.

Il est nécessaire que les systèmes prenant en charge des composants Network Manager soient placés dans le centre de données avec des connexions de réseau local Fast Ethernet 100 Mbps ou Gigabit

Ethernet au système DNS et au périphérique du réseau central à reconnaître et à gérer. Des vitesses de connexion moins rapides peuvent être utilisées, mais elles peuvent avoir un impact sur les temps de réponse des sessions clientes et doivent être adaptées aux charges de travail principales telles que l'interrogation (y compris les temps de réponse, le nombre de tentatives et le trafic réseau total induit).

Remarque : Lors de la reconnaissance d'un périphérique réseau, de nombreuses requêtes SNMP sont effectuées pour ce périphérique. Après la reconnaissance, l'interrogation de routine (ICMP et SNMP) peut induire un trafic significatif sur le réseau. Avec un réseau bénéficiant des vitesses des réseaux locaux modernes, ces charges de travail peuvent être prises en charge.

Pour plus d'informations sur les spécifications de bande passante pour la reconnaissance, voir «Exigences en bande passante de la reconnaissance», à la page 39.

Autres exigences

Une unité de DVD-ROM est également nécessaire, si vous n'installez pas le logiciel depuis un téléchargement.

Configuration requise pour les composants de l'interface graphique

Le serveur sur lequel vous installez les composants de l'interface graphique de Network Manager doit répondre aux critères matériels suivants.

Conseils d'utilisation sur le long terme de l'espace disque pour tous les composants de l'interface graphique et les produits connexes

Pour un système de production que vous prévoyez d'utiliser pendant une durée prolongée, vous devez disposer de suffisamment d'espace disque supplémentaire pour stocker les fichiers générés par l'exploitation des produits, par exemple les fichiers d'annulation. Si vous installez les composants de l'interface graphique de Network Manager, Dashboard Application Services Hub, Cognos Analytics, et Tivoli Netcool/OMNIbus Web GUI, vous avez besoin d'au moins 100 Go d'espace sur la partition sur laquelle sont installés les produits.

Configuration matérielle requise pour l'installation des composants de l'interface graphique de Network Manager

Pour permettre l'installation des composants principaux de l'interface graphique de Network Manager, votre serveur doit être conforme aux exigences suivantes :

- 5,5 Go d'espace disque libre.
- Un minimum de 4 Go de mémoire DRAM.

  Remarque : Le programme d'installation vérifie qu'un minimum de 3 Go de mémoire DRAM est disponible pour les déploiements de système de démonstration et de formation. Un minimum de 4 Go de mémoire DRAM est cependant requis dans les environnements de production.
- 500 Mo dans le répertoire `/tmp`.
- Unité de DVD-ROM si l'installation n'est pas effectuée à partir d'un téléchargement.

Configuration matérielle requise pour l'installation de Cognos Analytics

Pour activer les rapports de gestion de réseau, vous devez avoir installé Cognos Analytics. Cognos Analytics est un composant optionnel devant être installé séparément pour permettre la fontionnalité de production de rapports de Network Manager.

Examinez la configuration matérielle requise pour Cognos Analytics pour vous assurer de répondre à vos exigences en matière de performance.

Important : Vérifiez que vous disposez au moins 17 Go d'espace disque libre dans l'emplacement où vous souhaitez installer Cognos Analytics.

Pour des informations détaillées, référez-vous aux informations relatives aux exigences matérielles pour votre version de Cognos Analytics dans Cognos Analytics Knowledge Center à : https://www.ibm.com/support/knowledgecenter/SSEP7J.

Configuration requise pour le serveur de base de données topologiques

Lisez les informations sur les spécifications de la base de données topologiques de Network Manager.

Espace disque requis

Pour stocker des données Network Manager, assurez-vous de disposer de l'espace disque minimal suivant disponible pour votre base de données topologiques :

- 3 à 5 Go pour DB2.
- 3 à 5 Go pour Oracle.

Remarque : Ces chiffres correspondent à des valeurs minimales. L'espace disque réel requis dépend de la taille de votre réseau et de la quantité de données stockées. Le stockage de données de performance peut nécessiter une grande quantité d'espace disque. Si vous prévoyez de stocker de grandes quantités de données, prévoyez 50 Go pour l'espace disque relatif à Network Manager.

Dans le cas d'un réseau volumineux contenu dans un seul domaine, vous devez disposer de 5 Go pour les données topologiques et d'un total de 50 Go pour couvrir également le stockage des données. Pour plus d'informations sur la planification du déploiement de Network Manager pour votre réseau, y compris les considérations de taille et de domaines, voir «Déploiement de Network Manager», à la page 3.

Vérifiez que les disques du serveur où vous voulez exécuter la base de données topologiques répondent aux spécifications suivantes :

- Trois disques en configuration RAID 1 (davantage de disques pour RAID 5)
- Disques SATA ou SCSI grande vitesse

Espace disque pour les événements et les interfaces

Vous devez calculer et prévoir de l'espace disque supplémentaire pour les événements et les interfaces de votre installation.

Configuration matérielle supplémentaire pour Network Manager :

- 4 Ko d'espace disque pour chaque événement attendu, par jour de stockage requis
- 4 Ko d'espace disque pour chaque interface ou port d'une unité gérée

Par exemple, si vous disposez de 5 000 ports sur les unités de votre réseau, que vous attendez 3 000 événements par jour et que ces derniers doivent être stockés pendant 30 jours, vous avez besoin de :

```
3000 * 30 * 4 KB = 360 MB
```

L'espace disque total requis est donc de :

```
512 Mo + 512 Mo de mémoire cache + 360 Mo + (4 Ko * 5 000) = 1,4 Go
```

Spécifications d'espace de permutation (UNIX)

Sur les plateformes UNIX, vous devez vous assurer de disposer de l'espace disque libre approprié qui est configuré pour être utilisé comme espace de permutation.

La quantité exacte d'espace de permutation nécessaire dépend de la taille et de la composition de votre réseau et du type de reconnaissance. Pour les quantités inférieures de mémoire RAM, vous avez besoin de quantités proportionnellement supérieures d'espace de permutation. Les chiffres suivants montrent la quantité approximative d'espace de permutation selon la quantité de mémoire RAM physique.

4 Go de mémoire RAM
Configurez 10 Go d'espace de permutation.

8 Go de mémoire RAM
Configurez 16 Go d'espace de permutation.

12 Go de mémoire RAM
Configurez 18 Go d'espace de permutation.

Pour les quantités de mémoire RAM supérieures à 12 Go, configurez la même quantité d'espace de permutation. Par exemple, pour 24 Go de mémoire RAM, configurez 24 Go d'espace de permutation.

Exigences en mémoire de la reconnaissance

Lors de la reconnaissance de réseaux de très grandes tailles, le processus de reconnaissance (ncp_disco) et le processus de modèle de topologie (ncp_model) utilisent la plupart de la mémoire. Si votre réseau est de taille très importante, pensez à le diviser en plusieurs domaines.

Concepts associés

Instructions relatives au nombre de domaines réseau
Si votre réseau dépasse une certaine taille, il peut être nécessaire de fractionner le réseau en plusieurs domaines. Ces informations permettent de définir le nombre de domaines réseau requis pour votre déploiement.

Configuration logicielle

La configuration logicielle requise dépend du système d'exploitation,des produits et des fonctions de Network Manager que vous souhaitez utiliser.

Exigences de compatibilité pour d'autres produits

Vérifiez que la configuration requise des produits intégrés à Network Manager est respectée.

Produits requis par Network Manager

Les produits et composants suivants sont requis par Network Manager. Network Manager requiert des versions spécifiques de ces produits.

Remarque : Si vous utilisez Network Manager comme partie d'une solution, vous devez aussi contrôler la compatibilité des versions de tous les produits composants dans la documentation de la solution. Par exemple, si vous utilisez Netcool Operations Insight, contrôlez la matrice de version de produit et composant de pour votre version de Netcool Operations Insight à https://www.ibm.com/support/knowledgecenter/en/SSTPTP.

Java Runtime Environment (JRE)

Network Manager n'installe pas de JRE. Il utilise le JRE qui est installé par d'autres produits, comme WebSphere Application Server. Vous devez utiliser le JRE approprié pour la combinaison de produits ou de composants qui sont installés sur l'un des serveurs.

Network Manager lui-même, nécessite Java 8 ou ultérieur, pour les versions 4.2 Fix Packs 8 et 9. Il change la version par défaut de Java utilisée par WebSphere Application Server en Java 8. Pour Network Manager version 4.2 Fix Pack 10 ou ultérieur, le Java Development Kit est disponible dans le paquet pour utiliser WebSphere Application Server.

Si vous n'utilisez pas une version correcte de Java, vous pourriez voir des messages d'erreur similaires à ce qui suit :

```
ERROR IBM WebSphere SDK Java Technology Edition is not installed or selected to be
installed.
```

Avant d'installer Network Manager Fix Pack 8 ou 9, faites en sorte que Java 8 soit installé dans WebSphere. Listez les Kits de Développement Java disponibles en exécutant la commande suivante :

```
/opt/IBM/WebSphere/AppServer/bin/managesdk.sh -listAvailable
```

Si la sortie de commande n'inclut pas une ligne similaire à la suivante: `CWSDK1005I SDK name: 1.8_64`, téléchargez Java 8 ici : https://www.ibm.com/support/pages/ibm-websphere-java-sdks-websphere-application-server-v85514#SDK80, ajoutez le fichier zip en tant que répertoire à IBM Installation Manager, et utilisez l'option **Install** pour installer la nouvelle version de JDK.

Tivoli Netcool/OMNIbus

Network Manager requiert Tivoli Netcool/OMNIbus. Il prend en charge les versions suivantes de Tivoli Netcool/OMNIbus :

- version 7.4
- Version 8.1, Fix Pack 23 ou version ultérieure

Tivoli Netcool/OMNIbus Web GUI

Network Manager prend en charge Tivoli Netcool/OMNIbus Web GUI V8.1 Fix Pack 11 Fix Pack 20 ou version supérieure.

Dashboard Application Services Hub

Network Manager nécessite Dashboard Application Services Hub Version 3.1.3.8 ou ultérieures.

IBM Websphere Application Server

Network Manager requiert IBM Websphere Application Server Version 8.5.5.17 (version 8) ou 9.0.5.5 (version 9) ou ultérieur.

Remarque : Si vous voulez utiliser WebSphere Application Server version 9, vous devez avoir une nouvelle installation de WebSphere Application Server version 9, Network Manager Fix Pack 11 et Tivoli Netcool/OMNIbus Web GUI Version 8.1.0.20 ou ultérieur. Ceci parce que le chemin de mise à niveau n'est pas disponible pour WebSphere Application Server depuis la version 8 à la version 9.

IBM Websphere SDK

Network Manager nécessite IBM Websphere SDK Java Technology Edition Version 8.

IBM Installation Manager

Network Manager requiert IBM Installation Manager V1.9.1.3 ou ultérieur. Sur SuSE Linux V11 et V12 pour System z, seule la version 32 bits d'IBM Installation Manager est prise en charge.

Jazz for Service Management

Network Manager requiert Jazz for Service Management V1.1.3.8 ou ultérieur.

Versions précédentes de Network Manager

Installez Network Manager 4.2 dans un répertoire différent de Network Manager V4.1.1 ou version antérieure.

Exigences pour les produits compatibles avec Network Manager

Important : Ces exigences s'ajoutent notamment aux autres exigences relatives au matériel, aux logiciels, au répertoire d'installation et à l'utilisateur. Ces exigences sont présentées dans la documentation du produit. Avant d'installer un produit, assurez-vous d'en comprendre tous ses pré-requis et exigences.

Cognos Analytics

Si vous voulez exécuter des rapports, et installez Network Manager Reports, vous avez également de Cognos Analytics V11.

- Fix Pack 11 À partir de 4.2 Fix Pack 11, Tivoli Common Reporting n'est plus pas pris en charge. Vous devez utiliser Cognos Analytics.

- Fix Pack 1 Pour 4.2 Fix Pack 1, Tivoli Common Reporting V3.1.3.0. Jazz for Service Management V1.1.3.0 contient Tivoli Common Reporting V3.1.3.0.
- Pour la version 4.2 GA, Tivoli Common Reporting V3.1.2 Fix Pack 1. Jazz for Service Management V1.1.2.1 conteint Tivoli Common Reporting V3.1.2.

Important : Vérifiez que vous disposez au moins 17 Go d'espace disque libre dans l'emplacement où vous souhaitez installer Cognos Analytics.

IBM Tivoli Netcool Configuration Manager

Network Manager prend en charge IBM Tivoli Netcool Configuration Manager 6.4.2 ou ultérieure.

IBM Tivoli Monitoring

Network Manager est compatible avec IBM Tivoli Monitoring version 6.3 FP 2 ou une version ultérieure on AIX, Linux ou Windows. L'agent lui-même (IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition) s'exécute uniquement sous Linux et AIX, car la plateforme Windows n'est pas prise en charge pour Network Manager 4.2.

Remarque : IBM Tivoli Monitoring version 6.3 Fix Pack 2 est fourni avec le package Network Manager V4.2.

IBM Tivoli Business Service Manager

Network Manager prend en charge IBM Tivoli Business Service Manager 6.1.1.

IBM Tivoli Application Dependency Discovery Manager et IBM Tivoli Change and Configuration Management Database

Network Manager prend en charge IBM Tivoli Application Dependency Discovery Manager et IBM Tivoli Change and Configuration Management Database 7.2.1 ou version ultérieure.

Tâches associées

Configuration des intégrations à d'autres produits
Vous pouvez configurer Network Manager pour l'utiliser avec plusieurs produits Tivoli®. Consultez les informations relatives aux tâches de configuration requises pour configurer les intégrations disponibles.

Bases de données topologiques prises en charge

La base de données topologiques par défaut de Network Manager est IBM Db2 10.5 Enterprise Server Edition.

Network Manager prend en charge les bases de données topologiques suivantes :

- IBM Db2 version 10.1 Enterprise Server Edition
- IBM DB2 version 10.5 Workgroup Server Edition
- IBM DB2 version 10.5 Enterprise Server Edition
- IBM DB2 version 11.1 Enterprise Server Edition
- IBM Db2 version 11.5 Enterprise Server Edition
- Fix Pack 3 IBM Db2 version 11.1 Advance Enterprise Server Edition
- Oracle Database version 11g, Enterprise Edition avec option de partitionnement (prise en charge ajoutée dans Network Manager 4.2 correctif temporaire 2)
- Oracle Database version 12c, Enterprise Edition avec option de partitionnement
- Oracle Database version 19c, Enterprise Edition avec option de partitionnement

Important : Le fonction de partitionnement de table est incluse dans tous les systèmes de base de données cités ci-dessus. L'option de partitionnement est obligatoire pour les systèmes de base de données Oracle. Cette fonction est obligatoire pour que Network Manager fonctionne correctement.

Lors de la configuration de la reprise en ligne, vous pouvez configurer Network Manager pour qu'il fonctionne dans l'environnement Db2 High Availability Disaster Recovery (HADR) ou dans l'environnement

Oracle Real Application Clusters (RAC), selon votre base de données. Pour plus d'informations, voir «Configuration de la reprise en ligne», à la page 185.

Pour une matrice des bases de données et des systèmes d'exploitation pris en charge, voir le document détaillant les exigences du système à l'adresse suivante :

https://www.ibm.com/software/reports/compatibility/clarity/

Important : Vérifiez que tous les correctifs recommandés sont appliqués à votre base de données, notamment les niveaux de correctif les plus récents.

Tâches associées

Installation et configuration d'une base de données topologiques
Votre administrateur de base de données doit installer et configurer une base de données topologiques avant que vous puissiez installer Network Manager.

Systèmes d'exploitation pris en charge

Network Manager est pris en charge sur les systèmes d'exploitation suivants.

Pour obtenir des informations actualisées sur les systèmes pris en charge, voir le document décrivant en détail la configuration système requise à l'adresse suivante :

https://www.ibm.com/software/reports/compatibility/clarity/

Important : Vérifiez que tous les modules de correction recommandés sont installés sur le système d'exploitation, y compris les niveaux de correctif les plus récents.

AIX Sur les systèmes IBM PowerPC, les versions suivantes sont prises en charge :

- AIX 6.1 iSeries et pSeries
- AIX 7.1 iSeries et pSeries
- AIX 7.2 iSeries et pSeries

Linux Sur les processeurs Intel et Advanced Micro Devices (AMD) x86, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 6 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- Fix Pack 11 Red Hat Enterprise Linux Server 8 (x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 et SP3
- Fix Pack 3 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)
- Fix Pack 10 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP4
- Fix Pack 11 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP5

Fix Pack 3 Depuis Fix Pack 3 jusqu'à Fix Pack 5, sur Linux on IBM z Systems, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP1 sur IBM z Systems (s390x, 64 bits)

Fix Pack 6 Depuis Fix Pack 6 et au-delà, sur Linux on IBM z Systems, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP2 et SP3 on IBM z Systems (s390x, 64 bit)

Fix Pack 10 Depuis Fix Pack 10 et au-delà, sur Linux on IBM z Systems, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)

- SuSE Linux Enterprise Server (SLES) 12.0 SP5 sur IBM z Systems (s390x, 64 bits)

Les combinaisons suivantes de programme Hypervisor et de système d'exploitation sont prises en charge :

- VMware ESX 5.0, 5.5, 6.0 :
  - Red Hat Enterprise Linux Server 7 (x86-64)
  - SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 et SP3
  - Fix Pack 3 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)

Exigences supplémentaires pour AIX

AIX

Assurez-vous que vous avez installé les utilitaires unzip ou GNU tar afin de pouvoir décompresser le fichier d'installation. Pour installer ces utilitaires, accédez à : http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html.

Vérifiez que GTK2 est installé. Pour installer GTK2, consultez la note technique suivante : http://www.ibm.com/support/docview.wss?uid=swg21631478.

Bibliothèques requises pour les systèmes Linux

Linux

Les composants de Network Manager nécessitent les bibliothèques suivantes et les dépendances de ces packages. Assurez-vous d'avoir installé ces bibliothèques sur le système sur lequel vous souhaitez installer Network Manager ou installez les modules appropriés pour vous procurer les bibliothèques requises.

En plus des bibliothèques ci-après, assurez-vous de disposer des bibliothèques requises pour les versions appropriées des produits intégrés. Contrôlez particulièrement les exigences pour votre version de Jazz for Service Management dans la documentation Jazz for Service Management à : https://www.ibm.com/support/knowledgecenter/SSEKCU, et pour Cognos Analytics dans Cognos Analytics Knowledge Center à https://www.ibm.com/support/knowledgecenter/SSEP7J.

Tableau 4. Bibliothèques requises pour les systèmes Linux

Bibliothèque	Module Red Hat	Module SuSE	Requis par le composant
`libstdc++.so.6 (64-bit)`	`libstdc++-4.4.4-13+ libstdc++-4.8.2+`	`libstdc++46-4.6.1+`	Network Manager Core
`libpam.so.0 (64-bit)`	`pam-1.1.1`	`pam-64bit`	Tivoli Netcool/OMNIbus

Navigateurs pris en charge pour les applications Web

Vérifiez que les clients utilisent un des navigateurs Web pris en charge. Si votre navigateur Web n'est pas pris en charge, une application Web peut se bloquer ou s'arrêter.

La résolution d'écran minimale pour utiliser les applications Web est 1536 x 864.

Les navigateurs Internet suivants sont pris en charge :

- Fix Pack 7 Google Chrome
- Internet Explorer 10, 11
- Mozilla Firefox 38 Extended Support Release (ESR)
- Fix Pack 1 Mozilla Firefox 45 Extended Support Release (ESR)
- Fix Pack 4 Mozilla Firefox 52 Extended Support Release (ESR)

Outils de système d'exploitation

Assurez-vous que vous disposez des versions appropriées des outils de système d'exploitation requis.

La stabilité du processus d'installation dépendant de celle des outils du système d'exploitation, vérifiez que les versions de système d'exploitation des outils standard apparaissent avant les autres versions (utilitaires GNU, par exemple) des mêmes outils dans votre chemin.

Sous Linux, Network Manager nécessite Python 2 (mais pas Python 3), version 2.6.6 ou ultérieure, pour être installé sur le serveur sur lequel les composants principaux sont installés. Sous AIX, Network Manager nécessite Python 2 (mais pas Python 3), version 2.7.5 ou ultérieure.

Assurez-vous que l'interpréteur de commandes Bash soit installé sur le serveur où devront être installés les composants centraux Network Manager.

Exigences relatives à l'utilisateur sous UNIX

Sous les systèmes d'exploitation UNIX, assurez-vous que vous respectez toutes les exigences concernant les utilisateurs requis pour le système d'exploitation, ainsi que pour les installations root et non-root.

Utilisateur de l'agrégation de l'interrogateur

Si vous installez Network Manager en tant que superutilisateur, vous devez créer un utilisateur non superutilisateur avant d'installer Network Manager pour exécuter le moteur d'agrégation de l'interrogateur. Cet utilisateur du système d'exploitation doit avoir des droits en écriture sur le répertoire d'installation. Si vous installez Network Manager en tant qu'utilisateur non-root, l'utilisateur d'installation est sélectionné pour pour exécuter le moteur d'agrégation de l'interrogateur.

Restrictions en tant que superutilisateur et non superutilisateur

Si vous installez les applications Web Network Manager en tant que superutilisateur, Network Manager ne s'intègre pas avec IBM Tivoli Business Service Manager.

Si vous souhaitez utiliser Network Manager avec TBSM, vous devez créer un autre utilisateur afin d'installer et de gérer tous les produits Tivoli sur ce serveur.

Si vous installez Network Manager en tant que non superutilisateur, vous devez effectuer une procédure de configuration supplémentaire après l'installation afin d'exécuter les composants centraux en tant que superutilisateur.

Remarque : Vous devez toujours utiliser le même utilisateur pour installer, démarrer ou arrêter tous les produits installés à l'aide d'IBM Installation Manager. Vous ne pouvez pas utiliser un utilisateur différent même si les produits ont été installés en mode groupe. Cet utilisateur doit être un administrateur pour tous les produits installés sur ce serveur.

Si vous installez et exécutez Network Manager en tant que non superutilisateur, vous ne pouvez pas installer deux versions différentes de Network Manager sur le même serveur.

Tâches associées

Configuration des autorisations de superutilisateur/non superutilisateur
Sous UNIX, si vous avez installé Network Manager en tant que non superutilisateur, vous devez effectuer une configuration supplémentaire.

Exigences relatives au répertoire d'installation

Le répertoire dans lequel vous installez Network Manager doit répondre à certaines exigences.

Exigences communes à tous les systèmes d'exploitation

Le chemin complet d'accès au répertoire d'installation ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9), des tirets, des traits de soulignements, des points, deux points, des barres obliques ou des espaces.

Exigences des systèmes d'exploitation UNIX

L'utilisateur installant Network Manager doit avoir des droits en écriture sur le répertoire d'installation et sur les répertoires `/opt`, `/var` et `/tmp`.

Référence associée

Structure de répertoire par défaut
Utilisez ces informations pour comprendre la structure de répertoire de Network Manager.

Exigences relatives au descripteur de fichier

Sous les systèmes d'exploitation UNIX et Linux, vérifiez que suffisamment de descripteurs de fichier sont autorisés.

Si vous installez Network Manager sous UNIX ou Linux, assurez-vous que le nombre de fichiers ouverts pour les processus est défini sur une valeur appropriée dans tous les environnements de l'utilisateur exécutant Network Manager. Définissez le nombre de fichiers ouverts sur au moins 512 pour le serveur où les composants centraux sont installés, et sur 8192 pour le serveur de l'interface graphique. Vous pouvez vérifier cette valeur en entrant la commande suivante en tant qu'utilisateur exécutant Network Manager : `ulimit -n`

Vérifiez également que le nombre de processus par utilisateur est défini sur un minimum de 16384. Vous pouvez contrôler cette valeur à l'aide de la commande suivante : `ulimit -u`. La valeur 16384 est un un minimum. Il peut être nécessaire de l'ajuster à votre environnement en fonction de vos besoins.

Si cette valeur est trop faible, contactez votre administrateur système pour augmenter la valeur de l'utilisateur.

Remarque :

Si vous utilisez la rotation des fichiers journaux avec une taille de pool définie, rappelez-vous que le nombre de fichiers ouverts peut augmenter de façon importante. L'activation d'un pool de journalisation ajoute un nombre supplémentaire de fichiers ouverts qui est équivalent au nombre de processus Network Manager en cours d'exécution, multiplié par le nombre de fichiers journaux dans le pool. Assurez-vous que le nombre limite de fichiers ouverts est élevé et que les processus ne rencontrent pas de problèmes lors de l'ouverture de fichiers journaux.

Modification des valeurs sous Linux

Linux

Pour modifier `ulimit`, modifiez le fichier `/etc/security/limits.conf`. En tant qu'administrateur système (superutilisateur) vous pouvez ajouter les lignes suivantes à la fin du fichier /etc/security/limits.conf :

```
*         soft    nproc      16384
*         hard    nproc      16384
*         soft    nofile      8192
*         hard   nofile      8192
```

Modification des valeurs sous AIX

AIX

Les valeurs en cours sont répertoriées dans le fichier `/etc/security/limits`, dans les lignes contenant les paramètres `nofiles` et `nproc`. En tant qu'administrateur système (superutilisateur), vous pouvez utiliser la commande `ulimit` pour modifier ces valeurs. Pour plus d'informations, recherchez des informations sur la commande `ulimit` à l'adresse https://www-01.ibm.com/support/knowledgecenter/ssw_aix/welcome.

Exigences relatives aux mots de passe

Tous les mots de passe utilisés dans Network Manager doivent être conformes aux règles sur les mots de passe de l'environnement du serveur ou système.

Configuration requise du réseau

Assurez-vous que votre réseau répond aux critères avant d'installer Network Manager.

Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Liste des ports utilisés par le produit

Le Network Manager utilise différents ports à des fins de communication : certains sont fixes, certains sont définis par les fichiers de configuration, certains sont affectés par les systèmes d'exploitation.

Le tableau suivant présente les ports par défaut utilisés par le Network Manager.

Tableau 5. Ports par défaut utilisés par le Network Manager

Port	Protocole	Description
22	SSH au lieu de TCP/IP	Si la prise en charge SSH est possible, l'auxiliaire Telnet utilise ce port pour communiquer avec les périphériques réseau.
23	Telnet au lieu de TCP/IP	Si la prise en charge SSH est possible, l'auxiliaire Telnet utilise ce port pour communiquer avec les périphériques réseau.
161	SNMP	Le port 161 est le port par défaut des périphériques réseau vers lequel les analyses SNMP sont envoyées lors des processus de reconnaissance et de surveillance. Défini dans la colonne m_SnmpPort de la table de base de données snmpStack.verSecurityTable.
162	UDP	Port trap par défaut. Utilisé par l'agent d'interrogation d'interruptions. Si plusieurs applications/processus ont besoin d'accéder à ce port, ncp_trapmux, le multiplexeur d'interruptions SNMP, peut être utilisé pour réacheminer des interruptions. Le multiplexeur d'interruptions SNMP, l'agent de reconnaissance d'interruptions, et l'agent d'interrogation d'interruption peuvent être configurés de façon à utiliser chacun un port différent.
1883	Transport télémétrique de file d'attente de messages (MQTT)	Port par défaut utilisé par Courtier de messages très petits pour la communication inter-processus.
4100	TCP/IP	Port ObjectServer par défaut. Il doit être saisi au moment de l'installation. Défini dans les `interfaces.`*`Arch`* sur le poste de travail ObjectServer. Ce port est utilisé par le processus `ncp_g_event` pour communiquer avec l'ObjectServer.

Tableau 5. Ports par défaut utilisés par le Network Manager (suite)		
Port	**Protocole**	**Description**
7968	TCP/IP	Port par défaut permettant d'accéder au serveur Network Manager à partir de Dashboard Application Services Hub. Il est utilisé par l'interface de configuration de reconnaissance et est défini dans le fichier de configuration `ServiceData.cfg`. Si vous voulez modifier ce port, modifiez le fichier de configuration `ServiceData.cfg` et redémarrer le processus ncp_model et le processus ncp_config à l'aide de CTRL.
16310	HTTP	Port par défaut pour Dashboard Application Services Hub. Dashboard Application Services Hub Alloue les treize ports suivants depuis le port spécifié pour Dashboard Application Services Hub au cours de l'installation, pour sa propre utilisation. Par défaut, ce port est redirigé vers le port 16316.
16311	HTTPS	Port sécurisé par défaut de Dashboard Application Services Hub.
33000	TCP/IP	Par défaut, l'adresse IP de multidiffusion 225.13.13.13 et le port 33000 sont utilisés pour permettre aux auxiliaires et agents de reconnaissance de trouver l'emplacement du serveur auxiliaire. Cette adresse de multidiffusion est indiquée dans le fichier `$NCHOME/etc/precision/ServiceData.cfg`. Une fois que le processus a trouvé le serveur auxiliaire, une connexion TCP est établie sur le port affecté par le système d'exploitation.
50000	TCP/IP	Port de la base de données Db2 par défaut.
OS-assigned	TCP/IP	Les ports TCP sont affectés par le système d'exploitation pour la communication TCP entre les processus, par exemple, la communication entre les agents de reconnaissance et le serveur auxiliaire. Si cela pose problème, vous devez vérifier que votre pare-feu est externe au serveur de Network Manager, et que tous les processus de reconnaissance sont exécutés sur le même hôte.

1521	TCP/IP	Port par défaut de base de données Oracle.

Exigences du service de noms de domaine (DNS)

Vérifiez que le DNS des serveurs est configuré correctement avant d'installer Network Manager.

Noms de domaine

Vérifiez que tous les serveurs sur lesquels vous voulez installer des composants de Network Manager ont un nom d'hôte défini comme étant un nom de domaine qualifié complet. Une configuration DNS incomplète ou incorrecte peut occasionner des problèmes lors de l'installation ou de l'utilisation de Network Manager.

Sur les plateformes UNIX, le nom d'hôte est défini dans le fichier `/etc/hosts`.

Sur la machine sur laquelle vous installez les composants Network Manager, incluez bien l'adresse IP, le nom de domaine complet et le nom abrégé dans le fichier `/etc/hosts` avant d'installer Network Manager et vérifiez que le nom de domaine complet et le nom abrégé ne sont résolus que dans la même adresse IP et que la résolution inverse renvoie au nom de domaine complet ou au nom abrégé.

Le format est *`adresse IP nom de domaine complet nom abrégé`*. Par exemple, ajoutez une ligne similaire à la suivante dans `/etc/hosts` :
`9.10.11.12 yourserver.domainname.com yourserver`

Cette ligne garantit que le nom de domaine complet est défini en tant qu'entrée Hostname si Network Manager est installé.

Restriction : N'utilisez pas de trait de soulignement lors de la spécification des noms d'hôte. Sinon, l'installation de Dashboard Application Services Hub échouerait.

Exigences en bande passante de la reconnaissance

Les opérations de reconnaissance du réseau nécessitent au minimum une connexion à large bande.

Ne tentez pas de lancer des reconnaissances avec une connexion modem. Si la vitesse de connexion n'est pas suffisante, il est possible que des paquets soient perdus en raison de la quantité de trafic SNMP généré par les opérations de reconnaissance et de surveillance par défaut. Même avec une connexion à large bande, le nombre d'unités d'exécution des auxiliaires SNMP doit rester faible. La reconnaissance peut donc prendre beaucoup de temps.

Les reconnaissances doivent être exécutées lorsque vous disposez d'une connexion Ethernet (ou similaire). La vitesse requise de votre connexion Ethernet dépend de la taille de votre réseau :

- Une connexion 10 Mbits/s en duplex intégral est nécessaire pour prendre en charge jusqu'à 100 unités d'exécution d'auxiliaires SNMP et un nombre relativement faible d'unités. Si vous utilisez Telnet avec SSH pour accéder à de nombreuses unités de la reconnaissance, le nombre d'unités d'exécution de l'auxiliaire SNMP doit être réduit pour prendre en compte la bande passante utilisée par l'auxiliaire Telnet.
- Une connexion Fast Ethernet 100 Mbits/s en duplex intégral (ou équivalente) est nécessaire pour reconnaître un réseau de grande taille. La bande passante ne devrait pas poser de problème avec une connexion 100 Mbits/s, et ce quel que soit le nombre d'unités d'exécution de l'auxiliaire SNMP utilisées, sauf si des applications exigeant une bande passante importante partagent la liaison.

Les chiffres ci-dessus partent du principe qu'un aller-retour moyen pour un paquet SNMP est de 10 millisecondes et qu'un paquet a une taille de 125 octets en moyenne. Cela signifie que chaque unité d'exécution de l'auxiliaire SNMP peut transmettre et récupérer 12 500 octets par seconde, ce qui équivaut à 100 000 bits par seconde. Dans le cas de 20 unités d'exécution, 20 multiplié par 100 000 équivaut à 2 000 000 bits par seconde, soit 2 Mbits/s. Pour 100 unités d'exécution, cela nous donne 10 Mbits/s. Par défaut, l'auxiliaire SNMP exécute 120 unités d'exécution.

Ces estimations partent du principe que chaque unité d'exécution de l'auxiliaire SNMP est en activité en même temps, ce qui n'est généralement pas le cas. Cependant, si la bande passante est insuffisante, les paquets UDP utilisés pour transporter SNMP pourraient être perdus ou se retrouver en file d'attente et arriver à destination en retard.

Pour plus d'informations sur la configuration de l'auxiliaire SNMP, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

A propos de DNCIM

Le moteur de reconnaissance, **`ncp_disco`**, utilise une une base de données relationnelle intégrée appelée Discovery NCIM (DNCIM).

Au cours du processus de reconnaissance, les données sont collectées depuis le réseau, et la topologie de réseau est créée avec ces données. Lors de la collecte et du traitement des données dans une topologie de réseau, les données de la topologie de réseau sont stockées dans différentes bases de données. Une fois que le modèle de réseau final, comprenant la connectivité et le confinement, est généré, les données de topologie de réseau sont stockées dans DNCIM. DNCIM possède la même structure que la base de données topologiques NCIM.

Pour plus d'informations sur DNCIM, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Installations FIPS 140-2

La norme FIPS (Federal Information Processing Standard) 140–2 est une norme cryptographique fédérale des Etats-Unis. Vous pouvez installer Network Manager avec un ensemble d'algorithmes de cryptographie restreint.

Network Manager n'est pas reconnu conforme à la norme FIPS 140–2 et aucun élément de ce manuel ou du produit ne doit être considéré comme tel. Toutefois, Network Manager peut être installé d'une façon conçue pour prendre en compte les spécifications de la norme FIPS 140–2.

Restriction : Si la conformité à la norme FIPS 140–2 est importante pour vous, vous devez installer Network Manager avec un ensemble d'algorithmes de cryptographie restreint en désélectionnant la fonction **Routines cryptographiques supplémentaires** dans le programme d'installation. Si vous installez ces routines supplémentaires, votre installation utilise des routines cryptographiques non compatibles avec la norme FIPS 140-2c.

Si vos exigences se modifient ou si vous commettez une erreur durant l'installation, vous pouvez installer ou désinstaller la fonction **Routines cryptographiques supplémentaires** après l'installation. Pour ce faire, exécutez le programme d'installation et sélectionnez **Modifier**.

Intégration à d'autres produits

Si la conformité à la norme FIPS 140–2 est importante pour vous, vous devez également vérifier que tous les produits s'intégrant à Network Manager, comme IBM Tivoli Netcool/OMNIbus, disposent d'un mode FIPS. Si nécessaire, vous devez également configurer les produits. Vous devez également vérifier que votre système d'exploitation utilise uniquement des modules compatibles FIPS 140–2.

Différences dans une installation FIPS 140–2 de Network Manager

Une installation comportant des routines cryptographiques restreintes, prévue pour être utilisée dans un environnement compatible avec FIPS 140-2, diffère d'une installation normale comme suit :

- Les agents de reconnaissance Telnet n'utilisent pas SSHv1 pour interroger les unités. Cela peut provoquer une erreur lors de la connexion à une unité si celle-ci prend uniquement en charge les algorithmes SSHv1 ou uniquement les algorithmes SSHv2 non conformes à FIPS 140-2.
- L'aide programmable SNMP et le navigateur MIB ne peuvent pas être configurés pour utiliser le chiffrement MD5 DES. L'auxiliaire SNMP et le navigateur MIB prennent en charge les algorithmes SHA et SHA1 pour le résumé du message, ainsi que les normes 3-DES et AES 128 pour le chiffrement.

Chapitre 3. Préparation à l'installation

Avant de commencer à installer Network Manager, vous devez effectuer des tâches supplémentaires qui varient selon votre environnement.

Exécution des procédures d'installation et de maintenance en tant que superutilisateur ou non superutilisateur

Vous pouvez exécuter l'installation sans être superutilisateur. Toutefois, certaines actions de configuration de Network Manager doivent être exécutées par l'utilisateur `superutilisateur`. A la fin de l'assistant d'installation, un panneau vous rappelle de vous connecter en tant que superutilisateur et d'effectuer ces configurations manuellement.

Remarque : Vous devez toujours utiliser le même utilisateur pour installer, démarrer ou arrêter tous les produits installés à l'aide d'IBM Installation Manager. Vous ne pouvez pas utiliser un utilisateur différent même si les produits ont été installés en mode groupe. Cet utilisateur doit être un administrateur pour tous les produits installés sur ce serveur.

Concepts associés

Installations en tant que superutilisateur et non superutilisateur
Sous UNIX, vous pouvez installer Network Manager en tant que superutilisateur ou en tant que non superutilisateur.

Tâches associées

Configuration des composants centraux pour une exécution en tant que superutilisateur
Sous UNIX, si vous avez installé Network Manager en tant que non superutilisateur, vous devez procéder à une configuration supplémentaire pour exécuter les composants centraux en tant que superutilisateur.

Configuration de Red Hat Linux Enterprise Edition

Avant d'installer le produit sous Red Hat Linux Enterprise Edition, vous devez désactiver SELinux.

Pourquoi et quand exécuter cette tâche

Lors de l'installation de Red Hat Enterprise Linux, il se peut que SELinux soit activé. Pour désactiver SELinux, modifiez l'option SELinux en procédant comme suit :

Procédure

1. Ouvrez le fichier suivant :

   ```
   /etc/sysconfig/selinux
   ```

2. Recherchez la ligne suivante :

   ```
   SELINUX=enforcing
   ```

3. Remplacez-la par `SELINUX=disabled`.
4. Redémarrez le serveur.

Tâches de pré-installation sous AIX

Pour installer Network Manager sur des des systèmes d'exploitation AIX, il vous faut réaliser des tâches supplémentaires afin de préparer vos serveurs pour l'installation.

Pourquoi et quand exécuter cette tâche

Ces tâches ne sont pas nécessaires si vous utilisez d'autres systèmes d'exploitation.

Configuration de SSH (Secure Shell) pour AIX

Si vous prévoyez d'effectuer l'installation en tant que non superutilisateur root sous AIX et d'utiliser SSH pour accéder à votre serveur AIX, vous devez effectuer des étapes de configuration supplémentaires avant d'accéder au serveur AIX.

Pourquoi et quand exécuter cette tâche

Conseil : Si vous utilisez rlogin ou telnet pour accéder à votre serveur AIX, les étapes suivantes ne sont pas nécessaires.

Pour garantir le bon fonctionnement de l'installation, procédez comme suit :

Procédure

1. Ouvrez le fichier `/etc/ssh/sshd_config` sur le serveur AIX sur lequel vous souhaitez installer Network Manager.
2. Vérifiez que le fichier contient la ligne suivante :

   ```
   UseLogin yes
   ```

3. Sauvegardez et fermez le fichier.
4. Vous pouvez maintenant utiliser SSH pour accéder au serveur et installer Network Manager.

Installation d'un utilitaire `zip`

L'installation d'un utilitaire `zip` pour la compression de fichier est nécessaire pour exporter les personnalisations d'interface graphique avec le script `nmGuiExport`.

Avant d'exporter les données de personnalisation d'interface graphique à l'aide du script `nmGuiExport`, veillez à installer un utilitaire `zip` sur chaque serveur où sont installés les composants d'interface graphique de votre système précédent. Si un utilitaire `zip` n'est pas installé sur le serveur de votre système précédent, le script `nmGuiExport` échoue, l'archive `upgradeData.zip` n'est pas créée et le script affiche un message d'erreur.

Vérification des paramètres de port d'achèvement d'E-S (IOCP)

Si vous installez Network Manager sur AIX et que vous comptez vous connecter à une base de données Oracle, vous devez vous assurer que les paramètres de port d'achèvement d'E-S sont appropriés.

Pourquoi et quand exécuter cette tâche

Vous devez exécuter la procédure suivante en tant que superutilisateur.

Procédure

1. Emettez la commande suivante

   ```
   /usr/sbin/lsdev -c iocp -F status
   ```

   Procédez comme suit :

   - Si cette commande renvoie le résultat `Disponible`, vous n'avez pas besoin d'exécuter d'autres étapes au cours de cette tâche.
   - Si la commande renvoie un résultat autre que `Disponible`, par exemple, `Défini`, continuez la procédure avec les étapes suivantes pour cette tâche.

2. Entrez la commande suivante :

   ```
   smitty iocp2
   ```

3. Sélectionnez Modification/Affichage des caractéristiques des ports d'achèvement d'E-S.
4. Modifiez le paramètre STATE à configurer au redémarrage du système de Défini à Disponible.
5. Réamorcez le serveur AIX.

Chapitre 4. Installation de Network Manager et des produits connexes

Installez les prérequis, les produits connexes et les composants de Network Manager dans l'ordre dans lequel ils sont présentés ici.

Avant de commencer

Avant d'installer des produits, examinez tous les prérequis et exigences dans Chapitre 2, «Planification de l'installation», à la page 3 et exécutez les tâches de pré-installation nécessaires dans Chapitre 3, «Préparation à l'installation», à la page 41.

Pourquoi et quand exécuter cette tâche

Les instructions suivantes permettent d'installer un seul composant à la fois. Pour installer deux ou plusieurs composants dans un certain ordre sur le même serveur, sélectionnez-les afin de les installer simultanément, et IBM Installation Manager les installera alors dans l'ordre adéquat.

Liste de contrôle de l'installation

Avant de commencer l'installation, assurez-vous d'avoir préparé toutes les informations requises. Pendant l'installation, notez par écrit les informations dont vous aurez besoin par la suite.

Informations à rassembler avant l'installation

Collectez toute les informations ci-dessous relatives à votre déploiement avant de démarrer l'installation. Vous pouvez imprimer cette liste de contrôle.

IBM Installation Manager Informations sur

☐Emplacement d'installation : _____ Emplacement d'installation prévu pour IBM Installation Manager. Par exemple : `/opt/IBM/netcool/im`. Vous devez démarrer IBM Installation Manager à partir de cet emplacement après son installation.

☐Emplacement des données : _____ Emplacement dans lequel IBM Installation Manager décompacte les packages et les stocke en cas d'annulation. Assurez-vous que cet emplacement dispose d'au moins 10 Go d'espace libre. Ce répertoire ne doit pas se trouver dans le sous-dossier `eclipseIM` ou dans l'emplacement de partage de IBM Installation Manager et ne doit pas les contenir. Exemple d'emplacement des données : `/opt/IBM/netcool/IBMIMData`.

☐Emplacement de partage : _____ Le système vous demande d'indiquer cet emplacement lorsque vous installez le premier produit dans IBM Installation Manager, et non pendant l'installation de IBM Installation Manager lui-même. Ce répertoire ne doit pas se trouver dans le sous-dossier `eclipseIM` ou l'emplacement des données IBM Installation Manager, et ne doit pas les contenir. Exemple d'emplacement de partage : `/opt/IBM/netcool/IBMIMShare`.

Informations DB2 ou Oracle

Collectez les informations suivantes de la base de données de votre choix avant d'installer Network Manager.

☐Répertoire d'installation de DB2 ou d'Oracle : _____

☐Si vous utilisez DB2, nom d'utilisateur d'un système d'exploitation et de l'utilisateur DB2 nécessaire pour se connecter à la base de données DB2 : _____

☐Si vous utilisez Oracle, vérifiez que vous êtes autorisé à utiliser la fonction de partitionnement.

☐Nom de base de données DB2 ou nom de service Oracle : _____

☐Nom d'hôte du serveur sur lequel la base de données est installée:_____

Informations ObjectServer

Si vous souhaitez utiliser un ObjectServer existant pour les données d'événement de Network Manager, notez ici ses détails. Vous en aurez besoin lors de l'installation des composants principaux de Network Manager.

☐Nom de l'ObjectServer : _____

☐Nom d'hôte sur lequel est installé cet ObjectServer : _____

☐Port configuré pour les connexions à cet ObjectServer : _____

☐ID de superutilisateur de cet ObjectServer : _____

☐Mot de passe de cet utilisateur : _____

Network Manager Informations des composants principaux de

Collectez les informations suivantes des composants principaux avant d'installer Network Manager.

☐Chemin Python : _____ Le chemin complet d'accès à une version compatible de Python est nécessaire pour installer les composants principaux de Network Manager.

☐Utilisateur d'agrégation de l'interrogateur : _____ Si vous installez Network Manager en tant que superutilisateur, vous avez besoin d'un non superutilisateur pour exécuter le moteur d'agrégation de l'interrogateur. Cet utilisateur du système d'exploitation doit exister et doit avoir des droits en écriture sur le répertoire d'installation.

☐Groupe d'agrégation de l'interrogateur : _____ Groupe auquel appartient utilisateur d'agrégation de l'interrogateur. L'agrégation de l'interrogateur de l'utilisateur doit exister en tant que membre de ce groupe pour que l'agrégation de l'interrogateur soit possible.

Informations à rassembler pendant l'installation

Pendant l'installation, vous devez définir différents paramètres de configuration. Certains de ces paramètres de configuration sont nécessaires dans la suite de l'installation. Notez les informations suivantes lors de l'installation de Network Manager et des composants associés.

Informations ObjectServer

Si vous créez un ObjectServer pendant l'installation des composants principaux de Network Manager, notez ici ses informations.

☐Nom de l'ObjectServer créé en vue d'une utilisation avec Network Manager : _____

☐ Nom d'hôte sur lequel est installé cet ObjectServer : _____

☐ Port configuré pour les connexions à cet ObjectServer : _____

☐ ID de superutilisateur de cet ObjectServer : _____

☐ Mot de passe de cet utilisateur : _____

Autres informations des composants principaux de Network Manager

☐ Le nom de l'utilisateur qui exécute l'interrogateur de Network Manager : _____ Cet utilisateur doit aussi exécuter les scripts de mise à niveau des scripts lorsque vous migrez vers u ne nouvelle version.

☐ Mot de passe des utilisateurs par défaut Network Manager `itnmadmin` et `itnmuser` : _____

☐ Nom du domaine de réseau : _____ Il s'agit du nom choisi pendant l'installation des composants principaux de Network Manager.

WebSphere Application ServerInformations sur

Notez les informations suivantes lors de l'installation de WebSphere Application Server :

Emplacement d'installation de ☐ WebSphere Application Server : _____

Nom du serveur ☐ WebSphere Application Server : _____

Nom d'utilisateur de ☐ WebSphere Application Server : _____

Mot de passe de ☐ WebSphere Application Server : _____

☐ Port de transfert HTTP : _____

☐ Port de transfert sécurisé HTTPS : _____

☐ Port de la console d'administration : _____

☐ Port sécurisé de la console d'administration : _____

☐ Racine de contexte : _____

Dashboard Application Services Hub Informations sur

Notez les informations suivantes lors de l'installation de Dashboard Application Services Hub.

Répertoire d'installation ☐ Dashboard Application Services Hub : _____

Network ManagerInformations sur les composants d'interface graphique de

Collectez les informations suivantes lors de l'installation des composants d'interface graphique de Network Manager.

☐ Mot de passe des utilisateurs Network Manager : _____ Mot de passe des utilisateurs `itnmadmin` et `itnmuser`.

Installation et configuration d'IBM Installation Manager

Avant d'installer ou de mettre à jour Tivoli Netcool/OMNIbus, Network Manager, ou tout autre produit IBM, installez et mettez à jour IBM Installation Manager et configurez-le.

Pourquoi et quand exécuter cette tâche

Vous pouvez vous procurer les logiciels IBM Installation Manager et Network Manager de deux manières.

- Téléchargez IBM Installation Manager sur le serveur cible et connectez IBM Installation Manager à ibm.com ou un répertoire local. IBM Installation Manager peut télécharger d'autres produits.
- Téléchargez un progiciel compressé contenant IBM Installation Manager et Network Manager et copiez-le sur le serveur cible.

Installation d'IBM Installation Manager en téléchargeant les fichiers du produit

Si vous souhaitez installer IBM Installation Manager et Network Manager sur un serveur qui n'est pas connecté à Internet, téléchargez le logiciel sur un autre serveur à partir de Passport Advantage. Copiez-le ensuite sur le serveur où vous voulez installer le logiciel.

Avant de commencer

Créez un ID IBM à l'adresse http://www.ibm.com. Vous avez besoin d'un ID IBM pour télécharger le logiciel depuis Passport Advantage.

Pourquoi et quand exécuter cette tâche

Network Manager requiert IBM Installation Manager V1.9.1.3 ou ultérieur. Sur SuSE Linux V11 et V12 pour System z, seule la version 32 bits d'IBM Installation Manager est prise en charge.

Vous pouvez télécharger un fichier compressé depuis Passport Advantage qui contient IBM Installation Manager, Network Manager et les scripts de création de base de données.

Pour installer et configurer IBM Installation Manager, procédez comme suit :

Procédure

1. Recherchez le numéro de référence du logiciel Network Manager dans le document de téléchargement à l'emplacement suivant :

   http://www.ibm.com/support/docview.wss?uid=swg24043360
2. Suivez les instructions fournies dans le document de téléchargement pour télécharger le logiciel.
3. Décompressez le package que vous avez téléchargé.
4. Si vous souhaitez utiliser les scripts de création de base de données Network Manager sans exécuter IBM Installation Manager, vous pouvez les copier à partir du niveau supérieur du package d'installation décompressé.
5. Installez IBM Installation Manager en mode groupe (tous les modes sont pris en charge, mais pour contrôler au maximum l'emplacement de création des fichiers, utilisez de préférence le mode groupe et non le mode non-administrateur ou le mode admin). Procédez selon les instructions de la rubrique "Installation ou mise à jour d'Installation Manager" pour obtenir la version appropriée à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

   Remarque : Vous devez toujours utiliser le même utilisateur pour installer, démarrer ou arrêter tous les produits installés à l'aide d'IBM Installation Manager. Vous ne pouvez pas utiliser un utilisateur

différent même si les produits ont été installés en mode groupe. Cet utilisateur doit être un administrateur pour tous les produits installés sur ce serveur.

Une fois IBM Installation Manager installé, il redémarre et continue l'installation de Network Manager. Installez Network Manager comme indiqué dans «Installation des composants de base de Network Manager», à la page 59 et «Installation des composants principaux de l'interface graphique de Network Manager», à la page 69.

Que faire ensuite

La prochaine fois que vous utiliserez cette installation d'IBM Installation Manager, vous devrez configurer les référentiels nécessaires.

1. Cliquez sur **Fichier** > **Préférences**.
2. Si un référentiel a été configuré pour vous, cliquez sur **Repositories** et vérifiez que les référentiels adéquats ont été sélectionnés.
3. Si aucun référentiel n'a été configuré, et que vous souhaitez le faire vous-même, consultez les informations sur l'utilisation d'IBM Packaging Utility dans la documentation de IBM Installation Manager : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
4. Pour vous connecter directement au référentiel en ligne d'IBM pour accéder aux produits auxquels vous avez droit, cliquez sur Passport Advantage, sélectionnez Connect to Passport Advantage, puis cliquez sur **Apply**. Cliquez sur **OK**. Lorsque vous installez ou mettez à jour un produit, le système vous invite à indiquer vos données d'identification pour pouvoir accéder à IBM Passport Advantage.

Installation d'IBM Installation Manager via une connexion directe à Passport Advantage

Si vous souhaitez installer IBM Installation Manager et Network Manager sur un serveur qui peut se connecter à ibm.com, installez IBM Installation Manager et connectez-le àPassport Advantage.

Avant de commencer

Créez un ID IBM à l'adresse http://www.ibm.com. Vous avez besoin d'un ID IBM pour télécharger le logiciel depuis Passport Advantage.

Pourquoi et quand exécuter cette tâche

Network Manager requiert IBM Installation Manager V1.9.1.3 ou ultérieur. Sur SuSE Linux V11 et V12 pour System z, seule la version 32 bits d'IBM Installation Manager est prise en charge.

Remarque :

En cas de différence entre ces instructions et la documentation de votre version de IBM Installation Manager en raison de mises à jour ou de modifications, la documentation de IBM Installation Manager est prioritaire. Vous pouvez la consulter à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

Pour installer et configurer IBM Installation Manager, procédez comme suit :

Procédure

1. Si IBM Installation Manager est déjà installé, assurez-vous que sa version est la plus récente. Les commandes suivantes partent du principe que le serveur sur lequel vous effectuez l'installation est connecté à Internet, que vous êtes connecté aux référentiels ibm.com et que vous utilisez le mode assistant. Pour les autres scénarios, voir la documentation de IBM Installation Manager : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
   a) Démarrez IBM Installation Manager en modifiant le répertoire d'installation. Par défaut, le répertoire d'installation des trois modes d'installation est :

Mode groupe
/répertoire_base_utilisateur/IBM/InstallationManager_Group/eclipse

Mode non-administrateur
/répertoire_base_utilisateur/IBM/InstallationManager/eclipse

Mode Administrateur

```
/opt/IBM/InstallationManager/eclipse
```

et exécutez la commande suivante :

```
./IBMIM
```

b) Cliquez sur **Fichier** > **Préférences**.

c) Si vous pouvez accéder à ibm.com à partir de ce serveur, dans l'onglet **Repositories**, sélectionnez **Search service repositories during installation and updates**.

d) Si vous ne pouvez pas accéder à ibm.com à partir de ce serveur, dans l'onglet **Repositories**, ne sélectionnez pas **Search service repositories during installation and updates**. Sans accès à ibm.com, le délai d'attente de la mise à jour arrive à expiration. Dans ce cas, téléchargez les nouvelles mises à jour d'IBM Installation Manager dans votre référentiel local et vérifiez que le référentiel est configuré sous **Repositories**. Si aucun référentiel n'a été configuré, et que vous souhaitez le faire vous-même, consultez les informations sur l'utilisation d'IBM Packaging Utility dans la documentation de IBM Installation Manager : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

e) Cliquez sur **Updates** et sélectionnez l'option **Search for Installation Manager updates**.

f) Cliquez sur **OK** pour fermer la page des **Préférences**.

g) Cliquez sur l'un de ces assistants : **Installez** ou **Mettez à Jour**.

Installation Manager recherche ses propres mises à jour. Si une version plus récente est trouvée, vous êtes invité à mettre à jour Installation Manager.

h) Pour obtenir les informations de version, cliquez sur **Détails**.

i) Cliquez sur **Yes** pour mettre à jour Installation Manager.

2. Si vous n'avez pas installé IBM Installation Manager, installez-le maintenant.

a) Téléchargez la version la plus récente de IBM Installation Manager pour votre plateforme depuis le site Web suivant : https://www.ibm.com/support/pages/node/609575

b) Installez IBM Installation Manager en mode groupe (tous les modes sont pris en charge, mais pour contrôler au maximum l'emplacement de création des fichiers, utilisez de préférence le mode groupe). Procédez selon les instructions de la rubrique "Installation ou mise à jour d'Installation Manager" pour obtenir la version appropriée à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

Remarque : Vous devez toujours utiliser le même utilisateur pour installer, démarrer ou arrêter tous les produits installés à l'aide d'IBM Installation Manager. Vous ne pouvez pas utiliser un utilisateur différent même si les produits ont été installés en mode groupe. Cet utilisateur doit être un administrateur pour tous les produits installés sur ce serveur.

3. Connectez-vous à un référentiel contenant les produits à installer :

Un répertoire peut être sur un serveur local ou en ligne.

a) Cliquez sur **Fichier** > **Préférences**.

b) Si un référentiel a été configuré pour vous, cliquez sur **Repositories** et vérifiez que les référentiels adéquats ont été sélectionnés.

c) Si aucun répertoire n'a été configuré pour vous, et que vous voulez configurez vous-même un répertoire, consultez les informations sur la *gestion des paquets avec le IBM Packaging Utility* dans la documentation IBM Installation Manager : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

d) Pour vous connecter directement au référentiel en ligne d'IBM pour accéder aux produits auxquels vous avez droit, cliquez sur Passport Advantage, sélectionnez **Connect to Passport Advantage**, puis cliquez sur **Apply**. Cliquez sur **OK**.

Lorsque vous installez ou mettez à jour un produit, le système vous invite à indiquer vos données d'identification pour pouvoir accéder à IBM Passport Advantage.

Installation et configuration d'une base de données topologiques

Votre administrateur de base de données doit installer et configurer une base de données topologiques avant que vous puissiez installer Network Manager.

Pourquoi et quand exécuter cette tâche

Network Manager nécessite une base de données dans laquelle stocker la topologie réseau.

Network Manager prend en charge les bases de données topologiques suivantes :

- IBM Db2 version 10.1 Enterprise Server Edition
- IBM DB2 version 10.5 Workgroup Server Edition
- IBM DB2 version 10.5 Enterprise Server Edition
- IBM DB2 version 11.1 Enterprise Server Edition
- IBM Db2 version 11.5 Enterprise Server Edition
- Fix Pack 3 IBM Db2 version 11.1 Advance Enterprise Server Edition
- Oracle Database version 11g, Enterprise Edition avec option de partitionnement (prise en charge ajoutée dans Network Manager 4.2 correctif temporaire 2)
- Oracle Database version 12c, Enterprise Edition avec option de partitionnement
- Oracle Database version 19c, Enterprise Edition avec option de partitionnement

Important : Le fonction de partitionnement de table est incluse dans tous les systèmes de base de données cités ci-dessus. L'option de partitionnement est obligatoire pour les systèmes de base de données Oracle. Cette fonction est obligatoire pour que Network Manager fonctionne correctement.

Important : Vérifiez que tous les correctifs recommandés sont appliqués à votre base de données, notamment les niveaux de correctif les plus récents.

Pour installer et configurer une base de données, procédez comme suit :

Procédure

1. Installez l'une des bases de données prises en charge :
   - Installez DB2 à partir de Passport Advantage : http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
   - Installez Oracle fourni par votre éditeur logiciel.
2. Installez les scripts de création de la base de données topologiques de Network Manager à l'aide d'IBM Installation Manager.
3. Configurez la base de données à l'aide des informations des sections suivantes.

Tâches associées

Configuration de Cognos Analytics
Procédez comme suit pour configurer Cognos Analytics.

Référence associée

Bases de données topologiques prises en charge

La base de données topologiques par défaut de Network Manager est IBM Db2 10.5 Enterprise Server Edition.

Installation et exécution des scripts de la base de données Network Manager

Lorsqu'une base de données prise en charge a été installée, vous devez installer et exécuter les scripts de la base de données pour configurer la base de données topologiques en vue de son utilisation par Network Manager. Vous devez exécuter les scripts avant d'installer Network Manager.

Pourquoi et quand exécuter cette tâche

Si vous avez téléchargé le progiciel compressé depuis Passport Advantage, comme indiqué dans «Installation d'IBM Installation Manager en téléchargeant les fichiers du produit», à la page 48, les scripts de création de base de données sont inclus au niveau supérieur du fichier de logiciel non compressé. Copiez les scripts sur le serveur de base de données et utilisez-les.

Sinon, installez les scripts de création de base de données de topologie Network Manager en exécutant les tâches ci-dessous.

Procédure

1. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

      ```
      ./IBMIM
      ```

      IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
2. Cliquez sur **Installer**.
3. Dans l'écran d'**installation des packages**, dans lequel vous pouvez sélectionner les packages à installer, sélectionnez la dernière version disponible des **scripts de création de la base de données topologiques de Network Manager**.
4. Cliquez sur **Suivant**, acceptez les dispositions du contrat de licence et cliquez de nouveau sur **Suivant**.
5. Sélectionnez le groupe de packages **IBM Netcool Core Server** et cliquez sur **Suivant**.
6. Dans l'écran d'**installation des packages** dans lequel vous pouvez sélectionner les fonctions à installer, sélectionnez les scripts correspondant au type de votre base de données.
7. Cliquez sur **Suivant** et **Installer**.

Résultats

Les scripts de la base de données appropriés sont maintenant installés dans le répertoire `precision/scripts/` dans le répertoire d'installation (par défaut, IBM/netcool/core/precision/scripts/). Pour des raisons de commodité, un fichier compressé contenant les mêmes scripts de base de données est également créé dans le répertoire d'installation. Si vous avez installé les scripts sur un serveur différent du serveur de base de données, copiez le fichier compressé sur le serveur de base de données et décompressez-le pour utiliser les scripts de base de données. Utilisez les informations des sections suivantes afin de configurer la base de données topologiques avec les scripts.

Configuration des bases de données DB2 existantes sous UNIX

Pour pouvoir utiliser une base de données DB2 existante comme base de données topologiques sous UNIX, vous devez disposer d'une instance DB2 avant d'installer Network Manager.

Avant de commencer

La base de données de Network Manager est créée par des scripts qui sont installés dans le `precision/scripts/` dans le répertoire d'installation (par défaut, IBM/netcool/core/precision/scripts/). Vous devez avoir installé les scripts avant de tenter de créer la base de données. Pour de plus amples informations relatives à l'installation de scripts de base de données sur le serveur de base de données, voyez *Installing and running the Network Manager database scripts* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Pourquoi et quand exécuter cette tâche

Lors de l'installation de Network Manager, la base de données topologiques NCIM est installée dans la base de données DB2 créée.

Pour des informations sur l'installation et la configuration de DB2, consultez la documentation DB2 sur le site http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Procédure

1. Assurez-vous de disposer d'une instance DB2 dans laquelle le processus d'installation peut créer la base de données NCIM. Plusieurs domaines Network Manager peuvent partager la même instance.
2. Accédez au répertoire dans lequel l'instance est installée, puis accédez au sous-répertoire `sqllib`.
3. Pour configurer l'environnement, entrez la commande suivante :

Interpréteur de commandes	Commande
Bourne	`./db2profile`
C	`source db2cshrc`

   Les scripts encapsuleurs de l'application Network Manager configurent automatiquement l'environnement DB2.
4. Accédez au répertoire `precision/scripts/` dans le répertoire d'installation (par défaut, IBM/netcool/core/precision/scripts/).
5. En tant qu'administrateur, sous le nom d'utilisateur `db2inst1` par exemple, exécutez le script `create_db2_database.sh` en tant qu'administrateur DB2 en entrant la commande suivante sur le serveur DB2 :

   `./create_db2_database.sh` *`nom_base_de_données nom_utilisateur`* `-force`

   Où :

   `nom_base_de_données`
   Correspond au nom de la base de données.

   `nom_utilisateur`

   Correspond à l'utilisateur DB2 à utiliser pour se connecter à la base de données.

   Important : Cet utilisateur ne doit pas être l'administrateur. Il doit s'agir d'un utilisateur DB2 d'un système d'exploitation existant.

   `-force`
   Correspond à un argument forçant tout utilisateur DB2 à quitter l'instance avant que ne soit créée la base de données.

   Par exemple, pour créer une base de données DB2 appelée `ITNM` pour l'utilisateur DB2 `ncim`, entrez :

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

Après avoir exécuté `create_db2_database.sh`, redémarrez la base de données en tant qu'administrateur de DB2, comme suit : exécutez **db2stop** puis **db2start**.

6. Lors de l'exécution du programme d'installation de Network Manager par la suite, prenez soin de sélectionner l'option de configuration de la base de données DB2 existante. Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.

   Le programme d'installation remplit les propriétés de connexion dans les fichiers suivants. Vous pouvez consulter ces fichiers en cas de problème avec votre connexion à la base de données. Pour de plus amples informations relatives à la modification des fichiers suivants, référez-vous à *Configuring Network Manager for a changed IP address of the Db2 NCIM server* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

   - Les fichiers `DbLogins.`*`DOMAINE`*`.cfg` et `MibDbLogin.cfg` dans `NCHOME/etc/precision`. Ces fichiers sont utilisés par les processus de base de Network Manager.
   - Le fichier `tnm.properties` dans `$NMGUI_HOME/profile/etc/tnm`. Ces fichiers sont utilisés par l'interface graphique de Network Manager.

Concepts associés

Architecture de reprise en ligne Network Manager (processus centraux)

La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Installation et configuration de bases de données Oracle sous UNIX

Pour utiliser une base de données topologiques Oracle sous UNIX, vous devez installer Oracle, configurer un schéma, puis créer une base de données avant d'installer Network Manager. Lors de l'installation, la base de données topologiques NCIM est installée dans la base de données Oracle créée.

Avant de commencer

La base de données de Network Manager est créée par des scripts qui sont installés dans le `precision/scripts/` dans le répertoire d'installation (par défaut, IBM/netcool/core/precision/scripts/). Vous devez installer les scripts avant de tenter de créer la base de données.

Pour vous connecter à la base de données, il vous faut un accès à une ligne de commande qui utilise le client Oracle SQL*Plus.

Pourquoi et quand exécuter cette tâche

Si vous utilisez Oracle, vérifiez que vous êtes autorisé à utiliser la fonction de partitionnement. Cette fonction supplémentaire est obligatoire pour que Network Manager fonctionne correctement.

Pour des informations sur l'installation et la configuration d'Oracle, voir la documentation d'Oracle à l'adresse http://docs.oracle.com/en/database/.

Le script de création de la base de données crée des utilisateurs pour plusieurs utilisateurs Oracle. Seul l'utilisateur `ncim` a le droit de se connecter à la base de données. Il possède également un droit d'accès aux schémas des autres utilisateurs. Le mot de passe par défaut créé par le script est identique au nom de l'utilisateur, soit : `ncim`.

Procédure

1. Installez Oracle, y compris la fonction de partitionnement, et configurez un schéma dans lequel le processus d'installation peut créer la base de données NCIM.
2. Vérifiez l'absence de conflit de port avec le service HTTP de la base de données XML Oracle.

   Le service HTTP de la base de données XML Oracle est configuré pour utiliser le port par défaut 8888.

3. Vérifiez que le programme d'écoute TNS Oracle s'exécute sur le serveur Oracle en entrant la commande suivante : `$ORACLE_HOME/bin/lsnrctl status`.
4. Si le programme d'écoute TNS Oracle ne s'exécute pas, démarrez-le à l'aide de la commande suivante : `$ORACLE_HOME/bin/lsnrctl start`.
5. En tant qu'administrateur de base de données Oracle, accédez au répertoire `precision/scripts/` dans le répertoire d'installation (par défaut, IBM/netcool/core/precision/scripts/).
6. Si vous avez installé Oracle sur un serveur différent de Network Manager, copiez le fichier `oracle_creation_scripts.tar.gz` sur ce serveur et extrayez tous les fichiers.
7. Exécutez le script `create_oracle_ncadmin_user.sh` sur le serveur où est installée la base de données. Connectez-vous à l'hôte Oracle en tant qu'administrateur de la base de données Oracle, puis exécutez le script `create_oracle_ncadmin_user.sh` en indiquant le nom d'utilisateur et le mot de passe `sys`. Exécutez le script comme dans l'exemple ci-dessous.

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

   Où les paramètres suivants s'appliquent :

   mot de passe
   Indique le mot de passe de l'utilisateur `sys`.

   -pdb *nom_base_données_connectable*
   Facultatif : si vous exécutez Oracle 12c avec RAC, vous devez utiliser une base de données connectable. Dans ce cas, utilisez ce paramètre pour indiquer le nom de la base de données connectable Oracle 12c.
8. Pour créer la base de données, exécutez le script `./create_oracle_database.sh`. En tant qu'administrateur de base de données Oracle, exécutez le script `./create_oracle_database.sh` en indiquant le nom d'utilisateur et le mot de passe `system`. Sur le serveur Network Manager, le script se trouve dans le répertoire `$ITNMHOME/scripts/sql/oracle`. Exécutez le script sur le serveur où est installée la base de données. Exécutez le script comme dans l'exemple ci-dessous.

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

   Où les paramètres suivants s'appliquent :

   mot de passe
   Indique le mot de passe de l'utilisateur `system`.

   -asm
   Indiquez `-asm` si votre base de données Oracle utilise ASM.

   -pdb *nom_base_données_connectable*
   Facultatif : si vous exécutez Oracle 12c avec RAC, vous devez utiliser une base de données connectable. Dans ce cas, utilisez ce paramètre pour indiquer le nom de la base de données connectable Oracle 12c.
9. Lors de l'exécution du programme d'installation de Network Manager par la suite, sélectionnez l'option de connexion à une base de données Oracle existante. Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.

   Le programme d'installation remplit les propriétés de connexion dans les fichiers suivants. Vous pouvez consulter ces fichiers en cas de problème avec votre connexion à la base de données. Pour de plus amples informations relatives à la modification des fichiers suivants, référez-vous à *Configuring Network Manager for a changed IP address of the Db2 NCIM server* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

   - Les fichiers `DbLogins.DOMAINE.cfg` et `MibDbLogin.cfg` dans `NCHOME/etc/precision`. Ces fichiers sont utilisés par les processus de base de Network Manager.

- Le fichier `tnm.properties` dans `$NMGUI_HOME/profile/etc/tnm`. Ces fichiers sont utilisés par l'interface graphique de Network Manager.

Remarque : Si vous installez Network Manager dans un environnement à haute disponibilité Oracle qui utilise RAC (Real Application Clusters), installez Network Manager au préalable avec une connexion directe à un noeud unique dans le cluster Oracle. Après avoir réussi l'installation de Network Manager, vous pouvez établir une grande disponibilité pour Network Manager avec une adresse Oracle Single Client Access Name (SCAN) comme décrit dans *Configuring Network Manager to work with Db2 HADR or Oracle RAC* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

10. Facultatif : Après avoir installé Network Manager, exécutez le script `$NCHOME/precision/scripts/sql/oracle/restrict_oracle_privileges.sh` en tant qu'utilisateur disposant de privilèges système. Maintenant que toutes les bases de données et tous les schémas ont été créés, ce script peut être utilisé pour révoquer les privilèges de création de la base de données à partir de l'utilisateur de base de données NCIM. Seules les opérations requises pour Network Manager pendant l'exécution restent accordées.
11. Facultatif : Pour activer le Chiffrement de Réseau Oracle, établissez le chiffrement sur REQUIRED sur le serveur de base de données.

    Vous n'avez pas besoin de configurer Network Manager pour le Chiffrement de Réseau Oracle. Référez-vous à votre documentation Oracle pour connaître les détails sur la manière d'activer le Chiffrement de Réseau Oracle.

Paramétrer NCIM pour l'utilisation de caractères Multibyte.

Vous devez configurer la base de données NCIM pour utiliser les caractères Multibyte, tels que les caractère du chinois simplifié, si vous voulez que la base de données NCIM conserve les données Multibyte. Une telle configuration est utile lorsque, par exemple, vous avez besoin d'entrer des caractères multi-octets dans la zone Description d'une définition d'interrogation.

Pourquoi et quand exécuter cette tâche

Vérifiez que les paramètres suivants sont définis pour la base de données NCIM :

Db2

Si vous exécutez Network Manager dans un environnement local qui prend en charge des caractères multi-octets, aucune modification de configuration n'est requise. Par exemple, les deux environnements locaux suivants prennent en charge les caractères multi-octets lors de l'exécution de NCIM sous DB2 :

- ```
  LANG=zh_CN.gb18030
  LC_ALL=zh_CN.gb18030
  ```
- ```
  LANG=en_US.utf8
  LC_ALL=en_US.utf8
  ```

Configuration de NCIM pour la gestion des caractères multi-octets sur une base de données Oracle

Ces informations permettent de configurer la base de données NCIM en cours d'exécution sous Oracle pour la gestion des caractères multi-octets.

Pourquoi et quand exécuter cette tâche

Pour configurer NCIM en vue de prendre en charge les caractères multi-octets sur une base de données ORACLE :

Procédure

1. Attribuez à la variable d'environnement NLS_LANG Oracle une valeur appropriée.

Par exemple, si le système fonctionne sous la localisation zh_CN.gb18030, changez la définition NLS_LANG pour la valeur suivante : `SIMPLIFIED CHINESE_CHINA.ZHS32GB18030`.

Un ensemble complet de valeurs de variable d'environnement NLS_LANG pour différents environnements locaux est disponible sur le site Web Oracle.

2. Configurez l'environnement Network Manager afin de prendre en compte vos modifications après l'installation.
   - Accédez au répertoire $NCHOME et émettez la commande suivante : `source env.sh`.

Installation et configuration d'Tivoli Netcool/OMNIbus

Vous devez installer Tivoli Netcool/OMNIbus avant d'installer Network Manager.

Pourquoi et quand exécuter cette tâche

Network Manager requiert Tivoli Netcool/OMNIbus. Il prend en charge les versions suivantes de Tivoli Netcool/OMNIbus :

- version 7.4
- Version 8.1, Fix Pack 23 ou version ultérieure

Si vous n'avez pas déjà installé Tivoli Netcool/OMNIbus, et prévoyez de l'installer sur le même serveur que Network Manager, vous n'avez besoin d'effectuer aucune opération pour le moment.

Lorsque vous installez Network Manager, installez Tivoli Netcool/OMNIbus en même temps en sélectionnant les composants principaux deTivoli Netcool/OMNIbus et de Network Manager dans le package **IBM Netcool Core Components**.

Le programme d'installation du composant principal de Network Manager configure automatiquement Tivoli Netcool/OMNIbus pendant l'installation.

Si vous n'avez pas encore installé Tivoli Netcool/OMNIbus et prévoyez de l'installer sur un autre serveur que Network Manager, installez Tivoli Netcool/OMNIbus **avant** Network Manager.

Consultez les informations sur l'installation de votre version de Tivoli Netcool/OMNIbus à l'adresse suivante : http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Installez ensuite Netcool/OMNIbus Knowledge Library et la sonde de SNMP. Vous trouverez des informations sur l'installation de Netcool/OMNIbus Knowledge Library à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/nckl/wip/concept/nckl_intro.html, et sur l'installation de la sonde pour SNMP à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/snmp/wip/concept/snmp_introduction_c.html.

Si vous avez déjà installé Tivoli Netcool/OMNIbus, Netcool/OMNIbus Knowledge Library, et la sonde pour SNMP, vous pouvez maintenant installer Network Manager.

Le programme d'installation Network Manager configure automatiquement Tivoli Netcool/OMNIbus pendant l'installation.

Si vous avez déjà installé et configuré Network Manager et Tivoli Netcool/OMNIbus mais que l'ObjectServer a été modifié après l'installation, vous devez réintégrer l'ObjectServer à Network Manager. Pour réintégrer l'ObjectServer, vous devez posséder des connaissances dans les domaines suivants.

- Composants principaux (core) de Network Manager. Si le nom, le port ou le nom d'hôte d'ObjectServer change, vous devez modifier manuellement les composants principaux de Network Manager.
- Intégration à la source de données de Interface graphique Web. Pour plus d'informations sur l'intégration à la source de données Interface graphique Web, voir «Configuration du nom de la source de données Tivoli Netcool/OMNIbus Web GUI», à la page 92.
- Script `config_object_server_for_itnm.sh`. La prise en charge de ce script a été ajoutée à Network Manager 4.2 correctif temporaire 2 ; si vous avez le correctif temporaire 2, alors ce script remplace le script **`ConfigOMNI`**. Il fournit la possibilité de configurer un serveur ObjectServer Windows ou UNIX existant pour qu'il s'exécute avec Network Manager. Le script est exécuté sur le serveur central

Network Manager et peut être utilisé pour configurer un serveur ObjectServer soit sur le serveur local, soit sur le serveur distant.

- Script **ConfigOMNI**. Utilisez le script **ConfigOMNI** pour créer et configurer un serveur ObjectServer afin qu'il s'exécute avec Network Manager. Le script crée les déclencheurs Network Manager. Si l'ObjectServer se trouve sur un serveur distant, copiez le script `$NCHOME/precision/install/scripts/ConfigOMNI` et le script de support `$NCHOME/precision/scripts/create_itnm_triggers.sql`, puis placez-les dans le même répertoire sur l'ObjectServer distant. Si l'ObjectServer est local sur Network Manager, vous pouvez utiliser les deux scripts tels quels.

Tâches associées

Configuration d'un serveur ObjectServer à utiliser avec les processus centraux Network Manager
Pour les utilisateurs ayant Network Manager 4.2 correctif temporaire 2 uniquement, vous pouvez utiliser le script `config_object_server_for_itnm.sh` pour configurer un serveur ObjectServer à utiliser avec les processus centraux Network Manager. Ce script prend en charge un serveur ObjectServer s'exécutant sur Windows ainsi que sur UNIX. Le script configure la connexion au serveur ObjectServer et peut être utilisé pour configurer un serveur ObjectServer local ou distant. Il exécute aussi un certain nombre de commandes SQL qui créent et configurent dans le serveur ObjectServer les tables et les utilisateurs requis par Network Manager.

Options de ligne de commande ConfigOMNI

Le script `$NCHOME/precision/install/scripts/ConfigOMNI`, associé à des arguments facultatifs avancés permet de configurer Tivoli Netcool/OMNIbus en vue d'une utilisation avec Network Manager.

Le script **ConfigOMNI** est démarré par le biais de la ligne de commande suivante. Les arguments facultatifs sont présentés entre crochets.

```
ConfigOMNI -o name -p password [ -a ] [ -c ] [ -e ]
[ -h directory ]  [ -n portnumber ] [ -u password ] [ -z PA authentication ]
```

L'exemple suivant exécute le script dans ObjectServer DIAMOND avec le mot de passe d'administration p3w0d. Si le serveur d'objets ObjectServer DIAMOND n'existe pas, il est créé. En sélectionnant les options appropriées, vous pouvez configurer le script afin d'ajouter les utilisateurs `itnmadmin` et `itnmuser` au serveur d'objets ObjectServer, activer le chiffrement AES ainsi que le contrôle de processus pour le serveur Objectserver.

Remarque : Le script **ConfigOMNI** n'effectue aucune configuration sauf si les options appropriées de la ligne de commande sont fournies ou si vous répondez aux questions appropriées.

```
ConfigOMNI -o DIAMOND -p p3w0d
```

Remarque : Le script **ConfigOMNI** est utilisé lors de la première configuration d'un serveur ObjectServer. Si ce **ConfigOMNI** script est exécuté plusieurs fois sur le même hôte, il peut s'avérer nécessaire d'éditer les fichiers suivants :

1. Fichier `nco_p_mttrapd.props` pour supprimer les propriétés en double `Server`, `ServerBackup`, `RulesFile`, `MIBFile` et `QuietOutput` à la fin du fichier.
2. Fichier `nco_pa.conf` pour modifier les noms en double `nco_process` car le script fournit toujours des entrées ayant pour nom `MasterObjectServer` et `Mttrapd`. Pour plus d'informations sur l'édition de ce fichier, voir la documentation Tivoli Netcool/OMNIbus à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html et recherchez la rubrique "Defining processes in the process agent configuration file".

Le tableau suivant décrit les options de ligne de commande pour le script **ConfigOMNI**.

Tableau 6. Options de ligne de commande ConfigOMNI

Options de ligne de commande	Description
-o *nom*	Nom du serveur ObjectServer que vous voulez créer ou configurer.

Tableau 6. Options de ligne de commande ConfigOMNI (suite)	
Options de ligne de commande	**Description**
-p *mot de passe*	Mot de passe d'administration du serveur ObjectServer que vous voulez créer ou configurer.
-a	Facultatif. Exécute le script en mode interactif, ce qui fait que des invites sont émises pour toutes les informations.
-c	Facultatif. Configure ObjectServer pour qu'il s'exécute sous le contrôle du processus Tivoli Netcool/OMNIbus.
-e	Facultatif. Définit le chiffrement AES pour le mot de passe ObjectServer.
-h *répertoire*	Facultatif. Répertoire contenant l'installation Tivoli Netcool/OMNIbus (OMNIHOME).
-n *numéroport*	Facultatif. Numéro de port du serveur ObjectServer que vous voulez créer ou configurer.
-u *mot de passe*	Facultatif. Crée les utilisateurs `itnmadmin` et `itnmuser` sur le serveur ObjectServer.
-z *authentification_agent_processus*	Facultatif. Fournit l'authentification pour l'agent de processus Tivoli Netcool/OMNIbus `NCO_PA`, pour le moment où `NCO_PA`démarre. Si vous n'entrez pas de valeur, `PAM` est utilisé par défaut.

Installation des composants de base de Network Manager

Vous devez installer les composants principaux de Network Manager avant d'installer les composants de l'interface graphique ou en même temps.

Avant de commencer

Avant d'installer les composants principaux de Network Manager, vous devez installer et configurer une base de données topologiques, avoir installé IBM Installation Manager, et avoir installé et démarré Tivoli Netcool/OMNIbus.

Assurez-vous qu'une version compatible de Python est installée sur ce serveur avant de commencer.

Pourquoi et quand exécuter cette tâche

Fix Pack 11

Important : Si vous voulez utiliser WebSphere Application Server version 9, vous devez avoir une nouvelle installation de WebSphere Application Server version 9 et Network Manager Fix Pack 11. Ceci parce que le chemin de mise à niveau n'est pas disponible pour WebSphere Application Server depuis la version 8 à la version 9.

Fix Pack 6

Important : L'installation de Fix Pack 6 ou ultérieur supprime les fichiers MIB existants. Network Manager Ces Fix Packs ne contiennent pas de Base d'Information de Gestion (fichiers MIB). Network Manager Fix Pack 5 contient les fichiers MIB. Les MIB sont nécessaires à la reconnaissance de réseau.

Si vous actualisez depuis Fix Pack 5 ou antérieurs, menez à bien les étapes suivantes pour obtenir les fichiers MIB :

1. Situez un fichier zip nommé `com.ibm.tivoli.netcool.ncp.mibs.all.any_*.zip` dans l'emplacement partagé IBM Installation Manager qui contient les fichiers MIB depuis l'installation du Fix Pack précédent. Le chemin d'extraction peut être différent dans votre installation. Un exemple de chemin : `/opt/IBM/IBMIM/native/`
2. Décompressez ce fichier.
3. Chargez les MIB dans la base de données en exécutant la commande ncp_mib, comme décrit dans *Loading updated MIB information* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Si vous installez Fix Pack 6, 7, 8, ou 9 sans actualiser, ou si vous n'arrivez pas à situer les fichiers MIB en utilisant la procédure ci-dessus, menez à bien les étapes suivantes pour obtenir les fichiers MIB :

1. Exécutez la commande **ncp_mib**, comme décrit dans : *Chargement des informations MIB mises à jour* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.
2. Si vous avez installé Network Manager 4.2 Fix Pack 5, faites une sauvegarde des contenus du répertoire `$NCHOME/precision/mibs/` dans un répertoire de sauvegarde hors de `$NCHOME`. Par exemple, `/mibs_backup/`.
3. Si vous avez installé une version plus récente que 4.2 Fix Pack 5, menez à bien les étapes suivantes :
   a. Faites une sauvegarde des contenus du répertoire `$NCHOME/precision/mibs/` vers un répertoire de sauvegarde hors de `$NCHOME`. Par exemple, `/old_mibs/`. Gardez ce répertoire et les fichiers qu'il contient au cas où vous voudriez revenir à la version plus ancienne.
   b. Téléchargez les fichiers Network Manager Fix Pack 5 (4.2.0.5) depuis IBM Fix Central : https://www.ibm.com/support/fixcentral/

      Important : Téléchargez les fichiers pour Linux x86, sans considération pour la plateforme que vous utilisez.
   c. Décompressez le paquet Network Manager dans un répertoire temporaire.
   d. Décompressez l'archive `repositories/disk1/ad/native/file000876` dans un répertoire de backup hors de `$NCHOME`, par exemple, `/mibs_backup/`. Ce répertoire contient les fichiers MIB par défaut.
   e. Si vous avez des fichiers MIB personnalisés ou ajoutés, copiez les fichiers MIB personnalisés ou nouveaux depuis `/old_mibs/` en écrasant les fichiers par défaut de `/mibs_backup/`.
4. Quelle que soit la version de Network Manager que vous avez installé, le répertoire `/mibs_backup/` contient à présent l'ensemble de la plupart des fichiers MIB actuels du Fix Pack 5, plus toutes les additions et personnalisations.

Une fois que vous avez obtenu les fichiers MIB, installez la version la plus récente de Network Manager.

1. Installez Network Manager Fix Pack 6 ou ultérieur en suivant les consignes de cette procédure.
2. Copiez les fichiers MIB files depuis votre répertoire `/mibs_backup/` vers la l'emplacement suivant dans l'installation : `$NCHOME/precision/mibs/`
3. Exécutez la commande **ncp_mib**, comme décrit dans : *Chargement des informations MIB mises à jour* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Pour désinstaller Fix Pack 6 ou ultérieur et utiliser une version précédente, menez à bien les étapes suivantes :

1. Copier les fichiers MIB depuis le répertoire suivant vers un répertoire temporaire : `$NCHOME/precision/mibs/`
2. Effacez tous les fichiers dans le répertoire `$NCHOME/precision/mibs`.
3. Désinstallez Network Manager Fix Pack 6 ou ultérieur en suivant les consignes de désinstallation de packs de réparation : *Désinstallation des packs de réparation* dans *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.
4. Si vous revenez à 4.2 Fix Pack 5, copiez les fichiers MIB du répertoire temporaire vers le répertoire MIB : `$NCHOME/precision/mibs/`

5. Si vous revenez à une version précédente à 4.2 Fix Pack 5, copiez les fichiers MIB depuis le répertoire de backup `/old_mibs/` vers le répertoire MIB : `$NCHOME/precision/mibs/`
6. Exécutez la commande **ncp_mib**, comme décrit dans : *Chargement des informations MIB mises à jour* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*

Pour installer les composants principaux de Network Manager, procédez comme suit.

Procédure

1. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
2. Cliquez sur **Installer**.
3. Dans l'écran suivant d'**installation des packages**, dans lequel vous pouvez sélectionner les packages à installer, sélectionnez la dernière version disponible de **Network Manager Core Components**.

   Les prérequis d'installation du package sont évalués.
4. En cas de problèmes liés aux prérequis, résolvez-les à l'aide de l'information qui vous est fournie avant de continuer.
5. Cliquez sur **Suivant**, acceptez les dispositions du contrat de licence et cliquez de nouveau sur **Suivant**.
6. Sélectionnez le groupe de packages **IBM Netcool Core Components** et cliquez sur **Suivant**.

   Restriction : Si vous installez Network Manager sur le même serveur que Tivoli Netcool/OMNIbus, vous devez installer les composants principaux dans le même groupe de package que Tivoli Netcool/OMNIbus.
7. Sélectionnez les composants principaux (**Core composants**) à installer
8. Sélectionnez **Routines cryptographiques supplémentaires** si vous souhaitez utiliser toutes les options cryptographiques fournies par Network Manager. Désélectionnez cette option si vous devez mettre en place la conformité à la norme FIPS 140-2, car certains des composants ne sont pas conformes à cette norme. Pour plus d'informations, voir «Installations FIPS 140-2», à la page 40.
9. Dans les écrans d'**installation des packages** suivants, fournissez les informations de configuration des packages à installer. Utilisez **Suivant** et **Précédent** pour naviguer dans les options de configuration.
10. Facultatif : Si vous instalez Network Manager en même temps que Tivoli Netcool/OMNIbus,ou dans le même groupe de paquets qu'une installation de Tivoli Netcool/OMNIbus qui n'a pas été configurée pour une utilisation avec Network Manager, un nouvel ObjectServer agrégé est créé. Configurez le nouvel ObjectServer :

    Nom
    Acceptez le nom par défaut de NCO_AGG_P ou entrez un nouveau nom pour ObjectServer. Si cet ObjectServer doit être utilisé dans une architecture comportant plusieurs ObjectServers, gardez le suffixe _AGG_P avec le nom. Par convention, les noms ObjectServer sont en majuscules. Vous aurez besoin ultérieurement de ce nom pour démarrer et arrêter ObjectServer. Notez le nom dans «Liste de contrôle de l'installation», à la page 45.

    Hôte
    Entrez le nom d'hôte du serveur sur lequel Tivoli Netcool/OMNIbus est installé.

Port
Entrez le port à utiliser pour la connexion à ObjectServer ou pour accepter la valeur par défaut.

ID superutilisateur
L'installation utilise l'utilisateur `superutilisateur` Tivoli Netcool/OMNIbus.

Mot de passe
Entrez le mot de passe de l'utilisateur `superutilisateur`.

Confirmation du mot de passe
Entrez une seconde fois le mot de passe.

11. Facultatif : Si vous installez Network Manager sur un serveur autre que Tivoli Netcool/OMNIbus, Network Manager se connecte à un ObjectServer existant. L'ObjectServer doit être en cours d'exécution et être accessible depuis ce serveur. Indiquez les détails de l'ObjectServer auquel Network Manager doit se connecter.

    Nom
    Entrez le nom de l'ObjectServer.

    Hôte
    Entrez le nom d'hôte du serveur sur lequel Tivoli Netcool/OMNIbus est installé.

    Port
    Entrez le port à utiliser pour la connexion à ObjectServer ou pour accepter la valeur par défaut.

    ID superutilisateur
    Entrez le nom d'un utilisateur possédant les droits administratifs sur Tivoli Netcool/OMNIbus.

    Mot de passe
    Entrez le mot de passe de cet utilisateur.

    Les détails de connexion sont vérifiés par rapport à l'ObjectServer en cours d'exécution. Sélectionnez **Ignorer la vérification des détails de la connexion à ObjectServer** si vous ne pouvez pas vérifier les détails, par exemple si l'ObjectServer n'est pas accessible. Si vous sautez ce processus, vous devrez effectuer les modifications manuellement par la suite.

12. Configurez les utilisateurs par défaut de Network Manager. Les utilisateurs `itnmadmin` et `itnmuser` sont créés par le programme d'installation dans l'ObjectServer. Le même mot de passe est utilisé pour les deux utilisateurs.

    Mot de passe
    Indiquez le mot de passe de ces utilisateurs. Enregistrez le mot de passe.

    Confirmation du mot de passe
    Confirmez le mot de passe.

13. Entrez le nom du domaine de réseau. Ce nom est visible des opérateurs réseau et des administrateurs de produit. Vous pouvez aussi ajouter, supprimer et modifier les domaines par la suite. Enregistrez le nom que vous avez choisi. Vous avez besoin de ce nom pour démarrer les composants Network Manager.
14. Entrez les détails de la base de données topologiques installée. Notez ces détails. Vous en aurez besoin lors de l'installation des composants de l'interface graphique.
    a) Sélectionnez le type de base de données.
    b) Entrez les détails de la connexion à la base de données :

    Si vous avez sélectionné DB2 comme type de base de données, entrez les détails suivants :

    Nom de la base de données
    Entrez le nom de la base de données.

    Hôte serveur
    Entrez le nom d'hôte du serveur sur lequel la base de données est installée.

    Port du serveur
    Entrez le numéro de port de connexion à la base de données.

    User ID (ID utilisateur)
    Entrez l'ID d'un utilisateur DB2 autorisé à créer des tables.

Mot de passe
Entrez le mot de passe de cet utilisateur.

Si vous avez sélectionné Oracle comme type de base de données, entrez les détails suivants :

Nom de service Oracle
Entrez le nom de service de la base de données.

Hôte serveur
Entrez le nom d'hôte du serveur sur lequel la base de données est installée.

User ID (ID utilisateur)
Entrez l'ID d'un utilisateur Oracle existant autorisé à accéder aux tables NCIM. L'ID utilisateur par défaut est `ncim`.

Mot de passe
Entrez le mot de passe de cet utilisateur.

c) Sélectionnez **Créer des tables pour conserver les données topologiques dans la base de données sélectionnée** pour créer les tables de la base de données requises par Network Manager. Si vous avez déjà créé les tables de base de données à l'aide des scripts de création de base de données, vous n'avez pas besoin de sélectionner cette option. Si vous avez déjà créé les tables et sélectionnez de nouveau l'option permettant de les créer, vous recevez une erreur à la fin de l'installation. Cette erreur indique que les tables n'ont pas été créées.

d) Sélectionnez **Ignorez la vérification des détails de la connexion à la base de données** si vous ne souhaitez pas vérifier la connexion, si la base de données est inaccessible ou pour d'autres raisons.

15. Configurez les détails de l'agrégation d'un programme d'interrogation :

Chemin Python
Entrez le chemin d'accès complet à une version compatible de Python.

Utilisateur de l'agrégation de l'interrogateur

Si vous effectuez une installation en tant que superutilisateur, vous devez entrer le nom d'un utilisateur qui ne soit pas un superutilisateur, Cet utilisateur est nécessaire pour exécuter le moteur d'agrégation de l'interrogateur. Si vous effectuez une installation en tant qu'utilisateur non-root, l'utilisateur ayant fait l'installation exécute le moteur d'agrégation de l'interrogateur et cette option ne s'affiche pas dans l'interrogateur. Cet utilisateur doit être créé avant l'agrégation de l'interrogateur.

Groupe d'agrégation de l'interrogateur
Entrez le groupe auquel appartient l'utilisateur d'agrégation de l'interrogateur. Si l'utilisateur appartient à un groupe différent de celui de l'utilisateur ayant effectué l'installation, le programme d'installation modifie les droits d'accès par défaut sur les fichiers et les dossiers afin que l'agrégation de l'interrogateur puisse fonctionner. L'utilisateur doit exister en tant que membre de ce groupe pour que l'agrégation de l'interrogateur soit possible.

16. Vérifiez les informations récapitulatives puis cliquez sur **Installer**.

Résultats

Les composants principaux de Network Manager sont installés. Les erreurs éventuelles sont écrites dans le fichier journal de l'installation que vous pouvez afficher en cliquant sur **View Log File**. Les fichiers journaux sont conservés dans le répertoire `/logs/` dans l'emplacement de données d'IBM Installation Manager.

Tâches associées

Activation de l'interrogation historique

Si vous avez installé Network Manager en tant que superutilisateur, vous devez exécuter le script `setup_run_storm_as_non_root.sh` pour permettre aux processus des données d'interrogation

historiques de s'exécuter. Il n'est pas nécessaire d'exécuter le script si vous avez installé Network Manager en tant que non superutilisateur.

Installation de WebSphere Application Server

Vous devez installer les composants requis de WebSphere Application Server avant d'installer Jazz for Service Management.

Avant de commencer

Vous devez installer WebSphere Application Server sur le serveur sur lequel vous souhaitez installer les composants de l'interface graphique utilisateur de Network Manager.

Pourquoi et quand exécuter cette tâche

Remarque :

En cas de différence entre ces instructions et la documentation de votre version de WebSphere Application Server en raison de mises à jour ou de modifications, la documentation de WebSphere Application Server est prioritaire. Vous pouvez la consulter à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSEQTP/mapfiles/product_welcome_was.html

Procédure

1. Sur le serveur sur lequel vous souhaitez installer les composants de l'interface graphique de Network Manager, assurez-vous qu'IBM Installation Manager est installé.
2. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
3. Cliquez sur **Installer**.
4. Dans l'écran suivant d'**installation des packages**, dans lequel vous pouvez sélectionner les packages à installer, sélectionnez les composants suivants et cliquez sur **Suivant** :
   - IBM Websphere Application Server. Network Manager requiert IBM Websphere Application Server Version 8.5.5.17 (version 8) ou 9.0.5.5 (version 9) ou ultérieur.

     Remarque : Si vous voulez utiliser WebSphere Application Server version 9, vous devez avoir une nouvelle installation de WebSphere Application Server version 9, Network Manager Fix Pack 11 et Tivoli Netcool/OMNIbus Web GUI Version 8.1.0.20 ou ultérieur. Ceci parce que le chemin de mise à niveau n'est pas disponible pour WebSphere Application Server depuis la version 8 à la version 9.
   - IBM Websphere SDK Java Technology Edition. Pour Network Manager Fix Pack 9 et les versions antérieures, ce composant doit être installé séparément, et la version 8 est requise. Pour Network Manager Fix Pack 10 et versions ultérieures, ce composant est installé avec WebSphere Application Server et n'a pas besoin d'être ici sélectionné.
   - Jazz for Service Management extension for IBM Websphere. Utilisez la version correspondant à votre version d'IBM Websphere Application Server.

   Les prérequis d'installation du package sont évalués.

5. En cas de problèmes liés aux prérequis affichés, résolvez-les à l'aide de l'information qui vous est fournie avant de continuer.
6. Cliquez sur **Suivant**, acceptez les dispositions du contrat de licence et cliquez de nouveau sur **Suivant**.
7. Sélectionnez le groupe de packages **IBM Websphere Application Server**.
8. Entrez le répertoire d'installation du groupe de packages, par exemple un répertoire `/was/` situé sous le répertoire d'installation des produits IBM, puis cliquez sur **Suivant**.
9. Sélectionnez toutes les fonctionnalités d'IBM Websphere Application Server à installer sauf les **exemples d'applications**.
10. Sélectionnez la version 64 bits d'IBM Websphere SDK Java Technology Edition.
11. Sélectionnez l'extension JazzSM Websphere Extension à installer et cliquez sur **Suivant**.
12. Une fois les composants installés, le système vous demande quels programmes vous souhaitez démarrer. Sélectionnez **Aucun**.

Installation de Dashboard Application Services Hub

Vous devez installer Dashboard Application Services Hub avant d'installer les composants de l'interface graphique Network Manager.

Pourquoi et quand exécuter cette tâche

Dashboard Application Services Hub est un composant de Jazz for Service Management.

Avant d'installer des composants de Jazz for Service Management, vous devez exécuter IBM Prerequisite Scanner et vérifier les prérequis de tous les composants de Jazz for Service Management à installer. Pour plus d'informations, voir «Vérification des prérequis du système», à la page 22.

Remarque :

En cas de différence entre ces instructions et la documentation de votre version des composants de Jazz for Service Management à mettre à jour ou modifier, la documentation de Jazz for Service Management est prioritaire. Vous pouvez la consulter à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSEKCU

Procédure

1. Sur le serveur sur lequel vous souhaitez installer les composants de l'interface graphique de Network Manager, assurez-vous qu'IBM Installation Manager est installé.
2. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
3. Cliquez sur **Installer**.
4. Dans l'écran suivant d'**installation des packages**, dans lequel vous pouvez sélectionner les packages à installer, sélectionnez **IBM Dashboard Application Services Hub** et cliquez sur **Suivant**. Network Manager nécessite Dashboard Application Services Hub Version 3.1.3.8 ou ultérieures.

   Les prérequis d'installation du package sont évalués.

5. En cas de problèmes liés aux prérequis affichés, résolvez-les à l'aide de l'information qui vous est fournie avant de continuer.
6. Cliquez sur **Suivant**, acceptez les dispositions du contrat de licence et cliquez de nouveau sur **Suivant**.
7. Sélectionnez le groupe de packages **Core services in Jazz for Service Management**.
8. Entrez le répertoire d'installation du groupe de packages, par exemple un répertoire `/jazz/` situé sous le répertoire d'installation des produits IBM, puis cliquez sur **Suivant**.
9. Sélectionnez la version 64 bits d'IBM Dashboard Application Services Hub.
10. Sélectionnez toutes les fonctionnalités d'IBM Dashboard Application Services Hub à installer.
11. Dans les écrans d'**installation des packages** suivants, fournissez les informations de configuration des packages à installer. Utilisez **Suivant** et **Précédent** pour naviguer dans les options de configuration.
12. Facultatif : Configurez les détails de WebSphere Application Server.

    S'il s'agit du premier composant à installer dans WebSphere Application Server sur ce serveur, vous devez configurer tous les détails. Si un autre composant a déjà été installé dans WebSphere Application Server, les détails existants sont utilisés. Les détails configurés précédemment sont affichés en grisé, et vous devez reconfirmer uniquement le nom d'utilisateur et le mot de passe.

    Emplacement d'installation de WebSphere
    Indiquez l'emplacement où WebSphere Application Server a été installé.

    Type de déploiement du profil
    Sélectionnez **Create Websphere profile**. Un profil est une méthode permettant de regrouper des applications dans un WebSphere Application Server. Si votre déploiement de WebSphere Application Server est volumineux, adressez-vous à votre administrateur pour savoir quel profil utiliser.

    Emplacement du profil
    Conservez l'emplacement par défaut ou entrez le nouvel emplacement du profil. Les caractères suivants ne peuvent pas être utilisés dans le cheminWebSphere Application Server de profil.

    ```
    ` ! # $ % ^ & * + = { } [ ] | ; " < > , ? @ ~ .
    ```

    Nom du profil
    Entrez un nom descriptif unique pour le profil.

    Nom de nœud
    Entrez un nom descriptif unique pour le nœud.

    Nom du serveur
    Entrez un nom descriptif unique pour le serveur logique qui est créé dans WebSphere Application Server et qui est associé à ce profil. Notez ces informations : vous en aurez besoin lors de l'installation d'autres applications dans WebSphere Application Server.

    Nom d'utilisateur
    Conservez le nom d'utilisateur `smadmin` par défaut. Cet utilisateur sera créé dans WebSphere Application Server. Notez ces informations : vous en aurez besoin lors de l'installation d'autres applications dans WebSphere Application Server.

    Mot de passe
    Entrez un mot de passe pour cet utilisateur. Notez ces informations : vous en aurez besoin lors de l'installation d'autres applications dans WebSphere Application Server.

    Confirmation du mot de passe
    Confirmez le mot de passe.
13. Facultatif : Configurez les ports de WebSphere Application Server.

    S'il s'agit du premier composant à installer dans WebSphere Application Server, vous devez configurer les ports. Si un autre composant a déjà été installé dans WebSphere Application Server, cet écran ne s'affiche pas. Conservez les valeurs de port comme valeurs par défaut sauf s'il y a un conflit avec d'autres applications.

Port de transfert HTTP
Port utilisé pour accéder à WebSphere Application Server.

Important : Notez cette valeur par écrit. Vous en aurez besoin pour accéder aux applications installées dans WebSphere Application Server.

Port de transfert HTTPS
Port utilisé pour accéder à WebSphere Application Server avec HTTPS.

Important : Notez cette valeur par écrit. Vous en aurez besoin pour accéder aux applications installées dans WebSphere Application Server si vous utilisez HTTPS.

Port d'amorce
Port utilisé pour les applications s'exécutant en dehors du serveur d'applications pour se connecter au bus de messages.

Port du connecteur SOAP
Port utilisé pour établir les connexions Java Management Extensions (JMX) au serveur via Simple Object Access Protocol (SOAP).

Port de connexion IPC
Port utilisé pour établir les connexions Java Management Extensions (JMX) au serveur via Inter-Process Communications (IPC).

Port de la console d'administration
Port permettant d'accéder à la console d'administration de WebSphere Application Server.

Important : Notez cette valeur par écrit. Vous en aurez besoin pour accéder à la console d'administration de WebSphere Application Server.

Port sécurisé de la console d'administration
Port permettant d'accéder à la console d'administration de WebSphere Application Server avec HTTPS.

Port de communication du gestionnaire à haute disponibilité
Port permettant d'accéder au gestionnaire à haute disponibilité.

Port d'écoute ORB
Port utilisé par le courtier ORB (Object Request Broker).

Port d'authentification du serveur SSL SAS
Port d'authentification de Secure Authentication Service.

Port d'écoute d'authentification du client CSIV2
Port d'écoute du client Common Secure Interoperability Specification, Version 2 (CSIv2).

Port d'écoute d'authentification du serveur CSIV2
Port d'écoute du serveur Common Secure Interoperability Specification, Version 2 (CSIv2).

Port de notification REST
Port de notification Representational State Transfer (REST) associé aux applications applications installées dans le profil Jazz for Service Management WebSphere.

Pour plus d'informations sur les ports, consultez la documentation de votre version de WebSphere Application Server à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSEQTP/mapfiles/product_welcome_was.html

14. Entrez la valeur de la racine de contexte de Dashboard Application Services Hub dans la zone **Context Root**.

    Dashboard Application Services Hub est une application hébergée dans WebSphere Application Server.

    La racine de contexte de Dashboard Application Services Hub définit le répertoire dans le contexte WebSphere Application Server dans lequel s'exécute Dashboard Application Services Hub.

    Par exemple, si l'URL de la racine de WebSphere Application Server est `http://`*`nom_hôte`*`:16310`, et si vous définissez la racine de contexte `/ibm/console/` pour Dashboard Application Services Hub, l'adresse URL d'accès à Dashboard Application Services Hub est `http://`

nom_hôte:16310/ibm/console/. L'adresse URL d'accès aux applications hébergées dans Dashboard Application Services Hub, est dans ce cas http://*nom_hôte*:16310/ibm/console/*nom_application*.

15. Cliquez sur **Validation** pour valider les valeurs de configuration puis cliquez sur **Suivant**.
16. Vérifiez les informations récapitulatives puis cliquez sur **Installer**.
17. Une fois les composants installés, le système vous demande quels programmes vous souhaitez démarrer. Sélectionnez **Aucun**.

Installation de Tivoli Netcool/OMNIbus Web GUI

Vous devez installer Interface graphique Web avant d'installer les composants de l'interface graphique Network Manager.

Avant de commencer

Avant d'installer Tivoli Netcool/OMNIbus Web GUI, vous devez installer WebSphere Application Server et Jazz for Service Management.

Pourquoi et quand exécuter cette tâche

Vous devez installer Interface graphique Web sur le serveur sur lequel vous souhaitez installer les composants de l'interface graphique utilisateur de Network Manager.

En cas de différence entre ces instructions et la documentation de votre version des composants de Tivoli Netcool/OMNIbus Web GUI en raison de mises à jour ou de modifications, la documentation de Tivoli Netcool/OMNIbus Web GUI est prioritaire. Vous pouvez la consulter à l'adresse suivante : http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Procédure

1. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
2. Cliquez sur **Installer**.
3. Dans l'écran suivant d'**installation des packages**, dans lequel vous pouvez sélectionner les packages à installer, sélectionnez **IBM Tivoli Netcool/OMNIbus Web GUI** et cliquez sur **Suivant**.

   Les prérequis d'installation du package sont évalués.
4. En cas de problèmes liés aux prérequis affichés, résolvez-les à l'aide de l'information qui vous est fournie avant de continuer.
5. Cliquez sur **Suivant**, acceptez les dispositions du contrat de licence et cliquez de nouveau sur **Suivant**.
6. Sélectionnez le groupe de packages **IBM Netcool**.
7. Entrez le répertoire d'installation du groupe de packages, par exemple un répertoire /gui/ situé sous le répertoire d'installation des produits IBM, puis cliquez sur **Suivant**.
8. Sélectionnez **Install base features** ainsi que les autres fonctions nécessaires à vos intégrations de produit.

9. Dans les écrans d'**installation des packages** suivants, fournissez les informations de configuration des packages à installer. Utilisez **Suivant** et **Précédent** pour naviguer dans les options de configuration.
10. Configurez les propriétés de WebSphere Application Server et Jazz for Service Management.

    Répertoire d'installation de WebSphere Application Server
    Entrez le répertoire d'installation de WebSphere Application Server.

    INTERFACE UTILISATEUR DE Jazz for Service Management
    Entrez le répertoire d'installation de Dashboard Application Services Hub.

    Nom du serveur
    Entrez le nom du serveur logique créé dans WebSphere Application Server.

    Nom d'utilisateur
    Entrez le nom d'utilisateur configuré pour accéder à ce serveur logique.

    Mot de passe
    Entrez le mot de passe de cet utilisateur.
11. Vérifiez les informations récapitulatives puis cliquez sur **Installer**.

Installation des composants principaux de l'interface graphique de Network Manager

Installez les composants Network Manager GUI seulement après l'installation des composants fondamentaux. Installez les composants de GUI sur le serveur qui a déjà été installé Jazz for Service Management.

Pourquoi et quand exécuter cette tâche

Pour installer les composants principaux de l'interface graphique Network Manager, procédez comme suit :

Procédure

1. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
2. Cliquez sur **Installer**.
3. Dans l'écran suivant d'**installation des packages**, dans lequel vous pouvez sélectionner les packages à installer, sélectionnez la dernière version disponible de **Network Manager GUI Components**.

   Les prérequis d'installation du package sont évalués.
4. En cas de problèmes liés aux prérequis affichés, résolvez-les à l'aide de l'information qui vous est fournie avant de continuer.
5. Cliquez sur **Suivant**, acceptez les dispositions du contrat de licence et cliquez de nouveau sur **Suivant**.
6. Sélectionnez le groupe de packages **IBM Netcool GUI Server** et cliquez sur **Suivant**.

Restriction : Vous devez installer les composants d'interface graphique dans le même groupe de packages que Tivoli Netcool/OMNIbus Web GUI.

7. Sélectionnez les **Fichiers de produit** à installer et cliquez sur **Suivant**.
8. Dans les écrans d'**installation des packages** suivants, fournissez les informations de configuration des packages à installer. Utilisez **Suivant** et **Précédent** pour naviguer dans les options de configuration.
9. Confirmez les propriétés de l'instance de Jazz for Service Management sur laquelle vous voulez effectuer l'installation.

   Détails du répertoire d'installation
   Chemin d'accès complet à l'instance de Dashboard Application Services Hub.

   Nom d'utilisateur
   Entrez le nom d'un utilisateur possédant les droits administratifs dans Dashboard Application Services Hub. S'il n'y a pas eu de modification, vous pouvez choisir l'utilisateur par défaut `smadmin` avec le mot de passe `netcool`.
10. Network Manager se connecte à un ObjectServer existant. L'ObjectServer doit déjà exister, être en cours d'exécution et être accessible depuis ce serveur. Indiquez les détails de l'ObjectServer auquel Network Manager doit se connecter. Ces détails doivent correspondre à ceux entrés lors de l'installation des composants principaux.

    Nom
    Entrez le nom de l'ObjectServer.

    Hôte
    Entrez le nom d'hôte du serveur sur lequel Tivoli Netcool/OMNIbus est installé.

    Port
    Entrez le port à utiliser pour la connexion à ObjectServer ou pour accepter la valeur par défaut.

    ID superutilisateur
    Entrez le nom d'un utilisateur possédant les droits administratifs sur Tivoli Netcool/OMNIbus.

    Mot de passe
    Entrez le mot de passe de cet utilisateur.

    Sélectionnez **Ignorer la vérification des détails de la connexion à ObjectServer** si une ou plusieurs des conditions s'appliquent :

    - Tivoli Netcool/OMNIbus WebGUI est déjà configuré avec une source de données et une source d'authentification. Si vous configurez des détails différents, l'installation écrase la configuration existante.
    - Vous ne pouvez pas vérifier les détails à ce stade, par exemple si l'ObjectServer n'est pas accessible. Si vous sautez ce processus, vous devrez effectuer les modifications manuellement par la suite.

    Jazz for Service Management est configuré pour utiliser cet ObjectServer pour l'authentification.
11. Configurez les utilisateurs par défaut de Network Manager. Les utilisateurs `itnmadmin` et `itnmuser` sont créés par le programme d'installation dans l'ObjectServer. Le même mot de passe est utilisé pour tous les utilisateurs. S'il existe un ou plusieurs de ces utilisateurs, le mot de passe n'est pas modifié.

    Mot de passe
    Indiquez le mot de passe de ces utilisateurs. Enregistrez le mot de passe.

    Confirmation du mot de passe
    Confirmez le mot de passe.
12. Entrez les détails de la base de données topologiques installée. Ces détails doivent correspondre à ceux entrés lors de l'installation des composants principaux.
    a) Sélectionnez le type de base de données.
    b) Entrez les détails de la connexion à la base de données :

    Si vous avez sélectionné DB2 comme type de base de données, entrez les détails suivants :

Nom de la base de données
Entrez le nom de la base de données.

Hôte serveur
Entrez le nom d'hôte du serveur sur lequel la base de données est installée.

Port du serveur
Entrez le numéro de port de connexion à la base de données.

User ID (ID utilisateur)
Entrez l'ID d'un utilisateur DB2 autorisé à créer des tables.

Mot de passe
Entrez le mot de passe de cet utilisateur.

Si vous avez sélectionné Oracle comme type de base de données, entrez les détails suivants :

Nom de service Oracle
Entrez le nom de service de la base de données.

Hôte serveur
Entrez le nom d'hôte du serveur sur lequel la base de données est installée.

User ID (ID utilisateur)
Entrez l'ID d'un utilisateur Oracle existant autorisé à accéder aux tables NCIM. L'ID utilisateur par défaut est `ncim`.

Mot de passe
Entrez le mot de passe de cet utilisateur.

c) Sélectionnez **Créer des tables pour conserver les données topologiques dans la base de données sélectionnée** pour créer les tables de la base de données requises par Network Manager. Si vous avez déjà créé les tables de base de données à l'aide des scripts de création de base de données, vous n'avez pas besoin de sélectionner cette option. Si vous avez déjà créé les tables et sélectionnez de nouveau l'option permettant de les créer, vous recevez une erreur à la fin de l'installation. Cette erreur indique que les tables n'ont pas été créées.

d) Sélectionnez **Ignorez la vérification des détails de la connexion à la base de données** si vous ne souhaitez pas vérifier la connexion, si la base de données est inaccessible ou pour d'autres raisons.

13. Vérifiez les informations récapitulatives puis cliquez sur **Installer**.

Résultats
Les composants de l'interface graphique utilisateur de Network Manager sont installés.Les erreurs éventuelles sont écrites dans le fichier journal de l'installation que vous pouvez afficher en cliquant sur **View Log File**. Les fichiers journaux sont conservés dans le répertoire `/logs/` dans l'emplacement de données d'IBM Installation Manager.

Installation et configuration d'Cognos Analytics

À partir de Network Manager Fix Pack 11, Tivoli Common Reporting n'est plus pris en charge. Pour utiliser des rapports, vous devez installer et configurer Cognos Analytics.

Pourquoi et quand exécuter cette tâche
La documentation correspondant à votre version de Cognos Analytics contient les informations les plus récentes et les plus complètes sur la configuration de ce produit. En cas de différence entre les informations ci-après et la documentation Cognos Analytics, celle-ci est prioritaire. Consultez les informations sur à l'adresse https://www.ibm.com/support/knowledgecenter/SSEP7J

Procédez comme suit pour configurer Cognos Analytics.

Procédure
1. Téléchargez le dernier groupe de correctifs disponible pour Cognos Analytics V11.

2. Installez Cognos Analytics.

   Utilisez les informations détaillées sur les prérequis et la procédure d'installation dans la documentation de Cognos Analytics.

   a) Effectuez l'installation en tant que superutilisateur.

   b) Lorsque le programme vous demande d'installer des composants, sélectionnez les services d'application et la passerelle facultative.

3. Définissez la variable d'environnement `COGNOS_HOME` sur le répertoire d'installation de Cognos Analytics.

   Le chemin doit se terminer par `analytics`.

4. Si vous utilisez DB2 en tant que base de données topologiques, copiez les fichiers suivants du serveur de base de données DB2 au serveur **Production de rapports Cognos**.

   - Copiez `$Db2_HOME/sqllib/java/db2jcc.jar` vers `$COGNOS_HOME/webapps/p2pd/WEB-INF/lib/`.
   - Copiez `$Db2_HOME/sqllib/java/db2jcc_license_cu.jar` vers `$COGNOS_HOME/webapps/p2pd/WEB-INF/lib/`.
   - Copiez `$Db2_HOME/sqllib/java/db2jcc.jar` vers `$COGNOS_HOME/drivers/`.

5. Configurez les sources de données pour la génération de rapports.

   a) Démarrez IBM Cognos Configuration à l'aide de la commande appropriée.

   Par exemple : `$COGNOS_HOME/bin64/cogconfig.sh`

   b) Sélectionnez **Accès aux données** > **Content Manager** > **Content Store**. Entrez les informations détaillées de votre base de données NCIM.

   c) Cliquez sur **Actions** > **Start** pour démarrer le serveur Cognos.

   Le démarrage du serveur risque de prendre un certain temps.

   d) Connectez-vous à l'interface graphique Cognos Analytics.

   Par défaut, l'URL de connexion est `http://`*`hôte`*`:9300/bi`.

   e) Cliquez sur **Gérer** > **console d'administration** pour démarrer la console d'administration.

   f) Cliquez sur **Configuration** > **Data Source Connection** > **New Data Source** pour ajouter les connexions à la base de données.

   Ajoutez les connexions suivantes :

Tableau 7. Connexions à la base de données

Produit	Nom	Type	Paramètres de connexion JDBC
ITNM	IBM_TRAM	IBM DB2	currentSchema=NCIM;
	NCIM		currentSchema=NCIM;
	NCMONITOR		currentSchema=NCMONITOR;
	NCPGUI		currentSchema=NCPGUI;
	NCPOLLDATA		currentSchema=NCPOLLDATA;
	PARAMETERS		currentSchema=NCPOLLDATA;

   g) Testez les connexions en cliquant sur le bouton de barre d'outils **Test**.

   h) Si une erreur liée à `libdb2.so` est émise, ajoutez le répertoire qui contient la version 32 bits de cette bibliothèque à `LD_LIBRARY_PATH`.

i) Arrêtez le serveur Cognos à partir de l'interface graphique IBM Cognos Configuration en cliquant sur **Actions** > **Stop**.

j) Redémarrez l'interface graphique d'IBM Cognos Configuration.

k) Redémarrez le serveur Cognos en cliquant sur **Actions** > **Démarrer**.

6. Installez les rapports Network Manager à l'aide d'IBM Installation Manager.
7. Importez les rapports Network Manager.
   a) Copiez les rapports Network Manager de `$ITNM_HOME/precision_gui/reports/itnmcognos.zip` dans le répertoire `$COGNOS_HOME/deployment` sur le serveur Cognos.
   b) Importez les rapports en cliquant sur **Configuration** > **Administration de contenu** > **Nouvelle importation** et en sélectionnant le package **ITNM Reports**.
8. Configurez Cognos Analytics pour qu'il utilise HTTPS.
9. Configurez Cognos Analytics pour qu'il utilise l'authentification LDAP.

   Si vous effectuez cette action, pour conserver tous les comptes utilisateur à un emplacement unique, configurez Tivoli Netcool/OMNIbus pour qu'il utilise l'authentification LDAP. Consultez les informations de la rubrique *Configuration de l'authentification utilisateur* dans la documentation Tivoli Netcool/OMNIbus. Par exemple, consultez la rubrique *Configuration de l'authentification utilisateur* dans le document IBM Knowledge Center for Tivoli Netcool/OMNIbus http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.
10. Editez le fichier `$NMGUI_HOME/profile/etc/tnm/reporting.properties`. Suivez les instructions présentées au début du fichier pour modifier les propriétés suivantes :

```
reporting.useCognos=true
reporting.host=hostname
reporting.ui.path=/bi
reporting.path=/bi/v1/disp
```

11. Ajoutez le rôle utilisateur `ncp_reporting_user` au groupe d'utilisateurs Network Manager approprié.

    Seuls les utilisateurs ayant ce rôle ont accès à l'option de menu **Production de rapports Cognos**.
12. Redémarrez les composants d'interface graphique Network Manager.
13. Connectez-vous à l'interface graphique Cognos Analytics en tant qu'utilisateur disposant des droits appropriés et exécutez un rapport Network Manager à partir de **Contenu de l'équipe** > **Network Manager**.

Résultats

Les rapports sont disponibles en vue de leur exécution à partir du menu **Reporting** > **Production de rapports Cognos**.

Tâches associées

Configuration de Cognos Analytics

Procédez comme suit pour configurer Cognos Analytics.

Installation des rapports Network Manager

Avant d'installer les rapports spécifiques à Network Manager, vous devez avoir installé Cognos Analytics.

Pourquoi et quand exécuter cette tâche

Pour installer les rapports Network Manager, effectuez les tâches suivantes sur le serveur sur lequel vous avez installé Cognos Analytics.

Procédure

1. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.

b) Exécutez la commande :

```
./IBMIM
```

IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.

2. Cliquez sur **Installer**.
3. Dans l'écran suivant d'**installation des packages**, dans lequel vous pouvez sélectionner les packages à installer, sélectionnez la dernière version disponible de **Network Manager Reports**. Le package de rapports de Network Manager installe les rapports spécifiques à Network Manager.

   Les prérequis d'installation du package sont évalués.
4. En cas de problèmes liés aux prérequis affichés, résolvez-les à l'aide de l'information qui vous est fournie avant de continuer.
5. Cliquez sur **Suivant**, acceptez les dispositions du contrat de licence et cliquez de nouveau sur **Suivant**.
6. Sélectionnez le groupe de packages **IBM Netcool**.
7. Sélectionnez la version 64 bits et cliquez sur **Suivant**.
8. Sélectionnez toutes les fonctionnalités du package des **rapports Network Manager** à installer.
9. Dans les écrans d'**installation des packages** suivants, fournissez les informations de configuration des packages à installer. Utilisez **Suivant** et **Précédent** pour naviguer dans les options de configuration.
10. Confirmez les propriétés de l'instance de Jazz for Service Management sur laquelle vous voulez effectuer l'installation.

    Détails du répertoire d'installation
    Chemin d'accès complet à l'instance de Dashboard Application Services Hub.

    Nom d'utilisateur
    Entrez le nom d'un utilisateur possédant les droits administratifs dans Jazz for Service Management. S'il n'y a pas eu de modification, vous pouvez choisir l'utilisateur par défaut `smadmin` avec le mot de passe `netcool`.

    Mot de passe
    Entrez le mot de passe de cet utilisateur.
11. Confirmez les détails de la base de données topologiques Network Manager qui a été installée. Les rapports récupèrent les données dans cette base de données.

    a) Sélectionnez le type de base de données.

    b) Entrez les détails de la connexion à la base de données :

    Si vous avez sélectionné DB2 comme type de base de données, entrez les détails suivants :

    Nom de la base de données
    Entrez le nom de la base de données.

    Hôte serveur
    Entrez le nom d'hôte du serveur sur lequel la base de données est installée.

    Port du serveur
    Entrez le numéro de port de connexion à la base de données.

    User ID (ID utilisateur)
    Entrez l'ID d'un utilisateur DB2 autorisé à créer des tables.

    Mot de passe
    Entrez le mot de passe de cet utilisateur.

    Si vous avez sélectionné Oracle comme type de base de données, entrez les détails suivants :

Nom de service Oracle
Entrez le nom de service de la base de données.

Hôte serveur
Entrez le nom d'hôte du serveur sur lequel la base de données est installée.

User ID (ID utilisateur)
Entrez l'ID d'un utilisateur DB2 autorisé à créer des tables.

Mot de passe
Entrez le mot de passe de cet utilisateur.

c) Sélectionnez **Ignorez la vérification des détails de la connexion à la base de données** si vous ne souhaitez pas vérifier la connexion, par exemple si la base de données est inaccessible.

12. Vérifiez les informations récapitulatives puis cliquez sur **Installer**.

Que faire ensuite

Après avoir installé les rapports Network Manager, vous devez effectuer les tâches de configuration suivantes avant d'utiliser les rapports.

1. **Configurez le niveau d'isolement des sources de données de Network Manager (étapes obligatoires).**

   Modifiez le niveau d'isolement de chaque source de données Network Manager `NCPOLLDATA, PARAMETERS, NCPGUI, NCOMONITOR, NCIM, IBM_TRAM` sur `Lecteur non validée`. Les étapes de configuration de source de données suivantes sont obligatoires, car elles permettent d'éviter les problèmes d'interblocage de base de données. Effectuez les étapes ci-après.

   a. Ouvrez Dashboard Application Services Hub en spécifiant une URL similaire à `https://itnm7.hursley.ibm.com:16311/ibm/console/logon.jsp`.

   b. Connectez-vous à Dashboard Application Services Hub en tant qu'utilisateur `smadmin`.

   c. Cliquez l'icone **Reporting** et sélectionnez **Cognos Reporting**. Dans le widget sélectionnez **Manage** > **Administration Console**.

   d. Dans l'onglet **Configuration**, sélectionnez une source de données.

   e. Ouvrez **Propriétés**.

   f. Dans l'onglet **Connexion**, modifiez le niveau d'isolement sur `Lecture non validée`.

2. **Etendez la visibilité de la fonction de rapports à l'utilisateur `itnmadmin`.**

   Après avoir terminé l'installation, vous devez vous connecter en tant que `smadmin` pour voir la fonction de rapports. Si vous vous connectez en tant que `itnmadmin`, vous ne voyez pas cette fonction. Pour plus d'informations sur l'extension de la visibilité de la fonction de rapports à l'utilisateur `itnmadmin`, voir http://www-01.ibm.com/support/docview.wss?uid=swg21963430.

Installation du Tableau de bord d'état du réseau (clients Netcool Operations Insight uniquement)

Si vous êtes autorisé à utiliser Network Manager avec Netcool Operations Insight, vous pouvez installer Network Manager, appelé **Tableau de bord d'état du réseau**.

Pourquoi et quand exécuter cette tâche

Tableau de bord d'état du réseau Surveille une vue de réseau sélectionnée et affiche la disponibilité du périphérique et de l'interface dans cette vue de réseau. Il génère également des rapports sur les performances en présentant des graphiques, des tables et des traces de données KPI pour les périphériques et les interfaces surveillés. Un calendrier de tableau de bord signale les modifications de la configuration et le nombre d'événements ce qui vous permet de corréler les événements avec les modifications de la configuration. Le tableau de bord inclut l'afficheur d'événements qui fournit des informations détaillées sur les événements.

Consultez les informations d'installation du **Tableau de bord d'état du réseau** dans la documentation de Netcool Operations Insight à l'adresse suivante : http://www.ibm.com/support/knowledgecenter/SSTPTP/welcome.

L'installation du **Tableau de bord d'état du réseau** installe les rôles suivants qui permettent aux utilisateurs de travailler avec **Tableau de bord d'état du réseau** :

- `ncp_networkhealth_dashboard`
- `ncp_networkhealth_dashboard_admin`
- `ncp_event_analytics`

Installation et désinstallation de groupes de correctifs

Un groupe de correctifs correspond au passage d'une édition mineure à une autre à l'intérieur d'une même version (par exemple de 4.2.0.1 à 4.2.0.2). Ces versions sont généralement appelées V4.2 groupe de correctifs 1 et V4.2 groupe de correctifs 2. Vous pouvez installer des groupes de correctifs et annuler une installation pour revenir à une version précédente avec IBM Installation Manager.

Pourquoi et quand exécuter cette tâche

Vous devez installer la version de disponibilité générale de Network Manager avant d'installer un groupe de correctifs.

Tâches de post-installation

Après avoir installé Network Manager, vous devez effectuer plusieurs tâches de post-installation.

Pourquoi et quand exécuter cette tâche

Pour exécuter des tâches de post-installation :

Procédure

1. Vérifiez que votre installation de Network Manager est terminée.

   Vous pouvez vérifier que l'installation a abouti en examinant les packages installés par IBM Installation Manager, à l'aide des commandes suivantes :

   a) Dans IBM Installation Manager cliquez sur **File** > **Installation History**.

   b) Passez en revue le statut des packages installés.

      La colonne **Package Group Name** liste les packages installés. La colonne **Status** liste les résultats de l'installation de ce package.

   c) Cliquez sur **View Log** pour afficher le fichier journal d'un package sélectionné.

2. Si vous effectuez une intégration avec Netcool Configuration Manager, vous devez à présent l'installer et ensuite installer le Netcool Configuration Manager Integration Pack. Pour savoir comment installer ces composants, référez-vous à la documentation sur l'intégration à : http://www.ibm.com/support/knowledgecenter/SS7UH9/welcome

3. Selon les paramètres supplémentaires requis, exécutez les étapes décrites dans les rubriques suivantes :

Option	Description
Configuration de LDAP pour l'authentification utilisateur	Une fois l'installation de Network Manager terminée, vous pouvez configurer LDAP pour l'authentification utilisateur, comme décrit dans «Modification de la méthode d'authentification des utilisateurs», à la page 227.

Option	Description
Configuration du nom de la source de données Tivoli Netcool/OMNIbus Web GUI	Si vous avez installé les composants d'interface graphique de Network Manager et avez choisi de ne pas créer une nouvelle source de données Interface graphique Web, vous devez configurer Network Manager afin qu'il utilise une source de données existante.Consultez les instructions dans «Configuration du nom de la source de données Tivoli Netcool/OMNIbus Web GUI», à la page 92.
Tâches de post-installation en tant qu'utilisateur non root (UNIX seulement)	• Vous pouvez configurer l'utilisateur qui gère les processus Network Manager, comme indiqué dans «Configuration des autorisations de superutilisateur/non superutilisateur», à la page 161 • Pour les installations non root, vous pouvez configurer vos processus Network Manager de sorte qu'ils démarrent automatiquement lorsque votre système est démarré ou redémarré, comme décrit dans «Configuration des processus pour un démarrage automatique dans une installation non root», à la page 163. **Remarque :** Cette procédure n'est pas nécessaire si vous avez installé Network Manager en tant que superutilisateur. Le redémarrage automatique est configuré dans le cadre d'une installation root sans qu'il soit nécessaire d'effectuer cette étape de post-installation.
Configuration d'une base de données topologiques après l'installation pour Network Manager.	Pour des détails sur la façon de créer manuellement les schémas de base de données aprés installation, voir les tâches relatives à la création de schéma de bases de données topologiques dans *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
Activation de l'agrégation des données d'interrogation si vous avez installé Network Manager en tant que root	Si vous avez installé Network Manager en tant que superutilisateur, vous devez exécuter le script `setup_run_storm_as_non_root.sh` pour activer les processus des données d'interrogation historiques. Pour savoir comment procéder, voir «Activation de l'interrogation historique», à la page 165.
Mise à niveau à partir d'une version antérieure de Network Manager	Suivez les étapes décrites dans Chapitre 8, «Mise à niveau et migration», à la page 139.
Installation de l'agent de surveillance	Si vous voulez utiliser IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, suivez les étapes décrites dans «Intégration à IBM Tivoli Monitoring», à la page 128
Configuration de Network Manager pour différents fuseaux horaires.	Si vous installez des serveurs d'applications Web et de composants de base Network Manager distribués dont les fuseaux horaires sont différents, vous devez définir le même fuseau horaire sur tous les serveurs et notamment sur le serveur de base de données, les serveurs de base et les serveurs d'interface graphique. Ainsi, Network Manager pourra effectuer des comparaisons d'horodatages précises pour des processus se trouvant sur différents serveurs. Vous devez aussi avertir les utilisateurs, comme les opérateurs réseau, que le système peut afficher des heures différentes de celle du lieu où ils se trouvent.
Configuration de routines cryptographiques pour l'interface graphique	Par défaut, l'interface graphique n'utilise pas de routines cryptographiques exclues d'une installation FIPS140-2, quel que soit le statut d'installation du serveur central. Si vous souhaitez configurer les

Option	Description
	options de reconnaissance SNMP pour activer MD5 et DES, définissez `tnm.fips.mode=false` dans le fichier `tnm.properties`.
Définition de l'entretien de vue de réseau automatique	Si vous avez plusieurs serveurs GUI, vous devez les configurer de manière qu'un seul serveur réalise l'entretien automatique de la vue de réseau et de la vue de chemin. Si vous n'avez qu'un seul serveur GUI, vous n'avez pas besoin de réaliser cette tâche. Pour plus d'informations, voir *Définition de l'entretien de vue automatique* dans le *Guide de l'Utilisateur IBM Tivoli Network Manager*.

4. Selon vos exigences, il peut être nécessaire d'exécuter d'autres tâches de configuration. Vérifiez les informations de Chapitre 9, «Configuration de Network Manager», à la page 159.
5. A l'issue de l'installation et de la configuration de Network Manager, voir les sections de mise en route. Pour plus d'information, voir les tâches dans *Guide de l'Utilisateur IBM Tivoli Network Manager*.

Chapitre 5. Désinstallation de Network Manager

Si vous souhaitez supprimer entièrement le produit, ou d'annuler pour revenir à une version précédente, vous devez utiliser IBM Installation Manager. Le fait de désinstaller le produit en supprimant les fichiers et les répertoires provoque des problèmes lors de la réinstallation des composants.

Pourquoi et quand exécuter cette tâche

Vous devez désinstaller les produits et les composants dans l'ordre indiqué ci-après. IBM Installation Manager Ne supprime pas les fichiers qui ont été créés en exécutant les produits ou les commandes de configuration : journaux, fichiers de configuration mis à jour, données ou cache persisté.

Si vous désinstallez les composants dans un ordre différent, vous risquez de ne pas pouvoir supprimer certains composants.

Tâches associées

Suppression de rapports

Avant de désinstaller Network Manager, vous devez supprimer les rapports de Network Manager et les sources de données des rapports. Vous pouvez aussi désinstaller Cognos Analytics en même temps.

Désinstallation des applications de l'interface graphique

Vous pouvez désinstaller un des produits suivants ou tous les produits en même temps : Network Manager composant GUI, Tivoli Netcool/OMNIbus Web GUI, et Dashboard Application Services Hub.

Avant de commencer

L'utilisateur `itnm_user` doit être présent dans l'ObjectServer. L'ObjectServer doit être en cours d'exécution. Ne désinstallez pas WebSphere Application Server tant que tous les produits installés dans WebSphere Application Server n'ont pas été désinstallés.

Pourquoi et quand exécuter cette tâche

Pour désinstaller les applications de l'interface graphique, procédez comme suit :

Procédure

1. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
2. Cliquez sur **Désinstaller**.
3. Sélectionnez un ou plusieurs des composants suivants à désinstaller et cliquez sur **Suivant** :
   - **IBM Tivoli Netcool/OMNIbus Web GUI**
   - **Network Manager GUI Components**
   - **IBM Dashboard Application Services Hub**. Vous ne pouvez pas désinstaller Dashboard Application Services Hub tant que vous n'avez pas désinstallé tous les composants qui y sont installés.

4. Le système vous demande de fournir les informations de WebSphere Application Server et de Jazz for Service Management. Si ces détails n'ont pas changé depuis l'installation, vous pouvez conserver les valeurs par défaut.
5. Passez en revue les informations récapitulatives et cliquez sur **Désinstaller**.

Résultats

Les packages sélectionnés sont désinstallés.

Suppression de rapports

Avant de désinstaller Network Manager, vous devez supprimer les rapports de Network Manager et les sources de données des rapports. Vous pouvez aussi désinstaller Cognos Analytics en même temps.

Pourquoi et quand exécuter cette tâche

Restriction : Si vous supprimez Cognos Analytics, les rapports Network Manager ne fonctionnent pas. Si vous souhaitez utiliser les rapports Network Manager, ne désinstallez pas Cognos Analytics.

Pour supprimer les rapports de Network Manager et leurs paramètres de sources de données, procédez comme suit :

Procédure

1. Connectez-vous à l'interface graphique Network Manager dans un navigateur pris en charge en tant qu'utilisateur disposant des droits d'administration.
2. Cliquez sur **Common reporting** dans le panneau de navigation situé à gauche dans la fenêtre.
3. Sélectionnez la case à cocher correspondant à Network Manager.
4. Cliquez sur l'icône de suppression pour supprimer les rapports Network Manager.
5. Cliquez sur le menu **Lancer** dans la partie supérieure droite de la fenêtre. Cliquez sur **Administration Cognos** dans la liste, puis cliquez sur l'onglet **Configuration**.
6. Sélectionnez les cases à cocher qui correspondent aux sources de données suivantes :
   - IBM_TRAM
   - NCIM
   - NCMONITOR
   - NCPGUI
   - NCPOLLDATA
   - PARAMETERS
7. Cliquez sur l'icône de suppression pour supprimer les sources de données sélectionnées.
8. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

      ```
      ./IBMIM
      ```

      IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
9. Cliquez sur **Désinstaller**.
10. Sélectionnez **Network Manager Reports** et **Cognos Analytics**, puis cliquez sur **Suivant**.

11. Passez en revue les informations récapitulatives et cliquez sur **Désinstaller**.

Résultats
Les packages sélectionnés sont désinstallés.

Désinstallation des composants principaux de Network Manager et de Tivoli Netcool/OMNIbus

Vous pouvez désinstaller en même temps les composants principaux de Network Manager et de Tivoli Netcool/OMNIbus s'ils sont installés sur le même serveur.

Avant de commencer

Avant de désinstaller Network Manager, supprimez les rapports de Network Manager et de Cognos Analytics, comme indiqué dans «Suppression de rapports», à la page 80.

Pourquoi et quand exécuter cette tâche
Pour désinstaller Network Manager et Tivoli Netcool/OMNIbus, procédez comme suit :

Procédure

1. Facultatif : Si vous avez effectué l'installation en tant qu'utilisateur non superutilisateur, puis que vous avez exécuté **`create_all_control.sh -auto_only`** comme tâche post-installation pour configurer vos processus Network Manager afin qu'ils démarrent automatiquement au démarrage ou au redémarrage du système, exécutez **`create_all_control.sh`** avec l'option `-deinstall` en tant qu'utilisateur à l'origine de l'installation pour supprimez les scripts de démarrage du système.
2. Arrêtez les composants principaux de Network Manager pour chaque domaine à l'aide de la commande suivante : **`itnm_stop`** `ncp -domain` *`DOMAINE`*.
   Par exemple, pour arrêter le domaine NCOMS, entrez : `itnm_stop ncp -domain NCOMS`

   Remarque : Si vous n'indiquez pas de nom de domaine avec la commande **`itnm_stop`**, elle arrête le domaine par défaut créé lors de l'installation.

   Avant de continuer, vérifiez que tous les processus commençant par `ncp_` sont arrêtés avant de continuer. Arrêtez tous les processus Network Manager si nécessaire.
3. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
4. Cliquez sur **Désinstaller**.
5. Sélectionnez un ou plusieurs des composants suivants à désinstaller et cliquez sur **Suivant** :
   - **IBM Tivoli Netcool/OMNIbus**
   - **Network Manager Core Components**
6. Passez en revue les informations récapitulatives et cliquez sur **Désinstaller**.

Résultats
Les packages sélectionnés sont désinstallés.

Que faire ensuite
Si vous avez installé en tant qu'utilisateur non superutilisateur, certains fichiers et répertoires peuvent avoir été conservés. Un utilisateur possédant les droits appropriés peut supprimer ces fichiers manuellement. Ne supprimez pas de fichiers si Tivoli Netcool/OMNIbus ou Sondes est installé dans le même emplacement.

Désinstallation de WebSphere Application Server

Après avoir désinstallé les produits qui étaient installés dans WebSphere Application Server, vous pouvez désinstaller WebSphere Application Server.

Pourquoi et quand exécuter cette tâche
Pour désinstaller WebSphere Application Server, procédez comme suit :

Procédure
1. Supprimez le profil WebSphere Application Server créé par Jazz for Service Management :
   a) Arrêtez le profil WebSphere Application Server à l'aide de la commande suivante :
   ```
   stopServer.sh nom_serveur -username smadin -password mot de passe
   ```
   b) Listez les profils pour obtenir le nom du profil à l'aide de la commande suivante :
   `/opt/IBM/netcool/was/bin/manageprofiles.sh -listProfiles`
   c) Supprimez le profil à l'aide de la commande suivante :
   `/opt/IBM/netcool/was/bin/manageprofiles.sh -delete -profileName nom_profil`
2. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :
   ```
   ./IBMIM
   ```
   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
3. Cliquez sur **Désinstaller**.
4. Sélectionnez **WebSphere Application Server** et tous les sous-composants et cliquez sur **Suivant**.
5. Passez en revue les informations récapitulatives et cliquez sur **Désinstaller**.

Chapitre 6. Installation et désinstallation de groupes de correctifs

Un groupe de correctifs correspond au passage d'une édition mineure à une autre à l'intérieur d'une même version (par exemple de 4.2.0.1 à 4.2.0.2). Ces versions sont généralement appelées V4.2 groupe de correctifs 1 et V4.2 groupe de correctifs 2. Vous pouvez installer des groupes de correctifs et annuler une installation pour revenir à une version précédente avec IBM Installation Manager.

Pourquoi et quand exécuter cette tâche

Vous devez installer la version de disponibilité générale de Network Manager avant d'installer un groupe de correctifs.

Installation de groupes de correctifs

Un groupe de correctifs correspond au passage d'une édition mineure à une autre à l'intérieur d'une même version, par exemple de 4.2.0.1 à 4.2.0.2, ou V4.2 Fixpack 1 et V4.2 Fixpack 2.

Avant de commencer

Vous devez installer la version de disponibilité générale de Network Manager avant d'installer un groupe de correctifs.

Avant d'installer un groupe de correctifs, vous devez sauvegarder les produits et les données selon le cas. Par exemple, si vous exécutez Network Manager sur une machine virtuelle, faites un instantané de votre machine virtuelle.

Pourquoi et quand exécuter cette tâche

Restriction : Vous devez utiliser ensemble différentes versions des mêmes produits ou composants, à moins que vous ayez été avisé d'agir autrement selon des instructions dans IBM Knowledge Center ou par IBM Support. Si vous avez besoin de plusieurs instances d'un produit ou composant, vous devez les installer ou mettre à niveau la version et les correctifs. Vous devez également veiller à ce que le même ensemble de correctifs de test soit installé le cas échéant. Par exemple, si vous avez besoin de plusieurs instances de Network Manager GUI Components dans un déploiement, veillez à ce qu'elles mettent en œuvre la même version, le même correctif, et les même correctifs de test.

Vous devez mettre à jour les composants principaux de Network Manager avant de mettre à jour les composants de l'interface graphique ou en même temps. Par exemple, installez le groupe de correctifs sur le serveur central Network Manager, puis sur le serveur d'interface graphique.

Fix Pack 6

Important : L'installation de Fix Pack 6 ou ultérieur supprime les fichiers MIB existants. Network Manager Ces Fix Packs ne contiennent pas de Base d'Information de Gestion (fichiers MIB). Network Manager Fix Pack 5 contient les fichiers MIB. Les MIB sont nécessaires à la reconnaissance de réseau.

Si vous actualisez depuis Fix Pack 5 ou antérieurs, menez à bien les étapes suivantes pour obtenir les fichiers MIB :

1. Situez un fichier zip nommé `com.ibm.tivoli.netcool.ncp.mibs.all.any_*.zip` dans l'emplacement partagé IBM Installation Manager qui contient les fichiers MIB depuis l'installation du Fix Pack précédent. Le chemin d'extraction peut être différent dans votre installation. Un exemple de chemin : `/opt/IBM/IBMIM/native/`
2. Décompressez ce fichier.

3. Chargez les MIB dans la base de données en exécutant la commande ncp_mib, comme décrit dans *Loading updated MIB information* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Si vous installez Fix Pack 6, 7, 8, ou 9 sans actualiser, ou si vous n'arrivez pas à situer les fichiers MIB en utilisant la procédure ci-dessus, menez à bien les étapes suivantes pour obtenir les fichiers MIB :

1. Exécutez la commande **ncp_mib**, comme décrit dans : *Chargement des informations MIB mises à jour* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.
2. Si vous avez installé Network Manager 4.2 Fix Pack 5, faites une sauvegarde des contenus du répertoire `$NCHOME/precision/mibs/` dans un répertoire de sauvegarde hors de $NCHOME. Par exemple, `/mibs_backup/`.
3. Si vous avez installé une version plus récente que 4.2 Fix Pack 5, menez à bien les étapes suivantes :
   a. Faites une sauvegarde des contenus du répertoire `$NCHOME/precision/mibs/` vers un répertoire de sauvegarde hors de $NCHOME. Par exemple, `/old_mibs/`. Gardez ce répertoire et les fichiers qu'il contient au cas où vous voudriez revenir à la version plus ancienne.
   b. Téléchargez les fichiers Network Manager Fix Pack 5 (4.2.0.5) depuis IBM Fix Central : https://www.ibm.com/support/fixcentral/

      Important : Téléchargez les fichiers pour Linux x86, sans considération pour la plateforme que vous utilisez.
   c. Décompressez le paquet Network Manager dans un répertoire temporaire.
   d. Décompressez l'archive `repositories/disk1/ad/native/file000876` dans un répertoire de backup hors de $NCHOME, par exemple, `/mibs_backup/`. Ce répertoire contient les fichiers MIB par défaut.
   e. Si vous avez des fichiers MIB personnalisés ou ajoutés, copiez les fichiers MIB personnalisés ou nouveaux depuis `/old_mibs/` en écrasant les fichiers par défaut de `/mibs_backup/`.
4. Quelle que soit la version de Network Manager que vous avez installé, le répertoire `/mibs_backup/` contient à présent l'ensemble de la plupart des fichiers MIB actuels du Fix Pack 5, plus toutes les additions et personnalisations.

Une fois que vous avez obtenu les fichiers MIB, installez la version la plus récente de Network Manager.

1. Installez Network Manager Fix Pack 6 en suivant les consignes de cette procédure.
2. Copiez les fichiers MIB depuis votre répertoire `/mibs_backup/` vers la l'emplacement suivant dans l'installation : `$NCHOME/precision/mibs/`
3. Exécutez la commande **ncp_mib**, comme décrit dans : *Chargement des informations MIB mises à jour* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Pour installer un groupe de correctifs, procédez comme suit :

Procédure

1. Installez le groupe de correctifs sur tous les serveurs Network Manager, par exemple sur le serveur central et le serveur d'interface graphique, sauf indication contraire dans les notes sur l'édition du groupe de correctifs ou dans le fichier README.
2. Arrêtez tous les processus Network Manager en cours d'exécution.
3. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

```
./IBMIM
```

Fix Pack 1

: Si vos version logicielles sont faites de toute version Network Manager 4.2 avant le Fix Pack 1 avec Jazz for Service Management V1.1.2.1 et que vous surclassez Network Manager 4.2 Fix Pack 1

et Jazz for Service Management V1.1.3.0 en même temps, vous devez alors commencer IBM Installation Manager par exécuter le script `JazzSMgrpModeUpgrade.sh` et spécifier deux paramètres obligatoires, comme détaillé dans la note technique https://www.ibm.com/support/pages/node/283105.

Vous n'avez pas besoin de démarrer IBM Installation Manager en exécutant le script `JazzSMgrpModeUpgrade.sh` si vos versions logicielles sont Network Manager 4.2, versions antérieures au Fix Pack 1, avec Jazz for Service Management V1.1.3.0, et que vous faites une simple mise à niveau vers 4.2, Fix Pack 1, sans modifier la version de Jazz for Service Management.

IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.

4. Fix Pack 1
   Configurez les référentiels IBM Installation Manager de sorte qu'ils renvoient vers les emplacements des packages mis à jour.
5. Cliquez sur **Update**.
6. Choisissez le groupe de packages pour lequel vous souhaitez installer un groupe de correctifs. Sinon, sélectionnez **Update all packages with recommended updates and recommended fixes**. Cliquez sur **Suivant**.
7. Sélectionnez les mises à jour que vous souhaitez installer et cliquez sur **Suivant**.
8. Passez en revue les informations récapitulatives et cliquez sur **Update**.
9. Après une mise à niveau Fix Pack sur une installation non-root, vous devez exécuter les scripts suivants en tant que superutlisateur pour activer ces processus principaux qui nécessitent un accès root pour fonctionner normalement :
   - $NCHOME/precision/scripts/setup_run_as_setuid_root.sh
   - $NCHOME/precision/scripts/setup_run_storm_as_non_root.sh

Fix Pack 1 Application de mises à jour de schéma pour un groupe de correctifs

Exécutez le script du programme de mise à jour de schéma, `update_db_schemas.pl`, pour appliquer toutes les mises à jour nécessaires de schéma de base de données de topologie NCIM pour un ou plusieurs groupes de correctifs ou correctifs temporaires.

Avant de commencer

Avant de pouvoir exécuter le script `update_db_schemas.pl`, vous devez d'abord avoir installé le groupe de correctifs ou le correctif temporaire auquel vous souhaitez appliquer des mises à jour de schéma.

Pourquoi et quand exécuter cette tâche

Commençons par Network Manager V4.2. Lorsque vous téléchargez un nouveau Fix Pack 1ou correctif temporaire, le téléchargement inclut `update_db_schemas.pl` et les fichiers de mise à jour associés. Ces fichiers de mise à jour comprennent tous les changements de schéma de base de données de topologie NCIM pour l'ensemble des groupes de correctifs et des correctifs temporaires jusqu'au correctif actuel.

Vous pouvez mettre à jour votre base de données de topologie NCIM avec tous les changements de schéma pour le Fix Pack 1ou le correctif temporaire actuel en exécutant le script `update_db_schemas.pl`. Le script appliquera des changements de schéma également pour plusieurs groupes de correctifs ou correctifs temporaires. Par exemple, si pour une édition majeure spécifique, vous n'avez pas installé le Fix Pack 11, mais que vous installez le Fix Pack 12, l'exécution du script `update_db_schemas.pl` mettra à jour la base de données de topologie NCIM avec l'ensemble des changements de schéma à la fois pour le Fix Pack 11 et le Fix Pack 12.

Pour plus d'informations sur le script `update_db_schemas.pl`, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Procédure

1. Sourcez votre environnement.

   Sur le serveur où sont installés les composants de base de Network Manager, le script d'environnement est `répertoire_installation/netcool/core/env.sh`.

   Par exemple, sur des shells Bash, Bourne, et Korn, sourcez le script env.sh en utilisant une ligne de commande similaire à la suivante :

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

2. Exécutez le script en mode Aperçu pour répertorier les mises à jour de schéma qui seront appliquées.

   ```
   $NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/sql/
   update_db_schemas.pl -domain DOMAIN_NAME -preview
   ```

   Cette commande affiche à l'écran les changements devant être faits sur un fichier pour que vous les passiez en revue avant de les appliquer à la base de données. Par défaut, ce fichier se situe au chemin `/tmp/nm-update.sql`. Pour donner au fichier un nom différent, spécifiez le nom souhaité après l'option `-preview`. Si vous procédez ainsi, l'aperçu est écrit dans un fichier portant ce nom dans le répertoire de travail.

3. Exécutez le script à appliquer aux mises à jour de schéma.

   ```
   $NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/sql/
   update_db_schemas.pl -domain DOMAIN_NAME
   ```

   Remarque : Lorsque le programme de mise à jour de schéma a correctement appliqué tous les changements à un Fix Pack 1donné, il écrit une ligne dans la table `ncim.schemaAudit`, en indiquant le nom du fichier sur lequel ces changements ont été appliqués et l'horodatage auquel ils ont été appliqués.

Fix Pack 1 Vérification des mises à jour de schéma

Vous pouvez vérifier les mises à jour de schéma de groupe de correctifs et de correctifs temporaires ayant été appliquées à la base de données de topologie NCIM.

Pourquoi et quand exécuter cette tâche

Vous pouvez procéder à la vérification de l'une des façons suivantes :

- En exécutant l'instruction select suivante sur la base de données topologique NCIM :

  ```
  SELECT * FROM ncim.schemaAudit ORDER BY lastTraced;
  ```

- En exécutant le script `list_applied_updates.pl`. Pour ce faire, sourcez d'abord votre environement, et ensuite exécutez le script utilisant une commande similaire à ce qui suit :

  ```
  $NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/sql/
  list_applied_updates.pl -domain DOMAIN_NAME
  ```

  Remarque : Si plusieurs domaines partagent les mêmes données de connexion, vous ne devez exécuter le script que pour l'un des domaines. L'exécution du script pour les autres domaines qui utilisent les mêmes détails de connexion produira tout simplement la même sortie.

Désinstallation de groupes de correctifs

Vous pouvez désinstaller un groupe de correctifs déjà installé. Il s'agit d'une annulation avec rétrogradation vers une version antérieure.

Pourquoi et quand exécuter cette tâche

IBM Installation Manager stocke les fichiers d'installation dans son emplacement des données. Ces fichiers permettent de revenir à une version antérieure.

Si vous avez supprimé des fichiers d'annulation requis, consultez les informations sur la rétrogradation et les autorisations dans la documentation d'IBM Installation Manager à l'adresse : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

Important : Network Manager Fix Pack 6 ne contient pas la base informative de gestion, Management Information Base (fichiers MIB). Les MIB sont nécessaires à la reconnaissance de réseau.

Pour désinstaller Fix Pack 6 et utiliser une version précédente, menez à bien les étapes suivantes :

1. Copier les fichiers MIB depuis le répertoire suivant vers un répertoire temporaire : `$NCHOME/precision/mibs/`
2. Effacez tous les fichiers dans le répertoire `$NCHOME/precision/mibs`.
3. Désinstallez Network Manager Fix Pack 6 en suivant les consignes ci-dessous.
4. Si vous revenez à 4.2 Fix Pack 5, copiez les fichiers MIB du répertoire temporaire vers le répertoire MIB : `$NCHOME/precision/mibs/`
5. Si vous revenez à une version précédente à 4.2 Fix Pack 5, copiez les fichiers MIB depuis le répertoire de backup `/old_mibs/` vers le répertoire MIB : `$NCHOME/precision/mibs/`
6. Exécutez la commande **ncp_mib**, comme décrit dans : *Chargement des informations MIB mises à jour* dans le *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*

Pour désinstaller un groupe de correctifs, procédez comme suit :

Procédure

1. Arrêtez tous les processus Network Manager en cours d'exécution.
2. Démarrez IBM Installation Manager :
   a) Accédez au répertoire dans lequel IBM Installation Manager est installé.
   b) Exécutez la commande :

   ```
   ./IBMIM
   ```

   IBM Installation Manager démarre en mode assistant. Pour utiliser le mode de ligne de commande, le mode automatique, le mode console ou le mode de navigateur Web, consultez les informations sur la *Gestion des installations avec Installation Manager* dans la documentation d'IBM Installation Manager à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Tous les produits et composants ne prennent pas en charge tous les modes d'installation.
3. Cliquez sur **Roll Back**.
4. Dans la liste **Nom du groupe de packages**, sélectionnez le groupe de packages qui contient les packages que vous voulez rétrograder. Cliquez sur **Suivant**.
5. Sélectionnez la version du package que vous voulez rétablir et cliquez sur **Suivant**.
6. Passez en revue les informations récapitulatives et cliquez sur **Roll Back**.

Chapitre 7. Configuration des intégrations à d'autres produits

Vous pouvez configurer Network Manager pour l'utiliser avec plusieurs produits Tivoli®. Consultez les informations relatives aux tâches de configuration requises pour configurer les intégrations disponibles.

Pourquoi et quand exécuter cette tâche

Network Manager peut être intégré aux produits IBM suivants :

IBM Netcool Operations Insight
Network Manager est un composant clé au sein de cette solution, où il est étroitement intégré à Netcool/Impact, et IBM Operations Analytics - Log Analysis.

IBM Netcool Configuration Manager

Netcool Configuration Manager propose des fonctions étendues de gestion de la configuration pour les périphériques du réseau, ainsi que des fonctions de définition de seuils des règles réseau.

S'il est intégré avec Network Manager, vous pouvez alors utiliser**Configuration et calendrier des événements** dans **Tableau de bord d'état du réseau** pour corréller les données de configuration avec les données d'alerte.

Netcool Configuration Manager peut également être intégré à Network Manager et à Tivoli Netcool/OMNIbus afin de proposer des fonctions de diagnostic plus puissantes aux opérateurs réseau.

IBM Cognos Analytics
L'intégration à Cognos Analytics permet de proposer des rapports prêts à l'emploi, notamment des rapports contenant des informations sur la configuration du réseau.

IBM Tivoli Application Dependency Discovery Manager
IBM Tivoli Application Dependency Discovery Manager propose les fonctionnalités suivantes :

- Importe les informations de topologie de réseau reconnues par Network Manager dans IBM Tivoli Application Dependency Discovery Manager pour compléter la vue des dépendances entre application et réseau.
- Le rapport d'inventaire Network Manager est disponible dans IBM Tivoli Application Dependency Discovery Manager.
- Permet aux utilisateurs d'effectuer un lancement en contexte dans les vues Réseau afin d'identifier les problèmes d'infrastructure pouvant avoir des conséquences sur les performances des applications.
- Network Manager peut également effectuer un lancement en contexte dans IBM Tivoli Application Dependency Discovery Manager afin d'afficher la vue Change History et la vue Details associée aux périphériques.

IBM Tivoli Monitoring
IBM Tivoli Monitoring propose les fonctionnalités suivantes :

- Surveille la santé de l'application Network Manager et affiche des mesures et des situations clés aidant les administrateurs à surveiller la santé et l'état de Network Manager.
- Peut être utilisé pour surveiller les ressources du réseau Network Manager.
- Il est possible d'effectuer un lancement d'IBM Tivoli Monitoring directement dans Network Manager, bien qu'il ne s'agisse pas d'un lancement en contexte.

IBM Tivoli Business Service Manager
IBM Tivoli Business Service Manager propose les fonctionnalités suivantes :

- Renseigne le modèle de service métier en utilisant les informations de réseau reconnues par plusieurs applications, parmi lesquelles Network Manager.

- Mappe les événements depuis plusieurs sources vers les ressources de IBM Tivoli Business Service Manager, notamment les ressources reconnues dans Network Manager. Dans ce cas, les ressources font référence à des périphériques, interfaces, etc.
- Traite les incidents survenus dans l'infrastructure en effectuant un lancement en contexte à partir des vues de service IBM Tivoli Business Service Manager vers l'une des vues de topologie Network Manager.

Référence associée

Exigences de compatibilité pour d'autres produits
Vérifiez que la configuration requise des produits intégrés à Network Manager est respectée.

Configuration de Tivoli Netcool/OMNIbus pour une utilisation avec Network Manager

Si vous avez installé Tivoli Netcool/OMNIbus sans utiliser l'installation de Network Manager, vous devez effectuer un certain nombre de tâches de configuration.

Pourquoi et quand exécuter cette tâche

Tivoli Netcool/OMNIbus gère les événements fournis par Network Manager et d'autres sources d'événement et peut également être utilisé en tant que source d'authentification. Pour accéder aux rubriques qui vous intéressent, consultez la section **Rubriques connexes**.

Pour utiliser Tivoli Netcool/OMNIbus, vous devez modifier une table dans le serveur ObjectServer. Si vous exécutez Network Manager dans une installation FIPS 140–2, vous devez effectuer des opérations de configuration supplémentaires dans l'environnement d'exécution de Tivoli Netcool/OMNIbus.

Pour plus d'informations sur Tivoli Netcool/OMNIbus, y compris les considérations relatives à la configuration post installation et à FIPS 140–2, consultez les guides *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* et *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Tâches associées

Configuration de la reprise en ligne de la source de données pour Tivoli Netcool/OMNIbus Web GUI
Si vous disposez d'une paire de reprise en ligne de serveurs ObjectServer à laquelle doit se connecter Interface graphique Web, vous pouvez configurer la reprise en ligne de la source de données par le biais du fichier de configuration de la source de données `ncwDataSourceDefinitions.xml` dans l'installation de Interface graphique Web.

Configuration d'un serveur ObjectServer à utiliser avec les processus centraux Network Manager

Pour les utilisateurs ayant Network Manager 4.2 correctif temporaire 2 uniquement, vous pouvez utiliser le script `config_object_server_for_itnm.sh` pour configurer un serveur ObjectServer à utiliser avec les processus centraux Network Manager. Ce script prend en charge un serveur ObjectServer s'exécutant sur Windows ainsi que sur UNIX. Le script configure la connexion au serveur ObjectServer et peut être utilisé pour configurer un serveur ObjectServer local ou distant. Il exécute aussi un certain nombre de commandes SQL qui créent et configurent dans le serveur ObjectServer les tables et les utilisateurs requis par Network Manager.

Avant de commencer

Avant que vous n'exécutiez le script `config_object_server_for_itnm.sh`, vous devez vous assurer que le serveur ObjectServer est fonctionnel.

Vous devez exécuter le script `config_object_server_for_itnm.sh` sur le serveur où les processus centraux Network Manager sont installés.

Pourquoi et quand exécuter cette tâche

Pour configurer le serveur ObjectServer aux fins d'utilisation avec les processus centraux Network Manager, procédez comme suit :

Procédure

1. Sourcez les variables d'environnement centrales Network Manager.
2. Accédez au répertoire suivant :

   ```
   $NCHOME/precision/scripts
   ```

3. Emettez la commande suivante pour exécuter le script `config_object_server_for_itnm.sh` :

   ```
   ./config_object_server_for_itnm -o OS_name -u OS_admin_user
   -p OS_admin_password -I itnm_account_password
   ```

   Où :

   - *nom_SE* est le nom du serveur ObjectServer à configurer.
   - *utilisateur_admin_SE* est l'ID de l'utilisateur administrateur pour le serveur ObjectServer.
   - *mdp_admin_SE* est le mode de passe de l'utilisateur administrateur du serveur ObjectServer.
   - *mdp_compte_itnm* est le mot de passe des comptes utilisateur Network Manager itnmadmin et itnmuser qui seront créés sur le serveur ObjectServer.

   Au cours de l'exécution du script, vous serez invité à choisir si vous souhaitez utiliser une connexion ObjectServer existante définie dans le fichier de configuration `$NCHOME/etc/omni.dat`. Répondez à cette question comme suit :

   - y pour utiliser une connexion déjà définie dans le fichier de configuration `$NCHOME/etc/omni.dat`.
   - n pour définir les détails suivants de la nouvelle connexion de serveur ObjectServer :
     - Nom d'hôte.
     - Port.
     - Si la connexion utilise le SSL.

     Remarque : Si vous choisissez cette option, lorsque l'exécution du script sera terminée, les détails de la connexion seront écrits dans le fichier de configuration `$NCHOME/etc/omni.dat`.

Résultats

Une fois l'exécution terminée, le script indique que vous devez configurer une analyse pour le serveur ObjectServer.

Tâches associées

Installation et configuration d'analyses

Si vous n'avez pas installé Tivoli Netcool/OMNIbus en tant qu'élément de l'installation Network Manager, et que vous utilisez une installation Tivoli Netcool/OMNIbus existante, vous devez configurer certaines analyses.

Configuration du référentiel d'utilisateurs

Si vous souhaitez utiliser un serveur ObjectServer en tant que référentiel d'utilisateurs et que vous ne l'avez pas installé en même temps que Network Manager, vous devez alors exécuter des scripts pour configurer les utilisateurs et leur attribuer des rôles.

Pourquoi et quand exécuter cette tâche

Pour configurer le serveur ObjectServer en tant que référentiel d'utilisateurs, procédez comme suit :

Procédure

1. Connectez-vous à la machine sur laquelle se trouvent les composants d'interface graphique Network Manager.
2. Sourcez les variables d'environnement de l'interface graphique Network Manager.
3. Accédez au répertoire `$WAS_HOME/bin`.
4. Créez les utilisateurs à l'aide de la commande suivante :

   ```
   ./wsadmin.sh -conntype SOAP -user jazz_admin_name -password jazz_admin_password
   -lang jython -f $NMGUI_HOME/bin/scripts/users.py itnmadmin_password
   ```

   Où :

   - *nom_admin_jazz* correspond au nom d'utilisateur de l'administrateur pour Jazz for Service Management. Par défaut, il s'agit de `smadmin`.
   - *mot de passe_admin_jazz* est le mot de passe administrateur pour Jazz for Service Management.
   - *mot de passe_admin_itnm* est le mot de passe pour les comptes `itnmadmin` et `itnmuser`.
5. Attribuez des rôles aux utilisateurs et aux groupes d'utilisateurs à l'aide de la commande suivante :

   ```
    $NMGUI_HOME/bin/assigns_users_to_roles -u jazz_admin_name
   -p jazz_admin_password -r
   ```

   Où :

   - *nom_admin_jazz* correspond au nom d'utilisateur de l'administrateur pour Jazz for Service Management.
   - *mot de passe_admin_jazz* est le mot de passe administrateur pour Jazz for Service Management.
   - `- r` est un indicateur pour régénérer la liste d'ID utilisateur. Spécifiez cet indicateur pour attribuer des rôles à l'utilisateur administrateur Jazz for Service Management (par défaut, smadmin) ainsi qu'à tous les utilisateurs et groupes Network Manager.

Configuration du nom de la source de données Tivoli Netcool/OMNIbus Web GUI

Si vous avez installé les composants d'interface graphique de Network Manager et avez choisi de ne pas créer une nouvelle source de données Interface graphique Web, vous devez configurer Network Manager afin qu'il utilise une source de données existante. Vous pouvez également suivre ces instructions pour changer la source de données.

Pourquoi et quand exécuter cette tâche

Une source de données désigne un serveur ObjectServer ou une paire de reprise en ligne ObjectServer utilisée par Interface graphique Web pour des informations d'événements. Certains déploiements contiennent de nombreux serveurs ObjectServers, et Interface graphique Web peut contenir des événements provenant de divers serveurs ObjectServer. Pour afficher l'état des unités, les vues de réseau et de tronçon font correspondre l'enregistrement de topologie d'une unité avec tous les événements relatifs à cette unité. Pour effectuer cette corrélation, les applications Web doivent avoir accès au nom d'une source de données utilisée par Interface graphique Web.

Pour ajouter une nouvelle source de données dans Interface graphique Web, utilisez les instructions sur la *configuration des sources de données* dans la documentation de Interface graphique Web à l'emplacement suivant :

http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html

Vérifiez que Network Manager est configuré pour utiliser une source de données Interface graphique Web existante en procédant comme suit :

Procédure

1. Effectuez une copie de sauvegarde du fichier NCHOME/etc/precision/ModelNcimDb.*NOM_DOMAINE*.cfg, puis éditez-le.
2. Remplacez la propriété WebTopDataSource par le nom de la nouvelle source de données.
3. Sauvegardez et fermez le fichier.
4. Redémarrez le processus **ncp_model**.

Configuration des types d'événement de topologie

Pour que vous puissiez intégrer les vues de topologie et les vues de l'**Afficheur d'événements** filtrées, le nom et le type de la vue doivent correspondre. Si vous changez les valeurs par défaut dans l'**Afficheur d'événements**, vous devez configurer le nom et le type dans Network Manager.

Pourquoi et quand exécuter cette tâche

Dans une vue de l'**Afficheur d'événements** filtrée, vous pouvez configurer le nom et le type de la vue. Si vous changez le nom et le type de la vue et remplacez les valeurs par défaut NetworkManagementEvents et global, l'**Afficheur d'événements** ne peut pas communiquer avec les **Vues de réseau** et les outils accessibles via un clic avec le bouton droit de la souris.

Si les valeurs par défaut ont été changées, vous devez changer les valeurs sur le serveur Network Manager pour qu'elles correspondent.

Pour éditer le nom et le type de la vue utilisés pour la communication avec l'**Afficheur d'événements**, procédez comme suit :

Procédure

1. Sauvegardez et éditez le fichier $NMGUI_HOME/profile/etc/tnm/topoviz.properties.
2. Changez les valeurs des propriétés suivantes :

```
topoviz.webtop.view.name=NetworkManagementEvents
topoviz.webtop.view.type=global
```

Installation et configuration d'analyses

Si vous n'avez pas installé Tivoli Netcool/OMNIbus en tant qu'élément de l'installation Network Manager, et que vous utilisez une installation Tivoli Netcool/OMNIbus existante, vous devez configurer certaines analyses.

Pourquoi et quand exécuter cette tâche

Pour vérifier que votre installation Tivoli Netcool/OMNIbus reçoit des événements depuis le réseau, configurez les analyses Tivoli Netcool/OMNIbus correspondantes. En particulier, pour vous assurer que vous pouvez traiter les alertes SNMP provenant de votre réseau, vous devez installer et configurer l'alerte SNMP (également appelée alerte mttrapd).

Pour plus d'informations sur l'installation et la configuration d'une sonde, consultez le guide de référence de la sonde appropriée dans le Centre de documentation à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/common/kc_welcome-444.html.

Installation de Knowledge Library

Vous devez installer Netcool/OMNIbus Knowledge Library pour permettre à Network Manager de traiter entièrement les événements de réseau.

Pourquoi et quand exécuter cette tâche

Netcool/OMNIbus Knowledge Library Est un ensemble de fichiers de règles écrits selon une valeur standard commune et disponibles via l'installation de Tivoli Netcool/OMNIbus.

Référence d'intégration Tivoli Netcool/OMNIbus

Consultez les informations sur les paramètres pour une interaction supplémentaire entre Network Manager et Tivoli Netcool/OMNIbus.

Configuration de la Sonde pour Tivoli Netcool/OMNIbus

La Sonde pour Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) acquiert et traite les événements générés par les processus et les interrogations Network Manager et transmet ces événements au serveur ObjectServer.

La Sonde pour Tivoli Netcool/OMNIbus est installée dans le répertoire `$NCHOME/probes/`*arch*, où *arch* représente un répertoire de système d'exploitation. Vous pouvez configurer la sonde en utilisant ses fichiers de configuration, qui sont présentés ci-dessus.

- Fichier de propriétés : `nco_p_ncpmonitor.props`
- Fichier de règles : `nco_p_ncpmonitor.rules`

Remarque : Le fichier exécutable (ou commande **nco_p_ncpmonitor**) pour la sonde est également installé dans le répertoire `$NCHOME/probes/`*arch*. Toutefois, la sonde est configurée pour s'exécuter par défaut sous le contrôleur de processus de domaine. De plus, la commande **nco_p_ncpmonitor** doit être exécutée uniquement à des fins de traitement des incidents.

Les événements émis dans Network Manager sont spécifiques au domaine. Lorsque Network Manager s'exécute en mode de reprise en ligne, la sonde utilise par défaut le nom de domaine virtuel, à condition que le nom soit configuré dans le fichier `$NCHOME/etc/precision/ConfigItnm.cfg`.

Pour plus d'informations sur les concepts de sonde, voir le document *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* dans le centre de documentation de Tivoli Netcool/OMNIbus à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Tâches associées

Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg
Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.`*DOMAIN*`.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde.

A propos du fichier nco_p_ncpmonitor.props

Le fichier `$NCHOME/probes/`*arch*`/nco_p_ncpmonitor.props` définit l'environnement dans lequel s'exécute le programme Sonde pour Tivoli Netcool/OMNIbus.

Le fichier de propriétés est constitué de paires nom-valeur séparées par un signe deux-points. Le fichier de propriétés par défaut répertorie un sous-ensemble de propriétés prises en charge par l'analyse. Ces propriétés sont mises en commentaire à l'aide d'un signe numéro (#) placé en début de ligne. L'ensemble standard de propriétés d'analyse communes, applicables pour la version de Tivoli Netcool/OMNIbus en cours d'exécution, peut être spécifié pour le programme Sonde pour Tivoli Netcool/OMNIbus, le cas échéant.

Une pratique suggérée pour la modification des valeurs par défaut des propriétés consiste à ajouter une ligne nom-valeur pour chaque propriété requise au bas du fichier. Pour spécifier une propriété, vérifiez que la ligne n'est pas mise en commentaire et modifiez ensuite la valeur comme il convient. Les valeurs

de chaîne doivent être placées entre guillemets ; ce n'est pas nécessaire pour les autres types de valeur. Par exemple :

```
Buffering         :    1
BufferSize        :    15
```

Pour le traitement des incidents, vous pouvez configurer les propriétés d'analyse à partir de la ligne de commande en exécutant la commande **nco_p_ncpmonitor** avec les options de ligne de commande appropriées.

Remarque : Les propriétés suivantes ont des valeurs par défaut standard :

Server
Correspond par défaut au serveur ObjectServer identifié dans le schéma `ConfigItnm`, ce qui garantit la cohérence avec la passerelle Network Manager.

PropsFile
Correspond par défaut à `$NCHOME/probes/`*`plateforme`*`/nco_p_ncpmonitor.props`.

RulesFile
Correspond par défaut à `$NCHOME/probes/`*`plateforme`*`/nco_p_ncpmonitor.rules`.

MessageLog
Correspond par défaut à `$NCHOME/log/precision/nco_p_ncpmonitor.`*`nom_domaine`*`.log`.

RawCaptureFile
Correspond par défaut à `$NCHOME/var/precision/nco_p_ncpmonitor.`*`nom_domaine`*`.cap`.

Pour plus d'informations sur les propriétés communes des analyses, voir *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* dans le centre de documentation de Tivoli Netcool/OMNIbus à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Référence de configuration nco_p_ncpmonitor.rules

Le fichier `$NCHOME/probes/`*`arch`*`/nco_p_ncpmonitor.rules` commentSonde pour Tivoli Netcool/OMNIbus traite Network Manager les données d'événement pour créer un événement signifiant Tivoli Netcool/OMNIbus.

En pratique, ce fichier de règles mappe les données d'événement Network Manager vers les zones ObjectServer et peut être utilisé pour personnaliser le comportement de la sonde. Pour la configuration du fichier de règles, il est nécessaire de maîtriser la syntaxe des règles de sonde Tivoli Netcool/OMNIbus.

La sonde utilise des jetons et des éléments et applique des règles pour transformer les données source d'événement Network Manager en un format connu du serveur ObjectServer. Les données source d'événement brutes sont converties en jetons, qui sont ensuite analysés en éléments. Le fichier de règles permet d'effectuer le traitement conditionnel des éléments puis de mapper ces derniers vers les zones alerts.status du serveur ObjectServer. Dans le fichier de règles, les éléments sont identifiés par le symbole $ et les zones alerts.status par le symbole @. La configuration du fichier de règles mappe les éléments vers des zones, comme cela est présenté dans le code exemple suivant :

```
@Summary=$Description
```

Dans cet exemple, @Summary identifie la zone alerts.status et $Description identifie la zone d'entrée Network Manager.

Lorsque le champ Network Manager ExtraInfo est utilisé avec des champs imbriqués pour conserver des données supplémentaires sur des entités (par exemple, ExtraInfo-> ifIndex), ces champs sont disponibles au format suivant dans le fichier de règles :

```
$ExtraInfo_variable
```

Où *variable* représente une variable MIB (Management Information Base), telle ifIndex ou d'autres données (par exemple, des noms de colonne dans des tables NCIM). Les variables MIB sont spécifiées à la fois en minuscules et majuscules et les autres données en majuscules. Par exemple :

```
$ExtraInfo_ifIndex
$ExtraInfo_MONITOREDENTITYID
```

Pour configurer le fichier de règles pour la Sonde pour Tivoli Netcool/OMNIbus, il est nécessaire de connaître :

- Les données source d'événement Network Manager disponibles pour être utilisées dans le fichier de règles de sonde
- L'ensemble de zones alerts.status pouvant être chargées avec les données d'événement de Network Manager
- Le mappage des données entre Network Manager et les zones alerts.status

Pour plus d'informations sur la syntaxe utilisée dans les fichiers de règles de sonde, voir le document *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* dans le centre de documentation Tivoli Netcool/OMNIbus à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Exemple de traitement de fichier de règles
Cet exemple présente comment les données source de Network Manager sont traitées par le fichier de règles afin de générer les données de sortie insérées dans la table `alerts.status`.

L'exemple de code suivant présente un enregistrement de données d'événement Network Manager transmis à la Sonde pour Tivoli Netcool/OMNIbus pour traitement. Dans cet enregistrement, un événement de résolution a été créé lors du démarrage du processus **ncp_store** par **ncp_ctrl**.

```
{
    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;
        };
}
```

L'extrait suivant du fichier de règles de sonde présente la syntaxe utilisée pour le traitement et le mappage de ces zones d'entrée vers des zones 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
}
```

Une fois le traitement du fichier de règles terminé, les données de sortie transmises au serveur ObjectServer ont la forme suivante :

```
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;
}
```

En fonction du traitement du fichier de règles présenté dans cet exemple, vous pouvez voir que les zones d'entrée Network Manager sont associées aux zones alerts.status de la manière suivante :

Zone Network Manager	**Zone de la table alerts.status**
EventName	EventId

Zone Network Manager	Zone de la table alerts.status
Gravité	Gravité
EntityName	Node
Description	Récapitulatif
ExtraInfo->EVENTTYPE	Type
ExtraInfo->SOURCE	Agent
ExtraInfo->ALERTGROUP	AlertGroup
ExtraInfo->EVENTMAP	NmosEventMap
ExtraInfo->SERVICE	LocalPriObj

Remarque : Les entrées et les sorties complètes des règles de sonde sont visibles dans le fichier de trace de sonde. Définit la trace vers débogage 4 Le fichier de sonde de trace se trouve à : `$NCHOME/log/precision`. Pour plus d'informations sur la définition des niveaux de journalisation, reportez-vous à *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Référence associée

Zones de la table alerts.status utilisées par Network Manager
La table alerts.status d'ObjectServer contient les informations d'état sur les problèmes détectés par les sondes.

Zones des données d'événement Network Manager
Lorsque des événements sont générés dans Network Manager, les données associées sont insérées dans un certain nombre de zones (ou colonnes) dans les tables Network Manager. Bien que chaque événement n'utilise qu'un sous-ensemble des zones possibles, un certain nombre de zones sont communes à tous les types d'événement.

Le tableau suivant répertorie tous les noms des zones Network Manager pouvant être utilisées dans le fichier de règles d'analyse et décrit les données d'événement stockées dans chaque zone. Il identifie également les zones Network Manager communes à tous les événements et donc toujours disponibles dans le fichier de règles.

Tableau 8. Zones Network Manager qui renseignent les événements

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
Description	Courte description de l'événement.	Oui
Domaine	Domaine en cours. Si Network Manager est configuré pour le mode de reprise en ligne, cela correspond au domaine principal.	Oui (à condition que le fichier de mappe ne soit pas modifié)
EntityName	Pour les événements de réseau, il s'agit de la zone entityName de la table entityData NCIM pour l'entité par rapport à laquelle l'événement est émis. En ce qui concerne les événements de statut, il s'agit toujours du nom du domaine à propos duquel l'événement est généré.	Oui
EventName	Identificateur de l'événement. Par exemple, ItnmDiscoPhase.	Oui

Tableau 8. Zones Network Manager qui renseignent les événements (suite)

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
ExtraInfo_ACCESSIPADDRESS	Si l'entité de noeud principal ou d'interface identifiée par la zone d'entrée EntityName comporte une adresse IP accessible directement (zone accessIPAddress provenant des tables de l'interface ou du boîtier NCIM), elle est indiquée ici. Applicable aux événements de réseau uniquement.	Non
ExtraInfo_AGENT	Agent responsable d'un événement d'agent de reconnaissance (ItnmDiscoAgentStatus).	Oui (pour les événements ItnmDiscoAgentStatus)
ExtraInfo_ALERTGROUP	Groupe d'alerte de l'événement. En ce qui concerne les événements de statut Network Manager, le groupe d'alerte est `ITNM Status` et en ce qui concerne les événements de réseau, la valeur est `ITNM Monitor`.	Oui
ExtraInfo_ENTITYCLASS	Nom de classe affecté à l'entité, tel qu'identifié dans les tables NCIM entityClass et classMembers.	Oui (pour les événements de réseau et ItnmEntityCreation)
ExtraInfo_ENTITYTYPE	Type de l'entité, tel que défini dans la table NCIM entityType.	Oui (pour les événements de réseau)
ExtraInfo_LocalPriObj	Fournit une valeur pour la zone LocalPriObj dans l'enregistrement alerts.status. Cette zone a la même valeur que la zone dépréciée ExtraInfo_EventSnmpIndex, sauf qu'elle est précédée par l'identificateur pour l'entité MIB interrogée ; par exemple ifEntry, bgpPeerEntry.	Oui (pour les événements de réseau)
ExtraInfo_EVENTTYPE	Type de l'événement émis par Network Manager. Les valeurs sont les suivantes : • 1 : Problème • 2: Résolution • 13 : Informations	Oui
ExtraInfo_FINDER	L'outil de recherche responsable de l'événement d'outil de recherche de reconnaissance (ItnmDiscoFinderStatus).	Oui (pour les événements ItnmDiscoFinderStatus)
ExtraInfo_ifIndex	En ce qui concerne les événements émis par rapport à une interface comportant une valeur ifIndex dans la table d'interface NCIM, cette valeur est indiquée ici. Applicable uniquement aux événements de réseau par rapport aux interfaces.	Non

Tableau 8. Zones Network Manager qui renseignent les événements (suite)

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
ExtraInfo_IFALIAS	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la valeur ifAlias, si elle est connue. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_IFDESCR	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la valeur ifDescr, si elle est connue. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_IFNAME	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la valeur ifName, si elle est connue. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_IFTYPESTRING	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la représentation de chaîne de la valeur ifType. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_MAINNODEADDRESS	Interface de gestion du noeud principal contenant l'entité, telle qu'identifiée par la zone accessIPAddress de la table de boîtier NCIM. Applicable uniquement aux événements de réseau et ItnmEntityCreation.	Oui (pour les événements de réseau)
ExtraInfo_MAINNODEENTITYID	La zone entityId de la table entityData NCIM pour le noeud principal, tel qu'identifié par la zone accessIPAddress de la table de boîtier NCIM. Applicable uniquement aux événements de réseau.	Oui (pour les événements de réseau)
ExtraInfo_MAINNODEENTITYNAME	Zone entityName de la table entityData NCIM pour le noeud principal, telle qu'identifiée dans NCIM. Applicable uniquement aux événements de réseau.	Oui (pour les événements de réseau)
ExtraInfo_MONITOREDENTITYID	Zone entityId de la table entityData NCIM pour l'entité par rapport à laquelle l'événement est émis. Applicable uniquement aux événements de réseau et ItnmEntityCreation.	Non
ExtraInfo_MONITOREDINSTID	Enregistrement contenu dans la table ncpolldata.monitoredInstance.	Non
ExtraInfo_NEWPHASE	Phase de reconnaissance qui a démarré. Applicable uniquement aux événements de phase de reconnaissance (ItnmDiscoPhase).	Oui (pour les événements de phase de reconnaissance)

Tableau 8. Zones Network Manager qui renseignent les événements (suite)

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
ExtraInfo_OLDPHASE	Phase de reconnaissance terminée. Applicable uniquement aux événements de phase de reconnaissance (ItnmDiscoPhase).	Oui (pour les événements de phase de reconnaissance)
ExtraInfo_POLICYNAME	Nom de la règle d'interrogation ayant entraîné l'événement.	Oui (pour les événements de réseau)
ExtraInfo_PID	ID de processus du service Network Manager affecté. Applicable uniquement aux événements ItnmServiceState.	Oui (pour les événements d'état de service)
ExtraInfo_REMOTEDOMAIN	Nom du domaine distant. Applicable uniquement aux événements ItnmFailoverConnection.	Oui (pour les événements de connexion de reprise en ligne)
ExtraInfo_sysContact	Si disponible, la valeur sysContact est fournie uniquement pour les événements ItnmEntityCreation.	Non
ExtraInfo_sysLocation	Si disponible, la valeur sysLocation est fournie uniquement pour les événements ItnmEntityCreation	Non
ExtraInfo_sysObjectId	Si disponible, la valeur sysObjectId est fournie uniquement pour les événements ItnmEntityCreation	Non
ExtraInfo_SERVICE	Nom du service Network Manager affecté. Applicable uniquement aux événements ItnmServiceState.	Oui (pour les événements d'état de service)
ExtraInfo_SNMPSTATUS	Code de statut SNMP numérique.	Oui (pour les événements NmosSnmpPollFail)
ExtraInfo_SNMPSTATUSSTRING	Indication lisible par l'utilisateur de l'état d'échec SNMP.	Oui (pour les événements NmosSnmpPollFail)
ExtraInfo_SOURCE	Nom du processus d'où provient l'événement.	Oui
ExtraInfo_STITCHER	Programme stitcher responsable d'un événement de programme stitcher de reconnaissance (ItnmDiscoStitcherStatus).	Oui (pour les événements ItnmDiscoStitcherStatus)
Gravité	Niveau de gravité de l'événement. La gravité est une valeur différente de zéro.	Oui

Zones de la table alerts.status utilisées par Network Manager

La table alerts.status d'ObjectServer contient les informations d'état sur les problèmes détectés par les sondes.

Un sous-ensemble des zones standard de la table `alerts.status` est rempli avec les données d'événement Network Manager. De plus, un ensemble de zones dédiées de la table `alerts.status` est réservé pour conserver les données spécifiques à Network Manager. Les noms des zones `alerts.status` dédiées sont identifiés à l'aide du préfixe `Nmos`.

Le tableau suivant décrit les zones `alerts.status` remplies par les zones Network Manager. Des valeurs par défaut sont affectées à certaines zones `alerts.status` à partir du fichier de règles d'analyse (évitez de les modifier).

Tableau 9. Zones de la table alerts.status utilisées par Network Manager

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
Agent	varchar(64)	Nom du processus qui a été généré l'événement. Vous pouvez utiliser cette zone pour filtrer un **Afficheur d'événements** afin de n'afficher que les événements d'un type donné, par exemple, uniquement les événements de reconnaissance (avec la valeur ncp_disco).	ExtraInfo_SOURCE
AlertGroup	varchar(255)	Utilisée pour regrouper les événements par type. Les valeurs fournies par défaut à partir des événements Network Manager sont soit `ITNM Monitor` pour les événements liés au réseau, soit `ITNM Status` pour les événements de statut.	ExtraInfo_ALERTGROUP
AlertKey	varchar(255)	Chaîne de texte concaténant différents éléments relatifs à l'événement. Ces éléments peuvent inclure l'ID de l'événement, le domaine, la phase et le nom du processus. Cette zone permet de faire correspondre les événements de problème et de résolution.	Cette valeur est générée à partir des informations saisies pour veiller à ce que les événements de problème et de résolution soit correctement appariés au sein d'ObjectServer.
Classe	entier	Classe d'alerte affectée à la Sonde pour Tivoli Netcool/OMNIbus.	La valeur `8000` est réservée aux événements générés par Network Manager.
EventId	varchar(255)	Type de l'événement (par exemple, SNMPTRAP-linkDown). La passerelle d'événements utilise cette valeur pour rechercher le mappage d'événement et pour déterminer la priorité des événements.	EventName
ExpireTime	entier	Date d'expiration de l'événement dans la base de données. Cette zone n'est pas utilisée par Network Manager pour le moment.	
FirstOccurrence	heure	Horodatage correspondant à la première occurrence de l'événement.	
Identificateur	varchar(255)	Valeur unique pour chaque type d'événement sur une entité donnée (par exemple, un événement LinkDown pour une interface de périphérique spécifique). Cet identificateur contrôle le dédoublonnage.	Cette valeur est générée à partir des informations saisies pour veiller à ce que les événements d'ObjectServer soient dédoublonnés de manière appropriée. Dans le fichier de règles, l'identification est construit sous la forme de valeurs de zone concaténées.

Tableau 9. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
LastOccurrence	heure	Horodatage correspondant à la dernière occurrence de l'événement.	
LocalNodeAlias	varchar(64)	Adresse IP ou DNS du périphérique. Cette valeur fait généralement référence au boîtier, mais dans le cas précis des événements pingFails, elle peut correspondre à l'interface.	Pour les événements de réseau, cette zone a la même valeur que la zone Node. Aucune valeur n'est définie pour les événements de statut afin qu'ils ne soient pas retransmis à Network Manager via la passerelle d'événements.
LocalPriObj	varchar(255)	Entité spécifique pour laquelle l'événement est généré (par exemple, valeur de la zone ifIndex, ifDescr ou ifPhysAddress).	ExtraInfo_AGENT ou ExtraInfo_FINDER ou ExtraInfo_ifIndex ou ExtraInfo_NEWPHASE ou ExtraInfo_SERVICE ou ExtraInfo_STITCHER La valeur ExtraInfo_ifIndex est affichée en utilisant la syntaxe `ifEntry.<ifIndex>`; par exemple, `ifEntry.12`.
LocalRootObj	varchar(255)	Conteneur de l'entité référencée dans la zone LocalPriObj. Il n'est pas nécessaire que ce soit le boîtier, mais il peut s'agir, par exemple, d'un emplacement du boîtier. Le boîtier peut être identifié à l'aide de la zone LocalNodeAlias.	
LocalSecObj	varchar(255)	Objet secondaire référencé par l'événement.	ExtraInfo_OLDPHASE
Manager	varchar(64)	Nom descriptif qui identifie le système ayant transmis les événements.	La valeur `ITNM` est utilisée pour les événements générés par Network Manager version 3.8 ou toute version ultérieure. La valeur `Omnibus` est utilisée pour les versions antérieures.
NmosCauseType	entier	Etat de l'événement. Cette zone est remplie par la passerelle NMOS. Les valeurs possibles sont les suivantes : • 0 : Inconnu • 1 : Cause Fondamentale • 2 : Symptôme	

Tableau 9. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
NmosDomainName	varchar(64)	Nom du domaine réseau Network Manager qui a signalé l'événement. Le nom du domaine principal est utilisé en mode de reprise en ligne. Par défaut, cette zone est remplie uniquement pour les événements générés par Network Manager. Pour remplir cette zone pour d'autres sources d'événement, celles des autres sondes par exemple, vous devez modifier les fichiers de règles pour ces sondes. Cette zone est remplie par la passerelle d'événements si un événement correspond à une entité dans un domaine.	Domaine
NmosEntityId	entier	ID objet unique qui identifie l'entité topologique à laquelle l'événement est associé. Cette zone est identique à la zone NmosObjInst mais contient davantage d'informations. Par exemple, elle peut inclure l'ID d'une interface dans un périphérique. Pour les événements générés par le moteur d'interrogation, la zone NmosEntityId est remplie dans le fichier de règles d'analyse. Pour tous les autres événements, cette zone est remplie par la passerelle lorsqu'une entité est identifiée.	ExtraInfo_MONITOREDENTITYID
NmosEventMap	varchar(64)	Nom de la mappe d'événements et priorité facultative de l'événement, qui indique comment Network Manager doit traiter l'événement (par exemple, PrecisionMonitorEvent.910). Le numéro de priorité facultative peut être concaténé à la fin de la valeur, précédé d'un point (.) Si la priorité n'est pas spécifiée, la valeur 0 lui est affectée. **Remarque :** Cette valeur peut être remplacée par une insertion explicite de la table config.precedence de la passerelle d'événements, qui fournit les mêmes données.	

Tableau 9. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
NmosManagedStatus	entier	Statut géré de l'entité réseau pour laquelle l'événement a été généré. Lorsqu'une entité réseau n'est pas gérée, les interrogations Network Manager sont suspendues et les événements provenant d'autres sources sont marqués comme non gérés. Cette zone permet de filtrer les événements des entités non gérées. Les valeurs possibles pour cette zone sont les suivantes : • 0 : Géré • 1 : Non-géré Opérateur • 2 : Non-géré Système • 3: Hors de portée	
NmosObjInst	entier	ID objet unique qui identifie l'entité de boîtier topologique à laquelle l'événement est associé. Cette zone est remplie par la passerelle NMOS. **Conseil :** Cette zone peut être utilisée pour détecter si l'événement a été transmis pour enrichissement.	
NmosSerial	entier	Numéro de série de l'événement qui a supprimé l'événement en cours. Cette zone est remplie par la passerelle NMOS.	
Node	varchar(64)	Périphérique associé à la génération de l'événement. Si un événement est généré depuis une entité ayant une adresse IP accessible, cette adresse est utilisée. Sinon, la valeur entityName de la base de données NCIM est utilisée. Par défaut, la zone Node a la même valeur que la zone LocalNodeAlias.	ExtraInfo_ACCESSIPADDRESS ou EntityName La valeur EntityName est mappée vers la zone Node uniquement si la zone de saisie ExtraInfo_ACCESSIPADDRESS est vide.
NodeAlias	varchar(64)	Adresse IP du noeud principal, si disponible.	ExtraInfo_MAINNODEADDRESS

Tableau 9. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
RemoteNodeAlias	varchar(64)	Adresse réseau d'un noeud distant, si pertinent. Par exemple : • Une valeur vide (si une interface est défaillante) • Une adresse voisine (si une interface connectée est défaillante) • Le poste d'interrogation (pour un événement d'échec de commande PING)	
Serial	incr	ID unique par événement par instance de serveur ObjectServer. Lorsque des serveurs ObjectServer principal et de secours sont configurés, ces serveurs auront des numéros de série différents pour le même événement.	
ServerName	varchar(64)	Nom du serveur ObjectServer à l'origine de l'événement.	
ServerSerial	entier	Numéro de série de l'événement sur le serveur ObjectServer d'origine. Lorsque des serveurs ObjectServer principal et de secours sont configurés, ces serveurs auront des numéros de série différents pour le même événement. Si l'événement provient du serveur ObjectServer en cours, la valeur de la zone ServerSerial est la même que celle de la zone Serial.	
Gravité	entier	Niveau de gravité de l'événement stockés dans ObjectServer. Les valeurs par défaut sont les suivantes : • 0 : Effacé (VERT) • 1 : Indéterminé (VIOLET) • 2 : Avertissement (BLEU) • 3: Mineur (JAUNE) • 4: Majeur (ORANGE) • 5: Critique (ROUGE)	Gravité

Tableau 9. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
StateChange	heure	Horodatage correspondant à la dernière modification de l'événement. Cette zone peut être utilisée pour déterminer si un processus a modifié un événement après qu'il a été ajouté à ObjectServer.	
Récapitulatif	varchar(255)	Description textuelle de l'événement.	Description
Tally	entier	Comptage du nombre d'occurrences d'un événement. Cette valeur apparaît dans la colonne Count de la liste d'événements ou de l'**Afficheur d'événements** et dans la colonne Occurred de la table `mojo.events`.	
Type	entier	Type de l'alerte. Les valeurs pertinentes pour Network Manager sont les suivantes : • 1 : Problème • 2 : Résolution • 13 : Informations	ExtraInfo_EVENTTYPE

Pour plus d'informations sur la table `alerts.status`, consultez le manuel *IBM Tivoli Netcool/OMNIbus Administration Guide* dans le centre de documentation Tivoli Netcool/OMNIbus, à l'adresse IBM Tivoli Netcool/OMNIbus Informations sur le produit.

Automatisations Tivoli Netcool/OMNIbus ajoutées par Network Manager

Network Manager fournit de nombreuses automatisations Tivoli Netcool/OMNIbus. Chaque automatisation réalise différentes tâches dans l'installation de Network Manager.

Pour activer une automatisation, utilisez l'interface graphique d'administration Tivoli Netcool/OMNIbus.

Le tableau ci-dessous décrit les automatisations Tivoli Netcool/OMNIbus installées par Network Manager.

Tableau 10. Automatisations Tivoli Netcool/OMNIbus ajoutées par Network Manager

Automatisation	Description	Ajoutée pendant l'installation ?	Etat par défaut
severity_from_ causetype	Définit la gravité des événements dans la table ObjectServer alerts.status en fonction de la valeur de NmosCauseType, une zone énumérée qui contient les résultats des calculs Network Manager RCA (Root Cause Analysis). Les valeurs possibles de la zone NmosCauseType sont : • 0 - Inconnu • 1 - Origine du problème • 2 - Symptôme	Oui	Activé
suppress_cross_ domain_connections	Supprime les événements des unités connectées lorsque l'unité connectée se trouve dans un domaine différent. Cette automatisation est déclenchée lorsqu'un événement est mis à jour par la passerelle d'événements. **Restriction :** Network Manager modèle uniquement des connexions via les domaines réseau dans les réseaux MPLS entre les unités PE et CE, et dans les réseaux BGP entre les homologues BGP. Pour que l'automatisation fonctionne, les deux unités réseau doivent être connectées à la couche 3 sur un sous-réseau /30 (un sous-réseau de seulement deux hôtes). Chaque unité doit également être reconnue dans un domaine réseau différent et l'existence de son unité associée doit avoir été induite pendant la reconnaissance. Ceci signifie que dans chaque domaine une unité CE induite ou une entité homologue BGP induite doit avoir été créée.	Oui	Désactivé
update_service_ affecting_events	Génère des événements affectés par un service (SAE) lorsqu'elle rencontre des événements réseau sur des entités de support de service. Après chaque reconnaissance, les plug-in SAE de la passerelle d'événements analysent la topologie mise à jour et mettent à jour le serveur ObjectServer avec la liste des entités prenant en charge des services. Ces informations activent l'automatisation pour générer des événements affectés par un service lorsqu'elles rencontrent des événements réseau sur des entités de support de service.	Non	Non applicable

Configuration de l'intégration avec Netcool Configuration Manager

Pour ajouter des capacités de configuration réseau et de gestion des règles à votre solution de gestion réseau, configurez Network Manager et Tivoli Netcool/OMNIbus afin de fonctionner avec IBM Tivoli Netcool Configuration Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'intégration entre Network Manager, Tivoli Netcool/OMNIbus et Netcool Configuration Manager.

Vous devez installer Network Manager avant d'installer Netcool Configuration Manager. Vous devez installer Netcool Configuration Manager avec certaines options de configuration.

Pour trouver d'autres informations sur la configuration de l'intégration, sélectionnez votre version de Netcool Configuration Manager depuis le Knowledge Center à http://www.ibm.com/support/knowledgecenter/SS7UH9/welcome, et consultez les sujets *Integrating Netcool Configuration Manager with Network Manager et Tivoli Netcool/OMNIbus*. Vous pouvez également télécharger la version PDF, intitulée *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Remarque : Vous trouvez également sur Netcool Configuration Manager Knowledge Center les détails complets de la façon de supprimer l'intégration avec Netcool Configuration Manager.

Exportation de données de reconnaissance vers CCMDB, TADDM, et TBSM

Configurez et utilisez l'adaptateur de bibliothèque de reconnaissance (DLA) pour collecter des données sur les ressources et relations réseau à partir de Network Manager en vue de leur importation dans d'autres systèmes.

Pourquoi et quand exécuter cette tâche

L'adaptateur DLA collecte des données sur Network Manager et crée des livres de bibliothèque de reconnaissance XML (également appelés langage IML ou livres IdML) contenant des données sur les ressources découvertes et leurs relations connues par le système. Les livres sont conformes à Tivoli Common Data Model (CDM) version 2.10.10. Pour plus d'informations sur Tivoli CDM, voir http://www.redbooks.ibm.com/abstracts/redp4389.html.

Les livres de la bibliothèque de reconnaissance peuvent être importés dans d'autres systèmes dans lesquels se trouve l'outil Library Reader de reconnaissance. Le DLA prend en charge IPv4 ou IPv6.

Remarque : Pour charger les manuels de bibliothèque de reconnaissance (IdML) contenant des informations sur les machines virtuelles dans TADDM, vous devez avoir TADDM 7.2.1 Fix Pack 1 , ou une version supérieure.

L'adaptateur de bibliothèque de reconnaissance est installé par défaut avec Network Manager sur le serveur de l'interface graphique Dans le répertoire suivant : `$NCHOME/precision/adapters/ncp_dla`.

Prérequis pour l'utilisation du DLA

Avant de configurer et utiliser l'adaptateur de bibliothèque de reconnaissance (DLA), vérifiez que les pré-requis sont respectés.

- Une reconnaissance réseauNetwork Manager a été effectuée avec succès et la base de données Network Connectivity and Inventory Model (NCIM) a été remplie.
- Le DLA utilise par défaut le pool de connexions du serveur d'interface graphique. Si vous souhaitez utiliser une autre base de données NCIM que celle fournie lors de l'installation, vous devez disposer des droits d'accès pour cette base de données NCIM.

- Vous devez exécuter le script `ncp_dla.sh` avec un IBM Java JRE dans votre variable d'environnement $PATH. Pour contrôler votre version de Java, exécutez la commande suivante : `java -version`. Si la version de Java n'est pas IBM, situez un IBM JRE et ajoutez le répertoire qui le contient au départ de la variable d'environnement $PATH. Un JRE approprié est situé dans le répertoire suivant : `$WAS_HOME/java/bin`.
- Vous devez savoir comment est déployé le produit avec lequel vous souhaitez effectuer l'intégration.
  - Pour plus d'informations sur IBM Tivoli Application Dependency Discovery Manager, voir IBM Knowledge Center à l'adresse Web suivante :

    http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome
  - Pour plus d'informations sur IBM Tivoli Business Service Manager, voir IBM Knowledge Center à l'adresse Web suivante :

    http://www.ibm.com/support/knowledgecenter/SSSPFK/welcome
  - Pour plus d'informations sur IBM Tivoli Change and Configuration Management Database, voir IBM Knowledge Center à l'adresse Web suivante : : http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome

Configuration de l'adaptateur de bibliothèque de reconnaissance

L'adaptateur de bibliothèque de reconnaissance (DLA) requiert un fichier de propriétés de configuration pour déterminer la source de données à laquelle se connecter, le domaine à analyser, le répertoire cible pour les livres de bibliothèque de reconnaissance et les paramètres de connexion.

Pourquoi et quand exécuter cette tâche

Vous devez configurer les propriétés de l'adaptateur de bibliothèque de reconnaissance si vous disposez d'un serveur d'interface graphique distinct ou si vous souhaitez utiliser cet adaptateur avec une instance NCIM différente de celle par défaut fournie lors de l'installation.

Un fichier de configuration `ncp_dla.properties` préconfiguré est fourni dans le répertoire d'installation de l'adaptateur de bibliothèque de reconnaissance : `$NMGUI_HOME/adapters/ncp_dla`. La présence de 'XXXXXX' ou <'word'> dans le fichier de configuration indique que le paramètre doit être spécifié par l'utilisateur. Ce fichier de configuration fournit des valeurs par défaut utiles pour la plupart des options. Veillez cependant à les remplacer par les valeurs appropriées pour votre environnement.

Remarque : Par défaut, les paramètres d'accès NCIM requis pour l'utilisation de l'adaptateur de bibliothèque de reconnaissance sont dérivés du pool d'accès d'interface graphique Network Manager. Cette option est définie par le paramètre **`ncp.dla.datasource.autoConnect`**, où la valeur par défaut est "true". Si vous définissez cette valeur sur "false," vous devez indiquer des valeurs pour les paramètres répertoriés à l'étape «6», à la page 112. La définition du mode de connexion manuel à la base de données NCIM est utile lorsque l'accès au pool de connexion est impossible ou si vous voulez utiliser une instance NCIM différente de celle fournie par défaut au cours de l'installation.

Procédure

1. Accédez à `$NMGUI_HOMEadapters/ncp_dla` et copiez le fichier `ncp_dla.properties` vers une version spécifique de domaine en ajoutant le nom du fichier au nom de domaine, par exemple, `ncp_dla.properties.NCOMS`.
2. Indiquez le nom de domaine Network Manager en attribuant une valeur à la propriété **`ncp.dla.precisionDomain`**.

   Le nom de domaine par défaut est "NCOMS."
3. Facultatif : Vous pouvez définir le chemin d'accès à un répertoire temporaire devant être utilisé par l'adaptateur de bibliothèque de reconnaissance lors de la génération de la sortie si vous ne voulez pas que celui-ci utilise le répertoire temporaire par défaut du système d'exploitation. Utilisez le paramètre **`ncp.dla.scratchDirectory`** pour définir le chemin d'accès complet à un répertoire temporaire inscriptible, par exemple **`ncp.dla.scratchDirectory=/opt/space/temp`**.

4. Définissez les objets CDM pour lesquels vous voulez que des données soient générées. Utilisez le paramètre **ncp.dla.generationFilter** pour spécifier les valeurs dans la liste des valeurs séparées par une virgule. Les valeurs possibles sont les suivantes :
   - `ComputerSystem` - génère les données suivantes pour les périphériques :
     - ComputerSystem
     - SnmpSystemGroup
     - OperatingSystem
     - IpInterface pour IpDevice, périphériques sans accès SNMP
     - Routeur
     - Pont
   - LTE - génère les données suivantes pour les classes LTE :
     - Fonction
     - HomogeneousCollection
     - Zone
     - Carte
     - NetworkInterface
   - Mise en réseau - génère les données suivantes pour les réseaux :
     - L2Interface
     - IpInterface
     - IpV4Address
     - IpV6Address
     - IpNetwork
   - Physique - génère les données suivantes pour les classes physiques :
     - PowerSupply
     - Ventilateur
     - Boîtier
     - Détecteur
     - PhysicalPackage
     - Carte
     - Carte fille

   Pour générer des données vous devez ajouter une valeur utilisant le format suivant au paramètre **ncp.dla.generationFilter** :

   ```
   ncp_dla.generationFilter=ComputerSystem[,data]
   ```

   Où *data* est un des types de données spécifiques listé dans cette étape.

   Exemples :

   - Pour générer des données système, ajoutez les valeurs suivantes au paramètre :

     ```
     ncp_dla.generationFilter=ComputerSystem
     ```

     Remarque : Vous devez, au moins, spécifier cette valeur. Si vous ne spécifiez pas de valeur dans le paramètre **ncp.dla.generationFilter**, l'adaptateur de bibliothèque de reconnaissance ne génère pas de données.
   - Pour générer des données système et LTE, ajoutez les valeurs suivantes au paramètre :

     ```
     ncp_dla.generationFilter=ComputerSystem,LTE
     ```

- Pour générer des données système et celles relatives à la connectivité réseau, ajoutez les valeurs suivantes au paramètre :

```
ncp_dla.generationFilter=ComputerSystem,Networking
```

5. Facultatif : Vous pouvez définir l'adresse URL à utiliser pour le lancement contextuel dans d'autres systèmes. Définissez le paramètre **ncp.dla.contextualLaunchURL** à la valeur de topologie dans laquelle vous voulez effectuer le lancement et spécifiez le nom d'hôte et le port pour le serveur de topologie Topoviz. L'option par défaut consiste à effectuer le lancement dans la vue Tronçon.

   Par exemple, pour établir le lancement contextuel dans le Navigateur de Structure :

```
ncp.dla.contextualLaunchURL=https://hostname:16316/ibm/console/
ncp_structureview/Launch.do?entityId=
```

6. Facultatif : Si vous remplacez la valeur de **ncp.dla.datasource.autoConnect** par "false," spécifiez les détails d'accès RDBMS en modifiant les paramètres suivants qui définissent la base de données à laquelle se connecte l'adaptateur de bibliothèque de reconnaissance pour générer les manuels de la bibliothèque de reconnaissance :

   ncp.dla.datasource.type
   Spécifiez le type de système de gestion de base de données relationnelle ; le type par défaut est DB2 :

   - DB2 Db2
   - Oracle Oracle

   ncp.dla.datasource.driver
   Indiquez le pilote JDBC à utiliser :

   - DB2 `com.ibm.db2.jcc.Db2Driver`
   - Oracle `oracle.jdbc.driver.OracleDriver`

   ncp.dla.datasource.url
   Indiquez l'adresse URL JDBC de connexion à la base de données NCIM :

   - DB2 `jdbc:db2://`*`nom_hôte`*`:`*`numéro_port`*`/`*`nom_base_de_données`*
   - Oracle `jdbc:oracle:thin:@//`*`nom_hôte`*`:`*`numéo_port`*`/`*`nom_service`* où *nom_service* correspond au nom de service Oracle se référant à l'instance de base de données Oracle exécutée sur le serveur.

   ncp.dla.datasource.schema
   Nom du schéma de base de données NCIM, généralement "ncim"

   ncp.dla.datasource.ncpgui.schema
   Nom du schéma de base de données NCPGUI, généralement "ncpgui"

   ncp.dla.datasource.username
   Nom d'utilisateur de la base de données, généralement "ncim"

   ncp.dla.datasource.password
   Mot de passe utilisateur de la base de données

   ncp.dla.datasource.encrypted
   Indique si le mot de passe de base de données est codé [true|false]

   Si la valeur définie est true, vous devez indiquer une valeur valide pour `ncp.dla.datasource.keyFile` et utiliser le mot de passe codé référencé dans votre fichier `$NMGUI_HOME/profile/etc/tnm/tnm.properties`.

   ncp.dla.datasource.keyFile
   Indiquez le nom et le chemin d'accès complet du fichier de clé cryptographique utilisé dans le fichier `$NMGUI_HOME/profile/etc/tnm/tnm.properties`.

   ncp.dla.datasource.loginTimeout
   Délai d'attente de connexion, correspondant par défaut à 5 secondes

7. Utilisez le paramètre `ncp.dla.refresh.book` pour indiquer si le DLA doit actualiser les manuels de bibliothèque de reconnaissance existants ou en créer de nouveaux. L'option par défaut est `true` ; qui met à jour les instances existantes et en crée de nouvelles, si nécessaire.

   ```
   ncp.dla.refresh.book=true
   ```

8. Utilisez le paramètre `ncp.dla.lte.topology` pour exporter la topologie du contrôle LTE et du plan utilisateur. Cette option peut générer de grandes quantités de données pour les réseaux de grande taille. Le volume de données généré peut avoir un effet négatif sur votre déploiement TADDM. L'option par défaut est `false`.

   ```
   ncp.dla.lte.topology=false
   ```

9. Facultatif : Vous pouvez limiter la portée de la collecte des données à une ou plusieurs vues de réseau en définissant le paramètre **`ncp.dla.network.view`** de sorte qu'il filtre les données des vues de réseau sélectionnées uniquement.

   Par le biais des opérateurs SQL standard, définissez un segment SQL qui est ajouté à la zone **`networkView.name`** au cours de la requête de l'adaptateur de bibliothèque de reconnaissance. Le paramètre doit avoir une valeur commençant par l'un des opérateurs SQL suivants :

   - =
   - <>
   - !=
   - IN
   - NOT IN
   - LIKE
   - NOT LIKE

   Par exemple, la requête suivante définit la portée afin que seule la vue de réseau `Réseaux BGP` soit utilisée pour la portée de la collecte des données :

   ```
   ncp.dla.network.view=='BGP Networks'
   ```

   Remarque : L'adaptateur de bibliothèque de reconnaissance ne prend pas en charge les guillemets. Tous les éléments situés après le signe égal dans l'exemple précédent font partie de la valeur définie, même le second signe égal (=).

   Un autre exemple est celui dans lequel la portée de la collecte de données est définie comme étant n'importe quelle vue de réseau contenant le nom `Cisco` (remarquez l'utilisation du caractère générique SQL %) :

   ```
   ncp.dla.network.view=='BGP Networks'
   ```

10. Utilisez le paramètre `ncp.dla.entity.details` pour indiquer si le DLA doit demander des données de détails d'entité et exporter ces données en tant qu'attribut étendu. L'option par défaut est `false`.

    ```
    ncp.dla.entity.details=false
    ```

11. Utilisez le paramètre `ncp.dla.signatureGenExcludeMAC` pour exclure certaines adresses MAC de l'algorithme de génération de signatures.

    Cela peut être utile lorsque des adresses MAC présentes sur des périphériques réseau sont dupliquées sur le réseau et que vous souhaitez empêcher le processus de génération de signatures de générer plusieurs fois la même signature sans raison.

    Pour utiliser cette fonctionnalité, vous devez entrer, pour chaque adresse MAC potentiellement dupliquée sur le réseau, une propriété `signatureGenExcludeMAC`. Le format de cette propriété est le suivant : `ncp.dla.signatureGenExcludeMAC.`*`n=MAC`*

    Où :

- *n* est un nombre incrémentiel pour chaque exclusion, en commençant par 1.
- *MAC* est l'adresse MAC délimitée par un signe deux-points à exclure du processus de génération de signatures.

Par exemple, les valeurs par défaut du fichier ncp_dla.properties indiquent que les adresses MAC suivantes doivent être exclues du processus de génération de signatures :

- 00:00:00:00:00:00, qui est une adresse MAC par défaut composée uniquement de zéros.
- 02:00:00:00:00:04, qui est une adresse MAC d'interface interne Juniper fpx1.
- 00:0B:CA:FE:00:00, qui est une adresse MAC d'interface de gestion Juniper bme0.

```
ncp.dla.signatureGenExcludeMAC.1=00:00:00:00:00:00
ncp.dla.signatureGenExcludeMAC.2=02:00:00:00:00:04
ncp.dla.signatureGenExcludeMAC.3=00:0B:CA:FE:00:00
```

12. Utilisez le paramètre `ncp.dla.signatureOverride` pour configurer manuellement la signature utilisée par le DLA par unité, ce qui permet ainsi d'ignorer la génération automatisée de signatures.

    Cela est utile lorsque les unités exportées par le DLA ne sont pas correctement rapprochées dans TADDM, par exemple lorsque l'attribut de signature diffère pour la même unité.

    Pour utiliser cette fonctionnalité, vous devez, pour chaque unité pour laquelle vous souhaitez que la signature soit supprimée, connaître les informations suivantes :

    a. Network Manager entityName

    b. TADDM signature

    c. Propriété SignatureOverride

    Le format de cette propriété est le suivant :
    `ncp.dla.signatureOverride.`*`n=entityName=signature`*

    Où :

    - *n* est un nombre incrémentiel pour chaque écrasement, en commençant par 1.
    - *entityName* est le nom d'entité Network Manager de l'unité à laquelle appliquer la signature.
    - *signature* est la signature CDM valide de l'adresse IP de formulaire (adresse MAC) ou de l'adresse IP.

    Remarque : Vous devez vous assurer que vous choisissez une adresse IP et MAC de signature relative à l'unité spécifiée lors de l'utilisation de cette fonctionnalité.

    Par exemple pour écraser la signature pour les périphériques "fred" et "barney", ajoutez les propriétés de configuration suivantes :

    ```
    ncp.dla.signatureOverride.1=fred=172.20.1.6(00:21:28:FF:1A:3A)
    ncp.dla.signatureOverride.2=barney=172.20.1.7(00:21:EE:6B:1A:2A)
    ```

13. Indiquez la façon dont les livres de la bibliothèque de reconnaissance générés par l'adaptateur de bibliothèque de reconnaissance doivent être transférés en définissant le paramètre suivant :

    ncp.dla.datasink.type
    Méthode de transfert des livres de la bibliothèque de reconnaissance. Les options sont les suivantes :

    FILE
    Les livres de la bibliothèque de reconnaissance sont copiés en local dans le répertoire cible `/opt/IBM/netcool/core/var/precision/ccmdb`. Si vous définissez cette option, ignorez l'étape «14», à la page 115 et passez à l'étape «17», à la page 116.

    FTP
    Les livres de la bibliothèque de reconnaissance sont transférés vers un serveur distant par FTP. Si vous définissez cette option, vous devez effectuer l'étape «14», à la page 115

    ncp.dla.datasink.targetDirectory
    Répertoire cible des fichiers des livres de la bibliothèque de reconnaissance

Remarque : Si vous exécutez l'adaptateur de bibliothèque de reconnaissance (DLA) sur un serveur autre que le serveur d'interface graphique et souhaitez placer les livres générés sur ce serveur, vous pouvez spécifier les paramètres de connexion dans le fichier `ncp_dla.properties` en supprimant la mise en commentaire et en modifiant les paramètres autour de **`ncp.dla.datasink.targetDirectory`**.

14. Facultatif : Si vous avez défini l'option FTP pour la propriété **`ncp.dla.datasink.type`**, ajoutez les paramètres suivants :

    ncp.dla.datasink.server
    Adresse IP ou nom d'hôte du serveur FTP distant.

    ncp.dla.datasink.port
    Port TCP à utiliser (par défaut le 21)

    ncp.dla.datasink.binary
    Indique si des transferts FTP binaires doivent être utilisés [true|false]

    ncp.dla.datasink.passive
    Indique si des transferts FTP passifs doivent être effectués [true|false]

    ncp.dla.datasink.username
    Nom d'utilisateur FTP à utiliser

    ncp.dla.datasink.password
    Mot de passe utilisateur FTP à utiliser

    ncp.dla.datasink.encrypted
    Indique si le mot de passe FTP est codé [true|false]

    ncp.dla.datasink.keyFile
    Indiquez le nom et le chemin d'accès complet du fichier de clé cryptographique utilisé dans le fichier `$NMGUI_HOME/profile/etc/tnm/tnm.properties`.

15. Facultatif : Vous pouvez limiter la portée de la collecte des données en filtrant les résultats en fonction des identificateurs des boîtiers. Pour ce faire, indiquez une requête SQL dans le paramètre `ncp.dla.chassis.ids`.

    L'indication d'un filtre avec la propriété `ncp.dla.chassis.ids` vous permet de récupérer uniquement les enregistrements ComputerSystem correspondant aux ID d'entité renvoyés par la requête SQL.

    Remarque : Cette méthode de filtrage est préférable au filtrage effectué avec le paramètre `ncp.dla.network.view`, car elle vous permet définir plus précisément le boîtier qui vous intéresse.

    L'exemple suivant montre une requête SQL qui renvoie les identificateurs des boîtiers étiquetés en périphérique du réseau.

    Remarque : Pour en faciliter la lecture, cette requête SQL est présentée avec des retraits sur plusieurs lignes. Toutefois, dans le fichier de configuration `ncp_dla.properties`, la totalité de la requête SQL doit être présentée sur une seule ligne, sinon l'opération renvoie une erreur.

```
ncp.dla.chassis.ids=SELECT e.mainNodeEntityId
                    FROM entity e
                    INNER JOIN domainMgr  d ON d.domainMgrId = e.domainMgrId
                    WHERE d.domainName = 'NCPPUP' AND EXISTS
                         (SELECT ed.entityId FROM entityDetails ed
                          WHERE ed.entityId = e.entityId
                          AND ed.keyName = 'NetworkEdge'
                          AND ed.keyValue = 1)
                    GROUP BY e.mainNodeEntityId
```

16. Facultatif : Vous pouvez exclure les paramètres de modèle et de fabricant dans le résultat, en indiquant les paramètres `ncp.dla.ExcludeModel` et `ncp.dla.ExcludeManufacturer`.

    Le format de ces paramètres est le suivant :

```
ncp.dla.ExcludeModel.N=MODEL_NAME
ncp.dla.ExcludeManufacturer.N=MANUFACTURER_NAME
```

Where:

- *N* est un nombre qui est incrémenté avec chaque exclusion, à partir de 1.
- *MODEL_NAME* est le nom du modèle à exclure.
- *MANUFACTURER_NAME* est le nom du fabricant à exclure.

Les valeurs correspondantes sont supprimées du résultat.

L'exemple montre comment exclure les fabricants Windows et net-snmp.

```
ncp.dla.ExcludeManufacturer.1=Windows
ncp.dla.ExcludeManufacturer.2=net-snmp
```

17. Indiquez le niveau de débogage de l'adaptateur de bibliothèque de reconnaissance en attribuant une valeur à la propriété **log4j.rootLogger**.

    La valeur par défaut est FATAL et celles autorisées sont les suivantes :

    - DEBOG
    - INFO
    - WARN
    - ERROR
    - IRRECUPERABLE

18. Indiquez le nom et le chemin d'accès complet du fichier journal de l'adaptateur de bibliothèque de reconnaissance en définissant une valeur pour la propriété **log4j.appender.FILE.file**.

    Le nom par défaut est `dla.log`. Le fichier journal est écrit dans le répertoire d'installation de l'adaptateur de bibliothèque de reconnaissance.

19. Facultatif : La propriété obsolète **ncp.dla.validateComputerSystemFqdn** indique s'il convient de valider les noms des entités reconnues par Network Manager en tant que noms de domaine qualifiés complets.

    ATTENTION : Ne modifiez pas la valeur. Cette propriété est obsolète et n'est plus utilisée dans Network Manager versions 3.9 et suivante.

    Cette propriété peut prendre l'une des valeurs suivantes :

    True
    Il s'agit de la valeur par défaut. Les noms d'entité sont validés. L'adaptateur de bibliothèque de reconnaissance ajoute les attributs Fqdn aux instances ComputerSystem uniquement si le nom de périphérique est un nom de domaine qualifié complet valide.

    False
    Aucune validation n'est effectuée. L'adaptateur de bibliothèque de reconnaissance ajoute les attributs Fqdn aux instances ComputerSystem indépendamment du fait que le nom de périphérique soit un nom de domaine qualifié complet valide.

20. Créez une copie du fichier de configuration modifié, avec le nom de votre choix.
21. Créez une copie de la configuration pour chaque domaine Network Manager pour lequel vous souhaitez créer des livres de bibliothèque de reconnaissance.

    A faire : Créez un fichier de configuration pour chaque domaine Network Manager pour lequel vous voulez générer des manuels de la bibliothèque de reconnaissance et ajoutez le nom de ce fichier au nom du domaine (`ncp_dla.properties.NCOMS`, par exemple).

Que faire ensuite

Si vous voulez démarrer les GUI IBM Tivoli Application Dependency Discovery Manager depuis Network Manager, complétez les tâches de configuration additionnelle pour ajouter une option de menu aux GUI Network Manager et ajouter le rapport d'inventaire JSP à TADDM.

Création d'un manuel de la bibliothèque de reconnaissance

Pour créer un manuel de la bibliothèque de reconnaissance, exécutez l'adaptateur DLA avec le fichier de propriétés DLA approprié.

Avant de commencer

Avant d'exécuter DLA, le fichier de propriétés doit être correctement configuré.

Pourquoi et quand exécuter cette tâche

DLA possède deux modes de fonctionnement :

Mode principal
Génère des manuels de la bibliothèque de reconnaissance en interrogeant la base de données NCIM pour les domaines identifiés dans le fichier de configuration indiqué.

Mode importation
Permet l'importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM, afin d'ouvrir l'interface utilisateur TADDM à partir de Network Manager.

Procédure

1. Accédez au répertoire d'installation DLA sur le serveur des composants de l'interface graphique de Network Manager ; le répertoire par défaut est `$NCHOME/precision/adapters/ncp_dla`.
2. Exécutez l'adaptateur DLA et référencez le fichier de propriétés DLA approprié pour votre domaine afin de créer un manuel de la bibliothèque de reconnaissance :

   ```
   ./ncp_dla.sh ncp_dla.properties.domain_name [ -getmore ]
   ```

   Remarque : Le drapeau `-getmore` est optionnel. Il génère toutes les entités incluant les commutateurs empilés pour les filtres ComputerSystem CDM.

   Pour obtenir un exemple d'exécution de la commande et de réponse système, voir «Exemple», à la page 117.

Exemple

L'exemple suivant présente la manière dont il faut exécuter DLA, ainsi que la réponse du système :

```
[root@abc.test]# ./ncp_dla.sh ncp_dla.properties.NCOMS
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2013 By IBM Corporation.  All Rights Reserved.
See product license for details.

[IDML Generation Mode]
Initializing...
WARNING: user.install.root not defined, using /opt/IBM/netcool
/core/precision/profiles/TIPProfile
Loading properties from /opt/IBM/netcool/core/precision/profiles
/TIPProfile/etc/tnm/tnm.properties
FINE: database.type = db2
FINE: database.dbname = ITNM
FINE: database.jdbc.url = null
FINE: database.host = abc.test.ibm.com
FINE: database.port = 50000
FINE: database.username = ncim
FINE: database.connection.defaultFetchSize = null
FINE: database.connection.propertiesFile = null
FINE: Getting encrypted password
Jun 3, 2013 9:15:09 AM DbConnectionPool getJdbcURL
FINE: JDBC URL = jdbc:db2://abc.test.ibm.com:50000/ITNM
INFO: HNMXB0006I=JDBC Driver: com.ibm.db2.jcc.Db2Driver
INFO: HNMXB0007I=JDBC URL   : jdbc:db2://abc.test.ibm.com:50000/ITNM
INFO: HNMXB0007I=JDBC URL   : jdbc:db2://abc.test.ibm.com:50000/ITNM
Jun 3, 2013 9:15:10 AM DbConnectionPool getConnection
FINEST:  Connection Pool READ has size 0
Working on ITNM domain 'NCOMS'...
```

```
Processing 142 ComputerSystem(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Writing IDML Book to '/tmp/dla/ITNMIP39.9.42.16.62.2013-06-03T13.15.11.579Z.
refresh.xml'...
Shutting down...
Finished.
```

Tâches associées

Chargement des manuels de bibliothèque de reconnaissance et activation du lancement bidirectionnel
Vous devez charger le manuel de bibliothèque de reconnaissance (IdML) dans TADDM pour rendre les informations du manuel disponibles pour TADDM. L'importation du manuel active également le lancement contextuel bidirectionnel.

Optimisation de l'exportation de données

Pour proposer un ensemble de ressources et de relations plus facilement utilisables à d'autres systèmes que Network Manager, vous pouvez optimiser l'exportation et la collecte de données DLA. L'optimisation de l'exportation de données Network Manager permet à TADDM et à d'autres utilisateurs de livre de bibliothèque de reconnaissance (IdML) d'importer uniquement les ressources et les relations requises pour générer le lien approprié entre les ressources généralement gérées. De plus, le fait de disposer uniquement des données requises peut de manière significative faciliter le processus d'exportation et d'importation.

Pourquoi et quand exécuter cette tâche

Pour configurer une collecte et une exportation de données optimisées, procédez comme suit :

Procédure

1. Découvrez le réseau en utilisant Network Manager.
2. Exécutez l'utilitaire de balisage **itnmTagNetworkEdgeEntities.pl** pour identifier les entités de type réseau, comme cela est décrit dans «Identification des entités de périphérie du réseau», à la page 118.
3. Créez une vue réseau filtrée qui affiche uniquement la périphérie du réseau, comme cela est décrit dans «Création d'une vue de réseau filtrée pour la périphérie du réseau», à la page 120.
4. Modifiez le fichier de propriétés DLA `ncp_dla.properties.`*`nom_domaine`* afin d'inclure le nom de la vue réseau filtrée que vous avez créée et pour vous assurer que vous avez défini le paramètre **ncp.dla.generationFilter**, comme cela est décrit dans «Modification du fichier de propriétés DLA pour les entités de périphérie», à la page 121.
5. Exécutez l'adaptateur pour créer le livre de bibliothèque de reconnaissance, comme cela est décrit dans «Création d'un manuel de bibliothèque de reconnaissance pour les données de périphérie de réseau», à la page 122.

Identification des entités de périphérie du réseau

Employez l'utilitaire **itnmTagNetworkEdgeEntities.pl** pour baliser les entités non reconnues, telles les ports et les interfaces, comme étant à la périphérie du réseau. Dans la plupart des cas, vous pouvez exécuter l'utilitaire pour baliser automatiquement les entités considérées comme étant à la périphérie du réseau. Cet utilitaire identifie ensuite les noeuds finaux, tels les hôtes et les serveurs qui fournissent ou utilisent des services.

Avant de commencer

Vérifiez que Network Manager a reconnu votre réseau. Les noeuds finaux doivent être reconnus avant que nous ne puissiez utiliser l'option `-autoEndNodeTags` avec l'utilitaire **itnmTagNetworkEdgeEntities.pl**.

Pourquoi et quand exécuter cette tâche

Pour exécuter l'utilitaire afin de baliser automatiquement les entités considérées comme étant à la périphérie du réseau dans un domaine :

Procédure

1. Accédez au répertoire `NHCOME/precision/scripts/perl/scripts`.
2. Exécutez **`itnmTagNetworkEdgeEntities.pl`** avec l'option de ligne de commande `-autoEndNodeTags` pour le domaine dans lequel les entités doivent être balisées. Inclut automatiquement les noeuds finaux, les routeurs et les commutateurs directement connectés aux noeuds finaux. Par exemple, pour automatiquement baliser les interfaces considérées comme étant à la périphérie du réseau dans le domaine NCOMS, entrez :
   - `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags`
3. Facultatif : Vous pouvez utiliser l'option `-includeNextHop` avec l'option `-autoEndNodeTags` pour accéder à un niveau suivant dans les entités de périphérie. L'utilisation de l'option `-includeNextHop` inclut automatiquement les entités de périphérie incluses lors de l'utilisation exclusive de l'option `-autoEndNodeTags`, plus tout routeur ou commutateur directement connecté aux entités de périphérie. Par exemple, pour automatiquement baliser de telles interfaces, entrez :
   - `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags -includeNextHop`
4. Facultatif : Vous pouvez également déterminer quels périphériques doivent être considérés comme unité de périphérie en fonction du nombre de connexions du périphérique. Utilisez l'option `-autoDegreeTags` pour baliser les périphériques comme étant à la périphérie du réseau s'ils ont plusieurs connexions. Si vous utilisez uniquement l'option `-autoDegreeTags`, tous les périphériques avec une connexion sont considérés par défaut comme étant à la périphérie du réseau.

   Si vous souhaitez spécifier un grand nombre de connexions, utilisez l'option `-autoDegreeTags` avec l'option `-degree` *n* où *n* correspond au nombre maximal de connexions. Par exemple, l'exécution de la commande suivante balise tous les périphériques ayant au maximum deux connexions :
   - `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoDegreeTags -degree 2`

   Remarque : L'option `-autoDegreeTags` ne peut pas être utilisée avec l'option `-autoEndNodeTags`. Le mode d'option `-autoDegreeTags` permet d'inclure des périphériques comme partie de la périphérie du réseau et qui ne sont pas considérés comme des périphériques de noeud final par l'option `-autoEndNodeTags`. Il permet également de filtrer et d'identifier les périphériques qui ont un nombre spécifique maximal de connexions.
5. Facultatif : Vous pouvez ensuite affiner le balisage en définissant un nombre d'options, telles l'exclusion ou l'inclusion de périphériques spécifiques pour le balisage ou l'inclusion de périphériques n'ayant plus d'accès SNMP mais ayant des connexions de couche 2. Pour plus d'informations sur toutes les options disponibles, consultez l'aide sur l'utilitaire en entrant :
   - `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -help`

Résultats

L'utilitaire ajoute un attribut entityDetails-> NetworkEdge=1 dans la base de données ncimCache.entityData.

Que faire ensuite

Vous pouvez maintenant créer une vue réseau filtrée qui affiche uniquement la périphérie de votre réseau.

Création d'une vue de réseau filtrée pour la périphérie du réseau

Créez une vue réseau filtrée qui affiche uniquement la périphérie du réseau dans le domaine en fonction du balisage effectué par l'utilitaire **itnmTagNetworkEdgeEntities.pl**.

Avant de commencer

Conseil : Vous pouvez également utiliser la vue de réseau filtrée pour visualiser et surveiller la périphérie de votre réseau et pour voir quelles données sont exportées via l'adaptateur DLA.

Pourquoi et quand exécuter cette tâche

Pour créer une vue filtrée de la périphérie de votre réseau, procédez comme suit :

Procédure

1. Cliquez sur l'icône **Incident** et sélectionnez **Disponibilité du réseau** > **Vues de réseau** > **Bibliothèques**.
2. Cliquez sur **Nouvelle vue**  .
3. Renseignez l'onglet **Général**, comme suit :

   Nom
   Entrez le nom de la vue de réseau, vue dynamique ou du conteneur de la vue de réseau.

   Important : Il est recommandé d'utiliser des noms de vue de réseau contenant uniquement des caractères latins. Les noms de vues de réseau contenant des caractères non latins (par exemple, des caractères cyrilliques) ne sont pas pris en charge, car ils ne peuvent pas être importés et exportés lors de la migration vers une nouvelle version de Network Manager.

   Parent
   Sélectionnez le noeud dans lequel la vue apparaît dans la hiérarchie de l'**arborescence de navigation**. Pour afficher la vue sur le niveau supérieur, sélectionnez AUCUN.

   Type
   Sélectionnez `Filtrée`.

   Présentation
   Sélectionnez une présentation `Orthogonale`, `Circulaire`, `Symétrique`, `Hiérarchique` ou `Tabulaire`.

   Icône de mappe
   Si vous souhaitez représenter la vue par une icône différente de l'icône par défaut, cliquez sur **Parcourir**  pour rechercher une icône.

   Icône d'arbre
   Si vous souhaitez représenter la vue par une icône différente de l'icône par défaut, cliquez sur **Parcourir**  pour rechercher une icône.

   Image d'arrière-plan
   Cliquez sur **Parcourir**  pour rechercher une image à utiliser en arrière-plan dans la vue.

   Style d'arrière-plan
   Indiquez si l'image en arrière-plan doit être centrée ou en mosaïque.

   Statut de la ligne
   Spécifiez comment les lignes qui représentent les liens entre les unités doivent être rendues.

   Vous pouvez sélectionner de ne pas afficher de statut ou d'afficher le statut par défaut du système. Les lignes peuvent également être colorées en fonction de l'événement **Afficheur d'événements** avec la gravité la plus élevée, et peuvent apparaître avec une icône de gravité supplémentaire.

4. Configurez le filtre de la manière suivante :
   a) Cliquez sur l'onglet **Filtre**.
   b) Dans la liste **Domaine**, sélectionnez le domaine dans lequel vous avez exécuté l'utilitaire de balisage.
   c) Dans la colonne **Table**, sélectionnez l'attribut entityDetails
   d) Dans la colonne **Filtre**, entrez `keyName = 'NetworkEdge' and keyValue = '1'`.
5. Attribuez à l'option **Noeud finaux** la valeur `Inclusion`
6. Attribuez à l'option **Connectivité** la valeur `Couche 2`.
7. Cliquez sur **OK** puis sur **Sauvegarder**.

Que faire ensuite

Vous devez maintenant inclure le nom de cette vue réseau dans le fichier de propriétés DLA pour le domaine.

Modification du fichier de propriétés DLA pour les entités de périphérie

Modifiez le fichier `ncp_dla.properties` pour le domaine afin d'inclure le nom de la vue réseau filtrée créée et pour vous assurer que vous avez configuré les paramètres de génération de données appropriés.

Pourquoi et quand exécuter cette tâche

Pour modifier le fichier, procédez comme suit :

Procédure

1. Accédez au fichier de configuration `ncp_dla.properties` par défaut dans le répertoire d'installation DLA `$NCHOME/precision/adapters/ncp_dla`, ou à l'emplacement où se trouve votre fichier de propriétés DLA pour le domaine.
2. Ouvre le fichier `ncp_dla.properties.`*`nom_domaine`*.
3. Recherchez le paramètre **`ncp.dla.network.view`** et ajoutez le nom de la vue réseau filtrée créée. Par exemple, la vue filtrée appelée “Edge” doit être ajoutée à cette propriété, de la manière suivante : `ncp.dla.network.view=='Edge'`

   Remarque : L'utilisation du signe de double égalité (==) en tant qu'opérateur relationnel est intentionnelle.
4. Attribuez au paramètre **`ncp.dla.generationFilter`** la valeur `ComputerSystem` et `Networking`. Spécifiez les valeurs dans une liste dont chaque élément est séparé par une virgule, de la manière suivante :

   ```
   ncp_dla.generationFilter=ComputerSystem,Networking
   ```
5. Sauvegardez et fermez le fichier.

Que faire ensuite

Vous pouvez maintenant exécuter l'adaptateur DLA avec le fichier de propriétés DLA mis à jour pour exporter un sous-ensemble des données réseau Network Manager.

Tâches associées

Configuration de l'adaptateur de bibliothèque de reconnaissance

L'adaptateur de bibliothèque de reconnaissance (DLA) requiert un fichier de propriétés de configuration pour déterminer la source de données à laquelle se connecter, le domaine à analyser, le répertoire cible pour les livres de bibliothèque de reconnaissance et les paramètres de connexion.

Création d'un manuel de bibliothèque de reconnaissance pour les données de périphérie de réseau

Vous pouvez utiliser l'adaptateur de bibliothèque de reconnaissance (DLA) pour créer le manuel de bibliothèque de reconnaissance contenant uniquement les données pour vos entités réseau.

Avant de commencer

Assurez-vous d'avoir modifié le fichier `ncp_dla.properties` pour le domaine afin d'inclure le nom de la vue réseau filtrée contenant les entités réseau.

Pourquoi et quand exécuter cette tâche

Pour créer un manuel DLA contenant des données réseau, procédez comme suit :

Procédure

1. Accédez au répertoire d'installation DLA sur le serveur des composants de l'interface graphique de Network Manager ; le répertoire par défaut est `$NCHOME/precision/adapters/ncp_dla`.
2. Exécutez l'adaptateur DLA pour générer le fichier XML de manuel avec les données sur les entités réseau balisées :

   ```
   ./ncp_dla.sh ncp_dla.properties.domain_name [ -getmore ]
   ```

   Remarque : Le drapeau `-getmore` est optionnel. Il génère toutes les entités incluant les commutateurs empilés pour les filtres ComputerSystem CDM.

   Par exemple, pour exécuter l'adaptateur pour le domaine appelé NCOMS, entrez la commande suivante : `./ncp_dla.sh ncp_dla.properties.NCOMS`

Exemple

L'exemple suivant présente la réponse système pour l'exécution de l'adaptateur pour le domaine NCOMS :

```
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2011 By IBM Corporation.  All Rights Reserved.  See product
license for details.

[IDML Generation Mode]
Initializing...
Will use the following Network View(s) filter : ='FILTER'
Working on ITNM domain 'NCOMS'...
Processing 1148 IP Network(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Processing 772 ComputerSystem(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Processing 1 Topology(s)...
Processing 2535 Connection(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Writing IDML Book to '/opt/netcool/itnm39017/netcool/var/precision/ccmdb
/ITNMIP39.9.180.209.195.2010-10-05T13.33.37.314Z.refresh.xml'...
Shutting down...
Finished.
```

Le résultat est un fichier XML qui contient les périphériques inclus dans la vue réseau filtrée précédemment créée et spécifiée dans le fichier `ncp_dla.properties` pour le domaine. Le contenu du fichier XML dépend de la configuration du fichier de propriétés DLA.

Le fichier XML contient des segments CDM (Common Data Model) qui décrivent comment les périphériques sont connectés du point de vue d'une interface ou d'un port Network Manager spécifique. Le processus supprime les éléments en double et normalise les détails de connexion. Pour plus

d'informations sur les segments, consultez la documentation Tivoli Common Data Model (CDM) disponible à l'adressehttp://www.redbooks.ibm.com/abstracts/redp4389.html.

Les exemples suivants présentent des parties de la sortie de fichier XML. L'interface choisie pour être l'identité de segment est mise en évidence en gras, notamment chaque instance dans laquelle elle est référencée.

- Exemple d'une connexion point-to-multipoint depuis la perspective de l'interface choisie pour être le point de démarrage pour un segment :

```
<cdm:net.Segment id="SegmentVia_359525_L2Interface" >
                <cdm:Name>Layer 2 Segment via 359525_L2Interface</cdm:Name>
                <cdm:ManagedSystemName>itnmSgmnt:359525_L2Interface
</cdm:ManagedSystemName>
 </cdm:net.Segment>
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="359525_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358156_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404607_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358221_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358185_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404595_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358107_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="357775_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358232_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404589_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358300_L2Interface" />
```

- Exemple de connexion simple point-to-point :

```
<cdm:net.Segment id="SegmentVia_355664_L2Interface" >
                <cdm:Name>Layer 2 Segment via 355664_L2Interface</cdm:Name>
                <cdm:ManagedSystemName>itnmSgmnt:355664_L2Interface
</cdm:ManagedSystemName>
</cdm:net.Segment>
            <cdm:networks source="SegmentVia_355664_L2Interface"
target="355664_L2Interface" />
            <cdm:networks source="SegmentVia_355664_L2Interface"
target="357336_L2Interface" />
```

Chargement des manuels de bibliothèque de reconnaissance et activation du lancement bidirectionnel

Vous devez charger le manuel de bibliothèque de reconnaissance (IdML) dans TADDM pour rendre les informations du manuel disponibles pour TADDM. L'importation du manuel active également le lancement contextuel bidirectionnel.

Pourquoi et quand exécuter cette tâche

En plus de pouvoir lancer l'interface graphique d'IBM Tivoli Application Dependency Discovery Manager depuis Network Manager, vous pouvez également configurer TADDM pour lancer l'interface graphique de Network Manager.

Pour charger les manuels de bibliothèque de reconnaissance dans TADDM et configurer le lancement contextuel bidirectionnel, procédez comme suit :

Procédure

1. Créez un livre de bibliothèque de reconnaissance.

2. Si nécessaire, transférez le fichier de livre de bibliothèque de reconnaissance sur votre serveur TADDM.
3. En tant qu'utilisateur TADDM, exécutez le processus de chargement en bloc pour importer le livre de bibliothèque de reconnaissance.
   Par exemple :

```
user@host% cd $COLLATION_HOME/bin
user@host% ./loadidml.sh -x -f full path to and full name of discovery library
book file
```

   

   Avertissement : Vous devez entrer le chemin complet vers le fichier des livres de la bibliothèque de reconnaissance, ainsi que son nom de fichier complet seulement si le livre se trouve dans un autre répertoire.
4. Importez les identificateur globaux uniques (GUID) d'TADDM dans la base de données NCIM (voir les tâches connexes plus loin dans cette section).

Tâches associées

Création d'un manuel de la bibliothèque de reconnaissance
Pour créer un manuel de la bibliothèque de reconnaissance, exécutez l'adaptateur DLA avec le fichier de propriétés DLA approprié.

Importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM
Facultatif: Pour permettre aux utilisateurs d'ouvrir IBM Tivoli Application Dependency Discovery Manager l'UI depuis Network Manager, importez les GUID TADDM dans la table entityGUIDCache des bases de données Network Connectivity et Inventory Model (NCIM).

Configuration de IBM Tivoli Application Dependency Discovery Manager pour démarrer Network Manager

Facultatif: Pour voir un récapitulatif des ressources que Network Manager exporte vers et depuis IBM Tivoli Application Dependency Discovery Manager, ouvrez Network Manager, vous devez ajouter un rapport JSP.

Pourquoi et quand exécuter cette tâche

Important : Si vous utilisez une version antérieure d'TADDM que la version 7.2.1 Fix Pack 1, suivez ces instructions pour installer et configurer le rapport JSP. Par contre, si vous utilisez la version 7.2.1 Fix Pack 1 ou une version ultérieure, ignorez ces étapes. Dans la version 7.2.1 de Fix Pack 1 et ultérieure, le rapport pour montrer l'inventaire Network Manager et lancement contextuel est installé (ou mis à jour s'il existait déjà) par l'installation TADDM. Pour plus d'informations, voir la documentation de à l'adresse http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome.

Pour utiliser le rapport JSP fourni, les fichiers doivent être copiés à l'emplacement correct sur votre serveur TADDM.

Procédure

1. Connectez-vous au serveur TADDM.
2. Vérifiez que la variable d'environnement $COLLATION_HOME est définie correctement.
3. Copiez le fichier *répertoire_install_dla*`/integration/itnm_inventory.jsp` du serveur des composants de l'interface graphique Network Manager dans le répertoire `$COLLATION_HOME/deploy-tomcat/reports/WEB-INF/view` sur le serveur TADDM.
4. Copiez les deux fichiers GIF (`tivoli.gif` et `ibm_logo.gif`) dans le répertoire *répertoire_install_dla*`/integration/itnm_images` à partir du serveur des composants de l'interface graphique Network Manager vers le répertoire `$COLLATION_HOME/deploy-tomcat/images` sur le serveur TADDM.
5. Arrêtez votre serveur TADDM.

6. Modifiez le fichier $COLLATION_HOME/etc/cdm/xml/reports.xml en ajoutant la section suivante avant la balise de fermeture </beans> :

```
<bean class="com.collation.cdm.reports.viewer.JspReportViewer"
id="ITNMInventoryReport">

<property name="reportGroup">
        <value>Inventory Reports
</value>
    </property>

<property name="reportName">
        <value>ITNM IP Inventory Report
</value>
    </property>
    <!-- START NON-TRANSLATABLE -->
    <property name="jsp">
        <value>/WEB-INF/view/itnm_inventory.jsp</value>

    </property>
    <!-- END NON-TRANSLATABLE -->
</bean>
```

7. Redémarrez votre serveur TADDM.

Résultats

Le Network Manager**rapport d'inventaire** s'affiche dans la console **TADDM Domain Manager**. Il est constitué des sections suivantes :

- Server Summary : Apporte des informations sur les instances installées du produit Network Manager, incluant les versions installées de Network Manager, les adresses d'hôte des serveurs sur lesquels Network Manager est installé, et les URL pour accéder au GUI Network Manager.
- Resource Summary: Liste toutes les ressources Network Manager qui ont une relation avec ComputerSystem, incluant des informations sur leurs adresses IP, fabricant, type de resources (par exemple, routeur), et l'identifiant unique identifier dans la base de données Network Manager.

Configuration de Network Manager pour démarrer IBM Tivoli Application Dependency Discovery Manager

Facultatif: Pour activer Network Operators pour lancer le IBM Tivoli Application Dependency Discovery Manager GUI depuis Network Manager, vous devez configurer les TADDM options de menu sur Network Manager.

Avant de commencer

Les étapes suivantes supposent que l'adaptateur de bibliothèque de reconnaissance (DLA) est installé sur le même serveur que Dashboard Application Services Hub et les composants de l'interface graphique de Network Manager. Si le DLA est installé ailleurs, vous devez copier le répertoire d'installation du DLA et son contenu sur le serveur où Dashboard Application Services Hub et les composants de l'interface graphique Network Manager sont installés.

Pour plus d'informations à propos de IBM Tivoli Application Dependency Discovery Manager, voir : http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome

Procédure

1. Configurez les points d'origine à partir du menu lors de l'installation TADDM :
   a) Modifiez le fichier suivant : $NMGUI_HOME/profile/etc/tnm/tnm.properties
      i) Mettez à jour la propriété tnm.taddm.serverName avec l'adresse IP ou le nom d'hôte de votre serveur TADDM.
      ii) Mettez à jour la propriété tnm.taddm.serverPort avec le port TCP sur lequel votre serveur TADDM écoute.

iii) Mettez à jour les propriétés `tnm.taddm.username` et `tnm.taddm.password` avec le nom d'utilisateur et le mot de passe (non-chiffré) à utiliser pour accéder à votre serveur TADDM.

b) Facultatif : Pour configurer le démarrage d'TADDM dans la même fenêtre que Network Manager, modifiez la zone `target` de la propriété `url` dans chaque fichier de définition d'outil.

Par défaut, TADDM démarre dans une nouvelle fenêtre.

Par exemple, pour afficher les détails CCMDB dans la même fenêtre, modifiez la propriété dans le fichier `ncp_wt_ccmdb_details.xml` comme suit :

```
target="ccmdbDetails'"
```

2. Vérifiez que le sous-menu TADDM a été ajouté dans Network Manager :
   a) Connectez-vous à Network Manager.
   b) Sélectionnez **Disponibilité du réseau** > **Vues de réseau**
   c) Sélectionnez une vue de réseau, puis cliquez avec le bouton droit de la souris sur un périphérique.

   Dans le menu contextuel, les éléments de menu suivant TADDM doivent être affichés sous **Launch To...** > **TADDM/CCDMB**:

   Détails d'affichage
   View History (Historique des vues)

   Remarque : L'application des modifications peut prendre plusieurs minutes. Si cela prend plus de 5 minutes, déconnectez-vous, relancez votre navigateur et reconnectez-vous.

Que faire ensuite

Vous devez maintenant importer les GUID TADDM dans la base de données NCIM.

Tâches associées

Importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM

Facultatif: Pour permettre aux utilisateurs d'ouvrir IBM Tivoli Application Dependency Discovery Manager l'UI depuis Network Manager, importez les GUID TADDM dans la table entityGUIDCache des bases de données Network Connectivity et Inventory Model (NCIM).

Importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM

Facultatif: Pour permettre aux utilisateurs d'ouvrir IBM Tivoli Application Dependency Discovery Manager l'UI depuis Network Manager, importez les GUID TADDM dans la table entityGUIDCache des bases de données Network Connectivity et Inventory Model (NCIM).

Procédure

1. Exécutez l'adaptateur de bibliothèque de reconnaissance de sorte que les ressources et relations de Network Manager soient importées dans TADDM.
2. Connectez-vous au serveur où vos composants de l'interface graphique de Network Manager sont installés, et copiez le répertoire d'intégration DLA et son contenu de `ITNMHOME/adapters/ncp_dla/integration` vers votre serveur TADDM (par exemple `$COLLATION_HOME/sdk/dla/integration`). Assurez-vous que les autorisations sont définies de façon telle que l'utilisateur TADDM puisse accéder aux fichiers.
3. Sur le serveur TADDM, accédez au répertoire où vous avez copié les fichiers.
4. En tant qu'utilisateur TADDM, utilisez l'interface de programme d'application d'TADDM pour demander au CCMDB des données de système informatique et transmettre les résultats à un fichier XML appelé `itnm_guids.xml`.
   Par exemple :

```
user@host% $COLLATION_HOME/sdk/bin/api.sh -u user_name -p password find
ComputerSystem > itnm_guids.xml
```

5. Vérifiez que les fichiers `itnm_guids.xsl` et `itnm_guids.xml` existent dans le répertoire actuel.
6. En tant qu'utilisateur TADDM, utilisez le processeur XLST pour extraire les ID et les identificateurs uniques globaux des entités et les transmettre à un fichier CSV appelé `itnm_guids.csv`.
   Par exemple :

   ```
   user@host% $COLLATION_HOME/sdk/bin/xslt.sh -XSL ./itnm_guids.xsl >
   itnm_guids.csv
   ```

7. Recopiez le fichier `itnm_guids.csv` vers le serveur d'interface graphique Network Manager dans le répertoire de base ou dans le répertoire `ITNMHOME/adapters/ncp_dla`.
8. Exécutez l'adaptateur de bibliothèque de reconnaissance en mode d'importation pour importer les fichiers CSV dans la base de données NCIM de Network Manager.

   Voir «Exemple», à la page 127 pour un exemple présentant comment passer en mode d'importation et les réponses du système.

Exemple

L'exemple suivant présente comment exécuter l'adaptateur de bibliothèque de reconnaissance en mode d'importation et comment le système répond.

```
user@host% cd /opt/IBM/DiscoveryLibrary/ITNM
user@host% [./ncp_dla.sh | ncp_dla.bat ] -import
-file integration/itnm_guids.csv ncp_dla.properties.Db2
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2007 By IBM Corporation.  All Rights Reserved.
See product license for details.

[GUID Import Mode]
Initializing...
Importing GUIDs from 'integration/itnm_guids.csv'
Imported 15 GUID(s) into NCIM.
Shutting down...
Finished.
user@host%
```

Tâches associées

Chargement des manuels de bibliothèque de reconnaissance et activation du lancement bidirectionnel
Vous devez charger le manuel de bibliothèque de reconnaissance (IdML) dans TADDM pour rendre les informations du manuel disponibles pour TADDM. L'importation du manuel active également le lancement contextuel bidirectionnel.

Intégration à TBSM

Network Manager est par défaut intégré à IBM Tivoli Business Service Manager utilisant la Sonde pour Tivoli Netcool/OMNIbus (nco_p_ncpmonitor).

Avant de commencer

IBM Tivoli Network Manager IP Edition Et IBM Tivoli Business Service Manager doivent être installés et configurés.

Résultats

Cette sonde fournit à IBM Tivoli Business Service Manager des jetons BSM_Identity pour Network Manager.

Le jeton BSM_Identity est utilisé par défaut par TBSM pour associer les événements aux ressources. En utilisant l'adaptateur de bibliothèque de reconnaissance (DLA) deNetwork Manager, TBSM détecte les ressources de Network Manager.

La zone BSM_Identity est ajoutée à Network Manager en fonction du paramètre suivant dans le fichier `$NCHOME/probes/`*`arch`*`/nco_p_ncpmonitor.rules` :

```
@BSM_Identity = "ITNMIP:" + $ExtraInfo_MONITOREDENTITYID + "&domain=" + $Domain
```

Référence associée

Prérequis pour l'utilisation du DLA
Avant de configurer et utiliser l'adaptateur de bibliothèque de reconnaissance (DLA), vérifiez que les pré-requis sont respectés.

Configuration de Dashboard Application Services Hub

Une fois l'installation terminée, il se peut que vous deviez configurer la connexion unique ou la sécurité Dashboard Application Services Hub. Vous trouverez des informations sur la configuration de Dashboard Application Services Hub dans le Jazz for Service Management Knowledge Center.

Pourquoi et quand exécuter cette tâche

Le Jazz for Service Management Knowledge Center se trouve à l'adresse https://www.ibm.com/support/knowledgecenter/SSEKCU

Intégration à IBM Tivoli Monitoring

Vous pouvez installer IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition pour contrôler l'état de santé de votre installation Network Manager.

Avant de commencer

Vous devez avoir installé Network Manager avant d'installer IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur l'installation et la configuration d'IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, voir le manuel *IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition User's Guide*.

IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition

IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition est un agent qui s'exécute sur le serveur sur lequel est installé Network Manager.

L'agent fonctionne avec IBM Tivoli Monitoring et vous permet d'effectuer les tâches suivantes :

- Surveiller IBM Tivoli Network Manager IP Edition (Network Manager) afin de détecter les alertes sur les systèmes que vous gérez à l'aide de situations prédéfinies ou personnalisées,
- Etablir vos propres seuils de performance.
- Tracer les causes conduisant à une alerte.
- Recueillir des données exhaustives sur les conditions du système.
- utiliser des règles pour exécuter des actions, planifier le travail et automatiser des tâches manuelles.

L'agent est géré de la même manière que les autres agents IBM Tivoli Monitoring, à l'aide des mêmes interfaces graphiques.

Tivoli Enterprise Portal Est l'interface des produits IBM Tivoli Monitoring. Vous pouvez utiliser la vue consolidée de votre environnement fournie par Tivoli Enterprise Portal pour surveiller et résoudre les problèmes de performance.

Installation et configuration

Installez IBM Tivoli Monitoring, appliquez le support d'application aux composants d'IBM Tivoli Monitoring puis installez et configurez IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, procédez comme suit en respectant l'ordre indiqué :

Procédure

1. Installez et configurez une version compatible d'IBM Tivoli Monitoring. Procédez comme indiqué dans le manuel *IBM Tivoli Monitoring - Guide d'installation et de configuration*.
2. Vérifiez les conditions requis pour l'agent IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. Utilisez les informations de la rubrique «Exigences d'installation de l'agent de surveillance», à la page 133.
3. Appliquez le support d'application sur tous les serveurs sur lesquels les composants IBM Tivoli Monitoring sont installés. Utilisez les procédures décrites dans la section «Installation du support d'application », à la page 129.
4. Installez l'agent IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.Utilisez les procédures décrites dans «Installation de l'agent de surveillance », à la page 132.

Que faire ensuite

Configurez l'agent IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. Utilisez les procédures décrites dans «Configuration de l'agent de surveillance », à la page 135.

Installation du support d'application

Le support d'application garantit une communication correcte entre les composants IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition et IBM Tivoli Monitoring.

Avant de commencer

L'utilisation du support d'application implique d'arrêter et de redémarrer les composants d'IBM Tivoli Monitoring. Consultez votre administrateur d'IBM Tivoli Monitoring pour déterminer le moment opportun de cette opération.

Pourquoi et quand exécuter cette tâche

Vous installez le support d'application sur les composants IBM Tivoli Monitoring suivants qui stockent et analysent les données reçues de l'agent.

- serveur Tivoli Enterprise Monitoring
- serveur Tivoli Enterprise Portal
- Tivoli Enterprise Portal Desktop Client
- Navigateur de Tivoli Enterprise Portal (s'applique à la version UNIX du navigateur)

Cette tâche décrit l'installation de support d'application sur un serveur local. Pour plus d'informations sur la configuration du support d'application sur des serveurs distants, voir le manuel *IBM Tivoli Monitoring - Guide d'installation et de configuration*.

Installation du support d'application sur Linux et AIX

La procédure d'installation du support d'application sur Linux et AIX est différente par rapport aux autres plateformes.

Pourquoi et quand exécuter cette tâche

Le support d'application est pris en charge sur les versions de Linux et d'AIX prises en charge par Network Manager.

AIX Sur les systèmes IBM PowerPC, les versions suivantes sont prises en charge :

- AIX 6.1 iSeries et pSeries
- AIX 7.1 iSeries et pSeries
- AIX 7.2 iSeries et pSeries

Linux Sur les processeurs Intel et Advanced Micro Devices (AMD) x86, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 6 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- Fix Pack 11 Red Hat Enterprise Linux Server 8 (x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 et SP3
- Fix Pack 3 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)
- Fix Pack 10 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP4
- Fix Pack 11 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP5

Fix Pack 6 Depuis Fix Pack 6 et au-delà, sur Linux on IBM z Systems, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP2 et SP3 on IBM z Systems (s390x, 64 bit)

Pour appliquer le support d'application aux composants IBM Tivoli Monitoring sur des systèmes Linux et AIX, procédez comme suit.

Procédure

1. Sur le serveur sur lequel IBM Tivoli Monitoring est installé, téléchargez le module d'installation d'IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
2. Décompressez le package d'installation.
3. Démarrez l'assistant d'installation via le script `install.sh` dans le répertoire `ITMAgent`.
4. Acceptez le répertoire d'installation suggéré.

   L'installation recherche le répertoire d'installation d'IBM Tivoli Monitoring et l'affiche. Par défaut, son emplacement est `/opt/IBM/ITM`, mais il peut être différent si IBM Tivoli Monitoring a été installé à un autre emplacement.
5. Confirmez que vous pouvez redémarrer les processus existants.
6. Sélectionnez **Installer les produits sur le système hôte local**.
7. Acceptez la clé par défaut `IBMTivoliMonitoringEncryptionKey`, à moins d'utiliser une clé différente pour chaque produit.
8. Acceptez l'accord de licence.
9. Spécifiez un module de support d'application à installer. La liste des modules de support varie selon le système d'exploitation et les composants IBM Tivoli Monitoring installés. Installez tous les modules de support affichés.

10. Si le serveur Tivoli Enterprise Portal, serveur Tivoli Enterprise Monitoring, le bureau Tivoli Enterprise Portal et le navigateur Tivoli Enterprise Portal sont tous installés sur le même machine, configurez le support d'agent pour toutes ces applications à l'aide d'un script.

    Restriction : Utilisez cette option uniquement si tous les composants sont installés sur le même serveur.

    a) Accédez au répertoire IBM Tivoli Monitoring.

    b) Si vous n'utilisez pas l'emplacement par défaut `/opt/IBM/ITM`, définissez CANDLE_HOME comme répertoire d'installation d'IBM Tivoli Monitoring.

    c) Exécutez le script `setupITNMAgentSupport.sh`.
11. Si certains composants d'IBM Tivoli Monitoring sont installés sur d'autres serveurs, effectuez les étapes suivantes sur les serveurs appropriés :
12. Si le serveur Tivoli Enterprise Monitoring est installé sur un serveur différent, exécutez les commandes suivantes sur ce serveur à partir du répertoire `$ITMHOME/bin`, où `ITMHOME` correspond au répertoire d'installation d'IBM Tivoli Monitoring :

    a) S'il n'est pas déjà démarré, démarrez le serveur de surveillance à l'aide de la commande suivante, où *nom_tems* correspond au nom du serveur de surveillance. Vous pouvez trouver le nom du serveur de surveillance en recherchant la valeur `Nom TEMS` dans l'écran de configuration du serveur de surveillance.

    ```
    ./itmcmd server start nom_tems
    ```

    b) Activez le support d'application sur le serveur de surveillance à l'aide de la commande suivante.

    ```
    ./itmcmd support -f install -t tems_name np
    ```

    c) Arrêtez le serveur de surveillance à l'aide de la commande suivante :

    ```
    ./itmcmd server stop tems_name
    ```

    d) Redémarrez le serveur de surveillance à l'aide de la commande suivante :

    ```
    ./itmcmd server start nom_tems
    ```
13. Si le serveur Tivoli Enterprise Portal est installé sur un serveur différent, exécutez les commandes suivantes sur ce serveur à partir du répertoire `$ITMHOME/bin`, où `ITMHOME` correspond au répertoire d'installation d'IBM Tivoli Monitoring.

    a) Arrêtez le serveur de portail à l'aide de la commande suivante :

    ```
    ./itmcmd agent stop cq
    ```

    b) Configurez le serveur de portail avec les nouvelles informations d'agent à l'aide de la commande suivante :

    ```
    ./itmcmd config -A cq
    ```

    c) Redémarrez le serveur de portail à l'aide de la commande suivante :

    ```
    ./itmcmd agent start cq
    ```
14. Si le bureau Tivoli Enterprise Portal est installé sur un serveur différent, exécutez les commandes suivantes sur ce serveur à partir du répertoire `$ITMHOME/bin`, où `ITMHOME` correspond au répertoire dans lequel est installé le client bureautique.

    a) Arrêtez le client bureautique à l'aide de la commande suivante :

    ```
    ./itmcmd agent stop cj
    ```

    b) Configurez le client bureautique avec les nouvelles informations d'agent à l'aide de la commande suivante :

```
./itmcmd config -A cj
```

c) Redémarrez le client bureautique à l'aide de la commande suivante :

```
 ./itmcmd agent start cj
```

d) Redémarrez les clients Web Start Tivoli Enterprise Portal pour afficher les nouveaux espaces de travail d'agent.

Installation du support d'application sur Windows

La procédure d'installation du support d'application sur Windows est différente par rapport aux autres systèmes d'exploitation.

Pourquoi et quand exécuter cette tâche

Le support d'application est pris en charge sur les versions de Windows prises en charge par IBM Tivoli Monitoring. Reportez-vous à la documentation de votre version d'IBM Tivoli Monitoring pour obtenir des informations sur les versions de Windows prises en charge.

Pour appliquer le support d'application aux composants IBM Tivoli Monitoring sur des systèmes Windows, procédez comme suit.

Procédure

1. Sur le serveur sur lequel IBM Tivoli Monitoring est installé, téléchargez le module d'installation d'IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
2. Décompressez le package d'installation.
3. Accédez au répertoire `ITMagent/windows/` et exécutez le fichier `setup.exe` pour démarrer le programme d'installation de l'agent.
4. Acceptez la recommandation pour la version JRE.
5. Acceptez le répertoire d'installation suggéré. Par défaut, son emplacement est `/opt/IBM/ITM`, mais il peut être différent si IBM Tivoli Monitoring a été installé à un autre emplacement.
6. Si vous ne disposez pas d'une clé personnalisée pour le produit, acceptez la clé par défaut `IBMTivoliMonitoringEncryptionKey`.
7. Sélectionnez un plusieurs composants suivants auxquels appliquer le support d'application. Les composants s'affichent uniquement s'ils sont installés sur le serveur en cours.
   - Serveur Tivoli Enterprise Monitoring
   - serveur Tivoli Enterprise Portal
   - Tivoli Enterprise Portal Desktop Client

   Sélectionnez **IBM Tivoli Network Manager** pour chaque option que vous avez sélectionnée. Si l'infrastructure n'est pas installée sur votre système, sélectionnez aussi **Infrastructure d'agent TEMA** pour chaque option choisie.

Installation de l'agent de surveillance

Installez l'agent de surveillance sur le serveur où les composants principaux de Network Manager sont installés.

Pourquoi et quand exécuter cette tâche

Installez l'agent une seule fois. Configurez une instance de l'agent pour chaque domaine Network Manager.

Exigences d'installation de l'agent de surveillance

En plus des exigences décrites dans la documentation d'installation d'IBM Tivoli Monitoring, IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition est soumis aux exigences suivantes.

Logiciels prérequis

Installez les logiciels prérequis suivants avant d'installer l'agent de surveillance :

- IBM Tivoli Monitoring V6.3 Fix Pack 1 ou version ultérieure
- Tivoli Enterprise Portal V6.3 Fix Pack 1 ou version ultérieure

Exigences de dimensionnement

Un seul serveur hébergeant le serveur de surveillance du concentrateur, le serveur de portail et un agent de surveillance nécessite environ 300 Mo d'espace.

Un serveur hébergeant uniquement l'agent de surveillance nécessite environ 30 Mo d'espace, y compris le code d'activation spécifique à l'agent de surveillance. Davantage d'espace disque est requis pour chaque agent de surveillance supplémentaire déployé sur l'ordinateur de surveillance.

Systèmes d'exploitation pris en charge

L'agent de surveillance peut être installé sur n'importe lequel des systèmes d'exploitation pris en charge pour Network Manager 4.2.

AIX Sur les systèmes IBM PowerPC, les versions suivantes sont prises en charge :

- AIX 6.1 iSeries et pSeries
- AIX 7.1 iSeries et pSeries
- AIX 7.2 iSeries et pSeries

Linux Sur les processeurs Intel et Advanced Micro Devices (AMD) x86, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 6 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- Fix Pack 11 Red Hat Enterprise Linux Server 8 (x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 et SP3
- Fix Pack 3 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)
- Fix Pack 10 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP4
- Fix Pack 11 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP5

Fix Pack 3 Depuis Fix Pack 3 jusqu'à Fix Pack 5, sur Linux on IBM z Systems, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP1 sur IBM z Systems (s390x, 64 bits)

Fix Pack 6 Depuis Fix Pack 6 et au-delà, sur Linux on IBM z Systems, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP2 et SP3 on IBM z Systems (s390x, 64 bit)

Fix Pack 10 Depuis Fix Pack 10 et au-delà, sur Linux on IBM z Systems, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)

- SuSE Linux Enterprise Server (SLES) 12.0 SP5 sur IBM z Systems (s390x, 64 bits)

Les combinaisons suivantes de programme Hypervisor et de système d'exploitation sont prises en charge :

- VMware ESX 5.0, 5.5, 6.0 :
  - Red Hat Enterprise Linux Server 7 (x86-64)
  - SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 et SP3
  - Fix Pack 3 SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)

Exigences relatives à la recherche dans l'aide en ligne

Pour utiliser la fonction de recherche de l'aide en ligne de cet agent de surveillance, assurez-vous d'avoir coché la case **IBM Eclipse help server** lors de l'installation de Tivoli Enterprise Portal Server.

La rubrique "Recherche d'aide sur l'agent" de l'aide en ligne de cet agent de surveillance propose un lien vers l'aide Eclipse où la fonction de recherche est activée. Dans la table des matières du panneau de gauche de l'aide, sélectionnez la rubrique de recherche d'aide sur l'agent, afin d'afficher le lien vers l'aide Eclipse dans le panneau de droite.

Installation de l'agent de surveillance sur un serveur local

Procédez comme suit pour installer et configurer l'agent de surveillance sur le serveur Network Manager.

Avant de commencer

Si vous utilisez Red Hat Enterprise Linux 7 ou SuSE Linux Enterprise Server 12, lancez la commande suivante avant d'installer, désinstaller, démarrer ou arrêter l'agent de surveillance :

```
setarch $(uname -m) --uname-2.6
```

Procédure

1. Sur le serveur sur lequel vous souhaitez installer l'agent de surveillance, téléchargez le package d'installation d'IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
2. Décompressez le package d'installation.
3. Démarrez l'assistant d'installation via le script `install.sh` dans le répertoire `ITMAgent`.
4. Acceptez le répertoire d'installation suggéré.

   L'installation recherche le répertoire d'installation d'IBM Tivoli Monitoring et l'affiche. Par défaut, son emplacement est `/opt/IBM/ITM`, mais il peut être différent si IBM Tivoli Monitoring a été installé à un autre emplacement.
5. Sélectionnez **Installer les produits sur le système hôte local**.
6. Acceptez l'accord de licence.
7. Acceptez la clé par défaut `IBMTivoliMonitoringEncryptionKey`, à moins d'utiliser une clé différente pour chaque produit.
8. Si vous exécutez le programme d'installation en tant que non superutilisateur, indiquez le mot de passe root pour que l'agent puisse être redémarré automatiquement.
9. Indiquez un système d'exploitation ou un module de support d'application à installer. La liste varie en fonction de votre système d'exploitation et des composants IBM Tivoli Monitoring qui sont installés. Acceptez la valeur par défaut ou choisissez votre système d'exploitation dans la liste.
10. Sélectionnez **Tout ce qui précède** dans les options répertoriées ci-dessous.
    - IBM Tivoli Network Manager
    - Interface utilisateur Tivoli Enterprise Services
    - Tout ce qui précède

11. Lorsque le système vous demande si vous souhaitez installer des produits supplémentaires, choisissez **Non** pour quitter l'installation.

Que faire ensuite
Configurez une instance de l'agent pour chaque domaine.

Configuration de l'agent de surveillance

Vous n'installez l'agent qu'une seule fois, toutefois vous configurez une instance de l'agent pour chaque domaine Network Manager.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la configuration de l'agent de surveillance à l'aide la commande itmcmd config, de l'interface utilisateur Manage Tivoli Monitoring Services ou de Tivoli Enterprise Portal, voir la documentation IBM Tivoli Monitoring.

Pour configurer l'agent à partir de la ligne de commande, procédez comme suit :

Procédure

1. Exécutez la commande suivante pour instancier une instance de l'agent :

   ```
   $ITMHOME/bin/itmcmd config -A np
   ```

   Où *ITMHOME* correspond au chemin d'installation de l'agent.
2. Choisissez un nom pour chaque agent de surveillance et entrez ce nom dans la zone **Nom d'instance**. Définissez une nouvelle instance d'agent pour chaque domaine Network Manager.

   Le nom d'instance peut être un quelconque nom significatif unique. Par exemple, le nom d'instance de chaque agent peut inclure le nom du programme d'interrogation auquel il est associé.

   Remarque :

   Si vous employez plusieurs agents de surveillance et que vous souhaitez surveiller les interrogateurs individuellement à l'aide de l'espace de travail Disponibilité, vous devez définir un nom unique pour les interrogateurs en éditant le fichier `knp.ref`. Pour savoir comment éditer le fichier `knp.ref` de manière à nommer les interrogateurs, consultez la note technique suivante : http://www-01.ibm.com/support/docview.wss?uid=swg21600387
3. Spécifiez une valeur pour **NCHOME Path**. La valeur par défaut est `/opt/IBM/netcool/core`.
4. Spécifiez un nom de domaine Network Manager. La valeur par défaut est NCOMS.
5. Spécifiez une valeur pour le nom de l'interrogateur Network Manager. Si vous laissez cette zone à blanc, l'agent est mappé sur l'interrogateur par défaut. Si vous disposez de plusieurs interrogateurs, vous devez spécifier une valeur. Cette zone est vide si vous n'utilisez pas l'interrogation répartie.
6. Spécifiez un nom d'utilisateur pour la base de données OQL Network Manager. Par défaut, ce nom d'utilisateur est `admin`.
7. Spécifiez un nom d'utilisateur pour la base de données OQL Network Manager. Ce mot de passe est vide par défaut.
8. Spécifiez un intervalle de régénération en minutes. La valeur par défaut est 10. Ce nombre indique la durée maximale en minutes avant que les données ne soient placées en cache. Si vous indiquez une valeur de zéro, une requête de base de données est effectuée chaque fois que les données sont requises. Sinon, une requête de base de données est effectuée à l'intervalle de temps spécifié. La définition d'un nombre peu élevé peut avoir des effets sur les performances du serveur Network Manager car certaines requêtes nécessitent une période de temps considérable.
9. Sélectionnez **Oui** pour connecter l'agent à serveur Tivoli Enterprise Monitoring.
10. Spécifiez le nom DNS du serveur Tivoli Enterprise Monitoring lorsque vous le système vous invite à indiquer le nom d'hôte du serveur Tivoli Enterprise Monitoring.

Remarque : Ne spécifiez pas le nom du serveur Tivoli Enterprise Monitoring. Indiquez le nom DNS.

11. A moins que votre administrateur IBM Tivoli Monitoring ne vous donne des paramètres différents, acceptez les valeurs par défaut des options suivantes :
    - Protocole de réseau. La valeur par défaut est ip.pipe.
    - Choisissez le protocole suivant parmi les options suivantes :
      - sna
      - ip.spipe
      - 0 (aucun)
      - Protocole réseau 2 (la valeur par défaut est 0)
      - Numéro de port IP.PIPE (la valeur par défaut est 1918)
    - KDC_PARTITION (la valeur par défaut est null.)
    - Configurer la connexion pour un TEMS secondaire ? [1=YES, 2=NO] (La valeur par défaut est 2.)
    - Nom réseau principal facultatif (la valeur par défaut est 0 ou none.)
12. Facultatif : Dans le cas d'une installation non root uniquement, vous devez effectuer les tâches supplémentaires suivantes :
    a) Indiquez le mot de passe root pour mettre à jour les scripts de redémarrage automatique.
    b) En tant que superutilisateur, exécutez `ITMHOME/bin/SetPerm` à partir du répertoire d'installation d'IBM Tivoli Monitoring.
    c) En tant que superutilisateur, exécutez le script `ITMHOME/bin/UpdateAutoRun.sh` à partir du répertoire d'installation d'IBM Tivoli Monitoring.

    Si vous exécutez l'utilitaire SetPerm sous AIX 6.X ou 7.X, vous devez sélectionner les options AIX 5.X.
13. Répétez l'ensemble de la procédure pour configurer une instance de l'agent pour chaque domaine Network Manager. Utilisez des noms d'interrogateur différents pour chaque instance d'agent.

Que faire ensuite

Après avoir configuré IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, vous pouvez activer les vues de santé et le lancement en contexte à partir de Tivoli Enterprise Portal.

Démarrage de l'agent de surveillance

Utilisez une commande pour démarrer l'agent de surveillance.

Avant de commencer

Si vous utilisez Red Hat Enterprise Linux 7 ou SuSE Linux Enterprise Server 12, lancez la commande suivante avant d'installer, désinstaller, démarrer ou arrêter l'agent de surveillance :

```
setarch $(uname -m) --uname-2.6
```

Pourquoi et quand exécuter cette tâche

Lorsque vous installez l'agent de surveillance, les fichiers utilisés pour démarrer l'agent lors du redémarrage du système sont automatiquement configurées. Le fichier utilisé pour redémarrer l'agent est `/etc/init.d/ITMAgents2`. Si vous installez un autre agent, le 2 est incrémenté : par exemple, l'agent suivant installé est `ITMAgents3`.

Exécutez la commande suivante pour démarrer l'agent : `./ITMAgents2`

Accès aux données de reconnaissance à partir de dNCIM

Vous pouvez tirer parti des diffusions dNCIM post-reconnaissance pour extraire des mises à jour et les envoyer à la topologie de réseau après chaque exécution de la reconnaissance. Les processus Network Manager internes lisent ces informations à la fin d'une reconnaissance. Vous pouvez également configurer des systèmes tiers (basés sur Tivoli ou externes) pour qu'ils accèdent à ces données topologiques afin qu'ils disposent des dernières mises à jour de topologie.

Pourquoi et quand exécuter cette tâche

Les exemples de système tiers de ce type que vous pouvez configurer pour lire les données dNCIM sont les suivants :

- TADDM peut utiliser ces données afin d'alimenter sa reconnaissance d'applications. Les données provenant de dNCIM indiquent à TADDM quels hôtes sont présents sur le réseau, ce qui est une première étape vers la reconnaissance des applications sur ces hôtes.
- IBM Director peut utiliser ces données pour prendre en charge la reconnaissance des périphériques de stockage.
- Une base de données d'actifs peut utiliser ces données pour télécharger ses informations d'actif.
- Un système de sécurité peut utiliser ces données pour identifier d'éventuelles intrusions.

L'obtention de données à partir de dNCIM au lieu d'utiliser le DLA varie comme suit.

- Les données sont à un format différent du DLA.
- Les données dNCIM n'ont pas encore été envoyées au gestionnaire de topologie, ncp_model ; elles ne sont donc pas consolidées avec les reconnaissances précédentes :
- Les données sont moins volumineuses que celles qui peuvent être extraites à l'aide du DLA.
- Les diffusions dNCIM ont le même format que les diffusions NCIM transmises par ncp_model et les fichiers cache NCIM.

Pour configurer des systèmes tiers afin qu'ils accèdent aux données de reconnaissance à partir de dNCIM, vous devez écrire un script pour configurer l'API Java ou Perl afin qu'elle écoute les messages comportant l'objet DNCIM2NCIM, sur le bus de messages.

Pour plus d'informations sur le format des diffusions dNCIM, voir *IBM Tivoli Network Manager Reference*.

Chapitre 8. Mise à niveau et migration

La mise à niveau à partir d'une version précédente de Network Manager consiste à installer la nouvelle version puis à migrer vos configurations et vos personnalisations existantes.

A propos de la mise à niveau

Déterminez les options de mise à niveau auxquelles vous avez accès et ce que la mise à niveau implique.

Chemins de mise à niveau et limitations

Vous pouvez effectuer la mise à niveau vers Network Manager V4.2 à partir de certaines versions antérieures, moyennant quelques limitations.

Vous pouvez migrer depuis toutes les versions suivantes vers Network Manager V4.2 :

- V3.9 Fix Pack 3 ou version ultérieure
- V4.1
- Version 4.1.1

Si vous disposez d'une version de Network Manager antérieure à la version V3.9, effectuez d'abord la mise à niveau vers la V3.9 Fixpack 3.

Vous pouvez aussi utiliser la procédure de migration pour copier une installation de la V4.2 vers un autre serveur. La procédure de toutes ces versions est la même.

Remarque :

Si vous avez installé IBM Netcool Operations Insight V1.2 ou V1.3 et effectuez la mise à niveau vers IBM Netcool Operations Insight V1.4, exécutez IBM Installation Manager et désinstallez le composant **Network Management Integration for OMNIbus 8.1** avant d'installer Network Manager V4.2.

Les limitations suivantes s'appliquent à la mise à niveau :

- Vous ne pouvez effectuer la migration que sur un serveur 64 bits.
- La migration depuis des systèmes Windows n'est pas prise en charge.
- Les machines source et cible doivent utiliser le même type de base de données. Les seules exceptions sont les suivantes :
  - Version 3.9 : la migration depuis la source Informix par défaut antérieure vers la base de données DB2 par défaut ou une base de données Oracle dans la version 4.2 sur le système cible est prise en charge.
- Les systèmes source et cible doivent tous deux correspondre à des installations FIPS ou non FIPS. La migration d'une installation FIPS vers une installation non FIPS ou inversement n'est pas prise en charge.

Remarque : Si vous utilisez Network Manager comme partie d'une solution, vous devez aussi contrôler la compatibilité des versions de tous les produits composants dans la documentation de la solution. Par exemple, si vous utilisez Netcool Operations Insight, contrôlez la matrice de version de produit et composant de pour votre version de Netcool Operations Insight à https://www.ibm.com/support/knowledgecenter/en/SSTPTP.

Tâches associées

Désinstallation de Network Manager

Si vous souhaitez supprimer entièrement le produit, ou d'annuler pour revenir à une version précédente, vous devez utiliser IBM Installation Manager. Le fait de désinstaller le produit en supprimant les fichiers et les répertoires provoque des problèmes lors de la réinstallation des composants.

Emplacements par défaut des différentes versions de produit

Les différentes versions de Network Manager et les composants liés utilisent différentes structures de répertoire et ont des fichiers de configuration à différents emplacements.

Si vous recherchez un fichier ou un autre composant système en fonction de leur emplacement sur votre ancien système, utilisez le tableau suivant pour déterminer où trouver l'élément sur Network Manager 4.2. Le tableau suivant présente de manière générale comment l'emplacement par défaut des fichiers de configuration a changé au fil des versions.

Tableau 11. Emplacements par défaut des fichiers de configuration

Elément	Versions 3.9, 4.1 et 4.1.1	Version 4.2
NCHOME	`/opt/IBM/tivoli/netcool`	`/opt/IBM/netcool/core`
ITNMHOME	`/opt/IBM/tivoli/netcool/precision` **Remarque :** Par défaut, PRECISION_HOME est défini au même emplacement que ITNMHOME, mais il est utilisé par d'autres éléments du produit.	`/opt/IBM/netcool/core/precision` **Remarque :** Par défaut, PRECISION_HOME est défini au même emplacement que ITNMHOME, mais il est utilisé par d'autres éléments du produit.
TIPHOME	`/opt/IBM/tivoli/tipv2`	N'est plus applicable. Tivoli Integrated Portala été remplacé par Dashboard Application Services Hub
JazzSM_HOME	Non applicable	Pour plus de détails, voir le Jazz for Service Management Knowledge Center.
Fichiers des propriétés d'interface utilisateur	`ITNMHOME/profiles/TIPProfile/etc/tnm`	`$NMGUI_HOME/profile/etc/tnm/` **Remarque :** `$NMGUI_HOME` est l'emplacement d'installation des composants d'interface graphique Network Manager. Par défaut, il s'agit de `/opt/IBM/netcool/gui/precision_gui`.
Modèles de vue dynamique	`ITNMHOME/profiles/TIPProfile/etc/tnm/dynamictemplates`	`$NMGUI_HOME/profile/etc/tnm/dynamictemplates/`
Cliquez à l'aide du bouton droit sur le menu et sur les fichiers de définition d'outil	`ITNMHOME/profiles/TIPProfile/etc/tnm/menus`	`$NMGUI_HOME/profile/etc/tnm/menus/`
	`ITNMHOME/profiles/TIPProfile/etc/tnm/tools`	`$NMGUI_HOME/profile/etc/tnm/tools/`
Fichiers d'icône d'interface graphique	`ITNMHOME/profiles/TIPProfile/etc/tnm/resource`	`$NMGUI_HOME/profile/etc/tnm/resource/`

Tableau 11. Emplacements par défaut des fichiers de configuration (suite)		
Elément	**Versions 3.9, 4.1 et 4.1.1**	**Version 4.2**
Fichiers de configuration WebTools	`ITNMHOME/profiles/TIPProfile/etc/tnm/tools`	`$NMGUI_HOME/profile/etc/tnm/tools/`

Données faisant l'objet d'une migration

Network Manager migre la plupart des fichiers et met en évidence les fichiers que vous devez migrer manuellement.

Les fichiers qui ont été modifiés peuvent être classifiés de l'une des deux façons suivantes.

Modifications de configuration

Les paramètres standard de configuration des processus, de la reconnaissance et de la surveillance ainsi que les vues de topologie peuvent être migrés comme indiqué dans ce document. La personne effectuant la migration doit être l'administrateur ou avoir des compétences similaires concernant la gestion de Network Manager. Les fichiers de configuration sont entièrement ou partiellement migrés par le processus de migration. Tous les fichiers à migrer manuellement sont mis en évidence.

Modifications de personnalisation

Network Manager propose de nombreuses options de personnalisation qui permettent d'ajouter de nouvelles fonctions ou de l'intégrer à votre environnement. Voici quelques exemples de changements de la configuration :

- Prise en charge de nouveaux périphériques
- Données supplémentaires de périphériques et sources de données propriétaires du client pour la visualisation et la surveillance
- Logique modifiée permettant de créer des connexions dans et entre les périphériques réseau, et collections permettant le regroupement de périphériques.
- Création d'ensembles de vues de réseau à l'aide de l'API de modèle dynamique.
- Enrichissement d'événement via la passerelle d'événement et le fichiers de règles de sonde nco_p_ncpmonitor.
- Outils de mappe topologique activés par clic droit, utilisant les Webtools et d'autres technologies.
- Extension du système Service Affecting Events à d'autres collections.
- Intégrations à d'autres produits, dont LDAP et TADDM.

Toutes les modifications de personnalisation nécessitent un certain niveau de connaissances du flux de données et des API du produit, ainsi que des compétences en programmation. Ces compétences sont aussi indispensables pour réussir la migration de ces personnalisations. Vous devez aussi tenir compte des nouvelles modifications de logique qui peuvent nécessiter des changements du code personnalisé.

Les modifications de personnalisation ne sont pas migrées automatiquement. Le processus de mise à niveau met en évidence les fichiers qui ont été modifiés et doivent être migrés manuellement.

Données ne faisant pas l'objet d'une migration

Les types de donnés suivants ne peuvent pas être migrés :

- Les fichiers cache NCIM ne sont pas migrés entre les différentes versions de Network Manager. Les fichiers cache NCIM sont copiés d'une installation à l'autre uniquement si vous copiez une installation 4.2 existante vers une autre installation 4.2.
- Les fichiers cache de la reconnaissance

- La topologie de réseau n'est pas migrée. Vous devez effectuer une nouvelle reconnaissance de l'installation cible.

Données faisant l'objet d'une migration

Les types de donnés suivants sont migrés.

- Fichiers de configuration.
- Vues de réseau.
- Données de configuration de reconnaissance.
- Domaines multiples. Vos domaines sont recréés automatiquement et les vues de réseau et les règles de surveillance sont importées.
- Mots de passe et noms de communauté SNMP. Les données sont déchiffrées, importées, puis de nouveau chiffrées.
- Règles d'interrogation et définitions d'interrogation.
- Bases d'information de gestion (MIB). Les MIB SNMP ont été transférées depuis le serveur de l'interface graphique vers le serveur des composants dans Network Manager 4.2.
- Collecteurs de reconnaissance nouveaux ou personnalisés

Mise à niveau de Network Manager

Exécutez les tâches de mise à niveau dans l'ordre indiqué.

Pourquoi et quand exécuter cette tâche

Dans ces instructions, le serveur ou l'installation "source" désigne le serveur or installation de Network Manager à partir duquel vous effectuez la mise à niveau. En général, il s'agit d'une version précédente plus ancienne.

Le serveur ou l'installation "cible" désigne le serveur ou l'installation Network Manager vers lequel vous souhaitez effectuer la mise à niveau. En général, il s'agit de la version en cours : 4.2.

Important : Une mise à niveau Fix Pack déploie un nouveau fichier `.war` pour chaque application Web telles que Vues de Réseau, Navigateur de Structure, vues géographiques et ainsi de suite. Tous les fichiers modifiés dans le même répertoire comme le fichier WAR, sont écrasés. Vous devez faire un backup de tous les changements que vous avez faits sur les fichiers dans le répertoire de déploiement du fichier WAR.

Préparation de la mise à niveau

Vous devez préparer les systèmes cible avant de commencer la mise à niveau.

Pourquoi et quand exécuter cette tâche

Pour préparer la mise à niveau, procédez comme suit :

Procédure

1. Installez les composants principaux de Network Manager.
2. Démarrez les composants principaux de Network Manager.

   Ne configurez pas plus avant le domaine principal car cela limiterait la migration de la configuration automatique.
3. Installez les composants de l'interface graphique utilisateur de Network Manager.
4. Assurez-vous que vous pouvez vous connecter à l'interface graphique utilisateur de Network Manager.
5. Recréez tous les utilisateurs de Network Manager à partir de l'installation source sur l'installation cible. Créez les utilisateurs dans le répertoire approprié : LDAP ou ObjectServer. Si des utilisateurs ont

été créés dans Tivoli Integrated Portal, créez-les à nouveau. Network Manager 4.2 n'utilise pas Tivoli Integrated Portal. Notez par écrit les noms d'utilisateur et leurs mots de passe. Vous avez besoin de ces données d'identification lorsque vous migrez des rôles utilisateur.

6. Facultatif : Si vous migrez depuis une installation de Network Manager intégrée à IBM Tivoli Netcool Configuration Manager, exportez vos rapports personnalisés avant la mise à niveau. Si vous n'exportez pas vos rapports personnalisés, ils risquent d'être écrasés pendant la mise à niveau. Consultez les informations sur l'*exportation des rapports personnalisés* pour votre version de Netcool Configuration Manager à l'adresse suivante : http://www.ibm.com/support/knowledgecenter/SS7UH9/welcome.
7. Ne démarrez pas de reconnaissance et ne commencez pas à travailler avec Network Manager. Commencez la mise à niveau.

Mise à jour de la base de données

Vous devez identifier toutes les personnalisations que vous avez apportées à la base de données de la topologie NCIM et mettre à jour la nouvelle base de données avec ces personnalisations.

Avant de commencer

Dans le cadre de l'installation du système cible, vous devez installer la nouvelle base de données et exécuter Network Manager pour créer des scripts de schéma pour configurer les tables et les schémas.

Remarque : Il vous suffit d'exécuter le script `ncp_ncim_diff.pl` s'il existe des modifications personnalisées dans votre base de données source.

Vérifiez que les fichiers `DbLogins.`*`DOMAINE`*`.cfg` de l'installation précédente sont disponibles. Ces fichiers contiennent les informations de connexion à votre base de données NCIM.

Pourquoi et quand exécuter cette tâche

Pour mettre à jour le schéma de la base de données topologiques, procédez comme suit :

Procédure

1. Connectez-vous à votre installation Network Manager source.
2. Accédez au répertoire `$NCHOME/precision/scripts/perl/scripts` et exécutez la commande suivante :

   ```
   ./ncp_ncim_diff.pl -domain DOMAIN -password NCIM_database_password
   ```

   Où *DOMAINE* est obligatoire pour identifier un fichier `DbLogins.`*`DOMAINE`*`.cfg` contenant les options nécessaires pour la connexion à votre base de données NCIM. Cette commande génère des rapports sur tous les domaines et ne doit être exécutée qu'une seule fois.

   Pour plus d'informations sur le script Perl `ncp_ncim_diff.pl`, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

   Ce script identifie les différences entre votre schéma de base de données NCIM et le schéma NCIM par défaut de votre version de Network Manager.
3. Mettez à jour manuellement le schéma de base de données topologiques NCIM avec les personnalisations identifiées par le script.

   Le script peut signaler de nouvelles tables introduites avec un Fix Pack. Ces modifications sont déjà présentes dans le nouveau système et n'ont pas besoin d'être migrées. Soyez prudent lorsque vous appliquez les personnalisations au nouveau schéma NCIM, car les noms de table et les noms de zone peuvent avoir changé entre les versions.

Tâches associées

Installation et configuration d'une base de données topologiques

Votre administrateur de base de données doit installer et configurer une base de données topologiques avant que vous puissiez installer Network Manager.

Migration des composants principaux

Migration des composants principaux par exportation des données depuis le serveur source et importation sur le serveur cible. Démarrez et arrêtez tous les processus, importez les données, définissez plusieurs interrogateurs, définissez la portée de toutes les règles d'interrogation et exécutez les étapes manuelles requises.

Pourquoi et quand exécuter cette tâche

Si les composants principaux et les composants de l'interface graphique se trouvent sur le même serveur, vous devez toujours les faire migrer séparément en suivant la procédure appropriée.

Procédez comme suit pour faire migrer les composants principaux.

Procédure

1. Sur le serveur sur lequel sont installés les composants principaux, exécutez le script suivant :

   ```
   $ITNMHOME/install/scripts/makeExportPackageCore
   ```

   Le script crée un package contenant les scripts que vous utilisez pour exporter les données depuis l'installation source. Le package est appelé `ExportPackageCore.tar`.
2. Copiez le fichier `ExportPackageGUI.tar` dans un emplacement temporaire sur le serveur source où sont installés les composants de l'interface graphique.

   Remarque : L'emplacement ne doit pas se trouver dans le répertoire d'installation `$NCHOME`.
3. Décompactez le fichier `ExportPackageCore.tar`.
4. Dans le répertoire `scripts` qui a été créé en décompactant le fichier, exécutez le script `nmExport`. Fournissez les informations requises et choisissez l'emplacement dans lequel doit être sauvegardé le fichier d'exportation.

   Restriction : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

   Le script crée un fichier `.pkg` contenant les données de configuration de reconnaissance, les vues de réseau, les règles d'interrogation et les définitions, d'autres fichiers de configuration et des fichiers journaux contenant des informations sur la réussite de l'exportation. Si l'exportation échoue, les fichiers journaux sont enregistrés dans le répertoire `/itnmExportLogs/` dans votre répertoire de base.
5. Copiez le fichier `.pkg` qui a été créé sur le serveur cible.
6. Sur le serveur cible, vérifiez que tous les processus Network Manager sont en cours d'exécution. Pour ce faire, exécutez la commande suivante :

   ```
   itnm_start ncp -domain DOMAIN
   ```

   Exécutez cette commande pour tous les domaines qui existent sur le serveur cible. Indiquez explicitement le nom de domaine à chaque fois.
7. Arrêtez maintenant tous les processus Network Manager à l'aide de la commande suivante :

   ```
   itnm_stop ncp -domain DOMAIN
   ```

   Exécutez cette commande sur tous les domaines. Indiquez explicitement le nom de domaine à chaque fois. Le démarrage et l'arrêt des processus permettent de remplir les tables de base de données appropriées.

   Si la reprise en ligne est configurée, arrêtez aussi tous les domaines sur le serveur de secours.

8. Sur le serveur cible, accédez à l'emplacement $NCHOME/precision/install/data/ et extrayez le package ExportPackageCore.tar.
9. Avec l'identité du même utilisateur ayant installé le produit, exécutez le script nmImport à partir du répertoire scripts.
10. Fournissez l'information requise par le script lorsque vous y êtes invité. Lorsque vous y êtes invité, indiquez le chemin du fichier .pkg qui contient les données de personnalisation précédemment exportées.
11. Facultatif : Si vous migrez votre base de données topologiques NCIM vers une base de données Oracle utilisant la technologie Oracle de mise en cluster, fournissez les informations Oracle appropriées en respectant les invites suivantes :
    a) Après l'invite qui répertorie les paramètres de serveur de base de données en cours, répondez n à la question suivante :

    ```
    Are the server settings correct [y|n]?
    ```

    b) Répondez y à la question suivante :

    ```
    Is this an Oracle service name [y|n] ?
    ```

    c) Lorsque le script affiche les paramètres de serveur de base de données en cours, vérifiez que le paramètre suivant apparaît : oracleService = 1.
12. Lorsque le système vous demande si vous souhaitez allouer de nouveaux ID d'entité, qui sont des identificateurs de périphérique uniques pendant l'importation, répondez N afin de conserver les liens à d'autres produits utilisant les données Network Manager telles qu'TADDM, IBM Tivoli Business Service Manager, IBM Control Desk.

    Si vous avez déjà des données topologiques dans l'installation cible, par exemple depuis une précédente importation ou reconnaissance de réseau, vous ne pouvez pas préserver les ID des précécentes entités et devez répondre Y. Si vous répondez N le script renvoit une erreur déclarant que ces données d'entité existent déjà.

    Si vous avez un domaine sur le système cible qui porte le même nom que sur votre système précédent, vérifiez que le domaine sur le système cible ne contient pas de données de topologie. Les noms de domaine ne peuvent pas être modifiés pendant le processus de migration.
13. Examinez vos vues de réseau pour détecter les doublons. Des doublons peuvent être créés par exemple si une reconnaissance a été exécutée avant la mise à niveau. Vous pouvez supprimer les vues en double ou déplacer des sections de vue dans les vues existantes.
14. Changez le domaine par défaut, si nécessaire, en paramétrant la variable d'environnement PRECISION_DOMAIN sur le domaine par défaut souhaité

    Le domaine par défaut est le domaine créé à l'installation. Lorsque les scripts de contrôle, par exemple, itnm_start, sont utilisés sans argument -domain, les actions spécifiées dans les scripts sont appliquées au domaine par défaut.

Résultats

Le script d'importation importe les données de configuration depuis votre installation source dans l'installation cible. Les fichiers de journalisation suivants sont écrits dans le répertoire $NCHOME/log/precision : ITNMDataImport.log, get_policies.domain name.log, et ITNMImportNetworkViews.log.

Que faire ensuite

Vous devez vérifier les résultats de l'importation et exécuter les opérations de migration manuelle requises.

Migration de l'interrogation

Migrez les règles d'interrogation et, le cas échéant, les interrogateurs.

Pourquoi et quand exécuter cette tâche

Vous devez définir une portée pour chaque règle d'interrogation à utiliser. Vérifiez que toutes les règles sont associées à l'interrogateur indiqué approprié.

Procédure

1. Configurez les règles d'interrogation sur l'installation cible en exécutant la procédure suivante pour chaque règle d'interrogation que vous avez migrée :
   a) Connectez-vous aux applications Web sur votre nouvelle installation.
   b) Vérifiez que les vues de réseau existent pour votre système.
   c) Cliquez sur l'icône **Administration** et sélectionnez **Réseau** > **Interrogation du réseau**.
   d) Sélectionnez une règle qui était disponible sur le système source en cliquant sur le nom de la règle d'interrogation.
      L'**Editeur de règles d'interrogation** est affiché pour la règle que vous avez sélectionnée et ses paramètres sont automatiquement chargés dans les zones.
   e) Si nécessaire, réaffectez la règle à l'interrogateur nommé approprié.
   f) Sélectionnez les **Vues de réseau** et sélectionnez la vue de réseau utilisée sur le système source.
   g) Sélectionnez l'onglet **Filtre de périphériques** et configurez le filtre tel qu'il était sur le système source.
   h) Editez chaque définition d'interrogation et vérifiez que les filtres Classe et Interface sont configurés comme prévu. Des classes peuvent avoir été ajoutées ou supprimées entre les versions.
2. Facultatif : Les règles d'un seul interrogateur sur le système cible sont affectées automatiquement au nouvel interrogateur **ncp_poller_default** sur l'installation cible. Si vous avez utilisé plusieurs interrogateurs sur l'installation source, configurez plusieurs interrogateurs sur l'installation cible en procédant comme suit :
   a) Editez le fichier `CtrlServices.cfg` sur l'installation cible en utilisant les entrées du système source . Si vous utilisez le nouvel interrogateur **ncp_poller_default**, toutes les règles d'interrogation l'adoptent automatiquement par défaut.
   b) Répétez la procédure pour chaque domaine de l'installation cible.

Migration manuelle des fichiers des composants principaux

Certains fichiers contenant des modifications de configuration ne peuvent pas être migrés automatiquement. Consultez la liste des fichiers proposés et migrez manuellement les modifications.

Pourquoi et quand exécuter cette tâche

Le processus de migration met à jour une aussi grande partie que possible de la configuration sur le système cible. Les modifications sont gérées comme suit :

- Si un fichier de configuration par défaut a été modifié sur le système source, il est copié automatiquement et écrase le fichier équivalent sur le système cible. Le processus de migration applique automatiquement les modifications, à condition qu'il n'y ait pas de conflits.
- Si un fichier de configuration par défaut a été modifié sur le système source, mais que le fichier par défaut de la version du produit sur le système cible est différente de celui du système source, un conflit survient entre votre modification et une modification dans le produit. Si la différence ne peut pas être résolue automatiquement par les scripts de migration, le fichier est signalé comme nécessitant une révision.
- Si un fichier de configuration n'a pas été modifié sur le système source, il n'est pas migré.

- Si un fichier de configuration n'est plus nécessaire dans l'installation cible, il n'est pas migré.

Pour migrer manuellement les fichiers, procédez comme suit :

Procédure

1. Consultez le fichier journal `$NCHOME/log/precision/NMCoreFilesForManualReview.txt`. Exemple : `/opt/IBM/netcool/log/precision/NMCoreFilesForManualReview.txt`. Ce fichier contient une entrée pour chaque élément à traiter. Si une entrée indique qu'un fichier nécessite une migration manuelle, vous devez examiner chaque fichier et décider de la façon dont vous souhaitez incorporer les différences dans les fichiers dans l'installation cible.
2. Facultatif : Consultez le fichier `NMCoreFilesMigrated.txt` pour identifier tous les fichiers qui ont été migrés et ceux qui ne l'ont pas été. Il est vraisemblable qu'aucune action ne soit nécessaire pour les fichiers qui n'ont pas été migrés. Certains fichiers n'ont pas besoin d'être migrés. Si vous estimez que ce fichier contient des informations de configuration importantes à conserver, examinez le fichier. Examinez le fichier journal `$NCHOME/log/precision/NMCoreConfigFileAutoMigrationReport.txt` pour obtenir des informations supplémentaires sur les fichiers n'ayant pas pu être migrés.
3. En ce qui concerne les fichiers à migrer manuellement, recherchez les versions appropriées des fichiers à examiner.
   - En ce qui concerne les fichiers qui ont été modifiés par un utilisateur, comparez la version d'origine de l'installation source avec la version modifiée de l'installation source. Ces fichiers ont été copiés sur le serveur cible pour des raisons de commodité. Les emplacements diffèrent selon le type de fichier et sont listés dans le fichier `NMCoreFilesForManualReview.txt`.
   - En ce qui concerne les fichiers qui ont été modifiés par IBM entre deux versions, comparez la version de l'installation source avec la version de l'installation cible. Les fichiers du serveur source sont copiés sur le serveur cible pour des raisons de commodité. Les emplacements diffèrent selon le type de fichier et sont listés dans le fichier `NMCoreFilesForManualReview.txt`.
   - En ce qui concerne les fichiers qui ont été modifiés par un utilisateur et par IBM entre deux versions, comparez les trois versions. Les fichiers du serveur source sont copiés sur le serveur cible pour des raisons de commodité. Les emplacements diffèrent selon le type de fichier et sont listés dans le fichier `NMCoreFilesForManualReview.txt`.
4. Exécutez l'utilitaire **`ncp_mib`** si vous avez personnalisé des bases d'informations de gestion (MIB) sur le système source.

   Les bases d'informations de gestion (MIB) personnalisées de l'installation source sont copiées dans le répertoire `$NCHOME/precision/mibs/`. Les fichiers MIB ont été transférés depuis l'interface graphique vers le serveur des composants principaux dans la V4.2.
5. Passez en revue le ficier `DbEntityDetails.cfg` remplacez `&ExtraInfo` par `&m_ExtraInfo`.

   Cette modification est nécessaire en raison de changements de la base de données entre la version V3.9 et la version V4.1 et versions ultérieures.
6. Examinez les fichiers `DbLogins.cfg` sur l'installation cible en ajoutant les nouvelles informations de connexion à la base de données de l'installation cible.

   Les scripts de migration créent des fichiers `DbLogins.cfg` spécifiques au domaine pour chaque domaine à partir de l'installation source.
7. Facultatif : Si vous avez utilisé des collecteurs de reconnaissance sur l'installation source, copiez les fichiers `.cfg` et `.drv` sur l'installation cible et vérifiez que les collecteurs sont configurés correctement.
8. Facultatif : Si vous avez créé des collecteurs de reconnaissance sur l'installation source, consultez le document *EMS Collector Developer Guide* pour connaître les instructions de migration.
9. Si vous avez utilisé des fichiers de départ pour la reconnaissance sur le serveur source, copiez-les à l'emplacement équivalent sur le serveur cible. Lors de l'exécution d'une reconnaissance, mettez à jour la référence au fichier de départ dans l'onglet **Valeur de départ** de l'**interface graphique Configuration de la reconnaissance**.

10. Si vous avez utilisé des fichiers DNS pour la reconnaissance sur le serveur source, copiez-les à l'emplacement équivalent sur le serveur cible. Lors de l'exécution d'une reconnaissance, mettez à jour la référence au fichier DNS dans l'onglet **DNS** de l'**interface graphique Configuration de la reconnaissance**.
11. Examinez la liste des fichiers qui ne sont pas migrés dans «Référence de fichier des composants principaux», à la page 148 et déterminez si des modifications de personnalisation ont besoin d'être migrées.
12. Examinez les modifications apportées aux fichiers `NcoGateInserts.`*`DOMAIN`*`.cfg`, qui sont obsolètes dans Network Manager 4.2, pus migrez les modifications :
    a) Accédez au répertoire indiqué pour l'entrée `NcoGateInserts.`*`DOMAIN`*`.cfg` dans le fichier `$NCHOME/log/precision/NMCoreFilesForManualReview.txt`.
    b) Recherchez les fichiers `NcoGateInserts.`*`DOMAIN`*`.cfg` de chaque domaine pour lequel vous avez effectué des personnalisations.
    c) Recherchez vos personnalisations. Vous devez uniquement migrer les personnalisations que vous avez créées vous-même. Toutes les personnalisations par défaut ont été transférées depuis le fichier `NcoGateInserts.cfg` vers les règles de sonde dans Netcool/OMNIbus Knowledge Library V4.4.3.
    d) Sur le serveur sur lequel Netcool/OMNIbus Knowledge Library est installé, recherchez le fichier de règles correspondant à l'eventID du type d'événements que vous souhaitez personnaliser. En ce qui concerne les règles spécifiques à un fournisseur, les fichiers de règles se trouvent sous le répertoire du fournisseur, par exemple `include-snmptrap/cisco`.
    e) Recherchez le fichier de règles approprié à l'aide du suffixe `user.include.rules`. Par exemple : `/include-snmptrap/adtran/adtran-ADTRAN-ACTDAXL3-MIB.user.include.snmptrap.rules`. Le fait de placer vos personnalisations dans un fichier distinct permet de les identifier et de les sauvegarder plus facilement par la suite.
    f) Modifiez le fichier et recherchez la section correspondant au type d'interception à personnaliser. Par exemple pour passer outre les régles par défaut pour l'interruption `adACTDAXL3systemHdwFailureClear`, ajoutez les règles personnalisées sous la section suivante :

    ```
    case "906": ### adACTDAXL3systemHdwFailureClear
    ```

    g) Définissez la zone @NmosEventMap avec le format suivant : *nom_mappe_événement.valeur_précédence*.

    Par exemple :

    ```
    @NmosEventMap = "LinkDownIfIndex.910"
    ```

13. Facultatif : Pour examiner la liste des fichiers qui ont été migrés correctement, examinez les fichiers listés dans `NCHOME/log/precision/NMCoreFilesMigrated.txt`.

Référence de fichier des composants principaux

Les scripts de migration des composants principaux traitent les fichiers dans leur portée.

Fichiers compris dans la portée des scripts de migration des composants principaux

Les scripts de migration des composants principaux examinent les fichiers de configuration dans les répertoires suivants et les traitent comme indiqué dans «Migration manuelle des fichiers des composants principaux», à la page 146.

- `$NCHOME/precision/aoc/*.aoc`
- `$NCHOME/precision/disco/stitchers/*.stch`
- `$NCHOME/precision/disco/stitchers/DNCIM/*agnt`
- `$NCHOME/precision/disco/agents/*`

- $NCHOME/precision/adapters/ncp_dla/ncp_dla.properties.*
- $NCHOME/precision/eventGateway/stitchers/*
- $NCHOME/probes/*platform*/nco_p_ncpmonitor.rules*
- $NCHOME/precision/mibs/*.mib
- $NCHOME/etc/precision/*.cfg
- $NCHOME/precision/storm/conf/*.cfg, *.conf, *.yaml, *.properties

Fichiers non migrés par les scripts de migration des composants principaux

Les fichiers suivants ne sont pas migrés par les scripts de migration :

- $NCHOME/precision/scripts/webtools.

  Vous devez enregistrer manuellement ces fichiers dans l'installation source et les réimplémenter dans l'installation cible. Les paramètres de lancement dans IBM Tivoli Application Dependency Discovery Manager sont un exemple d'une telle personnalisation.
- $NCHOME/etc/omni.dat.

  Ces paramètres ne sont pas nécessaires car les détails de connexion sont définis pendant l'installation du système cible.
- $NCHOME/etc/interfaces.<arch>
- $NCHOME/precision/collectors. Si vous utilisez des collecteurs de reconnaissance, vous devez migrer manuellement les modifications de configuration pour le collecteur.
- $NCHOME/etc/precision/ConfigSchema.cfg
- $NCHOME/etc/precision/DbLogins.cfg
- $NCHOME/etc/precision/DiscoDncimDb.cfg. Ce fichier est obsolète dans la V4.2.
- $NCHOME/etc/precision/DncimDbEntityDetail.cfg. Ce fichier est obsolète dans la V4.2.
- $NCHOME/etc/precision/MibDbLogin.cfg
- $NCHOME/etc/precision/NcoLogin.cfg
- $NCHOME/etc/precision/ServiceData.cfg

Migration des composants de l'interface graphique

Migrez les composants de l'interface graphique en exportant les données de l'installation source vers l'installation cible. Importez les données, affectez des utilisateurs aux groupes et examinez le fichier NMGUIFilesForManualReview.txt pour savoir si des étapes manuelles sont requises.

Pourquoi et quand exécuter cette tâche

Migrez les données de l'interface graphique de Network Manager en suivant les instructions ci-dessous.

Pour savoir comment migrer Interface graphique Web, consultez les informations de votre version de Interface graphique Web à l'adresse suivante : http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Procédure

1. Sur le serveur cible où sont installés les composants d'interface graphique, vérifiez que les variables d'environnement pour Network Manager sont définies en exécutant le script d'environnement. Ce dernier se trouve à l'emplacement suivant : répertoire_installation/nmgui_profile.sh, par exemple, /opt/IBM/netcool/nmgui_profile.sh.
2. Sur le serveur cible sur lequel sont installés les composants de l'interface graphique, exécutez la commande suivante :

```
$NMGUI_HOME/install/scripts/makeExportPackageGUI -j $JazzSM_HOME -n $NMGUI_HOME
```

Où :

- $NMGUI_HOME est la variable d'environnement qui définit l'emplacement d'installation de l'interface graphique Network Manager. Par défaut, il s'agit de `/opt/IBM/netcool/gui/precision_gui`.
- $JazzSM_HOME est le répertoire d'installation de Jazz for Service Management. Par défaut, cet emplacement est `/opt/IBM/JazzSM`.

Par exemple, en utilisant les emplacements d'installation par défaut, exécutez la commande suivante :

```
/opt/IBM/netcool/gui/precision_gui/install/scripts/makeExportPackageGUI -j
 /opt/IBM/JazzSM -n /opt/IBM/netcool/gui/precision_gui
```

Le script crée un package contenant les scripts que vous utilisez pour exporter les données depuis l'installation source. Le package est appelé `ExportPackageGUI.tar`.

3. Copiez le fichier `ExportPackageGUI.tar` dans un emplacement temporaire sur le serveur source où sont installés les composants de l'interface graphique. Si des composants de l'interface graphique sont installés sur plusieurs serveurs, vous devez uniquement exporter les données depuis l'un des serveurs sauf si vous les avez configurés différemment.

   Remarque : L'emplacement ne doit pas se trouver dans le répertoire d'installation.
4. Sur le serveur source, décompactez le fichier `ExportPackageGUI.tar`.
5. Vérifiez que les variables d'environnement de Network Manager sont définies sur le serveur source en exécutant le script d'environnement approprié.

   Dans Network Manager 4.2, il existe deux scripts d'environnement.

   Sur le serveur où sont installés les composants d'interface graphique de Network Manager, le script est `répertoire_installation/nmgui_profile.sh`, par exemple, `/opt/IBM/netcool/nmgui_profile.sh`.

   Sur le serveur où sont installés les composants de base de Network Manager, le script d'environnement est `répertoire_installation/netcool/core/env.sh`.

   Dans les versions précédentes de Network Manager, le script est stocké dans le répertoire *répertoire_installation*`/netcool`.
6. Le fichier `ExportPackageGUI.tar` contient un fichier appelé `Preupgrade.tar`. Extrayez le fichier `Preupgrade.tar` à l'emplacement suivant sur le serveur source : `$TIPHOME/profiles/TIPProfile`.
7. Dans le répertoire `scripts` qui a été créé en décompactant le fichier, exécutez le script `nmGuiExport` à l'aide de la commande suivante :

```
nmGuiExport -u tipadmin|smadmin -p password
```

Où :

- -u prend soit le nom de l'administrateur de Tivoli Integrated Portal (par défaut, tipadmin) pour les versions de Network Manager antérieures à la V4.2, soit le nom de l'administrateur de Jazz for Service Management (par défaut, smadmin).
- *mot de passe* est le mot de passe de cet utilisateur.

Restriction : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

Le script crée un fichier `data.zip` dans l'un des répertoires suivants : `$TIPHOME/profiles/TIPProfile/output/` ou `$JazzSM_HOME/ui/upgrade/data/`. Le fichier contient des données de configuration, des rôles utilisateur et des pages, vues et rôles Tivoli Integrated Portal personnalisés. Les erreurs sont enregistrées dans l'un des répertoires suivants : `$TIPHOME/profiles/TIPProfile/logs/tipcli.log` ou `$JazzSM_HOME/ui/logs/consolecli.log`.

8. Créez le répertoire `$JazzSM_HOME/ui/input/` sur le serveur d'interface graphique cible et copiez-y le fichier d'exportation `data.zip`. Si vous installez plusieurs serveurs Dashboard Application Services Hub, copiez le fichier d'exportation sur chaque serveur.
9. Vérifiez que Dashboard Application Services Hub est en cours d'exécution.
10. Vérifiez que les variables d'environnement de Network Manager sont définies sur le serveur cible en exécutant le script *répertoire_installation*`/netcool/gui/precision_gui/nmgui_profile.sh`.
11. Dans le répertoire `scripts` sur le serveur cible, exécutez le `nmGuiImport` avec la commande suivante :

    ```
    nmGuiImport -u smadmin -p password [ -f path_to_zip_file ]
    ```

    Où :

    - -u prend le nom de l'administrateur de Jazz for Service Management (par défaut, smadmin).
    - *mot de passe* est le mot de passe de cet utilisateur.
    - *chemin_fichier_zip* est le chemin d'accès au fichier d'exportation `data.zip` contenant les données de l'interface graphique. Si l'option `-f` n'est pas indiquée, le script recherche le fichier `data.zip` dans l'emplacement par défaut : `$JazzSM_HOME/ui/input/`.

    Restriction : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

    Les données d'interface graphique exportées sont importées dans la nouvelle installation. Si les mêmes utilisateurs existent sur l'installation cible de Dashboard Application Services Hubet sur l'installation source, les mêmes rôles utilisateur leur sont ajoutés. Les résultats de l'importation sont consignés dans le fichier suivant : `$JazzSM_HOME/ui/logs/consolecli.log`
12. Ajoutez manuellement des utilisateurs aux groupes d'utilisateurs appropriés sur votre nouveau système. L'importation des données de l'interface graphique n'inclut pas les données d'appartenance aux groupes d'utilisateurs.
13. Examinez les pages personnalisées provenant de l'installation source qui contient la **Afficheur d'événements**. Remplacez chaque widget **Afficheur d'événements** par un widget **Afficheur d'événements**.

    Le **Afficheur d'événements** widget n'est pas disponible dans Network Manager V4.2. Pour des informations sur comment modifier des pages, référez-vous au sujet *Developing custom dashboards* dans *Guide de l'Utilisateur IBM Tivoli Network Manager*.
14. Si vous avez utilisé l'adaptateur de bibliothèque de reconnaissance sur le serveur source, migrez les paramètres.
    a) Accédez à l'emplacement sur le serveur source où sont stockées les propriétés DLA. Pour les versions de Network Manager antérieures à la version 4.2, l'emplacement est `$NCHOME/precision/adapters/ncp_dla/`. Pour Network Manager V4.2, l'emplacement est `$NMGUI_HOME/adapters/ncp_dla`. Recherchez les fichiers de propriétés DLA. Chaque domaine a un fichier `ncp_dla.properties.`*nom de domaine*. Utilisez les fichiers de propriétés DLA pour chaque domaine afin de recréer les mêmes paramètres LDA sur la nouvelle installation.
    b) Accédez au répertoire `$NMGUI_HOME/adapters/ncp_dla`.
    c) A l'aide du fichier `ncp_dla.properties` préconfiguré, créez un fichier de propriétés DLA équivalent basé sur le fichier DLA de chaque domaine précédent, en nommant les fichiers d'après chaque domaine, `ncp_dla.properties.NCOMS`, par exemple.
    d) Ouvrez le fichier de propriétés DLA pour chaque domaine et effectuez les mêmes paramétrages dans le nouveau fichier spécifique du domaine que dans le fichier `ncp_dla.properties.`*nom de domaine* précédent, ce qui recrée le fichier DLA pour chaque domaine respectif sur le nouveau système.

Restriction : Ne copiez-collez pas le contenu en l'état du fichier précédent dans le nouveau fichier, mais copiez les paramètres qui ont été modifiés sur le système précédent pour remplacer les précédents. Le nouveau fichier contient les nouveaux paramètres qui n'existaient pas dans les versions précédentes et pourraient ne pas fonctionner correctement si le contenu est écrasé.

15. Vérifiez les résultats de l'importation dans le fichier `NMGUIFilesForManualReview.txt` et exécutez les opérations de migration manuelle requises.

Référence associée

Systèmes d'exploitation pris en charge
Network Manager est pris en charge sur les systèmes d'exploitation suivants.

Migration manuelle des fichiers des composants de l'interface graphique

Certains fichiers contenant des modifications de configuration ne peuvent pas être migrés automatiquement. Consultez la liste des fichiers proposés et migrez manuellement les modifications.

Pourquoi et quand exécuter cette tâche

Le processus de migration met à jour une aussi grande partie que possible de la configuration sur le système cible. Les modifications sont gérées comme suit :

- Si un fichier de configuration par défaut a été modifié sur le système source, il est copié automatiquement et écrase le fichier équivalent sur le système cible. Le processus de migration applique automatiquement les modifications, à condition qu'il n'y ait pas de conflits.
- Si un fichier de configuration par défaut a été modifié sur le système source, mais que le fichier par défaut de la version du produit sur le système cible est différente de celui du système source, un conflit survient entre votre modification et une modification dans le produit. Si la différence ne peut pas être résolue automatiquement par les scripts de migration, le fichier est signalé comme nécessitant une révision.
- Si un fichier de configuration n'a pas été modifié sur le système source, il n'est pas migré.
- Si un fichier de configuration n'est plus nécessaire dans l'installation cible, il n'est pas migré.

Procédure

1. Révisez le fichier journal `$NMGUI_HOME/../log/install/NMGUIFilesForManualReview.txt` qui se trouve dans le répertoire d'installation des composants d'interface graphique. Par exemple : `/opt/IBM/netcool/gui/log/install/NMGUIFilesForManualReview.txt`. Ce fichier contient une entrée pour chaque élément à traiter.
   a) Si une entrée indique qu'un fichier a été fusionné automatiquement, aucune action n'est nécessaire.
   b) Si une entrée indique qu'un fichier n'a pas été migré, aucune action n'est probablement nécessaire. Certains fichiers n'ont pas besoin d'être migrés. Si vous estimez que ce fichier contient des informations de configuration importantes à conserver, examinez le fichier.

      Le fichier `$NMGUI_HOME/integration/properties/mergeDefinition.json` détermine ceux des fichiers qui sont migrés. Il n'est pas nécessaire de modifier ce fichier.
   c) Si une entrée indique qu'un fichier nécessite une migration manuelle, vous devez examiner chaque fichier et décider de la façon dont vous souhaitez incorporer les différences dans les fichiers dans l'installation cible.
2. En ce qui concerne les fichiers à migrer manuellement, recherchez les versions appropriées des fichiers à examiner.
   - En ce qui concerne les fichiers qui ont été modifiés par un utilisateur, comparez la version d'origine de l'installation source avec la version modifiée de l'installation source. Ces fichiers ont été copiés sur le serveur cible pour des raisons de commodité. Les emplacements diffèrent selon le type de fichier et sont listés dans le fichier `NMGUIFilesForManualReview.txt`.

- En ce qui concerne les fichiers qui ont été modifiés par IBM entre deux versions, comparez la version de l'installation source avec la version de l'installation cible. Les fichiers du serveur source sont copiés sur le serveur cible pour des raisons de commodité. Les emplacements diffèrent selon le type de fichier et sont listés dans le fichier `NMGUIFilesForManualReview.txt`.
- En ce qui concerne les fichiers qui ont été modifiés par un utilisateur et par IBM entre deux versions, comparez les trois versions. Les fichiers du serveur source sont copiés sur le serveur cible pour des raisons de commodité. Les emplacements diffèrent selon le type de fichier et sont listés dans le fichier `NMGUIFilesForManualReview.txt`.

Référence de fichier de l'interface graphique

Les scripts de migration de l'interface graphique traitent certains fichiers et en ignorent d'autres.

Fichiers compris dans la portée des scripts de migration de l'interface graphique

Les scripts de migration de l'interface graphique examinent les fichiers de configuration dans les répertoires suivants et les traitent comme indiqué dans «Migration manuelle des fichiers des composants de l'interface graphique», à la page 152.

- `$NMGUI_HOME/profile/etc/tnm/autoprovision/*`
- `$NMGUI_HOME/profile/etc/tnm/dynamictemplates/*`
- `$NMGUI_HOME/profile/etc/tnm/*`
- `$NMGUI_HOME/profile/etc/tnm/menus/*`
- `$NMGUI_HOME/profile/etc/tnm/tools/*`
- `$NMGUI_HOME/profile/etc/tnm/resource/*`

Fichiers ignorés par les scripts de migration de l'interface graphique

Les fichiers d'interface graphique suivants ne sont pas migrés par les scripts de migration :

- `tnm.properties`
- `ncpolldata.properties`. Ce fichier est obsolète dans Network Manager 4.2.
- `etc/tnm/locale/*`

Migration de la topologie de réseau

Pour vérifier que vous disposez d'une topologie de réseau sur le système cible, exécutez une reconnaissance complète. (Facultatif) Migrez l'état géré des périphériques et de toute topologie personnalisée créée manuellement.

Pourquoi et quand exécuter cette tâche

Pour migrer la topologie de réseau, procédez comme suit pour chaque domaine de reconnaissance :

Procédure

1. Arrêtez et démarrez tous les processus Network Manager sur l'installation cible afin de vérifier que les les modifications de personnalisation ont été appliquées au domaine.
2. Exécutez une nouvelle reconnaissance de l'installation cible.
3. Si vous avez créé une topologie manuelle de votre installation source, exécutez la procédure suivante dans son intégralité. Si vous n'avez pas ajouté ou supprimé manuellement de périphériques à votre topologie de réseau dans votre installation source, passez à l'étape 7.
4. Dans votre nouvelle installation, accédez à l'emplacement `$NCHOME/var/precision/export/manualtopology`.

Ce répertoire contient des fichiers XML qui répertorient les périphériques et les connexions ajoutés manuellement à chaque domaine sur le système précédent. Il existe un fichier pour chaque domaine. Chaque fichier est nommé comme suit :

```
ManualTopology.DOMAIN.xml
```

où *DOMAINE* est le nom du domaine en question.

5. Ouvrez le fichier XML du domaine à mettre à jour avec les données de la topologie créée manuellement.
6. Appliquez les modifications à votre nouvelle reconnaissance à l'aide des assistants de gestion de topologie dans la **Vue tronçon de réseau**.
   - Vous pouvez ajouter manuellement des périphériques dans n'importe quelle fenêtre de la **Vue tronçon de réseau**.
   - Pour ajouter manuellement des connexions, il est recommandé de faire pointer la fenêtre de la **Vue tronçon de réseau** vers le périphérique d'extrémité a (spécifié avec l'attribut `fromdevice` dans la connexion) et de créer une connexion manuelle au périphérique d'extrémité b (spécifié avec l'attribut `todevice`).

   Pour plus d'informations sur l'édition de la topologie de réseau à l'aide des assistants de gestion de topologie, voir *Guide de l'Utilisateur IBM Tivoli Network Manager*.

   Effectuez les opérations ci-après pour utiliser les assistants de gestion de topologie afin d'ajouter des périphériques et des connexions à l'exemple de fragment de code XML de la topologie.

   a) Cliquez sur l'icône **Incident** et sélectionnez **Disponibilité du réseau** > **Vue tronçon de réseau**.

   b) Sélectionnez un domaine de réseau dans la liste déroulante **Domaine** correspondant à la ligne 2 dans l'exemple de code XML ci-dessous.

   c) Ajoutez tous les périphériques spécifiés dans le fichier XML en procédant comme suit :

      i) Cliquez avec le bouton droit de la souris dans la **Vue tronçon de réseau**, puis cliquez sur **Gestion de la topologie** > **Ajouter un périphérique**.

      ii) Dans l'assistant **Ajouter un périphérique**, ajoutez le périphérique aog.dom39.1 en spécifiant les attributs répertoriés aux lignes 21 à 35 du fichier XML.

      Remarque : Tenez compte des points suivants :

      - Les attributs apparaissent dans le fichier XML par ordre alphabétique. Ce n'est pas l'ordre dans lequel ils sont demandés par l'interface graphique.
      - Il se peut que le fichier XML ne contienne pas tous les attributs demandés par l'interface graphique pour une connexion ou un périphérique donné. Si des attributs manquent, n'entrez pas leurs valeurs dans l'interface graphique.

      Renseignez tous les écrans de l'assistant et cliquez sur **Terminer**, puis sur **Fermer**. Le périphérique que vous avez ajouté apparaît dans la **Vue tronçon de réseau**.Pour plus d'informations sur l'édition de la topologie de réseau à l'aide des assistants de gestion de topologie, voir *Guide de l'Utilisateur IBM Tivoli Network Manager*.

      iii) Cliquez avec le bouton droit de la souris dans la **Vue tronçon de réseau**, puis cliquez sur **Gestion de la topologie** > **Ajouter un périphérique** et ajoutez le périphérique aog.dom39.2 en spécifiant les attributs répertoriés aux lignes 36 à 42 du fichier XML. Renseignez tous les écrans de l'assistant et cliquez sur **Terminer**, puis sur **Fermer**. Le périphérique que vous avez ajouté apparaît dans la **Vue tronçon de réseau**.

      iv) Cliquez avec le bouton droit de la souris dans la **Vue tronçon de réseau**, puis cliquez sur**Gestion de la topologie** > **Ajouter un périphérique** et ajoutez le périphérique aog.dom39.3 en spécifiant les attributs répertoriés aux lignes 43 à 48 du fichier XML. Renseignez tous les écrans de l'assistant et cliquez sur **Terminer**, puis sur **Fermer**. Le périphérique que vous avez ajouté apparaît dans la **Vue tronçon de réseau**.

   d) Ajoutez toutes les connexions spécifiées dans le fichier XML en procédant comme suit :

i) Dans la **Vue tronçon de réseau**, accédez à une vue panoramique contenant le périphérique aog.dom39.1.Pour plus d'informations sur la recherche de périphérique dans la **Vue tronçon de réseau**, voir *Guide de l'Utilisateur IBM Tivoli Network Manager*.

ii) Cliquez avec le bouton droit de la souris sur le périphérique aog.dom39.1 et cliquez sur **Gestion de la topologie** > **Ajouter une connexion**.

iii) Dans l'assistant **Ajouter une connexion**, ajoutez une connexion du périphérique aog.dom39.1 au périphérique aog.dom39.2 en spécifiant les attributs répertoriés aux lignes 4 à 8 du fichier XML. Finissez tous les écrans de l'assistant et cliquez **Finish**, suivi par **Recenter & Close**. La connexion que vous avez ajoutée apparaît dans la **Vue tronçon de réseau**.Pour plus d'informations sur l'édition de la topologie de réseau à l'aide des assistants de gestion de topologie, voir *Guide de l'Utilisateur IBM Tivoli Network Manager*.

iv) Dans la **Vue tronçon de réseau**, vérifiez que vous vous trouvez dans une vue panoramique contenant le périphérique aog.dom39.2, puis cliquez avec le bouton droit de la souris sur le périphérique aog.dom39.2 et cliquez sur **Gestion de la topologie** > **Ajouter une connexion**. Ajoutez une connexion du périphérique aog.dom39.2 à l'interface [GigabitEthernet0/1/0/1] sur le périphérique 172.20.1.3 en spécifiant les attributs répertoriés aux lignes 9 à 13 du fichier XML. Finissez tous les écrans de l'assistant et cliquez **Finish**, suivi par **Recenter & Close**. La connexion que vous avez ajoutée apparaît dans la **Vue tronçon de réseau**.

v) Dans la **Vue tronçon de réseau**, vérifiez que vous vous trouvez dans une vue panoramique contenant le périphérique 172.20.1.3, puis cliquez avec le bouton droit de la souris sur le périphérique 172.20.1.3 et cliquez sur **Gestion de la topologie** > **Ajouter une connexion**. Ajoutez une connexion de l'interface [Null0] sur le périphérique 172.20.1.3 à l'interface [Nu0] sur le périphérique 172.20.3.3 en spécifiant les attributs répertoriés aux lignes 14 à 20 du fichier XML. Finissez tous les écrans de l'assistant et cliquez **Finish**, suivi par **Recenter & Close**. La connexion que vous avez ajoutée apparaît dans la **Vue tronçon de réseau**.

7. Si vous aviez des périphériques sur votre installation source qui n'ont pas été gérés, procédez comme suit pour chaque domaine. Les périphériques non gérés ne sont pas interrogés par Network Manager et ne sont pas inclus dans la RCA. Si tous vos périphériques étaient gérés, vous n'avez pas besoin d'effectuer la procédure suivante.
8. Dans l'installation cible, placez-vous dans le répertoire suivant : `$NCHOME/precision/bin`
9. Exécutez le script `UnmanageNode.pl` pour le domaine à mettre à jour avec les données de statut gérées.

   Utilsez une commande similaire à la suivante :

   ```
   ncp_perl UnmanageNode.pl -domain DOMAIN_NAME -user ncim -pwd password
   -noMainNodeLookup -file

   $NCHOME/var/precision/export/managedstatus/UnmanagedEntities.DOMAIN_NAME.dat
   ```

   Où :

   - *NOM_DOMAINE* est le domaine que vous mettez à jour avec les données de statut gérées.
   - *mot_de_passe* est le mot de passe de l'utilisateur ncim.
   - Le fichier `.dat` est une liste d'entités non gérées qui a été générée par le processus d'exportation. Il existe une liste par domaine.

   Pour plus d'informations sur le script UnmanageNode, reportez-vous à *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

   Le script indique dans sa sortie les noms des interfaces et des noeuds principaux qui ont été associés au statut non géré. Par exemple :

   ```
   'aaa-11-12345.core.test.lab[ Lo0 ]' unmanaged.
   'bbb-22-12345.core.eu.test.lab' unmanaged.
   ```

Ajout d'un périphérique ajouté manuellement et connexion à la topologie de réseau

L'exemple suivant montre comment ajouter un périphérique et comment ajouter une connexion à l'aide d'un fragment de code XML provenant d'un fichier XML généré par le script d'importation. Le fragment de code XML ci-dessous représente trois périphériques ajoutés manuellement et trois connexions ajoutées manuellement.

Remarque : Les entrées de balise pour les connexions apparaissent avant les entrées relatives aux périphériques dans le fichier XML. Toutefois, lorsque vous réappliquez la topologie manuelle avec l'éditeur de topologie, vous devez d'abord ajouter tous les périphériques spécifiés dans le fichier, puis ajouter les connexions.

Tableau 12. Fragment de code XML provenant d'un fichier de topologie manuelle

```
1   <?xml version='1.0' standalone='yes'?>
2   <ManualTopology domain="DOMAIN_39"
3                   version="3.9" >
4   <Connection connectivity="Layer 3 Meshed Topology"
5                fromdevice="aog.dom39.1"
6                reason="reas"
7                speed="1111"
8                todevice="aog.dom39.2" />
9   <Connection connectivity="Layer 3 Meshed Topology"
10               fromdevice="aog.dom39.2"
11               reason=""
12               todevice="172.20.1.3"
13               tointerface="[ GigabitEthernet0/1/0/1 ]" />
14  <Connection connectivity="Layer 2 Topology"
15               fromdevice="172.20.1.3"
16               frominterface="[ Null0 ]"
17               reason=""
18               speed="2345"
19               todevice="172.20.3.3"
20               tointerface="[ Nu0 ]" />
21  <Device entityname="aog.dom39.1"
22            accessipaddress="192.168.11.1"
23            accessprotocol="IPv4"
24            classname="Cisco"
25            description="aog.dom39.1 desc"
26            displaylabel="aog.dom39.1"
27            ipforwarding="forwarding"
28            modelname="aog.dom39.1 modelname"
29            reason="aog.dom39.1 reason"
30            serialnumber="ser.123"
31            syscontact="aog.dom39.1 syscont"
32            sysdescr="aog.dom39.1 sysdesc"
33            syslocation="aog.dom39.1 sysloc"
34            sysname="aog.dom39.1 sysname"
35            typename="Chassis" />
36  <Device entityname="aog.dom39.2"
37            accessipaddress="192.168.11.2"
38            accessprotocol="IPv4"
39            classname="Cisco"
40            displaylabel="aog.dom39.2"
41            reason=""
42            typename="Chassis" />
43  <Device entityname="aog.dom39.3"
44            accessprotocol="IPv4"
45            classname="Cisco"
46            displaylabel="aog.dom39.3"
47            reason=""
48            typename="Chassis" />
49  </ManualTopology>
```

Le tableau suivant récapitule les éléments et les attributs figurant dans ce fragment de code XML :

Tableau 13. Description du fragment de code XML provenant d'un fichier de topologie manuelle.

Numéro de ligne	Description
2	Domaine auquel cette topologie manuelle s'applique.

Tableau 13. Description du fragment de code XML provenant d'un fichier de topologie manuelle. (suite)

Numéro de ligne	Description
4 à 8	Connexion manuelle entre un périphérique ajouté manuellement, "aog.dom39.1", et un autre périphérique ajouté manuellement, "aog.dom39.2".
9 à 13	Connexion manuelle entre un périphérique ajouté manuellement, "aog.dom39.2", et l'interface [GigabitEthernet0/1/0/1] sur le périphérique reconnu 172.20.1.3. **Remarque :** Le périphérique 172.20.1.3 n'apparait pas dans une balise <Device> dans ce fichier; ce n'est donc pas un périphérique ajouté manuellement et de fait doit être un périphérique reconnu.
14 à 20	Connexion manuelle entre l'interface [Null0] sur le périphérique reconnu 72.20.1.3 et l'interface [Nu0] sur le périphérique reconnu 172.20.3.3. **Remarque :** Le périphérique 172.20.3.3 n'apparait pas dans une balise <Device> dans ce fichier; ce n'est donc pas un périphérique ajouté manuellement et de fait doit être un périphérique reconnu.
21 à 35	Périphérique ajouté manuellement aog.dom39.1.
36 à 42	Périphérique ajouté manuellement aog.dom39.2.
43 à 49	Périphérique ajouté manuellement aog.dom39.3.

Chapitre 9. Configuration de Network Manager

Après l'installation de Network Manager, vous devez configurer Network Manager pour votre environnement et en fonction de vos exigences. Si votre environnement ou vos exigences changent ultérieurement ou si vous souhaitez intégrer Network Manager à d'autres produits, il peut être nécessaire d'effectuer des tâches de configuration supplémentaires.

Configuration des propriétés de connexion NCIM

Vous pouvez configurer des propriétés spécifiques au vendeur pour la gestion du pilote JDBC après l'installation de la base de données de topologie NCIM et les composants du GUI.

Pourquoi et quand exécuter cette tâche

Pour configurer des propriétés spécifiques au vendeur, pour la gestion du pilote JDBC, menez à bien les étapes suivantes :

Procédure

1. Créez un fichier de propriétés Java avec les propriétés et valeurs que vous voulez.

   Référez-vous à la documentation de la base de données du vendeur à propos de JDBC quant aux détails sur les propriétés disponibles.
2. Sauvegardez le fichier dans un répertoire sur le serveur où les composants GUI sont installés.

   `$NMGUI_HOME/profile/etc/tnm/`
3. Modifiez le fichier `$NMGUI_HOME/profile/etc/tnm/tnm.properties` et ajoutez une ligne qui lit :

   `tnm.database.connection.propertiesFile=`*`properties_file`*

   Où *properties_file* est le nom du fichier de propriétés que vous venez de créer.

Configuration de la longueur et du type de chiffrement

À partir de Network Manager Fix Pack 9, vous pouvez utiliser des clés de chiffrement entre 128 et 256 bits. Vous pouvez aussi choisir un chiffrement CBC ou EBC. Après une mise à niveau vers Fix Pack 9, vous devez terminer certaines étapes de configuration post-installation afin de changer celle par défaut de 128 bits.

Pourquoi et quand exécuter cette tâche

Pour utiliser le chiffrement 128-bit par défaut, vous n'avez pas besoin de faire de changement. Pour utiliser un chiffrement 192-bit ou 256-bit, vous devez configurer les composants principaux Network Manager ou les composants GUI manuellement. Le chiffrement pour les composants principaux et le GUI est séparé et peut être différent. Veillez à ce que Storm utilise le même fichier et type de chiffrement que les composants principaux.

Procédure

Configurez les composants principaux Network Manager.

1. Arrêter tous les processus Network Manager.

   Vous pouvez utiliser la commande `itnm_stop`.
2. Si vous voulez changer la longueur de la clé de chiffrement, modifiez le fichier `$NCHOME/etc/precision/ConfigSchema.cfg` et changez la valeur qui est insérée dans `config.settings.m_KeyLength` pour la longueur de la nouvelle clé en bits. Les valeurs permises sont 128, 192 et 256.

3. Si vous voulez configurer le type de chiffrement, changez la valeur `m_EncryptAlgorithm` pour AES_CBC ou AES_EBC.
4. Utilisez l'utilitaire **nco_keygen** pour générer une nouvelle clé de chiffrement. Vérifiez que vous indiquez le fichier de sortie suivant `$NCHOME/etc/security/keys/conf.key`.

   Pour plus d'informations, référez-vous au sujet *Génération d'une clé dans un fichier de clé* dans IBM Knowledge Center pour IBM Tivoli Netcool/OMNIbus à http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.
5. Redémarrez tous les processus Network Manager.

   Vous pouvez utiliser la commande `itnm_start .`
6. En utilisant la nouvelle clé de chiffrement, chiffrez à nouveau tous les mots de passe actuellement utilisés dans les fichiers de configuration en utilisant l'utilitaire **ncp_crypt** en saisissant la commande suivante.

   ```
   ncp_crypt -password password
   ```

   Où *password* est le mot de passe à chiffrer.

Si vous avez changé l'emplacement du fichier de clé ou le type de chiffrement pour les composants principaux, configurez Storm pour que ça corresponde.

7. Modifiez le fichier `$NCHOME/precision/storm/conf/NMStormTopology.properties`.
8. Configurez l'emplacement du fichier de clé en modifiant la propriété suivante :

   ```
   tnm.fips.key.location=/opt/IBM/tivoli/netcool/etc/security/keys/conf.key
   ```
9. Pour changer le mode de chiffrement, modifiez la propriété suivante et établissez-la sur CBC ou EBC:

   ```
   nm.cipher_mode=CBC
   ```

Configurez les composants GUI.

10. Arrêtez les processus GUI.

    Vous pouvez utiliser la commande `itnm_stop`.
11. Utilisez l'utilitaire **nco_keygen** pour générer une nouvelle clé de chiffrement. Veillez à spécifier le fichier de sortie en tant que `$NMGUI_HOME/profile/etc/tnm/encryption/keys/conf.key`. Vous pouvez écraser le fichier de clé existant ou utiliser un nouveau nom.
12. Si nécessaire, ajustez le propriétaire du fichier de clé pour qu'il soit la propriété de l'utilisateur du système opératoire qui exécute le GUI et ajustez les permissions du fichier de clé pour que l'utilisateur n'en ait que la permission de lecture.
13. Si vous donnez un nouveau nom au fichier de clé, modifiez le fichier `$NMGUI_HOME/profile/etc/tnm/tnm.properties` et changez `tnm.fips.key.location` pour qu'il pointe dessus. L'emplacement est relatif à `$NMGUI_HOME/profile/etc/tnm`.
14. Redémarrez les processus GUI.

    Vous pouvez utiliser la commande `itnm_start`.
15. Connectez-vous au GUI en tant qu'administrateur.
16. Sélectionnez **Administration** > **Configuration d'Accès à Base de Données** à partir du menu.
17. Saisissez le mot de passe de base de données topologique dans les boites **Mot de Passe** et **Confirmez le Mot de Passe**.
18. Cliquez l'Icône **Save**.
19. Déconnectez-vous.
20. Redémarrez une nouvelle fois le GUI.

Configuration de Network Manager pour les systèmes d'exploitation UNIX

Sur les systèmes UNIX, il peut être nécessaire d'effectuer des tâches de configuration supplémentaires avant d'utiliser le produit.

Configuration des autorisations de superutilisateur/non superutilisateur

Sous UNIX, si vous avez installé Network Manager en tant que non superutilisateur, vous devez effectuer une configuration supplémentaire.

Pourquoi et quand exécuter cette tâche

Certains composants de Network Manager nécessitent des autorisations de superutilisateur pour fonctionner. Vous devez effectuer différentes opérations si vous souhaitez exécuter Network Manager en tant que superutilisateur ou non superutilisateur.

Installations en tant que superutilisateur et non superutilisateur

Sous UNIX, vous pouvez installer Network Manager en tant que superutilisateur ou en tant que non superutilisateur.

Si vous avez installé tout autre produit IBM Tivoli dans le même répertoire d'installation, vous devez installer Network Manager à l'aide du même identifiant utilisateur que celui utilisé pour les autres produits.

Les applications Web Network Manager doivent toujours être exécutées par l'utilisateur ayant installé le produit.

Après l'installation, vous pouvez configurer les composants centraux de Network Manager pour qu'ils puissent être exécutés par un utilisateur différent. Par exemple, si vous avez installé le produit en tant que superutilisateur, vous pouvez configurer les composants centraux pour qu'ils puissent être exécutés par un non superutilisateur.

Restriction : Lorsque Network Manager est installé et exécuté en tant que root, des scripts qui redémarrent les processus Network Manager et Tivoli Netcool/OMNIbus lorsque le serveur est réamorcé sont également installés. Lorsque Network Manager est installé et exécuté en tant qu'utilisateur non root, les processus Network Manager et Tivoli Netcool/OMNIbus ne sont pas redémarrés automatiquement lorsque le serveur est réamorcé. Toutefois, dans le cas de tâches post-installation pour des installations non root, vous pouvez configurer les processus pour qu'ils démarrent automatiquement lorsque votre système est réamorcé, comme décrit dans «Configuration des processus pour un démarrage automatique dans une installation non root», à la page 163.

Restriction : IBM Tivoli Business Service Manager doit être exécuté en tant que non root. Lorsque Network Manager et IBM Tivoli Business Service Manager sont installés sur le même serveur, assurez-vous d'installer et d'exécuter les deux en tant qu'utilisateur non root.

Configuration des composants centraux pour une exécution en tant que superutilisateur

Sous UNIX, si vous avez installé Network Manager en tant que non superutilisateur, vous devez procéder à une configuration supplémentaire pour exécuter les composants centraux en tant que superutilisateur.

Avant de commencer

Les applications Web Network Manager doivent toujours être exécutées par l'utilisateur ayant installé le produit.

Pourquoi et quand exécuter cette tâche

Vous devez exécuter un script mettant à jour les droits d'accès aux fichiers afin de garantir l'accès du superutilisateur à tous les fichiers requis.

Si vous avez installé Network Manager en tant que superutilisateur, aucune configuration n'est nécessaire pour exécuter les composants centraux en tant que superutilisateur.

Procédure

1. Connectez-vous au serveur où les composants centraux de Network Manager sont installés. Connectez-vous en tant que superutilisateur.
2. Exécutez le script `NCHOME/precision/scripts/setup_run_as_root.sh`.

Configuration des composants centraux pour une exécution en tant que non superutilisateur

Sous UNIX, si vous avez installé Network Manager en tant que non superutilisateur et que vous souhaitez autoriser les droits utilisateur permettant d'exécuter les composants centraux, vous devez vous connecter en tant que superutilisateur et procéder à une configuration supplémentaire.

Avant de commencer

Avertissement : Procédez à des installations et exécutions en tant que non superutilisateur uniquement sur des serveurs sur lesquels seuls les utilisateurs de confiance sont autorisés à se connecter.

Les applications Web Network Manager doivent toujours être exécutées par l'utilisateur ayant installé le produit.

Pourquoi et quand exécuter cette tâche

Pour accorder ces droits à un non superutilisateur, vous devez exécuter un script. Il est impossible d'installer et d'exécuter Network Manager sans se connecter en tant que superutilisateur. Vous devez au minimum vous connecter temporairement en tant que superutilisateur pour exécuter le script.

Important : Sur Linux on IBM z Systems, vous devez installer le logiciel GSKit avant d'exécuter le script setuid.

Installation de GSKit sous AIX

Avant de configurer les composants centraux à exécuter en tant qu'utilisateur non superutilisateur sous AIX, vous devez installer IBM Global Secure ToolKit (GSKit).

Avant de commencer

Assurez-vous que vous disposez de la version 8.0.50.87, ou ultérieure, du GSKit. Ce logiciel de cryptographie IBM permet d'établir une communication SSL (Secure Socket Layer). Le kit GSKit est fourni avec le package d'installation de Network Manager.

Pourquoi et quand exécuter cette tâche

Avant d'exécuter le script `setup_run_as_setuid_root.sh`, vous devez installer GSKit dans le répertoire `/usr/lib`. Un processus exécuté en tant que bit ID utilisateur n'utilise pas la variable d'environnement LIBPATH, et ne peut donc pas utiliser le GSKit lorsqu'il est installé dans un sous-répertoire de $NCHOME.

Pour installer GSKit sous AIX dans /usr/lib à l'aide de la commande **`installp`**, effectuez les tâches suivantes.

Procédure

1. Connectez-vous en tant que superutilisateur.
2. Placez-vous dans le répertoire suivant : `$NCHOME/precision/scripts/`.
3. Ouvrez une invite de commande et entrez les commandes suivantes.

```
installp -acgXd .  GSKit8.gskcrypt64.ppc.rte
installp -acgXd . GSKit8.gskssl64.ppc.rte
```

   Où `-a` correspond à l'application, `-c` correspond à la validation, `-g` installe et valide automatiquement tout progiciel requis, `-X` développe le système de fichier si nécessaire, et `-d` indique l'emplacement du support d'installation.

Configuration des composants centraux pour une exécution en tant que non superutilisateur

Effectuez les étapes de configuration suivantes pour exécuter les composants principaux en tant que non superutilisateur.

Pourquoi et quand exécuter cette tâche

Procédure

1. Connectez-vous en tant que superutilisateur.
2. Exécutez le script `NCHOME/precision/scripts/setup_run_as_setuid_root.sh`.
3. Si vous exécutez la sonde mttrapd (également appelée sonde SNMP) sur le même serveur que Network Manager, procédez à une configuration supplémentaire pour pouvoir exécuter la sonde sans les droits root :

   - Configurez la sonde pour une exécution en tant qu'utilisateur non superutilisateur à l'aide des instructions de la section *Running probes as SUID root* du manuel *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*.
   - AIX Sous AIX, vous devez également suivre les instructions fournies à l'URL suivante : http://www.ibm.com/support/docview.wss?uid=swg21296292.

     Important : Notez que ces instructions impliquant la copie de bibliothèques Sybase dans le répertoire `/usr/lib`, cette opération peut affecter le fonctionnement des installations de Sybase se trouvant sur le même serveur que la sonde mttrapd.

Résultats

Une fois le script exécuté, l'utilisateur ayant installé Network Manager peut se connecter et exécuter les composants centraux de Network Manager.

Configuration des processus pour un démarrage automatique dans une installation non root

Sur les systèmes UNIX, en tant que tâche de post-installation pour des installations non root, vous pouvez configurer vos processus Network Manager de sorte qu'ils démarrent automatiquement lorsque votre système est démarré ou redémarré.

Avant de commencer

Votre installation Network Manager doit être terminée pour que vous puissiez commencer la procédure ci-dessous.

Remarque : Cette procédure n'est pas nécessaire si vous avez installé Network Manager en tant que superutilisateur. Le redémarrage automatique est configuré dans le cadre d'une installation root sans qu'il soit nécessaire d'effectuer cette étape de post-installation.

Pourquoi et quand exécuter cette tâche

Pour configurer les processus Network Manager de sorte qu'ils démarrent automatiquement :

Procédure

1. Connectez-vous au serveur où les composants centraux de Network Manager sont installés. Connectez-vous en tant que superutilisateur.
2. Exécutez le script `NCHOME/precision/install/scripts/create_all_control.sh -auto_only`.

Chargement des informations MIB mises à jour

Pour garantir que le navigateur de la base d'informations de gestion (MIB) contient les informations MIB les plus récentes, chargez les informations MIB mises à jour en exécutant l'application de ligne de commande **ncp_mib**.

Pourquoi et quand exécuter cette tâche

Vous ne devez exécuter l'application de ligne de commande **ncp_mib** que lorsque de nouvelles bases d'informations de gestion sont ajoutées au répertoire `NCHOME/precision/mibs`. Celle-ci est exécutée une fois lors de l'installation, donc si vous n'ajoutez pas de nouvelles informations MIB, vous ne devez pas l'exécuter à nouveau.

Important : Tous les éléments MIB doivent être valides afin de pouvoir être analysés. La commande **ncp_mib** distingue les majuscules des minuscules et attend une extension en `.mib` (et non `.MIB`). Le préfixe peut être une association entre majuscules et minuscules.

Une fois exécuté, **ncp_mib** remplit le schéma `ncmib` dans la base de données NCIM pour fournir un lieu de stockage central de toutes les informations MIB pouvant faire l'objet d'une requête par Network Manager. Le schéma `ncmib` au sein de la base de données NCIM est défini dans le répertoire `NCHOME/etc/precision/MibDbLogin.cfg`. La valeur par défaut est `MIB`.

Il n'existe qu'une seule base de données MIB pour tous les domaines. L'option `-domain`, si elle est spécifiée, configure **ncp_mib** pour l'utilisation d'un fichier `MibDbLogin.`*`domaine`*`.cfg` propre à un domaine. Si aucune option `-domain` n'est spécifiée, le fichier `MibDbLogin.cfg` générique est utilisé. Il n'existe pas de dépendances de processus pour cette commande.

Dans une installation répartie, `ncp_mib` est installé sur le serveur Dashboard Application Services Hub, c'est-à-dire sur le même serveur que les applications Web Network Manager.

Si votre base de données MIB est endommagée ou si vous voulez importer une nouvelle MIB en conflit avec l'une de celles importées précédemment, notez les différentes options de ligne de commande en exécutant **ncp_mib -help**.

Conseil : Si vous n'êtes pas certain du résultat, exécutez **ncp_mib** à l'aide de l'option **-dryrun**. Vous pouvez voir les résultats mais la base de données ne sera pas modifiée.

Pour mettre à jour les informations MIB, suivez la procédure suivante sur le serveur sur lequel Dashboard Application Services Hub est installé.

Procédure

1. Copiez tous les nouveaux fichiers MIB vers le répertoire `NCHOME/precision/mibs`.
2. Assurez-vous que les autorisations d'accès à la base de données sont correctes.

   Les seuls paramètres de configuration requis pour l'application de ligne de commande `ncp_mib` sont les autorisations d'accès à la base de données `ncim`. Ils sont stockées dans un fichier de configuration, `NCHOME/etc/precision/MibDbLogin.cfg`. Notez qu'en raison du fait que **ncp_mib** dépend du domaine, ce fichier ne dispose pas de variantes spécifiques au domaine comme les autres fichiers de configuration.

3. Démarrez le processus **ncp_mib** en émettant la commande **ncp_mib**.

Que faire ensuite

Pour vérifier qu'un MIB a réussi à charger, faite une requête sur la table de base de données `ncmib.mib_modules` en saisissant la commande suivante depuis l'invite de la base de données NCIM (cet exemple suppose que NCIM est exécutée sur Db2):

```
select * from ncmib.mib_modules where moduleName ='RFC1213-MIB';
```

Si MIB est chargée, une table est affichée contenant `moduleName` de RFC1213-MIB.

Vous pouvez également vérifier que les MIB sont chargées en exécutant la commande **ncp_mib** avec l'option `-messagelevel info`. Un message similaire au message suivant vous informe que les MIB sont en cours de traitement :

```
09/10/08 12:41:08: Informations: I-MIB-001-013: [1096571552t]
Resolving references for module 'RFC1213-MIB'
```

Lorsque le traitement est terminé, un message déclare que les MIBs ont été validés dans la base de données.

Conseil : Pour obtenir des informations sur l'utilisation du navigateur MIB SNMP et la création de graphiques à l'aide des variables MIB, consultez le guide *Guide de l'Utilisateur IBM Tivoli Network Manager*.

Configuration de Cognos Analytics

Procédez comme suit pour configurer Cognos Analytics.

Tâches associées

Installation et configuration d'une base de données topologiques

Votre administrateur de base de données doit installer et configurer une base de données topologiques avant que vous puissiez installer Network Manager.

Installation et configuration d'Cognos Analytics

À partir de Network Manager Fix Pack 11, Tivoli Common Reporting n'est plus pris en charge. Pour utiliser des rapports, vous devez installer et configurer Cognos Analytics.

Configuration de rapports pour des installations existantes

Vous pouvez configurer les rapports de gestion de réseau fournis par Network Manager en vue de leur utilisation avec Cognos Analytics.

Avant de commencer

Pour que vous puissiez activer des rapports de gestion de réseau, Cognos Analytics doit être installé. Si vous avez installé des composants d'interface graphique Network Manager sur une machine sur laquelle Cognos Analytics est déjà installé, il n'est pas nécessaire d'effectuer ces opérations.

Pourquoi et quand exécuter cette tâche

Pour configurer les rapports de gestion de réseau, utilisez les informations dans Cognos Analytics Knowledge Center à https://www.ibm.com/support/knowledgecenter/SSEP7J.

Activation de l'interrogation historique

Si vous avez installé Network Manager en tant que superutilisateur, vous devez exécuter le script `setup_run_storm_as_non_root.sh` pour permettre aux processus des données d'interrogation

historiques de s'exécuter. Il n'est pas nécessaire d'exécuter le script si vous avez installé Network Manager en tant que non superutilisateur.

Pourquoi et quand exécuter cette tâche

En tant que superutilisateur, exécutez le script `setup_run_storm_as_non_root.sh` sur le serveur où sont installés les composants principaux de Network Manager. Exécutez le script comme l'exemple suivant :

```
$NCHOME/precision/scripts/setup_run_storm_as_non_root.sh -g group_name
```

Où *group_name* est le nom du groupe d'aggrégation de l'interrogateur que vous aves spécifié lors de l'installation des Network Manager composants centraux.

Remarque : Lorsque vous avez installé les composants principaux de Network Manager, vous avez indiqué des valeurs pour le groupe d'agrégation de l'interrogateur et pour l'utilisateur de l'agrégation de l'interrogateur, qui est un membre du groupe d'agrégation de l'interrogateur. L'utilisateur du groupe d'agrégation est répertorié dans le fichier de configuration `$NCHOME/precision/storm/conf/supervisor.conf`, dans la zone `user` de la section `[supervisord]` de ce fichier.

Pour plus d'informations sur le script `setup_run_storm_as_non_root.sh`, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Tâches associées

Installation des composants de base de Network Manager
Vous devez installer les composants principaux de Network Manager avant d'installer les composants de l'interface graphique ou en même temps.

Activation de la reprise en ligne

Vous pouvez activer la reprise en ligne dans votre environnement Network Manager afin de garantir que les différents composants sont en cours d'exécution et disponibles.

A propos de la reprise en ligne

Dans votre environnement Network Manager, une architecture de reprise en ligne peut être utilisée pour configurer votre système pour une haute disponibilité, en minimisant l'impact d'un incident matériel ou réseau.

La reprise en ligne peut être implémentée pour chacun des produits et composants suivants, qui peuvent être installés lorsque vous utilisez le programme d'installation de Network Manager :

- Les composants centraux de Network Manager, notamment le moteur d'interrogation et la passerelle d'événement (qui imbrique le composant d'analyse origine du problème)
- La base de données topologiques NCIM
- Tivoli Netcool/OMNIbus, y compris le serveur ObjectServer (pour la gestion des événements)
- The Tivoli Netcool/OMNIbus Interface graphique Web, ui est installé dans l'infrastructure du serveur Dashboard Application Services Hub

  Restriction : Network Manager ne prend pas en charge la fonction d'équilibrage de charge Dashboard Application Services Hub gérée par Tivoli Netcool/OMNIbus Web GUI.

Vous devez déterminer quels éléments doivent mettre en oeuvre une reprise en ligne, ainsi que le nombre d'ordinateurs requis pour la haute disponibilité.

A propos de la haute disponibilité de la base de données topologiques NCIM

Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

La haute disponibilité se réfère à un environnement informatique dans lequel les composants matériels et logiciels restent opérationnels pendant les indisponibilités planifiées (par exemple des opérations de maintenance régulières) et non planifiées (par exemple des pannes de matériel, de réseau ou de logiciel inattendues). La base de données topologiques NCIM est un composant qui doit rester opérationnel à tout moment.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Pour définir une configuration de reprise en ligne pour la base de données topologiques NCIM et ainsi fournir aux utilisateurs un environnement à haute disponibilité pour l'exécution d'applications de base de données et l'accès aux informations stockées dans la base de données topologiques NCIM, vous devez vous familiariser avec les tâches et les rubriques d'arrière-plan suivantes :

- Stratégies de haute disponibilité fournies par la base de données
- Architecture de reprise en ligne pour la base de données topologiques NCIM et les processus de base Network Manager
- Tâches liées à l'installation de la base de données

Haute disponibilité avec DB2

Vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 pour configurer la réplication des données depuis une base de données principale vers une base de données de secours. La base de données principale traite normalement l'intégralité ou la majorité de la charge de travail des applications, mais la base de données de secours peut s'occuper de la charge de travail si la base de données principale est défaillante ; ainsi, la base de données reste disponible dans les applications utilisateur. Dans un environnement de reprise à haut niveau de disponibilité après incident (HADR) DB2, cette base de données secondaire est appelée base de données de secours.

Avec la fonction de reprise à haut niveau de disponibilité après incident (HADR), la fonction de redirection automatique du client (ACR) de DB2 permet la redirection des connexions client de Network Manager vers le serveur NCIM principal approprié.

Vous pouvez utiliser IBM Tivoli System Automation for Multiplatforms (SA MP) pour promouvoir automatiquement un serveur DB2 de secours en serveur principal en cas de panne du serveur principal.

Remarque : DB2 met à disposition les outils nécessaires à l'installation et à la configuration de la base de données topologiques NCIM (et des processus de base) en vue de l'utilisation de la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Pour des informations sur l'installation et la configuration de DB2, consultez la section Informations connexes plus loin afin de connaître les liens vers le centre de documentation DB2.

Mise en cluster et haute disponibilité à l'aide d'Oracle RAC

Oracle fournit la fonction RAC (Real Application Clusters) pour la mise en cluster et la haute disponibilité dans les environnements de base de données Oracle. A l'aide d'Oracle RAC, vous pouvez créer une configuration de haute disponibilité pour votre base de données topologiques NCIM. Pour plus d'informations sur l'installation et la configuration d'Oracle RAC, voir Informations connexes plus loin pour un lien vers la documentation Oracle.

Architecture de reprise en ligne pour la base de données topologiques NCIM et les processus de base Network Manager

Vous pouvez implémenter la reprise en ligne des processus de base Network Manager en configurant des installations Network Manager principale et de secours qui s'exécutent sur des serveurs et dans des domaines différents. Les deux installations peuvent être connectées à un unique Serveur d'Objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de Serveurs d'Objets. La reprise de Network Manager peut être implémentée avec ou sans base de données topologiques à haute disponibilité NCIM. Si vous choisissez d'implémenter la reprise en ligne avec la haute disponibilité de la base de données topologiques NCIM, appliquez la fonction de haute disponibilité mise à disposition par la base de données prise en charge. Par exemple, pour définir une configuration de reprise en ligne pour la base de données topologiques NCIM si vous utilisez une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) DB2. De même, si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) pour la reprise en ligne NCIM.

Tâches liées à l'installation de la base de données

Une base de données DB2 peut être installée et configurée par Network Manager. Pour utiliser une base de données DB2 ou Oracle indépendante, configurez-la conformément aux instructions de la rubrique «Installation et configuration d'une base de données topologiques», à la page 51.

Concepts associés

Architecture de reprise en ligne Network Manager (processus centraux)
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Exemple d'hébergement de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM
Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde.

Tâches associées

Installation et configuration d'une base de données topologiques
Votre administrateur de base de données doit installer et configurer une base de données topologiques avant que vous puissiez installer Network Manager.

Architectures de reprise en ligne

La reprise en ligne Network Manager est implémentée indépendamment de la reprise en ligne des produits et composants auxquels elle s'intègre. Avant la configuration de la reprise en ligne, vous devez comprendre les architectures de reprise en ligne pouvant être implémentées pour vous assurer de la haute disponibilité de votre installation Network Manager.

Une installation de reprise en ligne Network Manager contient des serveurs Network Manager principal et de secours sur lesquels les composants centraux sont installés. Si le serveur principal est défaillant en raison de problèmes liés aux matériels ou aux logiciels, le serveur de secours assume le rôle du serveur principal. Pour un environnement plus sûr, vous pouvez inclure une ou plusieurs configurations de reprise en ligne supplémentaires suivantes :

- Des serveurs d'objets Tivoli Netcool/OMNIbus principal et de secours
- Reprise en ligne de la source de données Tivoli Netcool/OMNIbus Web GUI
- Configuration de la haute disponibilité d'une base de données topologiques NCIM

  Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Cette configuration de la haute disponibilité de la base de données topologiques NCIM permet de s'assurer que l'interrogation du réseau peut se poursuivre sur l'installation de secours et que les vues de topologie sont répliquées.

Pour parer aux incidents matériels ou logiciels, et pour une performance optimale de votre environnement, implémentez votre solution de reprise en ligne sur plusieurs ordinateurs.

Architecture de reprise d'ObjectServer

Vous pouvez déployer Tivoli Netcool/OMNIbus par le biais d'une architecture à plusieurs niveaux évolutive afin que le système puisse continuer à fonctionner au maximum de sa capacité (et avec une perte d'événement minimale) en cas d'échec du serveur ObjectServer, de la passerelle ObjectServer ou du serveur proxy.

Les composants de l'architecture sont disposés par couches : collecte, agrégation et affichage. La configuration de reprise en ligne de base est constituée d'un serveur ObjectServer principal et d'un serveur ObjectServer de sauvegarde reliés par une passerelle ObjectServer bidirectionnelle dans la couche agrégation, sans lien avec une couche collecte ou affichage. La conception modulaire de l'architecture à plusieurs niveaux signifie qu'un système peut être constitué au départ par une paire unique de serveurs ObjectServer d'agrégation, auxquels des composants de collecte ou d'affichage peuvent être ajoutés ultérieurement.

La figure suivante montre un exemple de la configuration de reprise en ligne de base dans la couche d'agrégation.

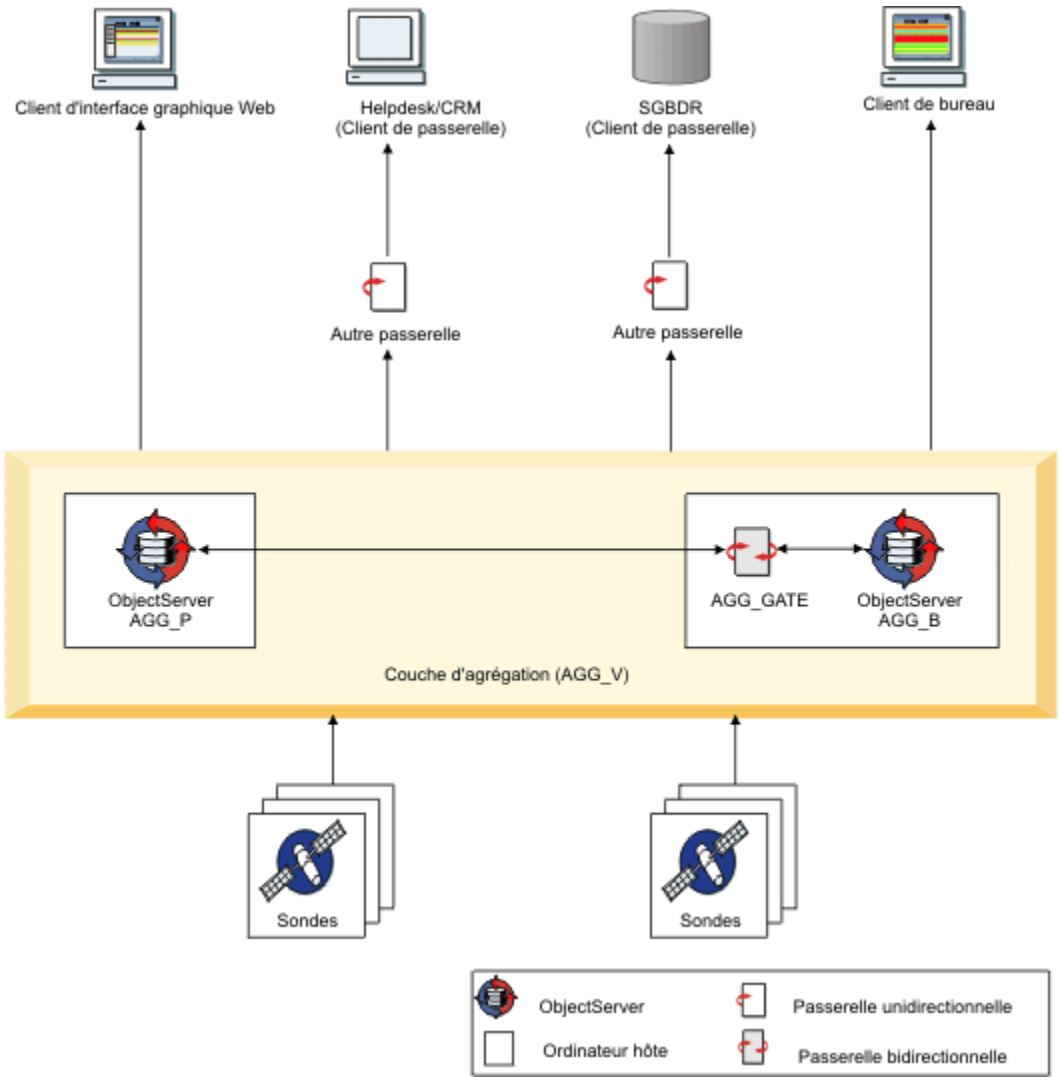

Figure 7. Architecture de reprise d'ObjectServer

Pour réduire l'impact de l'échec de l'ordinateur, l'ObjectServer principal (AGG_P) et l'ObjectServer de sauvegarde (AGG_B) s'exécutent sur deux ordinateurs distincts. La passerelle ObjectServer bidirectionnelle (AGG_GATE) s'exécute sur l'ObjectServer de sauvegarde et synchronise les serveurs d'objets. Les ObjectServer principal et de sauvegarde sont configurés en tant que paire d'agrégation virtuelle (AGG_V) auxquelles des analyses et d'autres clients tels la passerelle d'événements peuvent se connecter directement. Le concept de paire virtuelle contribue à faciliter une reprise en ligne transparente vers l'ObjectServer de sauvegarde en cas d'indisponibilité du serveur ObjectServer principal et la reprise par restauration lorsque l'ObjectServer principal est à nouveau actif. Dans la figure, les cibles exemple vers lesquelles les alertes peuvent être acheminées à partir de la couche agrégation sont également présentées.

Pour des informations complètes sur la configuration de la reprise en ligne d'un serveur ObjectServer dans les couches de collecte, d'agrégation et d'affichage de l'architecture à plusieurs niveaux, voir le document *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Concepts associés

Architecture de reprise en ligne Network Manager (processus centraux)

La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent

être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Tâches associées

Configuration de la reprise en ligne du serveur ObjectServer
La manière dont vous configurez la reprise en ligne du serveur ObjectServer dépend de la version de Tivoli Netcool/OMNIbus.

A propos des fichiers de configuration de reprise en ligne Tivoli Netcool/OMNIbus

Tivoli Netcool/OMNIbus Version 7.3 ou ultérieure fournit un ensemble de fichiers de configuration que vous pouvez appliquer aux serveurs ObjectServer et aux passerelles ObjectServer afin d'implémenter une architecture composée de plusieurs couches.

Ces fichiers sont disponibles dans le répertoire `$NCHOME/omnibus/extensions/multitier` et incluent :

- Les fichiers d'importation SQL pouvant être appliqués à chaque serveur ObjectServer, dans le but de mettre à jour le schéma de base de données avec la configuration requise. Par exemple, des colonnes supplémentaires, des conversions et des automatisations
- Les fichiers de passerelle ObjectServer pouvant être utilisés pour configurer les passerelles dans l'architecture

Important :

- Lors de l'utilisation des fichiers de configuration fournis dans Tivoli Netcool/OMNIbus version 7.3 ou ultérieure, vous devez vous conformer à la convention d'attribution de nom définie pour les composants de chaque couche de l'architecture composée de plusieurs couches. Pour implémenter la reprise en ligne dans la couche agrégation, utilisez les conventions de dénomination décrites dans la Figure 7, à la page 170, c'est-à-dire AGG_P pour le serveur ObjectServer principal, AGG_B pour le serveur ObjectServer de sauvegarde, AGG_V pour la paire virtuelle et AGG_GATE pour la passerelle ObjectServer bidirectionnelle.
- Dans les versions antérieures de Tivoli Netcool/OMNIbus, aucun fichier de configuration n'est fourni et la conformité à ces conventions de dénomination n'est pas obligatoire.

Pour plus d'informations sur les fichiers de configuration comportant plusieurs couches et les conventions de dénomination pour les composants de l'architecture comportant plusieurs couches, voir le manuel *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Architecture de reprise en ligne Network Manager (processus centraux)

La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Lorsque vous vous connectez à un serveur Network Manager, le domaine associé sous lequel le processus s'exécute doit être identifié. Network Manager fournit un domaine virtuel pouvant être utilisé lors d'une exécution en mode reprise. Toute connexion à ce domaine virtuel est routée vers l'installation de Network Manager qui s'exécute en tant que serveur principal dans l'architecture de reprise en ligne. Cette capacité de routage est fournie par le composant de domaine virtuel.

La figure suivante montre l'architecture de reprise en ligne de haut niveau pour les processus centraux de Network Manager qui sont configurés dans deux domaines distincts.

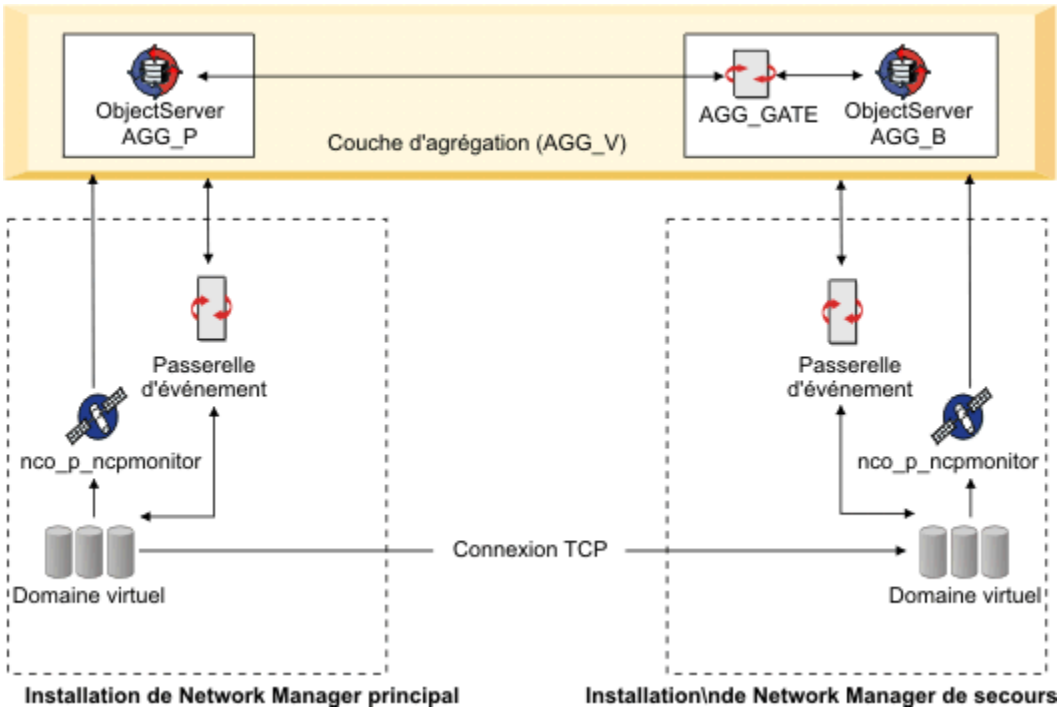

Figure 8. Network Managerarchitecture de reprise en ligne

Dans la figure, les deux installations principale et de secours se connectent à une paire virtuelle de serveurs d'objets.

Dans chaque domaine :

- Le composant de domaine virtuel (**ncp_virtualdomain**) gère la reprise en ligne et génère des événements de vérification d'intégrité pour indiquer si le domaine est en bonne santé.
- La Sonde pour Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) se connecte à la paire de serveurs d'objets virtuels et transfère les événements de vérification d'intégrité.
- La passerelle d'événement (**ncp_g_event**) se connecte à la paire de serveurs d'objets virtuels, lit tous les événements de vérification d'intégrité et transfère ensuite les événements au composant du domaine virtuel.

  Ces événements de vérification d'intégrité sont utilisés pour déclencher la reprise en ligne.

Une connexion de socket TCP est requise entre les processus de domaine virtuel pour copier des données du domaine principal vers le domaine de secours. Ceci garantit que la topologie est en synchronisation lorsque la reprise en ligne se produit.

Remarque : Si vous implémentez la reprise en ligne, vous devez veiller à ce que l'installation principale et celle de secours utilisent des clés de chiffrement identiques. Si les clés de chiffrement ne sont pas identiques, l'interrogateur de secours ne fonctionne pas correctement pendant la reprise en ligne. Pour garantir que l'installation principale et celle de secours utilisent des clés de chiffrement identiques, copiez le fichier suivant depuis le serveur principal vers le même emplacement sur le serveur de secours : `$NCHOME/etc/security/keys/conf.key`. Si vous entrez tous les noms de communauté SNMP en ligne de commande sans les chiffrer, vous n'avez pas besoin d'effectuer cette tâche. Pour plus d'informations sur la modification de la clé de chiffrement, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*. De plus, pour mettre à jour les mots de passe NCIM et ObjectServer, utilisez le script Perl `ncp_password_update.pl`. Pour plus d'informations sur le script Perl `ncp_password_update.pl`, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Implémentations NCIM pour la reprise en ligne

Vous pouvez configurer la reprise en ligne de Network Manager avec la fonction de haute disponibilité de la base de données topologiques NCIM. Cette configuration de reprise en ligne évite la perte de données en répliquant les modifications apportées aux données depuis la base de données topologiques NCIM source dans le domaine Network Manager principal dans une ou plusieurs bases de données topologiques NCIM cible dans le domaine Network Manager de secours. La base de données topologiques NCIM source est appelée base de données principale et la base de données topologiques NCIM cible est appelée base de données de secours. Cette approche supprime le point de défaillance unique car les domaines Network Manager principal et de secours se connectent tous les deux à la base de données qui sert de base de données principale.

Dans toute configuration de reprise en ligne, les domaines Network Manager principal et de secours se connectent à la même base de données, même si la haute disponibilité de la base de données est configurée. Par contre, la base de données est répliquée sur le serveur de base de données de secours.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Que la reprise en ligne soit configurée ou non avec ou sans la haute disponibilité de la base de données topologiques NCIM, les entités de la topologie sont stockées sous le nom du domaine principal et toutes les règles d'interrogation sont configurées pour le domaine principal. La table domainMgr ne comporte pas d'entrée pour le domaine de secours. En conséquence, la zone NmosDomainName d'un événement de la table alerts.status est toujours remplie avec le nom de domaine principal lorsque la reprise en ligne est configurée.

Remarque : Pour configurer la haute disponibilité de la base de données topologiques NCIM avec la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2, configurez l'environnement HADR en suivant les instructions qui figurent dans la documentation DB2. Consultez la rubrique Informations connexes ultérieurement pour connaître les liens vers votre centre de documentation DB2. Vous effectuez ensuite des tâches afin de configurer Network Manager pour qu'il fonctionne avec la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Si vous avez une base de données Oracle, configurez l'environnement Oracle RAC à l'aide des instructions fournies dans la documentation Oracle. Vois les liens connexes plus loin pour un lien vers la documentation Oracle. Vous effectuez ensuite des tâches afin de configurer Network Manager pour qu'il fonctionne dans l'environnement Oracle RAC.

Concepts associés

Architecture de reprise d'ObjectServer
Vous pouvez déployer Tivoli Netcool/OMNIbus par le biais d'une architecture à plusieurs niveaux évolutive afin que le système puisse continuer à fonctionner au maximum de sa capacité (et avec une perte d'événement minimale) en cas d'échec du serveur ObjectServer, de la passerelle ObjectServer ou du serveur proxy.

Reprise en ligne sur l'installation de sauvegarde
Tous les processus de l'installation de secours pointent vers la base de données topologiques NCIM sur l'installation principale. La base de données topologiques NCIM de l'installation principale peut être une base de données autonome ou une base de données configurée pour la haute disponibilité.

A propos de la haute disponibilité de la base de données topologiques NCIM
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une

défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Exemple d'hébergement de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM
Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde.

Tâches associées

Configuration de la reprise en ligne des processus centraux de Network Manager

Configuration des bases de données DB2 existantes sous UNIX
Pour pouvoir utiliser une base de données DB2 existante comme base de données topologiques sous UNIX, vous devez disposer d'une instance DB2 avant d'installer Network Manager.

Configuration de Network Manager pour qu'il fonctionne avec Db2 HADR ou Oracle RAC

Reprise en ligne de la source de données Tivoli Netcool/OMNIbus Web GUI

Interface graphique Web Implémente la reprise en ligne de la source de données. Si des serveurs d'objets principal et de sauvegarde sont disponibles, vous pouvez configurer des connexions vers ces deux serveurs d'objets de sorte que si le serveur d'objets principal échoue, Interface graphique Web procède à une reprise en ligne et utilise le serveur d'objets de sauvegarde comme source pour ses événements.

Tâches associées

Configuration de la reprise en ligne de la source de données pour Tivoli Netcool/OMNIbus Web GUI
Si vous disposez d'une paire de reprise en ligne de serveurs ObjectServer à laquelle doit se connecter Interface graphique Web, vous pouvez configurer la reprise en ligne de la source de données par le biais du fichier de configuration de la source de données `ncwDataSourceDefinitions.xml` dans l'installation de Interface graphique Web.

Allocation de serveur pour la reprise en ligne

Tout système principal doit être installé sur un hôte distinct d'un système de sauvegarde, de sorte que s'il tombe en panne, l'hôte de sauvegarde ne soit pas touché.

Dans l'idéal, le serveur d'objets principal, le serveur d'objets de sauvegarde, le serveur Network Manager principal, le serveur Network Manager de sauvegarde et le serveur Dashboard Application Services Hub devraient être installés sur des hôtes distincts. Toutefois, cela peut s'avérer ne pas être pratique.

Exemple d'hébergement de reprise en ligne sans haute disponibilité de la base de données topologiques NCIM

Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne ne comprend pas de copie de la base de données topologiques NCIM sur l'installation de secours.

Dans toute configuration de reprise en ligne, les domaines Network Manager principal et de secours se connectent à la même base de données, mais dans une configuration de reprise en ligne sans haute disponibilité de la base de données topologiques NCIM, la base de données n'est pas répliquée sur un serveur de secours.

La figure suivante présente un exemple de serveur d'objets d'hébergement et une reprise en ligne Network Manager utilisant quatre machines hôtes.

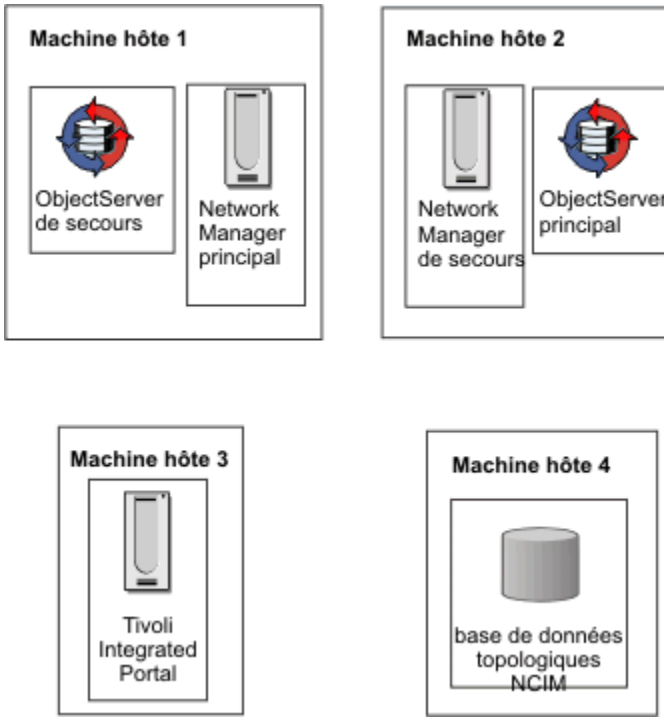

Figure 9. Exemple d'hébergement de reprise en ligne

Pour des questions de performance, la base de données topologiques NCIM doit être connectée au serveur Dashboard Application Services Hub via une liaison à large bande. Si la machine hôte 3 dispose de plusieurs unités centrales et de suffisamment de mémoire, vous pouvez y installer NCIM.

Installez les composants principaux sur les deux machines hôte 1 et 2 et installez les applications Web sur la machine hôte 3. Installez la base de données topologique NCIM sur la machine hôte 4.

Remarque : Si vous implémentez la reprise en ligne, vous devez veiller à ce que l'installation principale et celle de secours utilisent des clés de chiffrement identiques. Si les clés de chiffrement ne sont pas identiques, l'interrogateur de secours ne fonctionne pas correctement pendant la reprise en ligne. Pour garantir que l'installation principale et celle de secours utilisent des clés de chiffrement identiques, copiez le fichier suivant depuis le serveur principal vers le même emplacement sur le serveur de secours : `$NCHOME/etc/security/keys/conf.key`. Si vous entrez tous les noms de communauté SNMP en ligne de commande sans les chiffrer, vous n'avez pas besoin d'effectuer cette tâche. Pour plus d'informations sur la modification de la clé de chiffrement, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*. De plus, pour mettre à jour les mots de passe NCIM et ObjectServer, utilisez le script Perl `ncp_password_update.pl`. Pour plus d'informations sur le script Perl `ncp_password_update.pl`, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Concepts associés

A propos de la haute disponibilité de la base de données topologiques NCIM

Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Exemple d'hébergement de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM

Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde.

Exemple d'hébergement de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM

Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde.

Dans toute configuration de reprise en ligne, les domaines Network Manager principal et de secours se connectent à la même base de données, mais dans une configuration de reprise en ligne dans laquelle la haute disponibilité de la base de données est configurée, la base de données est répliquée sur le serveur de base de données de secours.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

La figure suivante présente un exemple de serveur d'objets d'hébergement et une reprise en ligne Network Manager utilisant cinq machines hôtes.

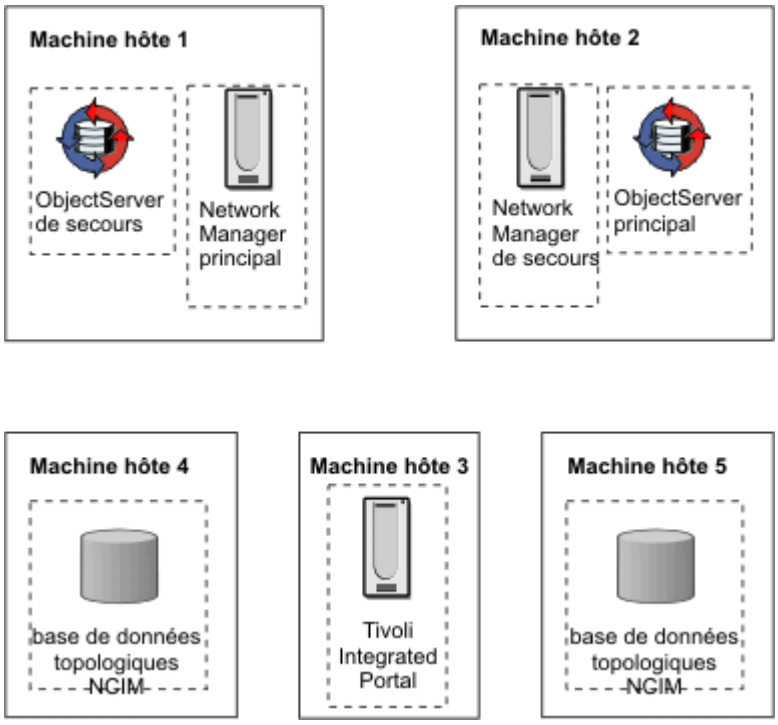

Figure 10. Exemple d'hébergement de reprise en ligne avec base de données topologiques NCIM de secours

Pour des questions de performance, la base de données topologiques NCIM doit être connectée au serveur Dashboard Application Services Hub via une liaison à large bande. Si la machine hôte 3 dispose de plusieurs unités centrales et de suffisamment de mémoire, vous pouvez y installer la base de données NCIM principale.

Installez les composants principaux sur les deux machines hôte 1 et 2 et installez les applications Web sur la machine hôte 3. Installez la base de données topologiques primaire NCIM sur la machine hôte 4 et la base de données topologique NCIM de sauvegarde sur la machine hôte 5.

Concepts associés

Reprise en ligne sur l'installation de sauvegarde
Tous les processus de l'installation de secours pointent vers la base de données topologiques NCIM sur l'installation principale. La base de données topologiques NCIM de l'installation principale peut être une base de données autonome ou une base de données configurée pour la haute disponibilité.

Exemple d'hébergement de reprise en ligne sans haute disponibilité de la base de données topologiques NCIM
Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne ne comprend pas de copie de la base de données topologiques NCIM sur l'installation de secours.

Architecture de reprise en ligne Network Manager (processus centraux)
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

A propos de la haute disponibilité de la base de données topologiques NCIM
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Opération de reprise en ligne des processus centraux de Network Manager

La reprise en ligne des processus Network Manager centraux est gérée par le processus de domaine virtuel, **ncp_virtualdomain**. Utilisez ces informations pour comprendre comment la reprise en ligne et la reprise par restauration de Network Manager sont déclenchées.

Evénements de vérification d'intégrité et reprise en ligne

La reprise en ligne est pilotée par les vérifications d'intégrité qui sont configurées pour s'exécuter périodiquement pour évaluer l'intégrité des domaines Network Manager principal et de secours.

Dans l'environnement de reprise en ligne, tous les processus des domaines principal et de secours sont démarrés par le contrôleur de processus maître, **ncp_ctrl**. Dans chaque domaine, **ncp_ctrl** surveille aussi régulièrement les processus qu'il contrôle et stocke leur statut dans la table state.services. Le processus de domaine virtuel applique des filtres (qui sont définis dans la table state.filters) aux enregistrements d'états de certains des processus, et génère des événements de vérification d'intégrité pour indiquer si un domaine est en état d'intégrité. Les filtres sont appliqués à :

- **ncp_poller**, le moteur d'interrogation

  Plusieurs filtres peuvent être définis pour le moteur d'interrogation, un pour chaque interrogateur défini dans le fichier `CtrlServices.cfg`.
- **ncp_g_event**, la passerelle d'événements
- **ncp_model**, le gestionnaire de topologie

Des événements de vérification d'intégrité sont générés localement dans chaque domaine et peuvent également être générés à distance par un domaine au nom de l'autre domaine :

- Domaine Local : Si tous les enregistrements de statut passent les filtres, le serveur Network Manager est considéré comme intègre et le Virtual Domain génère un événement de résolution de vérification d'intégrité pour ce domaine. Chaque domaine indique à l'autre domaine qu'il est intègre en envoyant un événement de résolution qui est acheminé via le serveur d'objets. Un domaine s'attend à recevoir un événement de résolution à un intervalle configuré dans le fichier schéma du processus de domaine virtuel (`$NCHOME/etc/precision/VirtualDomainSchema.cfg`).

  Si un ou plusieurs filtres échouent, indiquant l'échec d'un ou de plusieurs processus locaux, le domaine virtuel génère un événement de problème de vérification d'intégrité, et l'achemine vers l'autre domaine.
- Domaine Distant : Si un domaine local détecte que son équivalent distant n'a pas généré d'événement de résolution de vérification d'intégrité dans l'intervalle configuré, le domaine local génère un

événement de problème de vérification d'intégrité synthétique pour le domaine distant. Par exemple, si le domaine de secours ne reçoit pas d'événement de résolution de vérification d'intégrité du domaine principal, le domaine de secours génère un événement de problème de vérification d'intégrité pour le domaine principal.

Des événements de vérification d'intégrité sont également générés lorsque la connectivité avec la base de données NCIM est perdue.

Les événements de vérification d'intégrité comportent l'identificateur d'événement "ItnmHealthChk" dans la zone EventId de la table alerts.status.

Concepts associés

Reprise en ligne et reprise par restauration Network Manager

Tâches associées

Configuration des paramètres pour les vérifications d'intégrité

Si nécessaire, vous pouvez configurer des conditions préférées sous lesquelles les événements de vérification d'intégrité sont générés, en spécifiant des insertions OQL identiques dans le fichier de schéma du processus de domaine virtuel (`VirtualDomainSchema.cfg`) à la fois sur le serveur principal et sur le serveur de sauvegarde.

Flux de processus pour les événements de vérification d'intégrité

Les événements de résolution de vérification d'intégrité sont générés par chaque serveur Network Manager pour indiquer un niveau d'intégrité élevé. Un événement de problème de vérification d'intégrité est l'un des déclencheurs de la reprise en ligne Network Manager.

La figure suivante montre la progression à travers le système d'un événement de vérification d'intégrité généré par le serveur Network Manager principal.

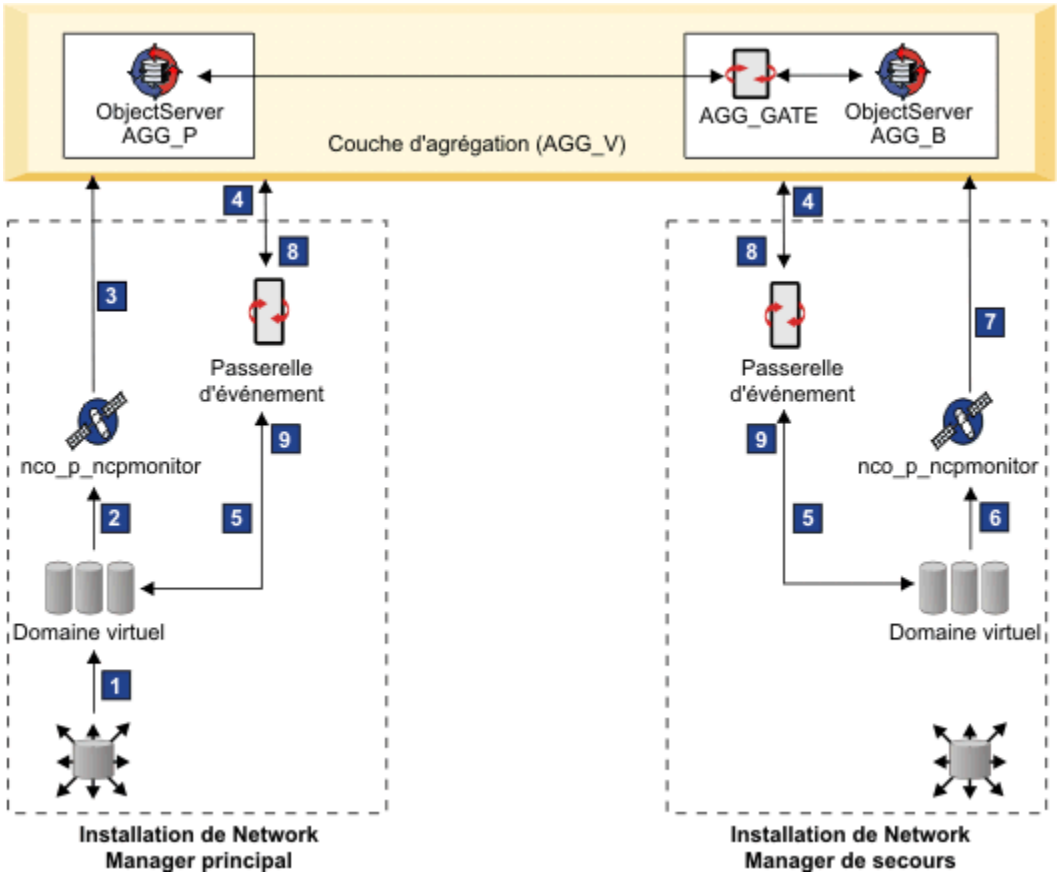

Figure 11. Flux de processus d'un événement de vérification d'intégrité

1 Rapport de statut

Le processus **ncp_ctrl** signale l'état de ses services gérés.

2 Diagnostic d'intégrité
Le processus de domaine virtuel utilise ses filtres pour effectuer un diagnostic de vérification d'intégrité :

- Si le système est dans un état de bonne intégrité, le domaine virtuel génère un événement de résolution de vérification d'intégrité et l'envoie à la Sonde pour Tivoli Netcool/OMNIbus. Par défaut, les événements de vérification d'intégrité sont envoyés à la sonde toutes les 60 secondes.
- Si le système est dans un état de faible intégrité, le domaine virtuel génère un événement de problème de vérification d'intégrité et l'envoie à la Sonde pour Tivoli Netcool/OMNIbus.

3 Evénement de vérification d'intégrité envoyé au serveur ObjectServer
La Sonde pour Tivoli Netcool/OMNIbus fait suivre l'événement de vérification d'intégrité au serveur ObjectServer.

4 Evénement de vérification d'intégrité envoyé à Event Gateway principal et de sauvegarde
Le serveur ObjectServer envoie l'événement de vérification d'intégrité à la passerelle d'événements des serveursprincipal et de secours.

5 Evénement de vérification d'intégrité renvoyé à Virtual Domain principal et de sauvegarde
La passerelle d'événements principale renvoie l'événement de vérification d'intégrité au domaine virtuel sur le serveur principal. La passerelle d'événements de secours renvoie l'événement de vérification d'intégrité au domaine virtuel sur le serveur de sauvegarde.

Pour un événement de résolution de vérification d'intégrité, le domaine virtuel contrôle l'horodatage de l'événement pour vérifier qu'il n'a pas plus de 5 minutes, puis met à jour la table state.domains pour indiquer que l'intégrité du serveur principal est bonne. (La passerelle d'événements écoute également les événements de vérification d'intégrité sur le serveur de sauvegarde. La table state.domains enregistre l'état en cours des serveurs principal et de secours.)

Pour un événement de problème de vérification d'intégrité, le domaine virtuel met à jour sa table state.domains pour indiquer que l'intégrité du serveur principal est faible. Le domaine virtuel fait passer le serveur de sauvegarde en mode actif, et le serveur principal passe en mode veille.

6 Échec de vérification d'intégrité généré pour le compte du domaine principal
Si le serveur de sauvegarde ne reçoit pas un événement de résolution de vérification d'intégrité provenant du serveur principal dans l'intervalle de temps configuré de 5 minutes, cela indique que le serveur principal ne fonctionne pas correctement ou qu'il existe un problème de communication avec le serveur ObjectServer. Le domaine virtuel de secours envoie un événement de problème de vérification d'intégrité à la Sonde pour Tivoli Netcool/OMNIbus pour le compte du serveur principal. Le domaine virtuel met à jour le tableau state.domains pour indiquer que le niveau d'intégrité du serveur principal est bas.

7, 8, et 9 Reprise déclenchée
La sonde envoie l'événement de problème de vérification d'intégrité au serveur ObjectServer, qui ensuite le fait suivre à la passerelle d'événements sur les serveurs Network Manager principal et de secours :

- La passerelle d'événements du serveur de sauvegarde envoie l'événement de problème de vérification d'intégrité au domaine virtuel, qui bascule ensuite le serveur de sauvegarde en mode actif.
- Si la passerelle d'événements principale est opérationnelle, elle transmet l'événement de problème de vérification d'intégrité au domaine virtuel principal. Si le domaine virtuel est opérationnel, il bascule le serveur principal en mode veille.

Lorsque le serveur de sauvegarde génère un événement de résolution de vérification d'intégrité, le flux de processus est identique à celui du serveur principal. Les événements de résolution de vérification d'intégrité régulièrement mis à jour relatifs aux serveurs principal et de sauvegarde sont conservés sur le serveur ObjectServer et peuvent être affichés à l'aide entre autre de l'**Afficheur d'événements**.

Si l'événement de problème de vérification d'intégrité est généré par le serveur de sauvegarde, pour indiquer que le serveur de sauvegarde est en état d'intégrité faible, les mêmes processus s'appliquent, excepté que le serveur principal n'est pas placé en veille et que le serveur de sauvegarde n'est pas

basculé en mode actif. L'événement de problème vérification d'intégrité pour le serveur de sauvegarde est présent sur le serveur ObjectServer et peut être affiché entre autre via l'**Afficheur d'événements**.

Remarque : La Sonde pour Tivoli Netcool/OMNIbus et la passerelle d'événements des deux domaines doivent être configurées pour accéder au même serveur d'objets afin que les événements de vérification d'intégrité soient acheminés avec succès dans le système.

Reprise en ligne et reprise par restauration Network Manager

La reprise en ligne peut être lancée par le domaine principal ou par le domaine de secours et est déclenchée lorsqu'un problème de vérification d'intégrité est généré pour le domaine principal. La reprise par restauration est déclenchée par un événement de résolution de vérification d'intégrité ultérieur du domaine principal.

Un événement ItnmFailover est généré par **ncp_virtualdomain** lorsqu'un domaine Network Manager fait l'objet d'une reprise en ligne ou d'une reprise par restauration.

Reprise après incident

Lorsqu'une reprise en ligne se produit, le domaine Network Manager principal passe en mode veille (s'il est toujours en cours d'exécution) et le domaine de secours devient actif.

Les modifications suivantes se produisent lorsque le domaine de secours devient actif :

- La passerelle d'événements synchronise les événements avec le serveur ObjectServer.
- Le processus **ncp_poller** rétablit le sondage.
- La passerelle d'événements bascule du filtre de veille (StandbyEventFilter) au filtre d'événements entrants (EventFilter).
- Network Manager continue de surveiller le réseau et effectue une analyse RCA. Toutefois, la reconnaissance du réseau n'est pas effectuée et la topologie de réseau reste statique.

Lorsqu'un serveur Network Manager principal passe en mode veille, les modifications suivantes se produisent :

- La passerelle d'événements bascule du filtre d'événements entrants (StandbyEventFilter) au filtre de veille (EventFilter).
- Le processus **ncp_poller** interrompt toutes les interrogations.

Pour plus d'informations sur le filtre de veille et le filtre d'événements entrants, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Le système de calcul en temps réel Apache Storm qui est utilisé pour agréger les données d'interrogation brutes en données d'interrogation historiques, effectue une reprise de manière différente de celle des autres processus principaux Network Manager. Dans une configuration de reprise en ligne, chaque Network Manager dispose d'un serveur Apache Storm fonctionnel qui procède à l'agrégation des données d'interrogation, mais un seul de ces serveurs Apache Storm à la fois est actif. Lorsqu'un serveur Apache Storm démarre, il consulte la base de données pour déterminer si les données d'interrogation sont déjà traitées par un autre serveur Apache Storm.

- Dans ce cas, le premier serveur Apache Storm passe à l'état de veille.
- Dans le cas contraire, Storm se charge de traiter les données d'interrogation.

Lors de la reprise en ligne, le serveur Apache Storm en cours n'arrête pas le traitement. Le serveur Apache Storm effectue une reprise en ligne uniquement s'il est arrêté par l'utilisateur ou s'il ne peut pas mettre à jour la base de données. Pour plus d'informations sur le fonctionnement de l'agrégation des données d'interrogation dans une configuration Network Manager multiple, consultez le document *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Reprise après incident

Lorsqu'un serveur Network Manager principal en mode veille reprend un fonctionnement normal, il génère un événement de résolution de vérification d'intégrité.

L'événement de résolution de vérification d'intégrité passe à travers le système et le serveur Network Manager restauré devient actif à nouveau.

Lorsque le processus de domaine virtuel du serveur Network Manager de secours reçoit l'événement de résolution de vérification d'intégrité, le domaine virtuel repasse le serveur de sauvegarde en mode veille.

L'automatisation GenericClear du serveur ObjectServer est déclenchée par l'événement de résolution de vérification d'intégrité et efface l'événement de problème de vérification d'intégrité existant.

Concepts associés

Evénements de vérification d'intégrité et reprise en ligne
La reprise en ligne est pilotée par les vérifications d'intégrité qui sont configurées pour s'exécuter périodiquement pour évaluer l'intégrité des domaines Network Manager principal et de secours.

Reprise en ligne sur l'installation de sauvegarde

Tous les processus de l'installation de secours pointent vers la base de données topologiques NCIM sur l'installation principale. La base de données topologiques NCIM de l'installation principale peut être une base de données autonome ou une base de données configurée pour la haute disponibilité.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

La figure ci-dessous présente un exemple d'architecture de reprise en ligne Network Manager, dans laquelle la base de données topologiques NCIM est configurée pour la haute disponibilité.

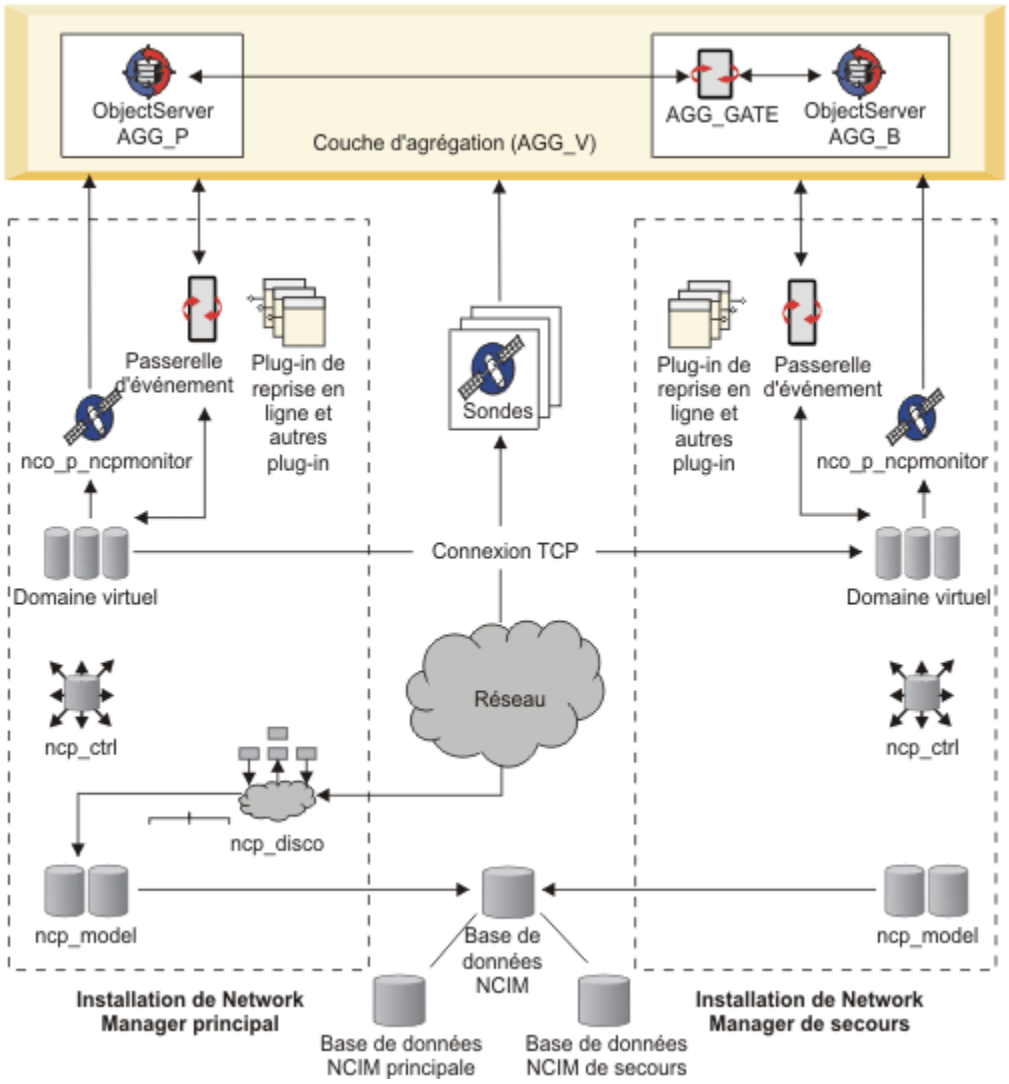

Figure 12. Exemple d'architecture de reprise en ligne avec haute disponibilité NCIM

La figure suivante diffère de la précédente en ce sens que la base de données topologiques NCIM n'est pas configurée pour la haute disponibilité.

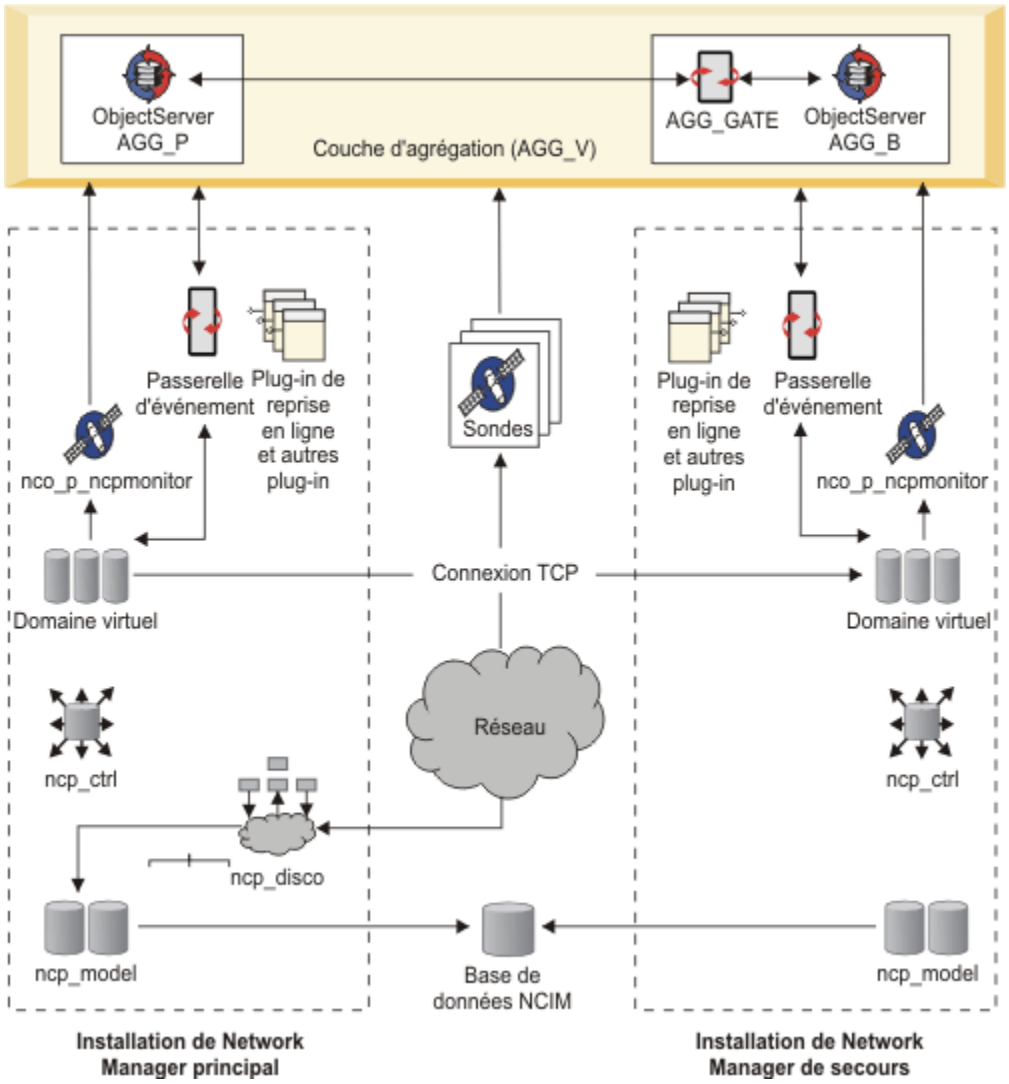

Figure 13. Exemple d'architecture de reprise en ligne sans haute disponibilité NCIM

Reconnaissance
Bien que le moteur de reconnaissance (**ncp_disco**) et le serveur auxiliaire SNMP (**ncp_d_helpserv**) soient en cours d'exécution, le serveur Network Manager de secours n'est pas utilisé pour la reconnaissance de réseau. Lorsque le domaine de secours est actif, la topologie ne change pas.

passerelle d'événements
Lorsque le domaine de secours est en mode veille, la passerelle d'événement n'enrichit pas d'événements sur le serveur ObjectServer. Lorsque le domaine de secours devient actif, la passerelle d'événement bascule du filtre de veille (StandbyEventFilter) au filtre d'événements entrants (EventFilter).

NCIM
Le processus de secours **ncp_model** ne met pas à jour la base de données topologiques NCIM. Le processus **ncp_model** continue cependant à fournir des services de topologie à des processus tels que la passerelle d'événement. La base de données topologiques NCIM utilisée par les vues de réseau et la vue panoramique conserve la version la plus récente de la topologie de réseau jusqu'à la restauration du serveur Network Manager principal et la reprise par restauration du système.

Sondage
Lorsque le domaine de secours est en mode veille, le moteur d'interrogation s'exécute, mais les interrogations sont suspendues. Lorsque le domaine de secours devient actif, son processus

ncp_poller démarre l'interrogation et utilise les détails de la cible SNMP et les règles d'interrogation provenant du domaine principal.

Le processus **ncp_poller** lit la configuration SNMP directement à partir de son fichier de configuration, sans passer par l'auxiliaire SNMP de reconnaissance pour lire ce fichier.

Domaine virtuel
Le composant de domaine virtuel de secours ouvre une connexion socket sur le domaine virtuel du serveur Network Manager principal. Les données topologiques, ainsi que toutes les mises à jour ultérieures de topologie, sont copiées du processus `ncp_model` sur le serveur principal vers le processus **ncp_model** sur le serveur de sauvegarde.

Concepts associés

Architecture de reprise en ligne Network Manager (processus centraux)
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

A propos de la haute disponibilité de la base de données topologiques NCIM
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Exemple d'hébergement de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM
Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde.

Référence associée

Restrictions du processus de reprise en ligne de Network Manager
Plusieurs restrictions s'appliquent au processus de reprise en ligne.

Restrictions du processus de reprise en ligne de Network Manager

Plusieurs restrictions s'appliquent au processus de reprise en ligne.

Le processus de reconnaissance (**ncp_disco**) effectue la reconnaissance de réseau seulement dans le domaine principal.

Le domaine de secours n'est pas utilisé pour la reconnaissance de réseau ; ainsi, lorsque le domaine de secours est actif, ne tentez pas de configurer la reconnaissance. De plus, lorsque le domaine de reconnaissance est actif, n'éditez pas la topologie de réseau reconnue pour ajouter ou supprimer manuellement des périphériques et des connexions.

Les Outils Web ne fonctionnent pas lorsque le serveur de backup est en mode primaire.

Les applications Web ne se connectent pas au serveur de sauvegarde lorsqu'il devient le serveur principal pour une reprise en ligne. Certaines applications Web comme le navigateur MIB SNMP et le générateur de graphe MIB SNMP ne fonctionnent pas quand le serveur de sauvegarde est en mode principal.

Restriction : Network Manager ne prend pas en charge la fonction d'équilibrage de charge Dashboard Application Services Hub gérée par Tivoli Netcool/OMNIbus Web GUI.

Si vous exécutez plusieurs serveurs Dashboard Application Services Hub, ils s'exécutent chacun indépendamment. Si un des serveurs Dashboard Application Services Hub est défaillant, tous les serveurs restants continuent de fonctionner en tant qu'entités individuelles. Pour minimiser l'effet d'un serveur défaillant :

- Une session utilisateur sur un serveur Dashboard Application Services Hub ne peut pas être transférée ou poursuivie sur un autre serveur. En cas d'échec du premier serveur Dashboard Application Services Hub, les utilisateurs doivent se connecter à un autre serveur Dashboard Application Services Hub actif.

- Assurez-vous que chacun des serveurs est configuré avec le même ensemble d'utilisateurs, de rôles, de groupes, de profils de préférences et de ressources telles que les pages, vues, widgets et rapports.
- Configurez les serveurs en fonction des besoins de la haute disponibilité de la base de données. Par exemple, pour DB2, configurez les serveurs en fonction des exigences de la fonction à haut niveau de disponibilité après incident (HADR) DB2. De même, si vous disposez d'une base de données Oracle, vous devez configurer les serveurs en fonction des exigences de la fonction RAC (Real Application Clusters).

Remarque : La reprise en ligne n'est pas prise en charge pour les agents de surveillance ITM dans l'architecture de reprise en ligne de Network Manager.

Tâches associées

Configuration de la reprise en ligne des processus centraux de Network Manager

Configuration de la reprise en ligne

Ces informations vous permettent de configurer la reprise en ligne dans vos installations Network Manager principales et de secours. Des instructions sont également disponibles pour la configuration facultative de la reprise en ligne de l'intégration de produits et de composants. Vous devez utiliser la documentation pour ces produits et références comme premier point de référence.

Avant de commencer

Avant de commencer à configurer la reprise en ligne, déterminez si vous souhaitez implémenter une solution de reprise en ligne complète pour tous les composants ou la repris en ligne pour Network Manager et un sous-ensemble de composants. Décidez également du nombre d'ordinateurs et des options de déploiement.

Pourquoi et quand exécuter cette tâche

Pour la configuration de la reprise en ligne :

Procédure

- Vous devez avoir installé et configuré IBM Tivoli Netcool/OMNIbus. Si vous envisagez d'exécuter un élément ObjectServer principal et de secours en mode de reprise en ligne, vous devez disposer de deux installations ObjectServer.

  Conseil : Si vous utilisez IBM Tivoli Netcool/OMNIbus version 7.3 ou une version ultérieure, avec les fichiers de configuration de reprise en ligne fournis, assurez-vous de respecter les conventions d'attribution nom pour vos éléments ObjectServer et ObjectServer Gateway.
- Vous devez avoir installé une base de données topologiques. Pour la haute disponibilité de la base de données topologiques NCIM, vous avez besoin de deux bases de données topologiques.

  Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

  – Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.

  – Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.
- Vous devez avoir installé et configuré Interface graphique Web et les applications Web Network Manager dans la structure de serveur Dashboard Application Services Hub.
- Vous devez avoir installé les processus centraux de Network Manager sur les serveurs principaux et de secours, sous deux domaines distincts.

Concepts associés

A propos des fichiers de configuration de reprise en ligne Tivoli Netcool/OMNIbus
Tivoli Netcool/OMNIbus Version 7.3 ou ultérieure fournit un ensemble de fichiers de configuration que vous pouvez appliquer aux serveurs ObjectServer et aux passerelles ObjectServer afin d'implémenter une architecture composée de plusieurs couches.

Configuration de la reprise en ligne du serveur ObjectServer

La manière dont vous configurez la reprise en ligne du serveur ObjectServer dépend de la version de Tivoli Netcool/OMNIbus.

Avant de commencer

Dans une installation Tivoli Netcool/OMNIbus, chaque ordinateur sur lequel s'exécutent les composants Tivoli Netcool/OMNIbus doit être configuré avec les informations de communication de serveur qui permettent aux composants de l'architecture de s'exécuter et de communiquer entre eux. Configurez le fichier de données des connexions avec tous les détails de composant, de la manière suivante :

- Linux Mettez à jour les informations de communication pour tous les composants de serveur Tivoli Netcool/OMNIbus dans le déploiement en modifiant manuellement le fichier de données des connexions `$NCHOME/etc/omni.dat` qui est utilisé pour créer le fichier d'interface.

  Une bonne pratique suggérée consiste à ajouter tous les composants dans le déploiement tout entier à un fichier `omni.dat` unique, qui peut ensuite être distribué au répertoire `$NCHOME/etc` sur tous les ordinateurs du déploiement. Vous pouvez ensuite générer les fichiers d'interfaces à partir de chaque ordinateur en exécutant la commande **$NCHOME/bin/nco_igen**. (Les fichiers d'interfaces sont nommés `$NCHOME/etc/interfaces.`*arch*, où *arch* est le nom du système d'exploitation.)

Exemple de configuration pour l'architecture de reprise en ligne de base (couche d'agrégation uniquement)

L'exemple de configuration suivant montre les détails des communications du serveur l'architecture de reprise en ligne de base dans le fichier `$NCHOME/etc/omni.dat`, où :

- AGG_P est le nom du serveur ObjectServer principal.
- AGG_B est le nom du serveur ObjectServer de secours.
- AGG_V est le nom de la paire de serveurs ObjectServer virtuels.
- AGG_GATE est le nom de la passerelle ObjectServer bidirectionnelle.
- NCO_PA représente le nom par défaut pour l'agent de processus. (Si vous avez configuré des agents de processus pour gérer les processus Tivoli Netcool/OMNIbus et pour exécuter des procédures externes, chaque agent de processus nommé de façon unique doit être ajouté avec le nom d'hôte et le numéro de port appropriés.)
- NCO_PROXY représente le nom par défaut pour le serveur proxy. (Si vous avez configuré un ou plusieurs serveurs proxy pour réduire le nombre de connexions de sonde directes aux serveurs ObjectServer, chaque serveur proxy nommé de façon unique doit être ajouté avec le nom d'hôte et le numéro de port appropriés.)

```
[AGG_P]
{
        Primary: primary_host.ibm.com 4100
}

[AGG_B]
{
        Primary: backup_host.ibm.com 4150
}

[AGG_V]
{
        Primary: primary_host.ibm.com 4100
        Backup: backup_host.ibm.com 4150
```

```
}

[AGG_GATE]
{
        Primary: backup_host.ibm.com 4105
}

[NCO_PA]
{
        Primary: primary_host.ibm.com 4200
}

[NCO_PROXY]
{
        Primary: primary_host.ibm.com 4400
}
```

Pour plus d'informations sur la configuration des informations de communication du serveur, les agents de processus et les serveurs proxy, consultez la documentation de Tivoli Netcool/OMNIbus à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Concepts associés

Architecture de reprise d'ObjectServer
Vous pouvez déployer Tivoli Netcool/OMNIbus par le biais d'une architecture à plusieurs niveaux évolutive afin que le système puisse continuer à fonctionner au maximum de sa capacité (et avec une perte d'événement minimale) en cas d'échec du serveur ObjectServer, de la passerelle ObjectServer ou du serveur proxy.

Configuration des serveurs ObjectServer et des passerelles pour la reprise en ligne

Les procédures suivantes indiquent comment configurer la reprise en ligne du serveur ObjectServer dans Tivoli Netcool/OMNIbus.

Pourquoi et quand exécuter cette tâche

«Tivoli Netcool/OMNIbus Version 7.3 ou suivante», à la page 187: Configuration de la reprise en ligne
«Tivoli Netcool/OMNIbus Version 7.2.1 ou antérieure», à la page 188: Configuration de la reprise en ligne

Pour obtenir les informations les plus récentes et complètes sur la reprise en ligne du serveur ObjectServer, voir la documentation Tivoli Netcool/OMNIbus disponible à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html. La documentation Tivoli Netcool/OMNIbus doit être consultée en priorité et prime par rapport aux informations présentées dans la documentation Network Manager.

Tivoli Netcool/OMNIbus Version 7.3 ou suivante

Pourquoi et quand exécuter cette tâche

Pour configurer la reprise en ligne :

Procédure

1. Si nécessaire, créez l'ObjectServer AGG_P d'agrégation principal sur l'ordinateur désigné et appliquez la personnalisation SQL en exécutant la commande **nco_dbinit** avec le fichier d'importation `aggregation.sql` fourni :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server AGG_P -customconfigfile $NCHOME/
   omnibus/extensions/multitier/objectserver/aggregation.sql
   ```

   Si l'ObjectServer est déjà installé et en cours d'exécution, appliquez à celui-ci le fichier d'importation `aggregation.sql` de la manière suivante :

   Linux
   ```
   $NCHOME/omnibus/bin/nco_sql -server AGG_P -user user_name –password
   password < $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```
2. Démarrez l'ObjectServer principal (si nécessaire) :

```
$NCHOME/omnibus/bin/nco_objserv -name AGG_P &
```

Si vous avez installé Tivoli Netcool/OMNIbus à l'aide du programme d'installation de Network Manager, vous pouvez aussi exécuter la commande **itnm_start** dans le répertoire $NCHOME/precision/bin :

Linux
```
itnm_start nco
```

3. Créez (ou mettez à jour) l'ObjectServer AGG_B d'agrégation de sauvegarde sur un autre ordinateur et appliquez la personnalisation SQL, comme indiqué à l'étape «1», à la page 187.

   Lorsque vous appliquez la personnalisation SQL, la propriété **BackupObjectServer** est définie automatiquement sur TRUE et les automatisations requises par l'ObjectServer de sauvegarde sont activées.
4. Démarrez l'ObjectServer de sauvegarde (si nécessaire), comme indiqué à l'étape «2», à la page 187.
5. Sur l'ordinateur sur lequel l'ObjectServer de sauvegarde est installé, configurez la passerelle ObjectServer d'agrégation bidirectionnelle AGG_GATE :
   a) Copiez les fichiers de propriétés composés de plusieurs couches pour la passerelle à partir de l'emplacement $NCHOME/omnibus/extensions/multitier/gateway vers l'emplacement par défaut ($NCHOME/omnibus/etc) où sont contenus les fichiers de configuration et de propriétés :
      - AGG_GATE.map
      - AGG_GATE.props
      - AGG_GATE.tblrep.def

   b) Démarrez la passerelle AGG_GATE :

      ```
      $NCHOME/omnibus/bin/nco_g_objserv_bi -propsfile $NCHOME/omnibus/etc/
      AGG_GATE.props &
      ```

Tivoli Netcool/OMNIbus Version 7.2.1 ou antérieure

Pourquoi et quand exécuter cette tâche

Pour configurer la reprise en ligne :

Procédure

1. Si ce n'est déjà fait, créez l'ObjectServer principal sur l'ordinateur désigné en exécutant la commande **nco_dbinit** :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server nom_serveur
   ```

   où *nom_serveur* est le nom désigné, par exemple NETCOOLPRI.
2. Démarrez l'ObjectServer principal (si nécessaire) :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name server_name &
   ```
3. Si ce n'est déjà fait, créez l'ObjectServer de sauvegarde sur un autre ordinateur, comme indiqué à l'étape «1», à la page 188.
4. Configurez l'ObjectServer de sauvegarde en modifiant son fichier de propriétés ($NCHOME/omnibus/etc/*nom_serveur*.props) et définissez la propriété **BackupObjectServer** sur True.
5. Démarrez l'ObjectServer de sauvegarde, comme indiqué à l'étape «2», à la page 188.
6. Sur l'ordinateur sur lequel l'ObjectServer de sauvegarde est installé, configurez la passerelle ObjectServer d'agrégation bidirectionnelle to_alert de sorte qu'elle échange des données d'alerte entre les ObjectServers principal et de sauvegarde :
   a) Créez le répertoire $NCHOME/omnibus/gates/*nom_passerelle* pour les fichiers de configuration de passerelle.
   b) Copiez tous les fichiers dans $NCHOME/omnibus/gates/objserv_bi vers le répertoire $NCHOME/omnibus/gates/*nom_passerelle*.

c) Renommez le fichier $NCHOME/omnibus/gates/*nom_passerelle*/objserv_bi.map en *nom_passerelle*.map.

d) Renommez le fichier $NCHOME/omnibus/gates/*nom_passerelle*/objserv_bi.props en *nom_passerelle*.props.

e) Modifiez les entrées suivantes dans le fichier *gateway_name*.props :

```
# Propriétés communes Netcool/OMNIbus.
MessageLog         : '$OMNIHOME/log/gateway_name.log'

# Propriétés communes Gateway.
Gate.MapFile         : '$OMNIHOME/gates/gateway_name/gateway_name.map'
Gate.StartupCmdFile     : '$OMNIHOME/gates/gateway_name/objserv_bi.startup.cmd'

# Bidirectional ObjectServer Gateway Properties.
Gate.ObjectServerA.Server     : 'primary_ObjectServer'
Gate.ObjectServerA.Username     : 'user_name'
Gate.ObjectServerA.Password     : 'password'
Gate.ObjectServerA.TblReplicateDefFile:
   '$OMNIHOME/gates/gateway_name/objserv_bi.objectservera.tblrep.def'

Gate.ObjectServerB.Server     : 'backup_ObjectServer'
Gate.ObjectServerB.Username     : 'user_name'
Gate.ObjectServerB.Password     : 'password'
Gate.ObjectServerB.TblReplicateDefFile:
   '$OMNIHOME/gates/gateway_name/objserv_bi.objectserverb.tblrep.def'
```

Remplacez *nom_passerelle* par le nom affecté à la passerelle, *primary_ObjectServer* et *backup_ObjectServer* par les noms ObjectServer, et indiquez le nom d'utilisateur et le mot de passe pour la connexion aux ObjectServers.

f) Copiez le fichier $NCHOME/omnibus/gates/*nom_passerelle*/*nom_passerelle*.props vers $NCHOME/omnibus/etc/*nom_passerelle*.props.

g) Démarrez la passerelle :

```
$NCHOME/omnibus/bin/nco_g_objserv_bi &
```

Connexion à une paire de reprise en ligne ObjectServer

Chaque installation Network Manager qui se connecte à un serveur ObjectServer doit disposer d'une copie du fichier d'interfaces .

Pourquoi et quand exécuter cette tâche

En supposant que les informations de communication de serveur ont été configurées dans vos installations Tivoli Netcool/OMNIbus, le fichier $NCHOME/etc/interfaces.*arch* (où *arch* représente le nom du système d'exploitation) doit être disponible à l'emplacement d'installation NCHOME.

Procédure

- Lorsque Tivoli Netcool/OMNIbus est installé sur le même serveur que Network Manager, ils doivent tous deux être installés dans le même emplacement NCHOME. Dans ce cas, aucune action supplémentaire n'est requise pour garantir que les processus Network Manager peuvent se connecter à une paire de reprise en ligne ObjectServer.
- Si Network Manager et Tivoli Netcool/OMNIbus sont installés sur des serveurs différents, effectuez les opérations suivantes sur les serveurs Network Manager principal et de secours.

  Copiez le fichier $NCHOME/etc/interfaces.*arch* de l'emplacement NCHOME de Tivoli Netcool/OMNIbus vers l'emplacement d'installation NCHOME sur le serveur sur lequel Network Manager est installé.

  Pour plus d'informations sur la configuration des informations de communication du serveur et savoir comment générer le fichier Tivoli Netcool/OMNIbus interfaces.*arch* file, voir la documentation de http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html à l'adresseTivoli Netcool/OMNIbus.

Remarque : Le nom de la paire virtuelle ObjectServer doit être spécifié dans le fichier `ConfigItnm.DOMAINE.cfg`.

Tâches associées

Configuration de la reprise en ligne du serveur ObjectServer
La manière dont vous configurez la reprise en ligne du serveur ObjectServer dépend de la version de Tivoli Netcool/OMNIbus.

Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg
Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde.

Configuration de la reprise en ligne de la source de données pour Tivoli Netcool/OMNIbus Web GUI

Si vous disposez d'une paire de reprise en ligne de serveurs ObjectServer à laquelle doit se connecter Interface graphique Web, vous pouvez configurer la reprise en ligne de la source de données par le biais du fichier de configuration de la source de données `ncwDataSourceDefinitions.xml` dans l'installation de Interface graphique Web.

Pourquoi et quand exécuter cette tâche

Ce fichier se trouve dans *rép_base_interface_web*`/etc/datasources`, où *rép_base_interface_web* est le répertoire d'installation de Interface graphique Web ; par exemple, `$NCHOME/omnibus_webgui`.

Pour configurer la reprise en ligne de la source de données :

Procédure

1. Sur le serveur Dashboard Application Services Hub où Interface graphique Web est installée, modifiez comme suit le fichier de configuration de la source de données :
   a) Utilisez l'attribut name de l'élément <ncwDataSourceEntry> pour spécifier l'étiquette pour la paire de reprise de ObjectServers ; par exemple, `VirtualObjectServerPair`.
   b) Définissez les détails de connexion pour les ObjectServers principal et de sauvegarde en utilisant l'élément <ncwDataSourceDefinition> et ses éléments enfant.

      Remarque : Les valeurs de l'attribut name des deux éléments <ncwDataSourceEntry> et <ncwDataSourceDefinition> doivent être identiques. Vous devez aussi définir les connexions ObjectServer en utilisant les noms d'hôte et les numéros de port plutôt que les noms de serveur ObjectServer qui sont configurés dans le fichier `omni.dat` ou `sql.ini`.

      Pour un exemple de la configuration requise, voir l'exemple de code dans «Exemple de configuration ncwDataSourceDefinitions.xml pour la reprise en ligne de la source de données», à la page 191.
   c) Redémarrez le serveur Dashboard Application Services Hub pour que les modifications soient prises en compte.

      Utilisez la commande suivante :

      - Linux `startServer.sh server1`

      Pour obtenir les informations les plus récentes et complètes sur la configuration de la reprise en ligne de la source de données dans Interface graphique Web, voir la documentation Interface graphique Web à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

      La documentation Interface graphique Web doit être consultée en priorité et prime par rapport aux informations présentées dans la documentation Network Manager.
2. Vous pouvez également définir la valeur WebTopDataSource dans le fichier `ModelNcimDb.domain_name.cfg` avec la même valeur que <ncwDataSourceEntry> est défini dans

le fichier ncwDataSourceDefinitions.xml. En utilisant les paramètres dans «Exemple de configuration ncwDataSourceDefinitions.xml pour la reprise en ligne de la source de données», à la page 191, l'exemple suivant indique les modifications que vous devez apporter :

a) Accédez au fichier NCHOME/etc/precision/ModelNcimDb.*nom_domaine*.cfg et ouvrez-le afin de le modifier.

b) Recherchez l'insertion qui définit WebTopDataSource :

```
insert into dbModel.access
(
EnumGroupFilter,
TransactionLength,
ValidateCacheFile,
WebTopDataSource
)
values
(
"enumGroup in ('ifAdminStatus', 'ifOperStatus', 'sysServices', 'ifType',
'cefcFRUPowerAdminStatus', 'cefcFRUPowerOperStatus', 'TruthValue',
'entSensorType', 'entSensorScale', 'entSensorStatus',
'cefcModuleAdminStatus', 'cefcModuleOperStatus', 'ipForwarding',
'cefcPowerRedundancyMode', 'EntityType', 'ospfIfState', 'ospfIfType',
'dot3StatsDuplexStatus', 'accessProtocol')",
500,
0,
"OS"
);
```

c) Changez la valeur WebTopDataSource dans l'interrogation d'insertion suivante pour correspondre à la source de données configurée dans <ncwDataSourceEntry> (dans ce cas, changez la valeur 0S to VirtualObjectServerPair):

```
insert into dbModel.access
(
EnumGroupFilter,
TransactionLength,
ValidateCacheFile,
WebTopDataSource
)
values
(
"enumGroup in ('ifAdminStatus', 'ifOperStatus', 'sysServices', 'ifType',
'cefcFRUPowerAdminStatus', 'cefcFRUPowerOperStatus', 'TruthValue',
'entSensorType', 'entSensorScale', 'entSensorStatus',
'cefcModuleAdminStatus', 'cefcModuleOperStatus', 'ipForwarding',
'cefcPowerRedundancyMode', 'EntityType', 'ospfIfState', 'ospfIfType',
'dot3StatsDuplexStatus', 'accessProtocol')",
500,
0,
"VirtualObjectServerPair"
);
```

Remarque : Le nom de la source de données de Interface graphique Web correspond à celui de la connexion et il est identique à celui défini dans Interface graphique Web. Le nom peut ne pas toujours être identique à celui du serveur ObjectServer.

d) Effectuez cette modification à la fois sur les serveurs Network Manager centraux principal et de sauvegarde.

e) Redémarrez ncp_ctrl.

Exemple de configuration ncwDataSourceDefinitions.xml pour la reprise en ligne de la source de données

Dans l'exemple de code suivant, le texte en gras indique les valeurs qui sont applicables à la reprise en ligne de la source de données.

```
<ncwDefaultDataSourceList>
    <ncwDataSourceEntry name="VirtualObjectServerPair"/>
</ncwDefaultDataSourceList>

...

<ncwDataSourceDefinition type="singleServerOSDataSource" name="VirtualObjectServerPair" enabled="true">
```

```
    <ncwFailOverPairDefinition>
        <!--
         ! The primary ObjectServer to connect to.
         ! - host : The hostname or IP address of the server the ObjectServer is installed on.
         ! - port : The port number the ObjectServer is listening on.
         ! - ssl  : Enables SSL connection to the ObjectServer. [false|true]
         ! - minPoolSize : Specifies the minimum number of connections that will be added to the connection pool.
Default value is 5.
         ! - maxPoolSize : Specifies the maximum number of connections that will be added to the connection pool.
Default value is 10.
         !-->
        <ncwPrimaryServer>
            <ncwOSConnection host="AGG_P_hostname" port="AGG_P_port" ssl="false" minPoolSize="5" maxPoolSize="10"/>
        </ncwPrimaryServer>
        <!--
         ! The optional failover ObjectServer to connect to.
         !-->
        <ncwBackUpServer>
            <ncwOSConnection host="AGG_B_hostname" port="AGG_B_port" ssl="false" minPoolSize="5" maxPoolSize="10"/>
        </ncwBackUpServer>
</ncwFailOverPairDefinition>

</ncwDataSourceDefinition>
```

Configuration de l'authentification du serveur ObjectServer

Si vous utilisez un serveur ObjectServer comme registre d'utilisateurs central pour la gestion et l'authentification des utilisateurs, et que vous voulez que le serveur ObjectServer soit dans un référentiel fédéré, vous devez utiliser le script fourni avec Dashboard Application Services Hub pour configurer l'adaptateur VMM (Virtual Member Manager) pour le serveur ObjectServer. Configurez l'adaptateur pour les deux serveurs ObjectServer de la paire de reprise en ligne.

Pourquoi et quand exécuter cette tâche

Sur chaque serveur Dashboard Application Services Hub où les applications Web Network Manager et Interface graphique Web sont installés :

Procédure

1. Accédez au répertoire `$WAS_HOME/bin`.
2. Entrez la commande suivante sur la ligne de commande :

   `./confvmm4ncos` *`rép_profil_jazzsm utilisateur mot de passe adresse port adresse2 port2`*

   Où :

   - *rép_profil_jazzsm* est le répertoire de profil Jazz for Service Management.
   - *utilisateur* est l'ID d'un utilisateur disposant de droits d'administration pour les serveurs ObjectServer.
   - *mot_de_passe* est le mot de passe pour l'ID utilisateur.
   - *adresse* est l'adresse IP du serveur ObjectServer principal.
   - *port* est le numéro de port utilisé par le serveur ObjectServer principal.
   - *adresse2* est l'adresse IP du serveur ObjectServer ObjectServer de sauvegarde.
   - *port2* est le numéro de port utilisé par le serveur ObjectServer de sauvegarde.
3. Redémarrez le serveur Dashboard Application Services Hub.

Configuration de la reprise en ligne des processus centraux de Network Manager

Vous pouvez configurer la reprise en ligne des processus centraux de Network Manager à l'aide du fichier `$NCHOME/etc/precision/ConfigItnm.cfg` pour activer la reprise en ligne.

Vous devez aussi utiliser le fichier `$NCHOME/etc/precision/ServiceData.cfg` pour configurer une connexion de socket TCP entre les domaines Network Manager principal et de secours.

Concepts associés

Architecture de reprise en ligne Network Manager (processus centraux)
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg

Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde.

Pourquoi et quand exécuter cette tâche

Le contenu du fichier `ConfigItnm.DOMAINE.cfg` doit être identique sur les serveurs de domaine principal et de secours.

Pour configurer la reprise en ligne à l'aide du fichier `ConfigItnm.DOMAINE.cfg` :

Procédure

1. Sur le serveur Network Manager principal, éditez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAINE_PRINCIPAL.cfg` comme suit :
   a) Activez la reprise en ligne et spécifiez les noms de domaine virtuel, de secours et principal pour les processus Network Manager. Vous pouvez insérer les valeurs requises dans la table `itnmDomain.failover` en modifiant la section suivante dans le fichier :

```
insert into itnmDomain.failover
(
    FailoverEnabled,
    PrimaryDomainName,
    BackupDomainName,
    VirtualDomainName
)
values
(
    0,
    "NCOMS_P",
    "NCOMS_B",
    "NCOMS_V"
);
```

   Renseignez la section `values` comme suit, dans l'ordre indiqué :

Colonne	Valeur requise
`FailoverEnabled`	Spécifiez `1` pour activer la reprise en ligne pour les domaines principal et de secours. La valeur par défaut `0` signifie que la reprise en ligne est désactivée.
`PrimaryDomainName`	Remplacez `NCOMS_P` par le nom réel du domaine principal Network Manager dans la paire de reprise en ligne. **Remarque :** Le nom de domaine principal `PrimaryDomainName` est le seul stocké dans NCIM et par conséquent, le seul nom qui s'affiche dans l'interface graphique. Le nom de domaine de secours n'est pas utilisé dans NCIM et il n'apparaît donc pas dans l'interface graphique.

Colonne	Valeur requise
BackupDomainName	Remplacez NCOMS_B par le nom réel du domaine principal de secours Network Manager dans la paire de reprise en ligne.
VirtualDomainName	Remplacez NCOMS_V par un nom désigné pour le domaine virtuel Network Manager dans la paire de reprise en ligne.

b) Spécifiez le nom d'ObjectServer auquel la Sonde pour Tivoli Netcool/OMNIbus et la passerelle d'événement se connecteront. Insérez la valeur requise dans la table itnmDomain.objectServer en modifiant la section suivante dans le fichier :

```
insert into itnmDomain.objectServer
(
    ServerName
)
values
(
    "NCOMS"
);
```

Renseignez la section values de la manière suivante :

Colonne	Valeur requise
ServerName	Si vous utilisez Tivoli Netcool/OMNIbus version 7.3 ou suivante, et que vous avez configuré la reprise en ligne du serveur d'objets ObjectServer en utilisant les fichiers de configuration comportant plusieurs couches fournis et les conventions de dénomination pour la configuration composée de plusieurs couches, spécifiez AGG_V comme nom de la paire d'agrégation virtuelle. La valeur initiale indiquée est soit le nom du serveur d'objets ObjectServer installé par le programme d'installation Network Manager, soit NCOMS si aucun serveur ObjectServer n'a été installé. Pour des versions antérieures de Tivoli Netcool/OMNIbus, spécifiez le nom de remplacement défini pour la paire virtuelle ObjectServer. Si la reprise en ligne d'ObjectServer n'est pas configurée, spécifiez le nom de l'ObjectServer unique utilisé.

Remarque : Aucune configuration de reprise en ligne supplémentaire n'est requise dans le fichier des propriétés d'analyse. Les paramètres de propriétés d'analyse par défaut fournissent la prise en charge appropriée pour la reprise en ligne lors de l'exécution de l'analyse.

2. Enregistrez le fichier.
3. Copiez le contenu entier du fichier $NCHOME/etc/precision/ConfigItnm.*DOMAINE_PRINCIPAL*.cfg du serveur principal vers le fichier $NCHOME/etc/precision/ConfigItnm.*DOMAINE_SECOURS*.cfg du serveur de secours.

Configuration de la connexion de socket TCP entre les domaines

Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées dans le domaine de secours.

Pourquoi et quand exécuter cette tâche

Pour configurer la connexion TCP :

Procédure

1. Sur le serveur principal Network Manager, démarrez manuellement le processus **ncp_virtualdomain** à partir du répertoire $NCHOME/precision/bin :

   ncp_virtualdomain -domain *PRIMARYDOMAIN_NAME*

   Lorsque le processus **ncp_virtualdomain** démarre pour la première fois, il écrit une ligne dans le fichier $NCHOME/etc/precision/ServiceData.cfg qui contient les informations de connexion TCP et multidiffusion pour les processus Network Manager. Cette ligne fait référence à ncp_virtualdomain et inclut le port sur lequel le composant Virtual Domain du serveur principal accepte les connexions TCP depuis le serveur de sauvegarde. Par exemple :

   ```
   SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ADDRESS: 127.123.209.55 PORT: 1234
    SERVERNAME: myhostname DYNAMIC: NON
   ```

   Conseil : Le paramètre DYNAMIC:NO force le processus **ncp_virtualdomain** à utiliser le même port et la même adresse lors de son prochain démarrage.
2. Enregistrez le fichier.
3. Arrêtez le processus **ncp_virtualdomain**.
4. Copie la ligne SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ... depuis le fichier $NCHOME/etc/precision/ServiceData.cfg sur le serveur primaire dans le fichier $NCHOME/etc/precision/ServiceData.cfg sur le serveur de sauvegarde. Veilliez à ce qu'une seule ligne SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ... soit présente dans le fichier.

   Important : La ligne SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ... dans le fichier $NCHOME/etc/precision/ServiceData.cfg dans les deux domaines.

   Pour plus d'informations sur la communication inter-processus et le fichier ServiceData.cfg, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Tâches associées

Définition d'un port fixe pour la connexion de socket TCP
Pour éviter des problèmes de pare-feu ou des conflits de port, vous pouvez définir un port fixe pour la connexion de socket TCP qui permet au processus Virtual Domain sur le serveur de sauvegarde d'établir une connexion au processus sur le serveur principal.

Définition d'un port fixe pour la connexion de socket TCP

Pour éviter des problèmes de pare-feu ou des conflits de port, vous pouvez définir un port fixe pour la connexion de socket TCP qui permet au processus Virtual Domain sur le serveur de sauvegarde d'établir une connexion au processus sur le serveur principal.

Pourquoi et quand exécuter cette tâche

Lors du démarrage initial, le processus **ncp_virtualdomain** sur le serveur principal ajoute une ligne au fichier NCHOME/etc/precision/ServiceData.cfg avec des informations sur ses détails de connexion, incluant le numéro de port. Pour définir un port fixe, vous devez remplacer le numéro de port initial par votre valeur requise.

Pour configurer un port fixe pour la reprise en ligne :

Procédure

1. Modifiez le fichier $NCHOME/etc/precision/ServiceData.cfg sur le serveur principal, en procédant comme suit :
   a) Recherchez la ligne qui référence ncp_virtualdomain.
   Par exemple:

   ```
   SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ADDRESS: 127.123.209.55
    PORT: 1234 SERVERNAME: myhostname DYNAMIC: NON
   ```

Dans cet exemple, le processus **ncp_virtualdomain** accepte les connexions du serveur de sauvegarde sur le port 1234.

b) Modifiez le paramètre PORT en le définissant à la valeur requise.

c) Notez le numéro de port puis enregistrez et fermez le fichier `ServiceData.cfg`.

2. Sur le serveur de sauvegarde, modifiez le fichier `$NCHOME/etc/precision/ServiceData.cfg` en mettant à jour le numéro de port spécifié sur la ligne qui référence `ncp_virtualdomain`.

   Important : Cette ligne du fichier `$NCHOME/etc/precision/ServiceData.cfg` doit être identique dans les deux domaines.

   Pour plus d'informations sur le fichier `ServiceData.cfg`, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Tâches associées

Configuration de la connexion de socket TCP entre les domaines
Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées dans le domaine de secours.

Passage à la configuration de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM

Vous pouvez modifier une architecture de reprise en ligne existante afin d'inclure la haute disponibilité de la base de données topologiques NCIM.

Pourquoi et quand exécuter cette tâche

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Pour configurer la haute disponibilité de la base de données topologiques NCIM :

Procédure

1. Configurez la haute disponibilité de la base de données topologiques NCIM en utilisant la fonction de haute disponibilité fournie par la base de données prise en charge.

   DB2 Si vous disposez d'une base de données DB2, suivez les procédures décrites dans la documentation DB2 afin de définir la configuration de reprise en ligne pour la base de données topologiques NCIM avec la fonction de reprise à haut niveau de disponibilité après incident (HADR). Consultez la rubrique Informations connexes ultérieurement pour connaître les liens vers votre centre de documentation DB2.

   Oracle Si vous disposez d'une base de données Oracle, suivez les procédures décrites dans la documentation Oracle pour configurer l'environnement RAC (Real Application Clusters) à haute disponibilité. A l'aide d'Oracle RAC, vous pouvez créer une configuration de haute disponibilité pour votre base de données topologiques NCIM. Pour plus d'informations sur l'installation et la configuration d'Oracle RAC, voir Informations connexes plus loin pour un lien vers la documentation Oracle.

2. Configurez Network Manager pour qu'il fonctionne avec la base de données prise en charge, comme décrit dans «Configuration de Network Manager pour qu'il fonctionne avec Db2 HADR ou Oracle RAC», à la page 197.

Concepts associés

A propos de la haute disponibilité de la base de données topologiques NCIM
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Tâches associées

Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg
Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde.

Configuration de Network Manager pour qu'il fonctionne avec Db2 HADR ou Oracle RAC

Configuration de Network Manager pour qu'il fonctionne avec Db2 HADR ou Oracle RAC

Vous pouvez configurer les processus centraux de Network Manager en vue de l'utilisation du catalogue DB2 et de l'interface graphique Network Manager pour qu'ils fonctionnent dans l'environnement de reprise à haut niveau de disponibilité après incident (HADR) de DB2. De la même manière, vous pouvez également configurer les processus principaux de Network Manager et l'interface graphique de Network Manager pour qu'ils fonctionnent dans l'environnement RAC (Real Application Clusters) d'Oracle.

DB2 Pour obtenir de l'aide sur les meilleures pratiques d'implémentation d'une solution à haute disponibilité à l'aide de Db2 HADR, reportez-vous à la rubrique *IBM Db2 High Availability for Tivoli Netcool products - Best Practices*, à l'adresse https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Netcool%20OMNIbus/page/Best%20Practices.

Remarque : Si vous implémentez la reprise en ligne, vous devez veiller à ce que l'installation principale et celle de secours utilisent des clés de chiffrement identiques. Si les clés de chiffrement ne sont pas identiques, l'interrogateur de secours ne fonctionne pas correctement pendant la reprise en ligne. Pour garantir que l'installation principale et celle de secours utilisent des clés de chiffrement identiques, copiez le fichier suivant depuis le serveur principal vers le même emplacement sur le serveur de secours : `$NCHOME/etc/security/keys/conf.key`. Si vous entrez tous les noms de communauté SNMP en ligne de commande sans les chiffrer, vous n'avez pas besoin d'effectuer cette tâche. Pour plus d'informations sur la modification de la clé de chiffrement, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*. De plus, pour mettre à jour les mots de passe NCIM et ObjectServer, utilisez le script Perl `ncp_password_update.pl`. Pour plus d'informations sur le script Perl `ncp_password_update.pl`, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Concepts associés

A propos de la haute disponibilité de la base de données topologiques NCIM
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Architecture de reprise en ligne Network Manager (processus centraux)
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent

être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Configuration de Network Manager pour l'utilisation de DB2HADR ou d'un Oracle RAC

Utilisez ces informations pour forcer les processus principaux de Network Manager à utiliser l'alias DB2 ou à se connecter à un nom de service Oracle RAC, en fonction de votre type de base de données.

Avant de commencer

DB2 Pour les bases de données DB2, les processus centraux Network Manager doivent utiliser l'alias DB2 afin d'obtenir des informations sur le serveur DB2 alternatif. Pour forcer les pricipaux processus Network Manager à utiliser l'alias Db2, modifiez deux fichiers de configuration (`DbLogins.`*`Domain`*`.cfg` et `MibDbLogin.cfg`) et ensuite modifier le fichier pilote :

```
$NCHOME/precision/platform/linux2x86/db2-version-number/odbc_cli/clidriver/ cfg/db2dsdriver.cfg
```

Où *version-number* le numéro de version Db2; par exemple, `10.5.0.5`.

Oracle Pour les bases de données Oracle, les processus principaux de Network Manager doivent se connecter au nom de service utilisé par Oracle RAC. Pour configurer les processus de base de Network Manager de sorte qu'ils utilisent un SID au lieu d'un nom de service, éditez les fichiers de configuration `DbLogins.`*`Domain`*`.cfg` et `MibDbLogin.cfg`.

Pourquoi et quand exécuter cette tâche

Les fichiers de configuration `DbLogins.`*`Domain`*`.cfg` et `MibDbLogin.cfg` font partie de l'installation de base de Network Manager. Ces fichiers sont stockés sur le serveur Network Manager. Si la reprise en ligne de Network Manager est configurée, éditez ces fichiers de configuration sur les serveurs Network Manager principal et de secours.

Procédure

1. Sur le serveur principal de Network Manager, ouvrez le fichier `$NCHOME/etc/precision/DbLogins.`*`Domaine`*`.cfg` et apportez les modifications suivantes en fonction de votre type de base de données :

Option	Description
DB2 **Pour les bases de données DB2**	a. Recherchez l'attribut `m_PortNum`. b. Attribuez la valeur 0 (zéro) à tous les attributs `m_PortNum`. c. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.
Oracle **Pour les bases de données Oracle**	a. Recherchez l'attribut `m_OracleService` et ajoutez-le après `m_PortNum` s'il n'existe pas déjà. b. Ne modifiez pas la valeur de l'attribut `m_OracleService` de `"DNCIM",`. Définissez la valeur de tous les autres attributs `m_OracleService` sur 1. c. Vérifiez que `m_DbName` est défini sur la valeur SERVICE_NAME d'Oracle, comme spécifié dans `$ORACLE_HOME/network/admin/tnsnames.ora` d. Vérifiez que le nom d'hôte SCAN d'Oracle RAC est spécifié pour `m_Hostname`. e. Vous pouvez, si vous le souhaitez, définir votre propre chaîne de connexion Oracle RAC personnalisée à l'aide de l'attribut `m_ConnectionString`, comme indiqué ici. Cette chaîne de connexion peut être utilisée pour se connecter à un cluster Oracle RAC, ou à d'autres fins.

Option	Description
	f. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.

2. Sur le serveur principal de Network Manager, ouvrez le fichier `$NCHOME/etc/precision/MibDbLogin.cfg` et apportez les modifications suivantes en fonction de votre type de base de données :

Option	Description
DB2 **Pour les bases de données DB2**	a. Recherchez l'attribut `m_PortNum`. b. Attribuez la valeur 0 (zéro) à l'attribut `m_PortNum`. c. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.
Oracle **Pour les bases de données Oracle**	a. Recherchez l'attribut `m_OracleService` et ajoutez-le après `m_PortNum` s'il n'existe pas déjà. b. Affectez à l'attribut `m_OracleService` la valeur `1`. c. Vérifiez que `m_DbName` est défini sur la valeur SERVICE_NAME d'Oracle, comme spécifié dans `$ORACLE_HOME/network/admin/tnsnames.ora` d. Vérifiez que le nom d'hôte SCAN d'Oracle RAC est spécifié pour `m_Hostname`. e. Vous pouvez, si vous le souhaitez, définir votre propre chaîne de connexion Oracle personnalisée à l'aide de l'attribut `m_ConnectionString`, comme indiqué ici. Cette chaîne de connexion peut être utilisée pour se connecter à un cluster Oracle RAC, ou à d'autres fins. f. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.

3. DB2

Pour les bases de données DB2, vous devez aussi exécuter la procédure suivante :

a) Copiez l'exemple suivant de fichier de pilote dans le même emplacement mais sous un nouveau nom, comme indiqué ci-dessous :

`cp $NCHOME/precision/platform/linux2x86/db2-`*`version-number`*`/odbc_cli/clidriver/cfg/db2dsdriver.cfg.sample $NCHOME/precision/platform/linux2x86/db2-`*`version-number`*`/odbc_cli/clidriver/cfg/db2dsdriver.cfg`

où *numéro-version* est le numéro de version de DB2, par exemple `10.5.0.5`

Remarque : Si vous utilisez déjà ce fichier de pilote, faites-en une copie de sauvegarde et éditez le fichier de pilote directement au lieu de copier l'exemple de fichier de pilote.

b) Trouvez la section `<configuration>` du fichier pilote.

c) Mettez à jour la section `<configuration>` comme suit :

```
<configuration>
    <dsncollection>
        <dsn alias="Database_alias"
        name="Primary_ database_name" host="Primary_database_host"
        port="Primary_database_port"/>
    </dsncollection>
    <databases>
        <database name="Primary_database_name"
        host="Primary_database_host" port="Primary_database_port"/>
          <wlb>
```

```
          <parameter name="enableWLB" value="true"/>
          <parameter name="maxTransports" value="50"/>
      </wlb>
      <acr>
          <parameter name="enableAcr" value="true" />
          <parameter name="maxAcrRetries" value="10" />
          <parameter name="acrRetryInterval" value="5" />
          <parameter name="enableAlternateServerListFirstConnect"
 value="true" />
      <alternateserverlist>
         <server name="server1" hostname="Standby_database_host"
         port="Standby_database_port" />
      </alternateserverlist>
      </acr>
    <database name="Standby_database_name"
        host="Standby_database_host"
        port="Standby_database_port"/>
    </databases>
</configuration>
```

où les éléments suivants sont tous listés dans le fichier de configuration DbLogins_*DOMAIN*.cfg :

- *alias_base de données* est le nom de la base de données principale.

  Remarque : Pour des raisons de commodité, le nom de la base de données principale est aussi utilisé comme alias de la base de données.
- *nom_base de données_principale* est le nom de la base de données principale.
- *hôte_base de données_principale* est le nom d'hôte de la base de données principale.
- *port_base de données principale* est le port de la base de données principale.
- *nom_base de données_ secours* est le nom de la base de données de secours.
- *hôte_base de données_secours* est le nom d'hôte de la base de données de secours.
- *port_base de données_secours* est le port de la base de données de secours.

d) Sauvegardez le fichier de pilote db2dsdriver.cfg.

Tâches associées

Définition d'une adresse URL de connexion personnalisée pour identifier les serveurs DB2 ou Oracle RAC
Utilisez ces informations pour définir une adresse URL de connexion personnalisée pour identifier les serveurs DB2 principal et de sauvegarde ou pour identifier le service Oracle RAC. Cette connexion permettra à l'interface graphique de Network Manager de fonctionner dans l'environnement DB2 HADR ou Oracle RAC, suivant votre type de base de données.

Chaîne de connexion Oracle personnalisée
Vous pouvez définir une chaîne de connexion Oracle personnalisée. Cette chaîne de connexion peut être utilisée pour se connecter à un cluster Oracle RAC, ou à d'autres fins.

Pour définir une chaine de connexion personnalisée ORACLE, modifiez le fichier de configuration $NCHOME/etc/precision/DbLogins.*Domain*.cfg, et configurez l'insertion dans le fichier pour inclure un champ m_ConnectionString ainsi l'insertion ressemblera à cela :

```
insert into config.dbserver
(
    m_DbId,
    m_Server,
    m_DbName,
    m_Schema,
    m_Hostname,
    m_Username,
    m_Password,
    m_PortNum,
    m_ConnectionString,
    m_EncryptedPwd,
    m_OracleService
)
values
(
    "NCIM",
    "oracle",
    "ORATEST",
    "ncim",
```

```
    "server1.location1.acme.com",
    "ncim",
    "ncim",
    1521,
    "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=server1.location1.acme.com3)
(PORT=1521))(CONNECT_DATA=(SID=ORATEST)))",
    0,
    1
);
```

En utilisant l'attribut `m_ConnectionString` de la sorte, vous remplacez les valeurs de `m_DbName`, `m_Hostname` et `m_PortNum`. Vous devez toujours fournir ces valeurs, elles seront remplacées par la valeur spécifiée dans l'attribut `m_ConnectionString` lors de la connexion à la base de données.

Définition d'une adresse URL de connexion personnalisée pour identifier les serveurs DB2 ou Oracle RAC

Utilisez ces informations pour définir une adresse URL de connexion personnalisée pour identifier les serveurs DB2 principal et de sauvegarde ou pour identifier le service Oracle RAC. Cette connexion permettra à l'interface graphique de Network Manager de fonctionner dans l'environnement DB2 HADR ou Oracle RAC, suivant votre type de base de données.

Pourquoi et quand exécuter cette tâche

Pour définir une URL de connexion personnalisée pour identifier les serveurs primaires et de backups Db2, ou identifier les serveurs Oracle RAC, modifiez les fichiers de propriétés appropriés et l'URL de connexion au serveurs. Spécifiez la même connexion d'URL dans chaque fichier de propriétés.

Le fichier de propriétés suivant est applicable à l'interface graphique utilisateur de Network Manager :

- `$NMGUI_HOME/profile/etc/tnm/tnm.properties`

Le fichier de propriétés suivant fait partie de l'installation de base de Network Manager : `$NCHOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties`

Pour définir une URL de connexion personnalisée, procédez comme suit :

Procédure

1. Ouvrez les fichiers `$NMGUI_HOME/profile/etc/tnm/tnm.properties` et `$NCHOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties` à des fins d'édition
2. Apportez les modifications suivantes aux deux, selon votre type de base de données :

Option	Description

DB2 **Pour les bases de données DB2**	Spécifiez la connexion d'URL aux serveurs DB2 principal et de sauvegarde, à l'aide de la syntaxe suivante :
	`tnm.database.jdbc.url=jdbc:db2://`
	`primary_db2_server``:`
	`primary_db2_port_number``/`
	`dbname``:clientRerouteAlternateServerName=`
	`backup_db2_server`
	`;clientRerouteAlternatePortNumber=`
	`backup_db2_port``;`
	où :
	• *serveur_db2_principal* : Spécifie le nom du serveur principal sur lequel s'exécute la base de données DB2.
	• *primary_db2_port_number* : Spécifie le numéro de port du serveur principal sur lequel la base de documents de DB2 fonctionne.
	• *dbname* Spécifie le nom de la base de données Db2.

Option	Description
	• *serveur_db2_sauvegarde* : Spécifie le nom du serveur de sauvegarde sur lequel s'exécute la base de données DB2. • *port_db2_sauvegarde* : Spécifie le numéro de port du serveur de sauvegarde sur lequel s'exécute la base de données DB2.

Oracle
Pour les bases de données Oracle
	Spécifiez la connexion d'URL aux serveurs Oracle RAC, à l'aide de la syntaxe suivante :
	`tnm.database.jdbc.url=jdbc:oracle:thin:`
	`@Oracle_RAC_SCAN_hostname:`
	`Oracle_RAC_port_number/`
	`Oracle_RAC_service_name`
	où :
	• *nom_service_Oracle_RAC* — Spécifie l'adresse SCAN (Single Client Access Name) d'Oracle sur laquelle la base de données Oracle RAC est exécutée.
	• *numéro_port_Oracle_RAC* — Spécifie le numéro de port sur lequel la base de données Oracle RAC est exécutée.
	• *nom_service_Oracle_RAC* — Spécifie le nom de service avec lequel la base de données Oracle RAC est exécutée.

3. Enregistrez et fermez les fichiers.

Tâches associées

Configuration de Network Manager pour l'utilisation de DB2HADR ou d'un Oracle RAC
Utilisez ces informations pour forcer les processus principaux de Network Manager à utiliser l'alias DB2 ou à se connecter à un nom de service Oracle RAC, en fonction de votre type de base de données.

Configuration des paramètres pour les vérifications d'intégrité

Si nécessaire, vous pouvez configurer des conditions préférées sous lesquelles les événements de vérification d'intégrité sont générés, en spécifiant des insertions OQL identiques dans le fichier de schéma du processus de domaine virtuel (`VirtualDomainSchema.cfg`) à la fois sur le serveur principal et sur le serveur de sauvegarde.

Pourquoi et quand exécuter cette tâche

Le composant de domaine virtuel utilise deux bases de données (config et state) pour prendre en charge la reprise en ligne de Network Manager. Les filtres et les enregistrements de vérification d'intégrité sont stockés dans ces tables, qui peuvent être mises à jour via le fichier `VirtualDomainSchema.cfg`. Pour plus d'informations sur les tables de base de données config et state, voir le manuel *IBM Tivoli Network Manager Reference*.

Pour modifier les valeurs par défaut pour les paramètres de vérification d'intégrité :

Procédure

1. Sur le serveur Network Manager principal, modifiez le fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg` en spécifiant les insertions OQM suivantes :
   - Mettez à jour les valeurs des colonnes dans la table config.defaults pour spécifier des périodes de temps différentes pour les vérifications d'intégrité de reprise en ligne.

     Par exemple, vous pouvez utiliser la colonne m_HealthCheckPeriod pour modifier l'intervalle de temps entre chaque vérification d'intégrité. Vous pouvez aussi utiliser la colonne m_FailoverTime pour modifier l'intervalle de temps après lequel la reprise en ligne est déclenchée par le domaine

de secours, lorsque le domaine principal est considéré comme étant de faible intégrité. Les valeurs par défaut sont les suivantes :

```
insert into config.defaults
(
    m_SocketKeepAlivePeriod,
    m_HealthCheckPeriod,
    m_FailoverTime,
    m_DirectoryScanPeriod,
    m_AutoTopologyDownload
)
values
(
    60,
    60,
    300,
    100,
    1
);
```

- Si nécessaire, mettez à jour la table state.filters pour définir des filtres individuels pour chaque interrogateur configuré dans le fichier $NCHOME/etc/precision/CtrlServices.cfg. Par exemple, pour le poller aditionnelement configuré, PingPoller :

```
insert into state.filters
(
    m_ServiceName,
    m_Filter,
    m_Description
)
values
(
    "PingPoller",
    "m_ChangeTime > eval(time,'$TIME - 300') and m_CtrlState <> 7",
    "The Poller has been running within the last 300 seconds"
);
```

2. Sauvegardez et fermez le fichier.
3. Apportez des modifications identiques au fichier $NCHOME/etc/precision/VirtualDomainSchema.cfg sur le serveur de sauvegarde.

Concepts associés

Evénements de vérification d'intégrité et reprise en ligne

La reprise en ligne est pilotée par les vérifications d'intégrité qui sont configurées pour s'exécuter périodiquement pour évaluer l'intégrité des domaines Network Manager principal et de secours.

Configuration de dépendances de processus pour la reprise en ligne

Lors de l'exécution de Network Manager en mode de reprise en ligne, vous devez démarrer les processus Network Manager à l'aide du processus **ncp_ctrl**. L'ordre dans lequel les processus démarrent est important et il est défini par les dépendances des processus qui sont configurées dans le fichier $NCHOME/etc/precision/CtrlServices.cfg.

Pourquoi et quand exécuter cette tâche

Le composant de domaine virtuel (**ncp_virtualdomain**), qui gère la reprise en ligne, dépend de tous les processus qu'il surveille car il ne peut pas correctement déterminer leur état tant que les processus sont en cours d'exécution. Dans le fichier CtrlServices.cfg dans les deux domaines, primaire et sauvegarde, l'entrée pour le processus **ncp_virtualdomain** a la configuration par défaut suivante :

```
dependsOn=[ "ncp_poller_default", "ncp_g_event" ];
```

Aucune autre configuration n'est nécessaire pour définir les dépendances de processus pour la reprise en ligne, à condition que cette valeur par défaut soit conservée.

Pour plus d'informations sur la gestion des dépendances de processus, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Traitement des incidents de reprise en ligne

Examinez ces informations pour vous aider à résoudre des problèmes que vous pourriez rencontrer avec la reprise en ligne.

Dépannage d'erreurs de base de données après basculement.

Si, après un basculement, vous voyez des erreurs dans les journaux du GUI relatifs à NETWORKVIEWSUMR ou à la table networkViewSumr, vous devez écarter et recréer cette table.

Pourquoi et quand exécuter cette tâche

La procédure pour écarter et recréer la table diffère sur DB2 et Oracle.

Procédure

1. Pour DB2, menez à bien les étapes suivantes :
   a) Saisissez les commandes suivantes à l'invite de commande DB2.

   ```
   SET SCHEMA ncpgui;
   DROP TABLE networkViewSumr;
   ```

   b) Trouvez la section de `$PRECISION_HOME/scripts/sql/db2/createPrecisionGUIDb.sql` qui crée `networkViewSumr` et copiez-la dans la lligne de commande DB2.
   c) Saisissez la commande suivante à l'invite de commande DB2 :

   ```
   COMMIT;
   ```

   d) Quittez la ligne de commande DB2.
2. Pour Oracle, menez à bien les étapes suivantes :
   a) Saisissez les commandes suivantes à l'invite de commande Oracle.

   ```
   ALTER SESSION SET CURRENT_SCHEMA = ncpgui;
   DROP TABLE networkViewSumr;
   ```

   b) Trouvez la section de `$PRECISION_HOME/scripts/sql/oracle/createPrecisionGUIDb.sql` qui crée `networkViewSumr` et copiez-la dans la ligne de commande Oracle.
   c) Quittez la ligne de commande Oracle.

Vérification de la configuration de la reprise en ligne des serveurs ObjectServer de Tivoli Netcool/OMNIbus

Si la reprise en ligne des serveurs ObjectServer est configurée, il peut être utile de vérifier sa configuration.

1. Après avoir démarré les deux serveurs ObjectServer, vérifiez que les événements transmis au serveur ObjectServer principal apparaissent dans l'**Afficheur d'événements**.
2. Arrêtez le serveur ObjectServer principal et recherchez s'il y a des messages de reprise en ligne dans le fichier journal du serveur ObjectServer (`$NCHOME/omnibus/log/`*`NOM_PRINCIPAL`*`.log`).
3. Consultez l'**Afficheur d'événements** pour vérifier que les événements transmis au serveur ObjectServer principal sont affichés.
4. Restaurez le serveur ObjectServer principal à un état d'exécution et vérifiez que la reprise par restauration s'est produite en consultant son fichier journal.

Pour des informations sur l'utilisation des commandes Tivoli Netcool/OMNIbus pour démarrer et arrêter le serveur ObjectServer, consultez la documentation de Tivoli Netcool/OMNIbus disponible à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Pour des informations sur le démarrage et l'arrêt du serveur ObjectServer à l'aide de commandes Network Manager, consultez le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Suivi de la reprise en ligne des processus centraux de Network Manager

Vous pouvez effectuer plusieurs actions et contrôles pour vérifier si la reprise en ligne des processus centraux de Network Manager fonctionne comme prévu.

Suivi de la reprise en ligne au démarrage

Pour s'assurer que le domaine principal démarre son exécution en tant que domaine actif, démarrez le domaine principal et son processus de domaine virtuel avant de démarrer le domaine de secours. Si le domaine de secours est démarré avant que le processus de domaine virtuel principal ait démarré, le domaine de secours peut devenir actif, commencer à interroger le réseau et générer des événements de problème de vérification d'intégrité à propos du domaine principal. Ce problème se résout cependant de lui-même après le démarrage du domaine virtuel principal et la transmission entre les domaines des événements de vérification d'intégrité.

Au démarrage, la topologie et les règles sont copiées du domaine principal vers le domaine de secours. Le domaine de secours ne peut cependant pas devenir actif (lors d'une reprise en ligne) tant qu'il n'a pas initialisé sa topologie. Pour vérifier que la topologie a été initialisée :

- Recherchez un fichier cache de topologie d'une taille différente de zéro (`Store.Cache.ncimCache.entityData.`*`domaine`*) dans le répertoire `$NCHOME/var/precision` du domaine de secours, où *domaine* est le nom du domaine en cours.

Event generation for startup : Surveillez l'**Afficheur d'événements** pour les événements Network Manager ItnmServiceState et ItnmFailoverConnectionevents afin de vérifier que les processus de domaine virtuel sont en cours d'exécution et que la connexion de socket TCP a été établie :

- Après le démarrage de chaque processus **ncp_virtualdomain** local, le processus **ncp_ctrl** génère un événement de résolution ItnmServiceState.
- Lorsqu'une connexion TCP est établie entre les processus de domaine virtuel, un événement de résolution ItnmFailoverConnection est généré.

Suivi de la reprise en ligne lorsque le système est dans un état stabilisé

Un comportement de reprise en ligne normal et en *état stabilisé* peut être obtenu seulement après le démarrage et la connexion des processus de domaine virtuel dans les domaines principal et de secours. Le comportement en état stabilisé peut être défini comme suit :

- Le domaine principal est actif et fonctionne comme s'il était le seul domaine. Le processus de reconnaissance reconnaît le réseau, qui est surveillé par l'interrogateur, et les événements sont enrichis par la passerelle d'événement.
- Le domaine de secours est en mode veille. La reconnaissance n'est pas initiée, et l'interrogateur fait le suivi des règles configurées dans le domaine principal, mais n'interroge pas les périphériques. De son côté, la passerelle d'événement ne met pas à jour les événements dans le serveur ObjectServer.

Vous pouvez exécuter des requêtes OQL sur chaque domaine pour vérifier l'état des processus :

- Vous pouvez vérifier l'état de processus Network Manager individuels en interrogeant la base de données du processus **ncp_ctrl**. Tous les processus qui s'exécutent sans problème doivent avoir la valeur `serviceState = 4` dans la table de base de données services.inTray pour indiquer que le service est "actif et en cours d'exécution".
- Les processus **ncp_poller** et **ncp_g_event** ont chacun une table de base de données config.failover associée, qui identifie leur état de reprise en ligne actuel. Lorsqu'ils s'exécutent correctement dans un état stabilisé, ces processus ont le paramètre `FailedOver = 0` dans la table OQL config.failover dans les deux domaines. (Le processus de domaine virtuel met à jour périodiquement la zone FailedOver.)

Pour plus d'informations sur l'exécution de requêtes OQL, voir le manuel *IBM Tivoli Network Manager Reference*. Pour plus d'informations sur la façon d'identifier les processus qui sont en cours d'exécution, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Event generation while in a steady state : Chaque domaine génère des événements sur son état, sur la base des filtres du fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg`. Ces événements sont générés selon un intervalle configuré dans la zone m_HealthCheckInterval. Surveillez l'**Afficheur d'événements** pour les événements ItnmHealthChk et ItnmDatabaseConnection Network Manager afin de vérifier si les domaines principal et de secours sont dans un bon état d'intégrité :

- Chaque domaine génère des événements de résolution ItnmHealthChk lorsque son état d'intégrité est bon.
- Le domaine principal génère un événement de problème ItnmDatabaseConnection si la connexion à la base de données NCIM principale est perdue. Si la connexion n'est pas rétablie dans l'intervalle de temps défini pour l'entrée state.filters NCIM dans le fichier `VirtualDomainSchema.cfg`, le domaine principal génère un événement de problème ItnmHealthChk à propos du domaine principal.
- Si le domaine de secours ne reçoit pas un événement de résolution ItnmHealthChk du domaine principal dans l'intervalle de temps m_FailoverTime configuré, le domaine de secours génère un événement de problème ItnmHealthChk synthétique pour le compte du domaine principal.

  Si le domaine principal ou le domaine de secours génère un événement de problème ItnmHealthChk pour le domaine principal, la reprise en ligne est déclenchée et le domaine de secours devient actif. Si le domaine principal est toujours en cours d'exécution, il passe en mode veille.

  Conseil : Pour les événements de vérification d'intégrité, la zone Node identifie le domaine pour lequel l'événement de vérification d'intégrité est généré. La zone Summary identifie le domaine à l'origine de l'événement et le domaine concerné par l'événement.

Suivi de la reprise en ligne et de la reprise par restauration

Lorsqu'une reprise en ligne se produit, le domaine de secours devient actif, l'interrogateur de secours surveille le réseau et la passerelle d'événement met à jour les événements du serveur ObjectServer. Vous pouvez exécuter des requêtes OQL pour vérifier l'état des processus **ncp_poller** et **ncp_g_event**. Ces processus ont chacun une table de base de données config.failover associée, qui identifie leur état de reprise en ligne actuel. Lorsque le domaine de secours est actif, ces processus ont le paramètre `FailedOver = 1` dans la table config.failover pour indiquer qu'ils sont dans un état de reprise en ligne. (Si le domaine principal est toujours en cours d'exécution, la valeur `FailedOver = 1` est également affectée aux processus associés.)

Lorsqu'une reprise par restauration se produit, le domaine de secours passe en veille et le domaine principal redevient actif. Ceci est analogue à ce qui se produit au démarrage.

Event generation on failover and failback : Surveillez l'**Afficheur d'événements** pour les événements ItnmHealthChk et ItnmFailover Network Manager afin de vérifier le comportement de la reprise en ligne et de la reprise par restauration :

- Un événement de problème ItnmHealthChk à propos du domaine principal indique qu'une reprise en ligne a été déclenchée. Un événement ultérieur de résolution ItnmHealthChk à propos du domaine principal indique qu'une reprise par restauration a été déclenchée.
- Des événements ItnmFailover sont générés pour indiquer quand un domaine Network Manager fait l'objet d'une reprise en ligne ou d'une reprise par restauration. La description de l'événement indique si le domaine est le domaine principal ou le domaine de secours, et s'il est devenu actif ou est passé en mode veille.

Recherche des causes d'une reprise en ligne

La reprise en ligne pouvant être initiée par le domaine principal ou par le domaine de secours, il est important d'identifier le domaine qui a initié la reprise en ligne.

Effectuez l'un ou l'autre des actions suivantes :

- Examinez le fichier journal du domaine virtuel ($NCHOME/log/precision/ncp_virtualdomain.*DOMAINE*.log) et le fichier journal de la passerelle d'événements ($NCHOME/log/precision/ncp_g_event.*DOMAINE*.log).
- Examinez les événements ItnmHealthChk et ItnmFailover dans la liste d'événements actifs. (Ceci est l'approche la plus simple.)

Si le domaine principal a initié la reprise en ligne, ceci indique une défaillance de l'un des processus du domaine principal. Vous pouvez vérifier l'état des processus en interrogeant la base de données du processus **ncp_ctrl**. La zone serviceState de la table de base de données services.inTray montre l'état opérationnel en cours pour chacun des processus. Pour plus d'informations sur la façon d'identifier les processus qui sont en cours d'exécution, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Si le domaine de secours a initié la reprise en ligne, ceci indique un échec de routage des événements de vérification d'intégrité à travers le système pour une des raisons suivantes :

- Le domaine principal n'a pas généré d'événement de vérification d'intégrité (par exemple parce que le serveur principal était hors fonction).
- Les processus de la Sonde pour Tivoli Netcool/OMNIbus ou de la passerelle d'événements des deux domaines ne sont pas configurés pour accéder au même serveur ObjectServer.
- Le plug-in de reprise en ligne de la passerelle d'événements n'est pas activé.
- Le fichier de règles de la Sonde pour Tivoli Netcool/OMNIbus a été modifié de sorte que l'événement de vérification d'intégrité ne contient pas les informations requises.
- La passerelle d'événements de sauvegarde ne laisse pas passer les événements de vérification d'intégrité à travers le filtre nco2ncp.

  Pour plus d'informations sur l'activation du plug-in de reprise en ligne et sur les filtres d'événements, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Vérifiez aussi que le domaine virtuel est configuré (dans le fichier $NCHOME/etc/precision/CtrlServices.cfg) pour avoir une dépendance de tous les processus dont la liste figure dans le fichier $NCHOME/etc/precision/VirtualDomainSchema.cfg.

Tâches associées

Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg
Lorsque vous utilisez le fichier $NCHOME/etc/precision/ConfigItnm.*DOMAIN*.cfg pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde.

Examen des problèmes de connexion TCP

Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées du domaine principal vers le domaine de secours.

Si la connexion TCP est perdue :

- Vérifiez que le domaine virtuel est configuré (dans $NCHOME/etc/precision/CtrlServices.cfg) pour avoir une dépendance de tous les processus dont la liste figure dans le fichier $NCHOME/etc/precision/VirtualDomainSchema.cfg.
- Vérifiez que le processus **ncp_config** est en cours d'exécution. Vous pouvez vérifier l'état de **ncp_config** en interrogeant la base de données du processus **ncp_ctrl**. S'il s'exécute sans problème, **ncp_config** doit avoir la valeur serviceState = 4 dans la table services.inTray. Pour plus d'informations sur la façon d'identifier les processus qui sont en cours d'exécution, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Si la connexion TCP n'est pas établie :

- Vérifiez que les fichiers $NCHOME/etc/precision/ServiceData.cfg des deux domaines ont la même entrée pour le processus de domaine virtuel.

- Vérifiez que les pare-feu de frontière entre les domaines autorisent la connexion TCP sur le port de serveur défini.
- Vérifiez que le port défini est disponible pour être utilisé sur le domaine principal.

Tâches associées

Configuration de dépendances de processus pour la reprise en ligne
Lors de l'exécution de Network Manager en mode de reprise en ligne, vous devez démarrer les processus Network Manager à l'aide du processus **ncp_ctrl**. L'ordre dans lequel les processus démarrent est important et il est défini par les dépendances des processus qui sont configurées dans le fichier `$NCHOME/etc/precision/CtrlServices.cfg`.

Configuration de la connexion de socket TCP entre les domaines
Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées dans le domaine de secours.

Séquence pour le redémarrage des processus serveur dans une configuration de reprise en ligne

Utilisez ces informations comme un guide pour le redémarrage des processus serveur si votre environnement de reprise en ligne Network Manager requiert un réamorçage de tous les serveurs.

Démarrez les processus dans l'ordre suivant :

1. Démarrez le serveur ObjectServer principal. Selon votre installation et votre configuration, vous pouvez utiliser un des méthodes suivantes :
   - Contrôle de processus Tivoli Netcool/OMNIbus sous UNIX et Linux
   - La commande **nco_objserv** de Tivoli Netcool/OMNIbus

   Pour des informations sur l'utilisation des commandes Tivoli Netcool/OMNIbus pour démarrer le serveur ObjectServer, consultez la documentation de Tivoli Netcool/OMNIbus disponible à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

   Pour des informations sur le démarrage du serveur ObjectServer à l'aide de commandes Network Manager, consultez le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
2. Démarrez le serveur ObjectServer de sauvegarde.
3. Démarrez la base de données topologiques si elle n'est pas déjà en cours d'exécution.
4. Démarrez le serveur Network Manager principal où les processus centraux sont installés à l'aide de la commande **itnm_start** ou bien en démarrant le contrôleur de processus maître, **ncp_ctrl**.

   Vérifiez aussi que le processus de domaine virtuel du domaine principal a démarré en exécutant la commande **itnm_status** dans le répertoire `$NCHOME/precision/bin`.

   Pour des informations sur le démarrage du serveur et des processus Network Manager, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
5. Démarrez le serveur Network Manager de sauvegarde où les processus centraux sont installés.

Conseil : Le serveur Dashboard Application Services Hub où les applications Web Network Manager et Tivoli Netcool/OMNIbus Web GUI sont installés démarre automatiquement lorsque l'ordinateur est démarré.

Configuration de la sécurité

Pour protéger votre installation ITNM contre des attaques malveillantes, vous devez exécuter les tâches suivantes.

Configuration des cookies

Les applications Web Network Manager utilisent des cookies pour suivre les utilisateurs et leurs requêtes. Bien que ces cookies ne soient pas sensibles eux-mêmes, ils peuvent être utilisés par un intrus pour usurper votre identité sur le système. Le trafic réseau empruntant souvent des réseaux non sécurisés, ces cookies doivent être chiffrés à l'aide de SSL.

Pourquoi et quand exécuter cette tâche

Configuration de cookies Dashboard Application Services Hub

Dans le cas de communications impliquant Dashboard Application Services Hub, le cookie le plus important est le cookie de session HTTP ; il doit donc être configuré pour n'être envoyé que sur SSL.

Pourquoi et quand exécuter cette tâche

Pour limiter le cookie de session HTTP à la communication uniquement à l'aide du protocole HTTPS, exécutez les étapes décrites dans la note technique située à l'emplacement suivant : https://www.ibm.com/support/pages/node/250915

Configuration du cookie LTPA WebSphere

Le mécanisme LTPA (Lightweight Third Party Authentication) est associé à des rôles et à l'authentification via votre session de connexion. Si un intrus peut intercepter le cookie LTPA, il peut alors usurper votre identité. Pour éviter cela, vous devez vous assurer que le cookie LTPA est uniquement transmis sur SSL.

Pourquoi et quand exécuter cette tâche

Procédure

1. Cliquez sur **Sécurité** > **Sécurité globale**.
2. Cliquez sur **Authentification** > **Web security** > **Single sign-on (SSO)**.
3. Cliquez sur **Requires SSL**.
4. Cliquez sur **OK**.
5. Redémarrez le serveur Dashboard Application Services Hub.

Protection contre le détournement de clic

Si vous intégrez des applications Web Network Manager à votre propre produit, sachez que l'intégration ne permettra pas d'afficher l'interface graphique Accès à la base de données et l'interface graphique Configuration de la reconnaissance en raison d'un filtre de protection implémenté dans Network Manager. Ces deux interfaces graphiques contiennent des informations sensibles ; l'impossibilité à les intégrer vous protège de tout détournement de clic, où un intrus créerait une surcouche d'interface graphique pour capturer des données. Vous pouvez désactiver ce filtre, ce n'est toutefois pas recommandé.

Pourquoi et quand exécuter cette tâche

Le filtre est implémenté à l'aide de la propriété `tnm.enableClickjackProtection` dans le fichier `tnm.properties`.

Remarque : Si cette propriété n'est pas présente dans le fichier, le filtrage est activé par défaut.

Procédure

1. Sauvegardez et modifiez le fichier `$NMGUI_HOME/profile/etc/tnm/tnm.properties`.
2. Recherchez l'entrée `tnm.enableClickjackProtection=true`.
3. Changez l'entrée pour `tnm.enableClickjackProtection=false`.

   Remarque : Si cette propriété n'est pas présente dans le fichier, entrez : `tnm.enableClickjackProtection=false`.

Changement de l'adresse IP et du nom d'hôte de l'installation Network Manager

Si vous changez l'adresse IP et le nom d'hôte du serveur sur lequel l'un des composants de Network Manager ou des produits intégrés est installé, vous devez configurer Network Manager ainsi que les produits et composants associés.

Changement de l'adresse IP et du nom d'hôte pour Network Manager

Si vous voulez changer l'adresse IP et le nom d'hôte du serveur sur lequel les composants centraux de Network Manager sont installés, vous devez effectuer certaines tâches de configuration.

Pourquoi et quand exécuter cette tâche

Effectuez les opérations suivantes pour changer l'adresse IP et le nom d'hôte sur le serveur Network Manager.

Procédure

1. Placez-vous dans le répertoire suivant : NCHOME/etc/.
2. Editez le fichier de configuration `itnm.cfg`.
3. Changez le paramètre suivant : `ncp`. Mettez-le à jour avec le nouveau nom d'hôte du serveur Network Manager, par exemple `ncp=myhost`
4. Sauvegardez le fichier `itnm.cfg`.
5. Placez-vous dans le répertoire suivant : `NCHOME/etc/precision/`.
6. Editez le fichier : `ServiceData.cfg`.
7. Changez la ligne suivante :

   ```
   SERVICE: ncp_config DOMAIN: NCOMS ADDRESS: Network_Manager_server_IP_address
   PORT: port_number SERVERNAME: Network_Manager_server_hostname DYNAMIC: NO
   ```

   Où :

   - *adresse_IP_serveur_Network_Manager* est la nouvelle adresse IP du serveur Network Manager.
   - *nom_hôte_serveur_Network_Manager* est le nouveau nom d'hôte du serveur Network Manager.
8. Sauvegardez le fichier `ServiceData.cfg`.

Changement de l'adresse IP et du nom d'hôte sur le serveur Tivoli Netcool/OMNIbus

Si vous voulez changer l'adresse IP et le nom d'hôte du serveur Tivoli Netcool/OMNIbus, vous devez effectuer certaines tâches de configuration.

Pourquoi et quand exécuter cette tâche

Effectuez les opérations suivantes pour changer l'adresse IP et le nom d'hôte sur le serveur Tivoli Netcool/OMNIbus :

Procédure

1. Placez-vous dans le répertoire suivant : NCHOME/etc/.
2. Editez le fichier omni.dat.
3. Recherchez les lignes contenant le serveur Tivoli Netcool/OMNIbus. Ces lignes sont similaires aux suivantes :

```
[NCOMS]
{
        Primary: OMNIbus_server_hostname 4100
}
[NCO_PA]
{
        Primary: OMNIbus_server_hostname 4200
}
```

   Où :

   - *nom_hôte_serveur_OMNIbus* est le nom d'hôte du serveur Tivoli Netcool/OMNIbus.

   Changez le nom d'hôte du serveur Tivoli Netcool/OMNIbus sur chacune de ces lignes.
4. Exécutez l'utilitaire NCHOME/bin/nco_igen pour appliquer les modifications.
5. Répétez les étapes précédentes sur chaque hôte se connectant au serveur Tivoli Netcool/OMNIbus ; par exemple, effectuez ces modifications pour les sondes, les passerelles et les serveurs d'objets connectés.

Mise à jour de Network Manager avec une nouvelle adresse IP et un nouveau nom d'hôte Tivoli Netcool/OMNIbus

Si vous mettez à jour l'adresse IP et le nom d'hôte du serveur Tivoli Netcool/OMNIbus, vous devez configurer Network Manager de sorte qu'il utilise la nouvelle adresse IP et le nouveau nom d'hôte.

Pourquoi et quand exécuter cette tâche

Effectuez les opérations suivantes pour mettre à jour Network Manager et qu'il prenne connaissance des modifications apportées au nom d'hôte du serveur Tivoli Netcool/OMNIbus :

Procédure

1. Mettez à jour les composants centraux de Network Manager en éditant le fichier de configuration NCHOME/etc/itnm.cfg.
2. Changez le paramètre suivant : nco. Mettez-le à jour avec le nouveau nom d'hôte du serveur Tivoli Netcool/OMNIbus, par exemple nco=omnihost.
3. Sauvegardez le fichier itnm.cfg.
4. Mettez à jour les composants de l'interface graphique de Network Manager en éditant le fichier rép_base_webgui/etc/datasources, où rép_base_webgui est le répertoire d'installation de l'interface graphique Web, par exemple $NCHOME/omnibus_webgui.
5. Mettez à jour les applications Web de Network Manager afin de les configurer de sorte qu'elles utilisent le nom d'hôte modifié du serveur Tivoli Netcool/OMNIbus :
   a) Modifiez le fichier suivant :

```
NCHOME/omnibus_webgui/etc/datasources/ncwDataSourceDefinitions.xml
```

   b) Changez les valeurs d'hôte et de port dans les sections suivantes pour qu'elles correspondent à la configuration mise à jour :

      - <ncwPrimaryServer>
      - <ncwBackUpServer>

      Remarque : Ne changez cette section que si un serveur d'objets Tivoli Netcool/OMNIbus de secours est configuré.

c) Sauvegardez le fichier `ncwDataSourceDefinitions.xml` modifié.

Mise à jour de Dashboard Application Services Hub avec une nouvelle adresse IP et un nouveau nom d'hôte Tivoli Netcool/OMNIbus

Si le serveur Dashboard Application Services Hub a été initialement configuré en vue de l'utilisation du serveur d'objets Tivoli Netcool/OMNIbus comme référentiel utilisateur principal et que vous mettez à jour l'adresse IP et le nom d'hôte du serveur Tivoli Netcool/OMNIbus, vous devez configurer Dashboard Application Services Hub de sorte qu'il utilise la nouvelle adresse IP et le nouveau nom d'hôte.

Pourquoi et quand exécuter cette tâche

Effectuez les opérations suivantes pour configurer Dashboard Application Services Hub en vue de l'utilisation du nouveau nom d'hôte du serveur Tivoli Netcool/OMNIbus :

Procédure

1. Modifiez le fichier suivant :

```
$JazzSM_HOME/profile/config/cells/JazzSMNode01Cell/wim/config/
wimconfig.xml
```

2. Changez les propriétés `host1` et `port1` pour qu'elles correspondent à votre configuration mise à jour dans le fichier suivant :

```
config:repositories adapterClassName=
"com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdapter"
```

3. Sauvegardez le fichier `wimconfig.xml` modifié.

Changement de l'adresse IP et du nom d'hôte sur le serveur Dashboard Application Services Hub

Si vous voulez changer l'adresse IP et le nom d'hôte de Dashboard Application Services Hub, vous devez configurer Dashboard Application Services Hub.

Pourquoi et quand exécuter cette tâche

Effectuez les opérations suivantes pour changer l'adresse IP et le nom d'hôte sur le serveur Dashboard Application Services Hub :

Procédure

1. Placez-vous dans le répertoire suivant : `$JazzSM_HOME/profile/bin/`.
2. Utilisez la commande `wsadmin` pour changer l'adresse IP et le nom d'hôte du serveur Dashboard Application Services Hub :

```
wsadmin.sh -user smadmin -password password
-c "\$AdminTask changeHostName {-hostName new_hostname -nodeName new_node}"
-c "\$AdminConfig save"
```

   La sortie est similaire à l'exemple suivant :

```
WASX7209I: Connecté au processus "server1" sur nœud Nodename
 en utilisant le connecteur SOAP ; Le type de processus est : UnManagedProcess
```

3. Redémarrez le serveur Dashboard Application Services Hub.

Mise à jour de Network Manager avec le nom d'hôte modifié du serveur Dashboard Application Services Hub

Si vous changez le nom d'hôte du serveur Dashboard Application Services Hub, vous devez configurer Network Manager en vue de l'utilisation du nouveau nom d'hôte.

Pourquoi et quand exécuter cette tâche

Pour configurer Network Manager en vue de l'utilisation du nouveau nom d'hôte, procédez comme suit :

Procédure

1. Mettez à jour les composants centraux de Network Manager en éditant le fichier de configuration `NCHOME/etc/itnm.cfg`.
2. Changez le paramètre suivant :

   ```
   astuce
   ```

   Mettez cela à jour vers le nouveau nom du Dashboard Application Services Hub serveur ; par exemple :

   ```
   tip=tiphost
   ```

3. Sauvegardez le fichier `itnm.cfg`.

Configuration de Network Manager pour une adresse IP modifiée du serveur NCIM DB2

Si vous changez l'adresse IP ou le nom d'hôte du serveur DB2 hébergeant la base de données topologiques NCIM, vous devez configurer Network Manager en vue de l'utilisation des nouveaux détails.

Pourquoi et quand exécuter cette tâche

Procédure

1. Sur le serveur sur lequel Network Manager est installé, éditez le fichier suivant :

   ```
   NCHOME/etc/precision/DbLogins.DOMAIN.cfg
   ```

2. Changez les paramètres de nom d'hôte dans ce fichier et sauvegardez le fichier.
3. Modifiez le fichier suivant :

   ```
   NCHOME/etc/precision/MibDbLogin.cfg
   ```

4. Changez les paramètres de nom d'hôte dans ce fichier et sauvegardez le fichier.
5. Sur le serveur sur lequel les applications Web de Network Manager sont installées, éditez le fichier suivant :

   ```
   $NMGUI_HOME/profile/logs/tnm/tnm.properties
   ```

6. Changez les paramètres de nom d'hôte dans ce fichier et sauvegardez le fichier.

Configuration des variables d'environnement

Avant de démarrer un composant ou de travailler avec un fichier de configuration, configurez les variables d'environnement appropriées en exécutant les scripts d'environnement.

Pourquoi et quand exécuter cette tâche

Les scripts d'environnement définissent les variables d'environnement requises suivantes. Ils sont configurés automatiquement avec les emplacements adéquats dans lesquels les composants sont installés. Le cas échéant, les autres variables d'environnement sont définies automatiquement par les composants Network Manager.

$NCHOME
L'emplacement d'origine Netcool qui correspond par défaut au répertoire `netcool` situé sous le répertoire d'installation :

- `/opt/IBM/netcool/core`

$NMGUI_HOME
Emplacement d'installation des composants de l'interface graphique de Network Manager. Par défaut, il s'agit de `/opt/IBM/netcool/gui/precision_gui`.

$ITNMHOME et $PRECISION_HOME
Emplacement d'origine de Network Manager qui est par défaut `$NCHOME/precision` :

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

Remarque : Le script définit également $PRECISION_HOME. Par défaut, $PRECISION_HOME est défini sur le même emplacement que $ITNMHOME, mais est utilisé par d'autres parties du produit.

$DASH_HOME
Emplacement d'installation de Dashboard Application Services Hub. Par défaut, cet emplacement est `/opt/IBM/JazzSM/ui`.

$JazzSM_HOME
Emplacement d'installation de Jazz for Service Management. Par défaut, cet emplacement est `/opt/IBM/JazzSM`.

Pour définir les variables d'environnement, Network Manager, exécutez le script adapté aux composants que vous avez installés. Il existe des scripts différents sur le serveur où sont installés les composants principaux et sur le serveur où sont installés les composants d'interface graphique.

Important : Si vous avez installé les composants principaux et les composants d'interface graphique sur le même serveur, exécutez les deux scripts.

Procédure

- Exécutez le script d'environnement approprié :

  Sur le serveur où sont installés les composants de base de Network Manager, le script d'environnement est `répertoire_installation/netcool/core/env.sh`.

  Par exemple, sur des shells Bash, Bourne, et Korn, sourcez le script env.sh en utilisant une ligne de commande similaire à la suivante :

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

  Sur le serveur où sont installés les composants d'interface graphique de Network Manager, le script est `répertoire_installation/nmgui_profile.sh`, par exemple, `/opt/IBM/netcool/nmgui_profile.sh`.

  Par exemple, sur des shells Bash, Bourne, et Korn, sourcez le script nmgui_profile.sh en utilisant une ligne de commande similaire à la suivante :

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

Que faire ensuite

Après avoir défini les variables d'environnement, démarrez Network Manager et assurez-vous qu'il fonctionne correctement.

Structure de répertoire par défaut

Utilisez ces informations pour comprendre la structure de répertoire de Network Manager.

Structure de répertoire de niveau supérieur

Dans le répertoire dans lequel est installé Network Manager, le sous-répertoire `netcool` est créé. Ce répertoire `netcool` contient lui-même les sous-répertoires suivants :

- `core` : contient les fichiers de configuration des processus dorsaux de Network Manager.
- `gui` : contient les fichiers de configuration des processus de l'interface graphique :
  - `omnibus_gui`: S'il existe, contient des fichiers Tivoli Netcool/OMNIbus Web GUI.
  - `precision_gui` : contient des fichiers de l'interface graphique Network Manager.

Pour des informations sur les répertoires d'installation pour Tivoli Netcool/OMNIbus et Tivoli Netcool/OMNIbus Web GUI, voir le manuel *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*.

Répertoires utilisés par le programme d'installation

Le programme d'installation installe les fichiers dans NCHOME, et dans d'autres répertoires, selon le système d'exploitation sur lequel a lieu l'installation et l'utilisateur qui exécute l'installation. Le tableau suivant répertorie les répertoires supplémentaires utilisés par le programme d'installation.

Remarque : A partir de la version 4.2, NCHOME est *`installation_directory`*`/netcool/core`; par exemple, `opt/ibm/netcool/core`.

Tableau 14. Répertoires utilisés par le programme d'installation

Installation	Répertoires utilisés pour les fichiers d'installation
Systèmes d'exploitation UNIX, superutilisateur	`/usr/ibm/common/acsi`
	`/var/ibm/common/acsi`
Systèmes d'exploitation UNIX, utilisateur non superutilisateur	`~/.acsi_$HOSTNAME`
	`~/tivoli`
	`~/.cit` (i.e. le répertoire de base de l'utilisateur)

Contenu du répertoire netcool

Le tableau suivant décrit le contenu du répertoire `netcool/core`. Tous les chemins indiqués sont relatifs à `NCHOME`. Dans ce tableau, *arch* indique un répertoire du système d'exploitation. Le nom de ce répertoire varie en fonction du système d'exploitation sur lequel le logiciel est installé :

- Linux – `linux2x86`
- AIX – `aix5`
- zLinux - `linux2s390`

Si vous avez installé d'autres produits IBM Tivoli, comme IBM Tivoli Business Service Manager, sur le même serveur que Network Manager, des dossiers et des fichiers supplémentaires peuvent être présents. Voir la documentation pour tout autre produit que vous avez installé pour plus d'informations sur leurs répertoires et fichiers.

Tableau 15. Répertoires de NCHOME	
Répertoire	**Description**
`bin`	Contient des scripts encapsuleurs qui définissent l'environnement et exécutent les fichiers binaires pour le produit ou les composants fournis avec Network Manager.
`etc`	Contient des fichiers de configuration pour les produits ou les composants fournis avec Network Manager.
`etc/precision`	Fichiers de configuration de l'ensemble des composants de Network Manager.
`licence`	Contient le texte de l'accord de licence du produit en différentes langues.
`journal`	Contient des fichiers journaux.
`log/install`	Contient des fichiers journaux pour l'installation.
`log/precision`	Contient des fichiers journaux créés par les processus Network Manager.
`omnibus`	S'il existe, contient des fichiers IBM Tivoli Netcool/OMNIbus.
`platform/`*`arch`*	Contient les fichiers du Java Development Kit (JDK) et du Java Runtime Environment (JRE). **Remarque :** Dashboard Application Services Hub utilise l'environnement d'exécution Java (JRE) de WebSphere Application Server.
`precision`	Contient des fichiers pour Network Manager. Voir plus loin dans cette rubrique.
`probes`	Contient des fichiers pour l'analyse pour IBM Tivoli Netcool/OMNIbus et le processus nco_p_ncpmonitor.
`properties`	Contient des fichiers utilisés par le processus d'installation. Vous ne devriez pas avoir à modifier le contenu de ce répertoire.
`var`	Contient des données d'application permanentes.
`var/install`	Contient des fichiers base de données pour le processus d'installation.
`var/precision`	Utilisé par le processus ncp_store pour conserver des informations placées dans la mémoire cache pouvant être utilisées pour restaurer les bases de données si un processus se termine inopinément.

Contenu du répertoire precision

Le tableau suivant décrit le contenu du répertoire `NCHOME/precision`. Tous les chemins indiqués sont relatifs à `NCHOME/precision`.

Dans ce tableau, *arch* indique un répertoire du système d'exploitation. Le nom de ce répertoire varie en fonction du système d'exploitation sur lequel le logiciel est installé :

- Linux – `linux2x86`
- AIX – `aix5`
- zLinux - `linux2s390`

Remarque : `NCHOME/precision` correspond au chemin d'accès défini par défaut pour PRECISION_HOME et ITNMHOME.

Tableau 16. Répertoires de NCHOME/precision	
Répertoire	**Description**
adapters/ncp_dla	Contient des fichiers pour l'adaptateur de bibliothèque utilisé pour l'intégration avec des produits tels que IBM Tivoli Application Dependency Discovery Manager.
aoc	Contient les fichiers de classe d'objet active (AOC) utilisés par le système de distribution et de gestion de classe dynamique, CLASS.
bin	Contient des scripts encapsuleurs pour tous les fichiers exécutables. Les fichiers exécutables sont conservés à l'emplacement suivant : platform/*arch*/bin
collectors/perlCollectors	Contient des fichiers pour les intégrations EMS.
contrib	Contient des utilitaires non pris en charge de gestion de Network Manager. Egalement utilisé par la solution Netcool for Asset Management afin de contenir des exemples de rapports SQL*Plus.
cshrc	Seulement sur les systèmes d'exploitation UNIX. Utilisé pour configurer l'environnement de l'interpréteur de commandes C.
disco	Contient des fichiers utilisés par DISCO. Contient les fichiers de définition des agents, les agents de reconnaissance, les outils de recherche, les fichiers des auxiliaires et les programmes stitcher.
embeddedDb	Contient les fichiers pour dNCIM.
eventGateway	Contient les programmes stitcher pour la passerelle d'événements et RCA.
integration	Contient les fichiers pour l'intégration de l'interface graphique de composant.
installation	Contient des fichiers utilisés par le processus d'installation.
java_api	Contient l'interface de programme d'application JAVA permettant de développer des applications Java qui s'intègrent aux composants de Network Manager.
mibs	Contient des fichiers MIB (Management Information Base).
PD	Tout fichier principal généré par Network Manager est écrit dans un sous-répertoire du répertoire PD. Les fichiers principaux peuvent faciliter le diagnostic de la cause d'un incident.
perl	Contient les fichiers perl utilisés dans Network Manager.
platform/*arch*	Contient les sous-répertoires spécifiques au système d'exploitation sur lequel vous avez installé Network Manager.
platform/*arch*/bin	Contient des fichiers exécutables pour les composants de Network Manager. Les fichiers sont ajoutés à votre environnement PATH. Les scripts encapsuleurs correspondant à ces fichiers exécutables se trouvent dans le répertoire NCHOME/precision/bin.
platform/*arch*/jre	Contient l'environnement d'exécution JAVA utilisé par Network Manager.
platform/*arch*/lib	Contient les bibliothèques d'objets utilisées par tous les composants de Network Manager.

Tableau 16. Répertoires de NCHOME/precision (suite)	
Répertoire	**Description**
platform/java/lib	Installation de l'interface graphique de la configuration de surveillance. Installation de l'outil de configuration des utilisateurs.
products	Contient les fichiers d'interface graphique pour les produits intégrés.
profil	Seulement sur les systèmes d'exploitation UNIX. Utilisé pour configurer l'environnement de l'interpréteur de commandes bash.
profils	Contient les fichiers liés à l'interface graphique. **Remarque :** Tous les fichiers spécifiques à Network Manager qui se trouvaient précédemment dans le répertoire TIPHOME/profiles se trouvent maintenant dans le répertoire ITNMHOME/profiles.
scripts	Contient des scripts fournis avec les produits Network Manager. Il est conseillé de conserver les scripts définis par l'utilisateur dans ce répertoire afin d'en faciliter la gestion.
storm	Contient les scripts Apache Storm.
system	Contient les fichiers pour le fonctionnement du produit.
systemApps	Contient les fichiers pour les applications Web.

Référence associée

Exigences relatives au répertoire d'installation
Le répertoire dans lequel vous installez Network Manager doit répondre à certaines exigences.

Configuration de périphériques Juniper PE

L'une des interrogations de périphérique activées par défaut est l'interrogation PING distant Juniper. Pour garantir l'extraction de données par cette interrogation, vous devez configurer chaque périphérique Juniper PE pour fournir l'accès à certaines tables au sein du périphérique.

Les opérations d'interrogation PING distant sur les périphériques Juniper requièrent l'accès aux tables pingCtlTable et jnxPingCtlTable au sein des périphériques Juniper PE. Pour cela, utilisez le modèle de contrôle d'accès basé sur la vue SNMP (VACM) pour la vue PrecisionIP.

Assurez-vous de configurer chaque périphérique Juniper PE pour garantir l'accès à ces tables pour la vue PrecisionIP avant d'activer la stratégie d'interrogation PING distant Juniper.

L'exemple suivant montre comment configurer un périphérique Juniper PE pour fournir l'accès pour la vue PrecisionIP dans les tables requises pour l'interrogation PING distant.

Configuration de l'accès à l'aide du VACM

Procédez comme suit pour garantir l'accès aux tables pingCtlTable et jnxPingCtlTable pour la vue PrecisionIP sur un périphérique Juniper PE :

1. Exécutez la commande telnet pour vous connecter au périphérique PE.
2. Saisissez configure pour lancer la ligne de commande d'édition.
3. Saisissez edit snmp, puis appuyez sur **Entrée**.
4. Saisissez edit view PrecisionIP, puis appuyez sur **Entrée**.
5. Saisissez set oid 1.3.6.1.2.1.80 include, puis appuyez sur **Entrée**.
6. Saisissez set oid 1.3.6.1.4.1.2636.3.7 include, puis appuyez sur **Entrée**.
7. Saisissez up, puis appuyez sur **Entrée**.

8. Saisissez `edit community watermelon`, puis appuyez sur **Entrée**, où `watermelon` est le nouveau nom de communauté d'écriture.
9. Saisissez `set view PrecisionIP`, puis appuyez sur **Entrée**.
10. Saisissez `set authorization read-write`, puis appuyez sur **Entrée**.
11. Saisissez `commit`, puis appuyez sur **Entrée**.
12. Saisissez `exit`, puis appuyez sur **Entrée**. De nouvelles entrées sont créées pour la vue `PrecisionIP` dans la table MIB `vacmViewTreeFamilyTable` sur le périphérique PE.

    Pour consulter le récapitulatif de la section insérée, saisissez `show configuration snmp`, puis appuyez sur **Entrée**. L'écran suivant s'affiche :

    ```
    view PrecisionIP {
    oid 1.3.6.1.2.1.80 include;
    oid 1.3.6.1.4.1.2636.3.7 include;
    }
    community watermelon {
    view PrecisionIP;
    authorization read-write;
    }
    ```

    Ces paramètres fournissent l'accès aux tables requises pour les opérations d'interrogation PING distant avec le nom de communauté `watermelon`.

Configuration de domaines

Vous pouvez configurer des domaines réseau pour qu'ils correspondent à votre environnement.

Création et configuration de domaines réseau supplémentaires

Pour ajouter des domaines réseau supplémentaires, configurez le contrôle de processus des domaines et enregistrez ces derniers avec la base de données topologiques NCIM. Les configurations et les interrogations peuvent être copiées depuis des domaines existants. Configurez ou reconfigurez les vues de réseau pour afficher les périphériques dans les nouveaux domaines.

Pourquoi et quand exécuter cette tâche

Utilisez une instance du processus **`ncp_ctrl`** pour exécuter et gérer chaque domaine. Si le processus **`ncp_ctrl`** d'un domaine n'est pas en cours, ce dernier ne peut pas être configuré dans l'interface graphique.

Vous pouvez exécuter le script `domain_create.pl` pour copier les données de configuration à partir d'un domaine existant. Le script ne copie pas la topologie du domaine d'origine.Pour des instructions sur le nombre de domaines réseau requis pour un déploiement, voir *Guide de l'Utilisateur IBM Tivoli Network Manager*.

Procédure

1. Sauvegardez le fichier `$NCHOME\etc\precision\CtrlServices.cfg` pour le domaine qui a été créé au cours de l'installation du produit.
2. Faites une copie du fichier `CtrlServices.cfg` et renommez-le `CtrlServices.`*`DOMAINE`*`.cfg`, où *DOMAINE* représente le domaine.

   Restriction : Utilisez uniquement des caractères alphanumériques et des traits de soulignement (_) pour les noms de domaine. Tous les autres caractères, notamment le trait d'union le (-), ne sont pas autorisés.

   Par exemple, `CtrlServices.MASTER.cfg`.

   Ensuite, effectuez les modifications requises dans le fichier `CtrlServices.`*`DOMAINE`*`.cfg`.
3. Pour configurer une reconnaissance pour le domaine :

a) Sauvegardez et créez des versions spécifiques au domaine des fichiers de configuration de la reconnaissance.
Par exemple, `DiscoPingFinderSeeds.MASTER.cfg`.

b) Configurez les paramètres des fichiers spécifiques au domaine.

4. Sauvegardez et créez une version spécifique au domaine du fichier `$NCHOME/etc/precision/ConfigItnm.cfg`.
Par exemple, `ConfigItnm.MASTER.cfg`.

   Ensuite, définissez les détails de la connexion pour le serveur d'objets dans ce fichier.
5. Pour enregistrer le nouveau domaine avec la base de données topologiques NCIM, sauvegardez et créez une version spécifique au domaine du fichier `$NCHOME/etc/precision/DbLogins.cfg`. Ensuite, éditez les informations de la connexion de base de données dans ce fichier.
6. Pour vous connecter à une autre source de données Tivoli Netcool/OMNIbus Web GUI :
   a) Sauvegardez et créez une copie spécifique au domaine du fichier `$NCHOME/etc/precisionModelNcimDb.cfg`.
   Par exemple, `ModelNcimDb.MASTER.cfg`.
   b) Dans le fichier spécifique au domaine, remplacez la propriété **m_WebTopDataSource** par le nom de la source de données.
7. Pour copier la configuration et les interrogations réseau d'un domaine existant, exécutez le script `domain_create.pl`.
L'exemple suivant crée un domaine appelé MASTER avec le mot de passe PASSWORD.

```
$NCHOME/precision/bin/ncp_perl
$NCHOME/precision/scripts/perl/scripts/domain_create.pl -domain MASTER
 -password PASSWORD
```

8. Démarrez les processus Network Manager sur le domaine.
Par exemple :

```
itnm_start ncp -domain MASTER
```

9. Créez des vues de réseau dans le domaine, ou modifiez vos vues de réseau existantes.

   Dans l'onglet **Filtre**, sélectionnez le nouveau domaine. Si vous ne définissez pas le nouveau domaine dans les vues de réseau, vous ne pouvez pas afficher ses périphériques. Si vous avez utilisé précédemment des scripts d'auto-approvisionnement pour créer automatiquement vos vues de réseau, vous devez les relancer en indiquant le nouveau domaine. Lorsqu'une reconnaissance du réseau est exécutée dans le nouveau domaine, les vues de réseau sont remplies avec les périphériques. Pour plus d'informations sur les vues de réseau, reportez-vous à la rubrique *Guide de l'Utilisateur IBM Tivoli Network Manager*.
10. Répétez les étapes pour configurer tous les domaines.

Que faire ensuite

Une fois **ncp_ctrl** a été démarré sur le domaine, vous pouvez configurer ce dernier. Par exemple, configurez la reconnaissance sur l'interface graphique **Reconnaissance de réseau**, éditez les fichiers de configuration ou configurez l'interrogation du réseau. Sélectionnez le domaine avant de configurer la reconnaissance ou l'interrogation.

Pour plus d'informations sur la configuration de la reconnaissance, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*. Pour plus d'informations sur l'interrogation du réseau, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Etant donné que la reconnaissance de réseau est un processus nécessitant beaucoup de ressources, les reconnaissances sont généralement exécutées pour un domaine à la fois. Pour exécuter des reconnaissances sur plusieurs domaines simultanément, vérifiez que vous disposez de suffisamment de ressources. Les vérifications habituelles sont les suivantes :

- Vérifiez qu'un nombre suffisant de connexions de base de données sont configurées.
- Assurez-vous que le trafic sur les périphériques réseau n'est pas trop chargé.

- Assurez-vous que la mémoire disponible est suffisante sur l'hôte pour exécuter la reconnaissance, par exemple en vérifiant l'utilisation de la mémoire des processus Network Manager.

Concepts associés

Domaines réseau

Avant l'installation, vous devez déterminer si vous souhaitez partitionner votre réseau en domaines ou si vous souhaitez conserver un domaine unique pour l'ensemble de votre réseau. Un domaine réseau est une collection d'entités réseau définie pour être reconnue et gérée.

Liaison d'un domaine à un contrôleur d'interface réseau (NIC)

La liaison de différents domaines client à différents contrôleurs d'interface réseau peut résoudre des problèmes d'adressage d'unités. Par exemple, si deux de vos domaines client ont des adresses IP se chevauchant, et que vous utilisez Network Manager sur un serveur unique pour gérer ces deux réseaux, la liaison de ces deux domaines client pour séparer les contrôleurs d'interface réseau permet à Network Manager de n'accéder qu'à ces adresses IP.

Pourquoi et quand exécuter cette tâche

Par exemple, supposons que vous ayez deux clients, A et B, et que ces deux clients aient des plages d'adresses IP qui se chevauchent. Supposons qu'ils aient tous deux un routeur avec l'adresse IP 192.168.1.1. Vous utilisez Network Manager sur un serveur unique pour gérer les deux réseaux client. Le problème est le suivant : comment les processus Network Manager peuvent-ils distinguer ces deux unités ? Par exemple, si vous exécutez une commande PING sur l'adresse IP 192.168.1.1, sur quel client la commande PING est-elle exécutée ?

Pour résoudre ce problème, ainsi que les problèmes similaires, procédez comme suit :

Procédure

1. Installez deux contrôleurs d'interface réseau distincts sur le serveur Network Manager.

   Le câble du contrôleur d'interface réseau A conduit au réseau du client A et le câble du contrôleur d'interface réseau B conduit au réseau du client B.

   Remarque : Il est possible que vous deviez installer plus de deux contrôleurs d'interface réseau. Les étapes indiquées ici sont fournies à titre d'illustration et s'appliquent à l'exemple donné précédemment dans cette rubrique.
2. Affectez le contrôleur d'interface réseau A au domaine du client A et le contrôleur d'interface réseau B au domaine du client B en ajoutant les lignes suivantes au fichier de configuration `$NCHOME/etc/precision/ServiceData.cfg`.

   ```
   SERVICE: IPv4BindAddress DOMAIN: CUST_A_DOMAIN ADDRESS: NIC_A_IP_ADDR PORT: 0
   SERVERNAME: itnmserver DYNAMIC: NO
   SERVICE: IPv4BindAddress DOMAIN: CUST_B_DOMAIN ADDRESS: NIC_B_IP_ADDR PORT: 0
   SERVERNAME: itnmserver DYNAMIC: NO
   ```

   Où :

   - *CUST_A_DOMAIN* correspond au nom de domaine du client A.
   - *CUST_B_DOMAIN* correspond au nom de domaine du client B.
   - *NIC_A_IP_ADDR* correspond à l'adresse IP du contrôleur d'interface réseau affecté au domaine du client A.
   - *NIC_B_IP_ADDR* correspond à l'adresse IP du contrôleur d'interface réseau affecté au domaine du client B.

   Cela permet de s'assurer que chaque domaine utilisera un contrôleur d'interface réseau différent et que les paquets de chaque domaine iront au client approprié.
3. Enregistrez le fichier de configuration `$NCHOME/etc/precision/ServiceData.cfg`.

Configuration d'une base de données dNCIM sous Linux on IBM z Systems

Sur Linux on IBM z Systems, vous devez apporter des changements de configuration à la base de données dNCIM. Par défaut, la base de données dNCIM est implémentée à l'aide de la base de données SolidDB. Cette base de données est automatiquement installée et ne nécessite pas de tâches de configuration. Toutefois, SolidDB n'est pas pris en charge sous Linux on IBM z Systems. Si vous travaillez sous Linux on IBM z Systems et souhaitez utiliser dNCIM, vous devez installer une autre base de données et la configurer pour qu'elle soit compatible avec le moteur de reconnaissance, **ncp_disco**.

Pourquoi et quand exécuter cette tâche

Pour configurer une base de données dNCIM sur Linux on IBM z Systems, procédez comme suit :

Procédure

1. Créez une entrée pour la base de données dans le ficher `DbLogins.`*`domaine`*`.cfg` où *domaine* correspond au nom de votre domaine.
   Par exemple:

```
insert into config.dbserver
(
    m_DbId,
    m_Server,
    m_DbName,
    m_Schema,
    m_Hostname,
    m_Username,
    m_Password,
    m_PortNum,
    m_EncryptedPwd
    m_EmbeddedProcess
    m_ScriptTimeoutSecs
)
values
(
    "DNCIM",
    "Db2",
    "ITNM",
    "dncim",
    "localhost",
    "user",
    "password",
    50000,
    1
    "ncp_disco"
    100
);
```

   Dans cet extrait, l'argument `m_ScriptTimeoutSecs` définit un délai en secondes pour tout script SQL qui est exécuté sur cette base de données. Un délai d'expiration peut s'avérer nécessaire si la base de données dNCIM est lente, par exemple lorsqu'elle n'est pas intégrée dans **ncp_disco** ou lorsqu'un serveur de base de données est lent.

   Remarque : Dans cet exemple, la base de données est au même emplacement que le moteur de reconnaissance, **ncp_disco**. L'attribut `m_Hostname` a donc la valeur `localhost`. Le fait que la base de données soit au même emplacement que le processus de reconnaissance garantit des reconnaissances plus rapides.
2. Remplissez le schéma de la base de données en utilisant le script Perl `$NCHOME/precision/scripts/sql/create_db_schemas.pl`.
   Par exemple :

   `./create_db_schemas.pl -server oracle|db2|| -dbname` *`nomBaseDeDonnées`* `-schema` *`schéma`* `-host` *`nomHôte`* `-username` *`nomUtilisateur`* `-password` *`motDePasse`* `-port` *`port`* `-action ncim`

   Où :

- L'attribut `-server` est le type de la base de données.
- L'attribut *dbname* varie selon le type de base de données.
  - Sur Oracle, utilisez la valeur SID.
  - Sur DB2, utilisez la valeur `m_DbId` du fichier `DbLogins.domain.cfg`.
- Le *schéma* correspond à l'argument `m_Schema` de l'insertion `DbLogins.domaine.cfg`. Par exemple, attribuez la valeur `dncim` à *schéma* pour que cette valeur corresponde à l'exemple d'insertion de l'étape 1.

  Remarque : Vous pouvez attribuer n'importe quel nom au schéma de base de données. La valeur utilisée pour `m_Schema` dans le fichier `DbLogins.domain.cfg` doit correspondre à la valeur utilisée pour l'argument `-schema` dans le script `create_db_schemas.pl`.
- L'attribut `-action` prend la valeur `ncim` car les bases de données dNCIM et NCIM sont de format identique.

Configuration de l'auxiliaire SNMP

L'auxiliaire SNMP est utilisé par les fonctions de reconnaissance et d'interrogation pour envoyer des demandes SNMP à des périphériques réseau. Vous pouvez configurer la façon dont l'auxiliaire SNMP émet les demandes SNMP ainsi que la façon dont il traite les résultats des demandes SNMP.

Pourquoi et quand exécuter cette tâche

Pour des informations sur les endroits où est utilisé l'auxiliaire SNMP dans les fonctions de reconnaissance et d'interrogation, voir les guides suivants :

- Pour la reconnaissance, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
- Pour l'interrogation, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Configuration de la régulation de l'auxiliaire SNMP

Vous pouvez activer la régulation dans l'auxiliaire SNMP. L'activation de la régulation augmente le délai entre les demandes SNMP de Network Manager envoyées à un périphérique réseau. Ainsi, la charge sur le périphérique réseau est moindre. Par défaut, la régulation est désactivée dans l'auxiliaire SNMP.

A propos de la régulation de l'auxiliaire SNMP

La régulation de l'auxiliaire SNMP établit un délai entre les demandes SNMP envoyées par l'auxiliaire SNMP avec une formule utilisant les paramètres GeneralSlowdown, GetNextBoundary et GetNextSlowdown.

Voici comment l'auxiliaire SNMP envoie des demandes sans régulation (par défaut) et avec régulation :

- Si la régulation est désactivée, les opérations GetNext SNMP fonctionnent comme suit : l'auxiliaire SNMP envoie la première demande Get SNMP et une fois que Network Manager obtient une réponse, l'auxiliaire SNMP envoie immédiatement la demande GetNext.
- Lorsque la régulation est activée, un délai est appliqué entre les demandes GetNext. Il s'agit généralement d'un délai défini court ou long. Le système effectue le suivi des demandes GetNext envoyées à un périphérique réseau et une fois que le nombre dépasse une certaine valeur, le délai plus long est appliqué ; sinon, le délai plus court est appliqué. Le système utilise les paramètres `GeneralSlowdown`, `GetNextBoundary` et `GetNextSlowdown` définis dans la table de base de données snmpStack.accessParameters afin de déterminer le délai à appliquer. Pour plus d'informations sur la table de base de données snmpStack.accessParameters, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Activation de la régulation de l'auxiliaire SNMP

Vous pouvez activer la régulation de l'auxiliaire SNMP.

Pourquoi et quand exécuter cette tâche

Pour activer la régulation de l'auxiliaire SNMP, procédez comme suit :

Procédure

1. Modifiez le fichier de configuration `NCHOME/etc/precision/NcPollerSchema.cfg`.

   Remarque : Vous pouvez rendre le domaine du fichier NcPollerSchema.cfg spécifique en le copiant dans le répertoire `NCHOME/etc/precision/NcPollerSchema.`*`NOM_DOMAINE`*`.cfg`, où *NOM_DOMAINE* correspond au nom du domaine.
2. Ajoutez la ligne suivante à la fin du fichier :

   ```
   update config.properties set EnableThrottling = 1;
   ```
3. Sauvegardez le fichier `NCHOME/etc/precision/NcPollerSchema.cfg`.
4. Activez les modifications en exécutant l'une des actions suivantes ou les deux :
   - Démarrez ou planifiez un nouvelle reconnaissance complète. Désormais, la reconnaissance utilisera la régulation.
   - Redémarrez le moteur d'interrogation, ncp_poller, avec l'option de ligne de commande `-readsnmpconfig` spécifiée.

Configuration de la prise en charge de GetBulk pour SNMP v2 et v3

Vous pouvez configurer l'auxiliaire SNMP pour utiliser l'opération GetBulk lorsque SNMP v2 ou v3 est utilisé. L'utilisation de l'opération GetBulk améliore la vitesse de la reconnaissance et l'efficacité de l'interrogation. Par défaut, l'auxiliaire SNMP n'utilise pas GetBulk.

A propos de GetBulk

Les commandes SNMP v2 et SNMP v3 GetBulk permettent de transférer des données de manière plus efficace. L'activation de l'auxiliaire SNMP pour l'utilisation de GetBulk réduit le temps nécessaire aux phases de collecte de données de reconnaissance. L'utilisation de GetBulk augmente également l'efficacité de l'interrogation.

La configuration de l'auxiliaire SNMP pour l'utilisation de GetBulk réduit l'empreinte des ressources de Network Manager des manières suivantes :

- Elle réduit l'impact sur la gestion du réseau car le nombre de paquets SNMP échangés est moins important.
- Elle réduit l'impact sur les unités gérées car le nombre de paquets SNMP traités est moins important.
- Elle réduit le temps UC requis par les processus Network Manager, comme le moteur de reconnaissance, ncp_disco, et le moteur d'interrogation, ncp_poller, en raison des frais généraux réduits.

L'utilisation de GetBulk réduit le temps nécessaire aux phases de collecte de données de reconnaissance ; un pourcentage élevé du temps requis pour la collecte de données étant un temps d'attente consacré au passage des paquets à travers le réseau. Cela réduit considérablement le temps nécessaire à la collecte de données pour les tables de grandes tailles, telles que les tables d'interface et de routage.

Configuration de Network Manager pour utiliser GetBulk

Vous pouvez configurer l'auxiliaire SNMP pour utiliser GetBulk. Vous pouvez également exclure des unités spécifiques de la prise en charge GetBulk.

Pourquoi et quand exécuter cette tâche

Si vous configurez l'auxiliaire SNMP pour utiliser GetBulk, cette configuration s'applique à tous les interrogateurs du domaine en cours. L'auxiliaire SNMP utilise également GetBulk pour toutes les unités du domaine accessibles à l'aide de SNMP v2 ou de SNMP v3, sauf si vous excluez des unités spécifiques comme indiqué dans les étapes suivantes.

Remarque : Lorsque GetBulk est activé, une requête GetBulk est toujours envoyée à la place d'une requête GetNext pour chaque unité compatible avec GetBulk.

Pour configurer l'auxiliaire SNMP pour utiliser GetBulk, procédez comme suit.

Procédure

1. Modifiez le fichier de configuration `NCHOME/etc/precision/NcPollerSchema.cfg`.

   Remarque : Vous pouvez rendre le domaine du fichier NcPollerSchema.cfg spécifique en le copiant dans le répertoire `NCHOME/etc/precision/NcPollerSchema.`*`NOM_DOMAINE`*`.cfg`, où *NOM_DOMAINE* correspond au nom du domaine.
2. Recherchez l'insertion dans la base de données `config.properties` et définissez la valeur de la propriété `UseGetBulk` à `1`.
3. Sauvegardez le fichier `NCHOME/etc/precision/NcPollerSchema.cfg`.
4. Facultatif : Si vous disposez d'unités réseau ne prenant pas en charge GetBulk, vous pouvez alors exclure ces unités une par une en procédant comme suit :
   a) Modifiez le fichier de configuration suivant : `NCHOME/etc/precision/SnmpStackSecurityInfo.cfg`.

      Remarque : Vous pouvez rendre le fichier `SnmpStackSecurityInfo.cfg` spécifique au domaine en le copiant dans `NCHOME/etc/precision/SnmpStackSecurityInfo.`*`NOM_DOMAINE`*`.cfg`, où *NOM_DOMAINE* est le nom du domaine.
   b) Pour chaque périphérique que vous voulez exclure de la prise en charge GetBulk, ajoutez une insertion dans le fichier de configuration `SnmpStackSecurityInfo.cfg`, similaire à l'exemple suivant.
   L'extrait exemple suivant exclut le périphérique 10.0.13.74 de la prise en charge GetBulk.

   ```
   insert into snmpStack.accessParameters
       ( m_NetAddress, m_UseGetBulk )
   values
       ( '10.0.13.74', 0 );
   ```

   c) Une fois l'insertion ajoutée pour chaque unité à exclure, enregistrez le fichier `NCHOME/etc/precision/ SnmpStackSecurityInfo.cfg`.
5. Activez les modifications en exécutant l'une des actions suivantes ou les deux :
   - Démarrez ou planifiez un nouvelle reconnaissance complète. La reconnaissance utilise maintenant GetBulk.
   - Redémarrez le moteur d'interrogation, ncp_poller, avec l'option de ligne de commande `-readsnmpconfig` spécifiée.

Configuration du nombre maximal de répétitions pour les requêtes GetBulk

La commande GetBulk est utilisée pour récupérer toutes les lignes d'une table à partir d'une ressource du réseau, par exemple pour récupérer toutes les lignes d'une table de routage à partir d'un routeur. Le paramètre max-repetitions indique le nombre de lignes de la table à récupérer en une seule opération

GetBulk. Vous pouvez ajuster les paramètres de configuration GetBulk afin de réduire le nombre de paquets échangés dans le cadre de l'opération GetBulk.

Pourquoi et quand exécuter cette tâche

Le SNMP Helper détermine la valeur maximale du nombre de répétitions pour les requêtes GetBulk (le paramètre `max-repetitions`) sur la base du calcul suivant :

```
max-repetitions = DefaultGetBulkMaxReps / #varbinds
```

Où :

- La propriété *DefaultGetBulkMaxReps* est définie dans le fichier `$NCHOME/etc/precision/NcPollerSchema.cfg`. La valeur par défaut est 20. Cette propriété définit le nombre affecté à la zone `max-repetitions` dans les requêtes GetBulk émises par les processus Network Manager. La valeur 20 est utilisée lorsque la requête GetBulk contient une valeur varbind unique. Si plusieurs valeurs varbind sont incluses, la valeur est ajustée en conséquence (divisée par le nombre de varbinds), de sorte que les réponses contiennent toujours un nombre similaire de varbinds.
- *#varbinds* correspond au nombre de liaisons de variable demandées. Dans SNMP Helper, cette valeur est habituellement 1. Toutefois, celle-ci peut varier en fonction de l'emplacement sur lequel SNMP Helper est déployé et des facteurs suivants :
  - Dans le moteur de reconnaissance, ncp_disco, la valeur *#varbinds* peut varier en fonction du code dans l'agent de reconnaissance.
  - Dans le moteur d'interrogation, ncp_poller, la valeur *#varbinds* peut varier en fonction des objets MIB inclus dans la définition d'interrogation.

Procédure

1. Modifiez le fichier de configuration `$NCHOME/etc/precision/NcPollerSchema.cfg`.

   Remarque : Vous pouvez rendre le domaine du fichier NcPollerSchema.cfg spécifique en le copiant dans le répertoire `$NCHOME/etc/precision/NcPollerSchema.`*`NOM_DOMAINE`*`.cfg`, où *NOM_DOMAINE* correspond au nom du domaine.
2. Recherchez la ligne qui définit la valeur de la propriété *DefaultGetBulkMaxReps*.
3. Changez la valeur affectée à la propriété *DefaultGetBulkMaxReps*.
4. Sauvegardez le fichier `$NCHOME/etc/precision/NcPollerSchema.cfg`.
5. Redémarrez le moteur d'interrogation, ncp_poller, pour activer les changements de configuration.

Configuration de l'authentification

Vous pouvez configurer différents composants de Network Manager afin qu'ils utilisent des méthodes d'authentification différentes.

Pourquoi et quand exécuter cette tâche

Pour plus d'information sur la connexion unique, consultez la section *Configuring Jazz for Service Management for SSO* dans l'Jazz for Service Management IBM Knowledge Center à l'adresse https://www.ibm.com/support/knowledgecenter/SSEKCU.

Modification de la méthode d'authentification des utilisateurs

Lorsque vous installez Network Manager vous pouvez choisir d'authentifier les utilisateurs de Network Manager dans un système d'authentification basé sur un fichier ou dans Tivoli Netcool/OMNIbus ObjectServer.

Pourquoi et quand exécuter cette tâche

Si vous souhaitez modifier la méthode d'authentification après l'installation, par exemple pour utiliser LDAP, suivez les mêmes instructions que pour modifier la méthode d'authentification de Tivoli Netcool/OMNIbus. Consultez les informations de la rubrique *Configuration de l'authentification utilisateur*

Configuration de l'authentification du fournisseur de services OQL

Les requêtes sur les bases de données du composant Network Manager peuvent être exécutées à partir de la ligne de commande à l'aide du processus du fournisseur de services OQL, ncp_oql. Vous pouvez configurer ncp_oql pour une authentification sur la base de données NCIM ou sur Tivoli Netcool/OMNIbus ObjectServer. Sinon, vous pouvez configurer ncp_oql pour autoriser l'exécution de requêtes sans authentification.

Pourquoi et quand exécuter cette tâche

Le moteur d'authentification du fournisseur de services OQL, ncp_auth, n'est plus utilisé dans Network Manager versions 3.9 et suivantes. Par défaut, il n'y a pas d'authentification pour les requêtes ncp_oql provenant de la ligne de commande. Vous pouvez configurer le fournisseur de services OQL pour s'authentifier sur la base de données NCIM ou sur ObjectServer, en procédant comme suit :

- *Authentification sur la base de données NCIM* : force le fournisseur de services OQL à s'authentifier à l'aide du nom d'utilisateur et du mot de passe de la base de données NCIM, comme indiqué lors de l'installation et comme configuré dans le fichier de configuration DbLogins.cfg.
- *Authentification sur ObjectServer* : force le fournisseur de services OQL à s'authentifier à l'aide du nom de compte administrateur et du mot de passe de Tivoli Netcool/OMNIbus, comme indiqué lors de l'installation.

L'authentification du fournisseur de services OQL est contrôlée par la valeur de `m_OQLAuthenticationMode` dans la table config.settings. La zone accepte les valeurs suivantes :

- 0 : Aucune authentification. Le nom d'utilisateur et le mot de passe ne sont pas requis. S'ils sont spécifiés sur la ligne de commande, ils sont ignorés.
- 1 : Authentication sur base de données NCIM database.
- 2 : Authentication sur Tivoli Netcool/OMNIbus ObjectServer.

Pour configurer l'authentification du fournisseur de services OQL :

Procédure

1. Modifiez le fichier de configuration **ncp_config**, `$NCHOME/etc/precision/ConfigSchema.cfg`.
2. Configurez l'une des insertions suivantes dans la table config.settings :
   - Configure authentication against the NCIM database.

     ```
     insert into config.settings
     (
             m_OQLAuthenticationMode,
     )
     values
     (
             1,
     );
     ```

   - Configure authentication against the ObjectServer.

```
insert into config.settings
(
        m_OQLAuthenticationMode,
)
values
(
        2,
);
```

IBM Support Assistant (ISA)

IBM Support Assistant est un outil vous permettant de rechercher des informations de support et de formation sur les produits.

Si vous avez besoin d'ouvrir un PMR (Problem Management Record), IBM Support Assistant peut vous faire gagner du temps en récupérant automatiquement les informations de support. IBM Support Assistant fournit les services suivants :

- Accès amélioré aux informations de support IBM, aux forums IBM et aux autres ressources via une interface de recherche fédérée (une seule recherche sur plusieurs ressources)
- Accès simple aux supports de formation IBM et aux calendriers de formation sur les produits.
- Accès simple aux pages d'accueil des produits, aux pages de support produit et aux forums sur les produits IBM via des liens appropriés.
- Temps de résolution des PMR amélioré via la collecte d'informations systèmes clés et l'envoi des données à IBM via la création électronique d'un PMR.

Un plugin Network Manager est disponible pour IBM Support Assistant. Ce plugin est nécessaire pour qu'IBM Support Assistant puisse diagnostiquer les problèmes de Network Manager.

Pour plus d'informations sur IBM Support Assistant, reportez-vous au site Web IBM suivant : https://www.ibm.com/support/knowledgecenter/SSLLVC/welcome/isa_welcome.html

Installation du collecteur IBM Support Assistant Lite

Le collecteur IBM Support Assistant (ISA) Lite pour Network Manager fournit une collecte des données automatisée sur des systèmes où Network Manager est installé. Il peut collecter les informations sur les journaux, les fichiers de règles, les données de configuration, etc.

Pourquoi et quand exécuter cette tâche

Pour installer le collecteur ISA Lite, procédez selon les étapes suivantes :

Procédure

1. Installez Network Manager.
2. Ouvrez la note technique suivante : http://www.ibm.com/support/docview.wss?uid=swg27015867
3. Suivez les étapes de la note technique pour configurer et utiliser le collecteur ISA Lite pour Network Manager.

Remarques

Ces informations s'appliquent au document PDF d'IBM Tivoli Network Manager IP Edition.

:NONE.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.</sli></sl> Pour le Canada, veuillez adresser votre courrier à : <ul linespace="COMPACT" ultype="SIMPLE"> <ph style="italic">IBM Director of Commercial Relations</ph> <ph style="italic">IBM Canada Ltd</ph> <ph style="italic">3600 Steeles Avenue East</ph> <ph style="italic">Markham, Ontario</ph> <ph style="italic">L3R 9Z7 Canada</ph>

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues auprès d'IBM écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japon, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
958/NH04
IBM Centre, St Leonards
601 Pacific Hwy
St Leonards, NSW, 2069
Australie

IBM Corporation
896471/H128B
76 Upper Ground
Londres
SE1 9PZ
Royaume-Uni

IBM Corporation
JBF1/SOM1 294
Route 100
Somers, NY, 10589-0100
Etats-Unis

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programme d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Marques

Les termes figurant dans le Tableau 17, à la page 231 sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

Tableau 17. Marques 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
Serveur de stockage Enterprise	PowerPC	
IBM	PowerVM	

Adobe, Acrobat, Portable Document Format (PDF), PostScript ainsi que toutes les marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Cette Offre Logiciels peut collecter des adresses IP, des noms d'utilisateur et des mots de passe pour la reconnaissance de réseau. Si la collecte de ces informations n'est pas activée, il est probable que des fonctionnalités essentielles mises à disposition par cette Offre Logiciels ne soient pas disponibles. En tant que client, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation de diverses technologies à ces fins, notamment des cookies, consultez les règles de confidentialité d'IBM à l'adresse http://www.ibm.com/privacy et la déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details, et lisez la section

intitulée "Cookies, pixels espions et autres technologies" et la page IBM Software Products and Software-as-a-Service Privacy Statement à l'adresse http://www.ibm.com/privacy.

Référence :

Printed in the Republic of Ireland

(1P) P/N:

2021-4212-01