

Dell Wyse Device Manager 5.7.3

Guía de instalación



Notas, precauciones y advertencias

 **NOTA:** Una NOTA señala información importante que lo ayuda a hacer un mejor uso de su producto.

 **PRECAUCIÓN:** Una PRECAUCIÓN indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

 **ADVERTENCIA:** Una señal de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

© 2018 Dell Inc. o sus filiales. Todos los derechos reservados. Dell, EMC, y otras marcas comerciales son marcas comerciales de Dell Inc. o de sus subsidiarias. Otras marcas pueden ser marcas comerciales de sus respectivos propietarios.

1 Introducción.....	6
Matriz del instalador.....	6
Matriz de compatibilidad.....	7
Compatibilidad de localización.....	10
Soporte técnico de Dell Wyse.....	10
Documentación y servicios relacionados.....	11
Comunidad en línea de Dell Wyse.....	11
2 Requisitos previos.....	12
Lista de verificación previa a la instalación.....	12
Requisitos de hardware.....	12
Requisitos de puertos de comunicación.....	13
Requisitos para la administración de dispositivos PCoIP.....	15
Lista de verificación para instalar WDM Enterprise Edition.....	15
3 Instalar Dell Wyse Device Manager.....	17
Instalar la WDM Workgroup Edition.....	17
Instalar WDM Enterprise Edition.....	28
Instalar WDM en un ambiente de nube.....	41
Instalar WDM en una configuración distribuida.....	54
Instalar la base de datos de WDM.....	55
Instalar los servicios de administración.....	56
Instalar el repositorio de software.....	57
Actualizar WDM.....	58
Configurar comunicaciones seguras.....	59
4 Desinstalar la instalación independiente de WDM.....	63
Desinstalar WDM en una configuración distribuida.....	63
5 Configurar agrupación en clústeres de bases de datos de alta disponibilidad para WDM.....	65
Componentes necesarios para agrupación en clústeres de bases de datos.....	66
Requisitos previos para la agrupación en clústeres de bases de datos.....	66
Configurar las máquinas virtuales principal y secundaria.....	66
Validar una configuración.....	67
Crear un clúster en el nodo principal.....	68
Implementar un nodo y cuórum de mayoría de recursos compartidos.....	68
Instalar .NET Framework en los nodos principal y secundario.....	69
Instalar SQL Server en los nodos principal y secundario.....	69
Instalar un clúster de conmutación por error de SQL Server en el nodo principal.....	70
Procedimiento después de la agrupación en clústeres.....	71
Ejecutar la utilidad de configuración de HA.....	73
Agregar una licencia en WDM.....	73

6 Configurar el equilibrio de carga.....	74
Configurar el servidor proxy de ARR.....	74
Instalar los servicios de información de Internet (IIS).....	75
Instalar el módulo ARR.....	76
Configurar el proceso de grupo de aplicaciones para ARR.....	77
Crear una granja de servidores de administración de WDM.....	78
Configurar SSL.....	79
Configurar las propiedades de la granja de servidores para ARR.....	80
Configurar el filtrado de solicitudes.....	81
Configurar el FQDN del proxy en Preferencias de WDM.....	82
Instalar los componentes de WDM.....	82
Configurar el equilibrio de carga de los dispositivos ThreadX 4.x.....	82
Configurar el equilibrio de carga de los dispositivos ThreadX 5.x.....	83
Instalar y configurar el proxy de alta disponibilidad.....	91
Instalar los servidores proxy de dispositivos Teradici.....	93
Agregar servidores proxy de dispositivos Teradici a WDM.....	95
Agregar proxy de alta disponibilidad a WDM.....	96
Reiniciar API de Threadx.....	97
7 Configurar la alta disponibilidad del servicio WebUI.....	100
Configurar el servidor proxy de ARR.....	100
Instalar los servicios de información de Internet (IIS).....	101
Instalar el módulo ARR.....	102
Cambiar el modelo de proceso del grupo de aplicaciones para la solicitud de enrutamiento de aplicaciones....	103
Crear una granja de servidores WebUI.....	104
Configurar SSL en el servidor proxy.....	107
Configurar las propiedades de la granja de servidores para la solicitud de enrutamiento de aplicaciones.....	108
Iniciar sesión en el navegador del WebUI.....	109
8 Instalar manualmente la base de datos de WDM por medio de scripts.....	110
Requisitos.....	110
Forma sugerida de instalar la base de datos de WDM.....	110
Archivos de script.....	110
9 Solución de problemas.....	113
Error de instalación de .NET Framework en Windows 2012 y Windows Server 2016.....	113
Falla al conectar la base de datos.....	114
Error al instalar la base de datos de WDM en una configuración distribuida.....	114
Falla de instalación de la base de datos después de la desinstalación manual de SQL Server Express 2014.....	114
Después de actualizar de WDM 5.5.1 a WDM 5.7, el repositorio de software no es seguro.....	115
Solución de problemas después de la implementación.....	115
Solución de problemas del equilibrio de carga.....	115
Falla de la función de prueba de condición en el proxy de ARR con SSL.....	115
El proxy de ARR arroja el código de error HTTP 502.3.....	116
El proxy de ARR arroja el código de error HTTP 502.4.....	116
Activar la descarga de SSL en el proxy.....	116

Transición indefinida durante la instalación.....	116
Problema del equilibrador de carga.....	117
Actualizar WDM en Windows 2008 SP2 de 32 bits.....	117
Error en la instalación de la actualización de WDM.....	117
Problema de configuración del ambiente de nube.....	117
Error en la instalación de WDM en la configuración de actualización.....	117

Introducción

Dell Wyse Device Manager (WDM) es un software que administra a todos los clientes ligeros y clientes cero de Dell Wyse. WDM permite a los administradores de TI ejecutar las siguientes funciones:

- Creación de imágenes de software, actualización y configuración de dispositivos de clientes ligeros y cero
- Rastreo de activos de dispositivos
- Monitoreo de la condición de los dispositivos
- Administración de la configuración de las políticas y la red en dispositivos
- Administración y replicación remota de los dispositivos

WDM utiliza los protocolos de comunicación estándar de la industria y una arquitectura basada en componentes para administrar de manera eficiente los dispositivos en la red. En esta guía se proporciona información sobre los requisitos previos para instalar WDM, y los pasos para instalar y configurar WDM en su ambiente.

Temas:

- [Matriz del instalador](#)
- [Matriz de compatibilidad](#)
- [Compatibilidad de localización](#)
- [Soporte técnico de Dell Wyse](#)

Matriz del instalador

En la siguiente matriz se describen las distintas combinaciones de Microsoft SQL Server y Microsoft Windows Server que son compatibles con el instalador.

Tabla 1. Matriz del instalador

			Windows Server 2008 R2 SP1			
Autenticación de RapportDB	SQL		Windows			
	Enterprise	Workgroup	Distribuido	Enterprise	Workgroup	Distribuido
Windows 2008 R2 SP1 + SQL Server 2008 R2	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2008 R2 SP1 + SQL Server 2008	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2008 R2 SP1 + SQL Server 2012	Sí	Sí	Sí	Sí	Sí	Sí
			Windows Server 2012			

Windows 2012 + SQL Express 2016 SP1	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2012 + SQL Server 2008 R2	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2012 + SQL Server 2008	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2012 + SQL Server 2012	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2012 + SQL Server 2014	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2012 + SQL Server 2016	Sí	Sí	Sí	Sí	Sí	Sí
			Windows Server 2016			
Windows 2016 + SQL Express 2016 SP1	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2016 + SQL Server 2012	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2016 + SQL Server 2014	Sí	Sí	Sí	Sí	Sí	Sí
Windows 2016 + SQL Server 2016	Sí	Sí	Sí	Sí	Sí	Sí

Matriz de compatibilidad

Tabla 2. Matriz de compatibilidad

Sistemas operativos compatibles con el servidor WDM	<ul style="list-style-type: none"> Windows Server 2008 R2 Enterprise SP1 Windows Server 2012 Standard Windows Server 2012 R2 Windows Server 2016 Windows 7 Enterprise SP1 (64 bits)
Sistemas operativos compatibles para actualizar todos los componentes de WDM	<ul style="list-style-type: none"> Windows 2008 R2 SP1 Enterprise Windows 2008 Service Pack 2 (32 bits) Windows 7 Enterprise SP1 (32 bits) Windows Server 2012 Standard Windows Server 2012 R2
Bases de datos compatibles	<ul style="list-style-type: none"> Microsoft SQL Server 2008 R2 (inglés) Microsoft SQL Server 2008 Enterprise (32 bits) Microsoft SQL Server 2012 Microsoft SQL Server 2014 Microsoft SQL Server 2016

- Microsoft SQL Server 2012 Enterprise Edition para alta disponibilidad
- Microsoft SQL Server 2016 Express SP1

Thin clients compatibles

Wyse ThinOS

- Wyse 3010 thin client con ThinOS
- Wyse 3020 thin client con ThinOS
- Wyse 3040 thin client con ThinOS
- Wyse 5010 thin client con ThinOS
- Wyse 5040 thin client con ThinOS
- Wyse 3030 LT thin client con ThinOS
- Wyse 5060 thin client con ThinOS
- Wyse 7010 thin client con ThinOS

Wyse ThinOS PCoIP

- Wyse 5040 thin client con PCoIP
- Wyse 5010 thin client con PCoIP
- Wyse 3030 LT thin client con PCoIP
- Wyse 5060 thin client con PCoIP

Wyse Enhanced Microsoft Windows Embedded Standard 7, compilación 818 o posterior

- Wyse 5010 thin client con WES7
- Wyse 5020 thin client con WES7
- Wyse 7010 thin client con WES7
- Wyse 7020 thin client con WES7
- Wyse 7010 thin client de chasis extendido con WES7
- Wyse 3030 thin client con WES7

Wyse Enhanced Microsoft Windows Embedded Standard 7p, compilación 850 o posterior

- Wyse 7010 thin client con WES7P
- Wyse 7010 thin client de chasis extendido con WES7P
- Wyse 5020 thin client con WES7P
- Wyse 7020 thin client con WES7P
- Wyse 7040 thin client con WES7P
- Dell Latitude E7270 thin client móvil
- Wyse 5060 thin client con WES7P
- Dell Latitude 3460 thin client móvil

Wyse Enhanced Microsoft Windows Embedded 8 Standard (64 bits)

- Wyse 5010 thin client con WE8S
- Wyse 5020 thin client con WE8S
- Wyse 7010 thin client con WE8S
- Wyse 7020 thin client con WE8S

Windows 10 IoT Enterprise (64 bits)

- Wyse 5020 thin client con Win10 IoT
- Wyse 7020 thin client con Win10 IoT

- Wyse 7040 thin client con Win10 IoT

Wyse Enhanced SUSE Linux Enterprise

- Wyse 5010 thin client con Linux
- Wyse 5020 thin client con Linux
- Wyse 7010 thin client con Linux
- Wyse 7020 thin client con Linux

ThinOS Lite

- Wyse 3010 cliente cero para Citrix
- Wyse 3020 cliente cero para Citrix
- Wyse 5010 cliente cero para Citrix

ThreadX/View cliente cero:

- Wyse 5030 cliente cero
- Wyse 7030 cliente cero
- Wyse 5050 AIO cliente cero con PCoIP

ThinLinux

- Wyse 3030 LT thin client con ThinLinux
- Wyse 3040 thin client con ThinLinux
- Wyse 7020 thin client con ThinLinux
- Wyse 5020 thin client con ThinLinux
- Wyse 5060 thin client con ThinLinux

Plataformas EOL Dell Wyse thin client compatibles

Wyse Enhanced Microsoft Windows Embedded Standard 7, compilación 818 o posterior

- C90LE7
- R90L7
- R90LE7
- X90c7
- X90m7
- Z90s7

Wyse Enhanced Microsoft Windows Embedded Standard 7P

- X90m7P
- Z90s7P

Wyse Enhanced Microsoft Windows Embedded 8 Standard (32 bits)

- Wyse 5010 thin client con WE8S
- Wyse 7010 thin client con WE8S
- Z90D8E

Wyse Enhanced SUSE Linux Enterprise

- C50LE
- R50L
- R50LE
- X50c
- X50M

- Z50S

ThinOS Lite

- C00X
- R00X

ThreadX/View cliente cero:

- P20

Wyse ThinOS

- C10LE
- R10L

Wyse Enhanced Microsoft Windows Embedded Standard 2009, compilación 641 o posterior

- C90LEW
- 5010
- R90LW
- R90LEW
- V90LEW
- X90CW
- X90MW
- 7010
- Z90SW

Compatibilidad de localización

Para el servidor WDM, se proporciona compatibilidad de localización en Windows 2008 R2 SP1 Enterprise Edition, Windows 2012 Standard R2 y Windows 2016 Standard R2 para los siguientes idiomas:

- Francés
- Alemán
- Español
- Japonés
- Chino simplificado

Soporte técnico de Dell Wyse

Para acceder al portal de autoservicio de recursos técnicos, la base de conocimientos, descargas de software, registro, ampliaciones de garantía/RMA, manuales de referencia, etc., visite www.dell.com/wyse/support. Para acceder al servicio al cliente, visite www.dell.com/support/contents/us/en/19/article/Contact-Information/International-Support-Services/international-contact-center?ref=contactus, y los números de teléfono de asistencia básica y Pro están disponibles en www.dell.com/supportcontacts.

NOTA: Antes de continuar, verifique si su producto tiene una etiqueta de servicio Dell. Para conocer los productos con etiqueta de servicio Dell, vaya a www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse para obtener más información.

Documentación y servicios relacionados

Los folletos informativos contienen las funciones de los productos de hardware que están disponibles en el sitio web de Dell Wyse. Vaya a <http://www.dell.com/wyse> y seleccione su producto de hardware para buscar y descargar el folleto informativo.

Para obtener soporte para su producto Wyse, compruebe la etiqueta de servicio del producto o el número de serie.

- Para productos con etiqueta de servicio de Dell, localice los artículos de la base de conocimientos y los controladores en las páginas de productos de Dell Wyse.
- Para productos sin etiqueta de servicio de Dell, busque la asistencia necesaria en el dominio de soporte de Wyse.

Comunidad en línea de Dell Wyse

Dell Wyse mantiene una comunidad en línea donde los usuarios de nuestros productos pueden solicitar e intercambiar información en foros. Visite los foros de la comunidad en línea de Dell Wyse en: en.community.dell.com/techcenter/enterprise-client/wyse_general_forum/.

Requisitos previos

En esta sección se enumeran los requisitos previos, los requisitos de hardware y software con los que debe cumplir a fin de preparar su ambiente e instalar y configurar WDM. Esta sección consta de:

- Lista de verificación previa a la instalación
- Requisitos de hardware
- Requisitos de software
- Requisitos de puertos de comunicación
- Requisitos de actualización
- Requisitos para la administración de dispositivos PCoIP

Temas:

- [Lista de verificación previa a la instalación](#)
- [Requisitos de hardware](#)
- [Requisitos de puertos de comunicación](#)
- [Requisitos para la administración de dispositivos PCoIP](#)
- [Lista de verificación para instalar WDM Enterprise Edition](#)

Lista de verificación previa a la instalación

Antes de iniciar la instalación de WDM, asegúrese de cumplir con los siguientes requisitos:

- El servidor en el que instalará WDM debe estar dedicado a los servicios de WDM y no debe realizar funciones adicionales. Por ejemplo, el servidor no se debe utilizar como un controlador de dominio, un controlador de respaldo, un servidor de correo electrónico, un servidor web de producción, un servidor DHCP, un servidor MSMQ o un servidor de aplicaciones.
- Instale un sistema operativo compatible en el servidor en el que instale WDM. Para obtener más información, consulte la [Información de soporte](#).
- Asegúrese de que no haya ninguna otra aplicación que requiera que los IIS se estén ejecutando en el sistema en el que instalará WDM.
- Asegúrese de que todos los puertos de comunicación estén disponibles y ábralos para la comunicación entre servidores, enrutadores y conmutadores. Para obtener más información, consulte [Requisitos de puertos de comunicación](#).
- Durante la instalación, asegúrese de que tiene acceso al CD-ROM de su sistema operativo y los archivos del sistema de Microsoft Windows. El instalador de WDM comprueba que el sistema cumpla con todos los requisitos de software. Si algún software no está instalado, el instalador le pedirá que instale el que sea necesario. Por lo tanto, debe tener acceso al CD-ROM de su sistema operativo o la ubicación de red para acceder a los archivos de sistema de Microsoft Windows.
- Instale Adobe Acrobat Reader para leer el Contrato de licencia para el usuario final (CLUF) y la Guía de instalación.
- El servidor debe estar instalado con los componentes de ThreadX 5x en Windows 2012 y posteriores.

Requisitos de hardware

El sistema en el que instale WDM debe cumplir o superar los requisitos mínimos del sistema, y depende del sistema operativo que utilice. El espacio libre real necesario depende del número y tamaño de los paquetes que registre, y también en el número de dispositivos que administrará.

Tabla 3. Requisitos de hardware de servidor para SO de 32 bits

Categoría	Requisitos mínimos	Configuración recomendada
CPU	2,5 GHz doble core Intel o AMD	Cuatro núcleos Intel o AMD
RAM	4 GB En el caso de una máquina virtual, debe tener 2 GB asignados inicialmente	4 GB
Espacio libre mínimo	40 GB	40 GB

Tabla 4. Requisitos de hardware de servidor para SO de 64 bits

Categoría	Requisitos mínimos	Configuración recomendada
CPU	2,5 GHz doble core Intel o AMD	Cuatro núcleos Intel o AMD
RAM	6 GB	8 GB
Espacio libre mínimo	40 GB	40 GB

Requisitos de puertos de comunicación

Los componentes de software de WDM requieren que algunos puertos de comunicación permanezcan abiertos en sus servidores, enrutadores y conmutadores. Por ejemplo, WDM depende de los puertos de comunicaciones HTTP/HTTPS para las operaciones iniciadas por este y aplicadas a los dispositivos.

Las operaciones aplicadas incluyen:

- Ejecutar comandos del dispositivo rápidos, como actualizar la información del dispositivo, reiniciar, cambiar la información del dispositivo o la red, obtener configuración del dispositivo, etc.
- Distribuir los paquetes en un momento específico.

Normalmente, el puerto 80 es el puerto HTTP predeterminado y el puerto 443 es el puerto HTTPS predeterminado. Si cualquiera de estos puertos está cerrado, WDM no puede aplicar las actualizaciones o los comandos rápidos a los dispositivos.

Tabla 5. Puertos de comunicaciones

Componente de WDM	Protocolo y puertos correspondientes	Puerto	Función
GUI	HTTP	80 280	Comunicarse con el servicio web y el servicio estándar
	FTP	21	Registrar nuevos paquetes en el repositorio de software maestro
	Base de datos OLE	1433 (valor predeterminado) Se puede configurar durante la instalación	Comunicarse con la base de datos de WDM
	VNC	5800 5900	Dispositivos sombra remota.

Componente de WDM	Protocolo y puertos correspondientes	Puerto	Función
Servicio web	HTTP	80 280	Comunicarse con el agente web, la interfaz gráfica de usuario y el servicio estándar
	HTTPS	443 8443	Comunicación segura con el agente web, la interfaz gráfica de usuario y el servicio estándar
	Base de datos OLE	1433 (valor predeterminado) Se puede configurar durante la instalación	Comunicarse con la base de datos de WDM
Agente web	HTTP	80 280	Comunicación con el servicio web.
	FTP	21	Leer y escribir archivos en los repositorios de software maestro y remoto.
Proxy DHCP y servicios TFTP	Base de datos OLE	1433 (valor predeterminado) Se puede configurar durante la instalación	Comunicarse con la base de datos de WDM
	HTTP	8008	Comunicarse con la interfaz gráfica de usuario y el servicio web
Proxy DHCP, servicios TFTP y PXE	DHCP	67 68 4011	Solicitudes de proceso UDP desde dispositivos con PXE habilitado al servicio estándar.
	TFTP	69	Descargar imagen de arranque para habilitar el procesamiento de administración
	HTTP	80	Comunicarse con el servicio web con respecto a las actividades y el estado de la tarea en curso
	FTP	21	Cargar y descargar archivos en los repositorios de software maestro y remoto
Proxy DHCP, TFTP servicios y compatibilidad heredada con los agentes anteriores de WDM	UDP	44956 44957	Detectar dispositivos mediante transmisiones dirigidas de subred que tengan instalados agentes anteriores de WDM (5.0.0.x y anteriores)
	TCP	44955	Detectar dispositivos utilizando escaneo de rango IP Actualizar los dispositivos que tengan instalado un agente anterior de WDM (5.0.0.x y anteriores)

Componente de WDM	Protocolo y puertos correspondientes	Puerto	Función
Servicio de administrador de ThreadX 4.x	TCP	9880 50000	Comunicarse con dispositivos ThreadX 4.x
Servicio de administrador de ThreadX 5.x	TCP	49159 5172	Comunicarse con dispositivos ThreadX 5.x <div style="border-left: 1px solid black; padding-left: 5px;"> <p>NOTA: Debe agregar ambos puertos de comunicación a las reglas de entrada del firewall. Si es necesario, se puede personalizar el número de puerto 49159. Para personalizar el puerto 49159 predeterminado, debe agregarlo manualmente.</p> </div>

Requisitos para la administración de dispositivos PCoIP

Los dispositivos PCoIP que ejecutan el firmware ThreadX requieren registro de recursos de ubicación de servicio DNS (SRV) para realizar las siguientes acciones:

- **Partial Check-In (heartbeat) (Registro parcial [latidos]):** el dispositivo realiza un registro de latidos cada hora.
- **Firmware Download Completion Status (Estado de finalización de carga de firmware):** el servidor inicia la carga de firmware y el dispositivo que usa el registro SRV de DNS inicia la finalización de descarga.
- **ThreadX 4.x:** configure FTP si tiene previsto utilizar la función de actualización del firmware para los dispositivos PCoIP (ThreadX 4.x). Debe activar esta opción en el repositorio de software. Para obtener más información sobre cómo activar FTP en el repositorio de software, consulte *Dell Wyse Device Manager Administrator's Guide (Guía del administrador de Wyse Device Manager)*.
- **ThreadX 5.x:** configure CIFS si tiene previsto utilizar la función de actualización del firmware para los dispositivos PCoIP (ThreadX 5.x). Debe activar esta opción en el repositorio de software. Para obtener más información sobre cómo activar CIFS en el repositorio de software, consulte *Dell Wyse Device Manager Administrator's Guide (Guía del administrador de Wyse Device Manager)*.

Lista de verificación para instalar WDM Enterprise Edition

Si va a instalar WDM Enterprise Edition, asegúrese de lo siguiente:

- Obtenga acceso a su clave de WDM Enterprise Edition o la evaluación de Enterprise, según necesite durante la instalación.
- Instale la versión compatible de SQL Server. El instalador de WDM proporciona Microsoft SQL Express 2014 como la opción predeterminada, pero puede elegir otra versión compatible de SQL Express.
- Debe instalar FTP Services y activarlo para utilizar FTP para los dispositivos Dell Wyse PCoIP (ThreadX 4.x).
- Debe instalar FTP Services y activarlo para utilizar CIFS para los dispositivos Dell Wyse PCoIP (ThreadX 5.x).

NOTA:

Si tiene pensado utilizar PColP (Thread X), cree y configure un registro de recursos de ubicación de servicio DNS (SRV). Para obtener más información, consulte [Configurar el equilibrio de carga de los dispositivos ThreadX 4.x](#) y [Configurar el equilibrio de carga de los dispositivos ThreadX 5.x](#).

Instalar Dell Wyse Device Manager

WDM consiste en los siguientes componentes:

- Base de datos
- Servidor de administración
- Repositorio de software
- Otros servicios
- Web UI

Puede instalar todos los componentes en el mismo sistema o puede tener una instalación distribuida en la que cada componente se instale en un sistema diferente.

WDM está disponible en las siguientes ediciones:

- **Enterprise Edition:** esta edición necesita una clave de licencia específica e incluye todas las funciones de WDM. Puede administrar un gran número de dispositivos de thin client con esta edición. Puede instalar esta edición en un ambiente distribuido y puede instalar todos los componentes en diferentes sistemas.
- **Workgroup Edition:** esta edición consta de una clave de licencia gratuita y determinadas funciones de WDM están desactivadas. Puede administrar hasta 10.000 dispositivos de thin client con esta edición. Debe instalar todos los componentes en el mismo sistema y no puede tener una instalación distribuida con esta edición.

NOTA: Debe activar la licencia Workgroup.

NOTA:

- Para ejecutar el instalador de WDM (setup.exe), debe iniciar sesión en el sistema como administrador.
- No puede instalar WDM en servidores que estén ejecutando otros servicios, como el DNS, DHCP, los servicios de dominio de AD o los servicios que entren en conflicto con la funcionalidad y los recursos de WDM.
- Cuando instala la base de datos de WDM en una configuración independiente o distribuida, y desea utilizar una base de datos de SQL existente, asegúrese de que sea una versión completa de SQL Server y no SQL Server Express.
- Los foros de la Comunidad Dell dan soporte a WDM Workgroup Edition.
- Los componentes de administración de Threadx 5x solo son compatibles con Enterprise Edition.

Temas:

- [Instalar la WDM Workgroup Edition](#)
- [Instalar WDM Enterprise Edition](#)
- [Instalar WDM en un ambiente de nube](#)
- [Instalar WDM en una configuración distribuida](#)
- [Actualizar WDM](#)

Instalar la WDM Workgroup Edition

Pasos

- 1 Extraiga el contenido del instalador de WDM en el sistema en donde desea instalar WDM.
- 2 Vaya a la carpeta en la que extrajo el instalador y ejecute **setup.exe**.

Se muestra la pantalla de **Welcome** (Bienvenida).



Figura 1. Pantalla de bienvenida

- 3 Haga clic en **NEXT** (Siguiente).
- 4 En el tipo de licencia, seleccione **WORKGROUP** y haga clic en **NEXT** (Siguiente).

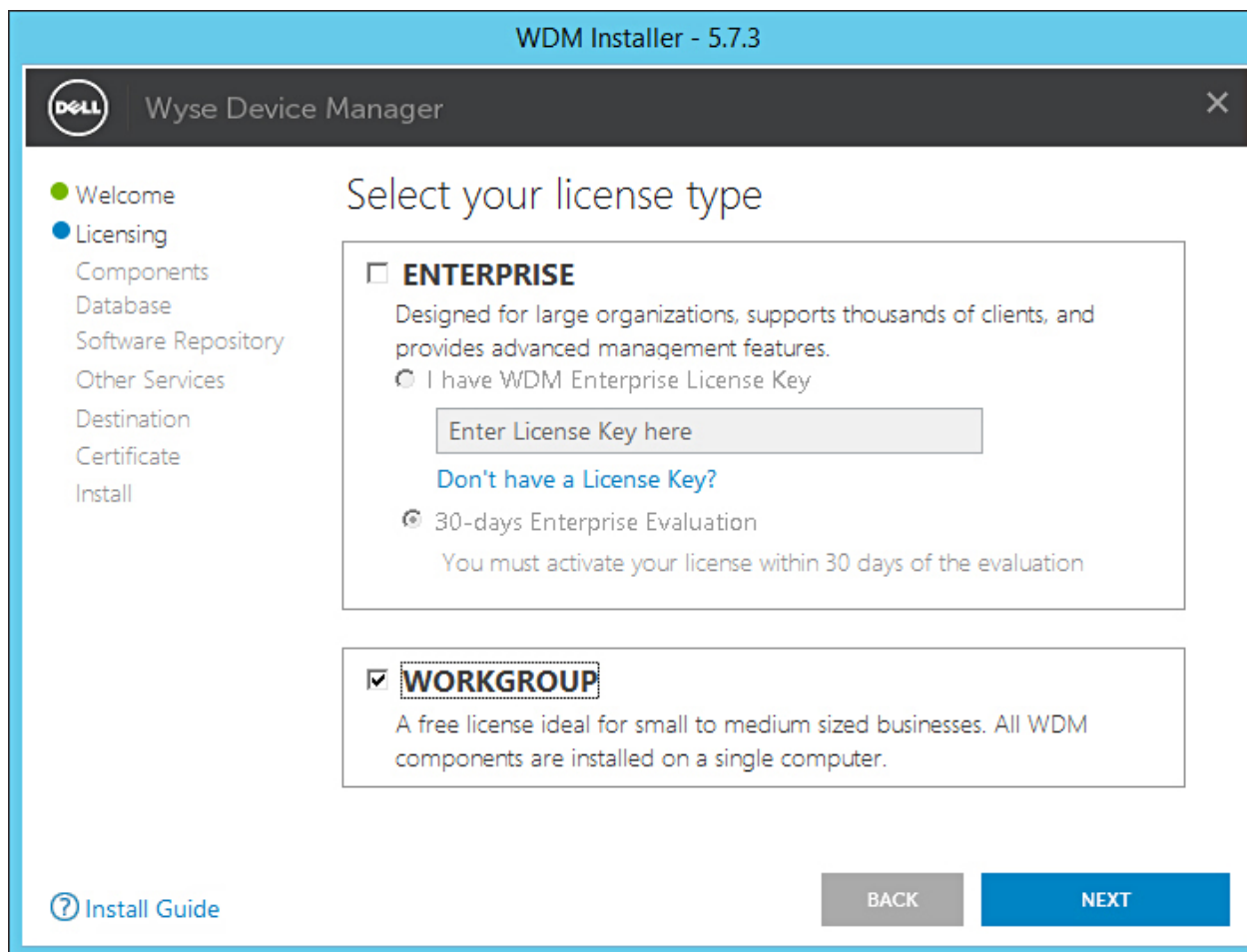


Figura 2. Tipo de licencia Workgroup

NOTA: En Workgroup Edition, la clave de licencia se incluye con el instalador y no es necesario ingresar ningún detalle.

Se muestra la pantalla **Components** (Componentes).

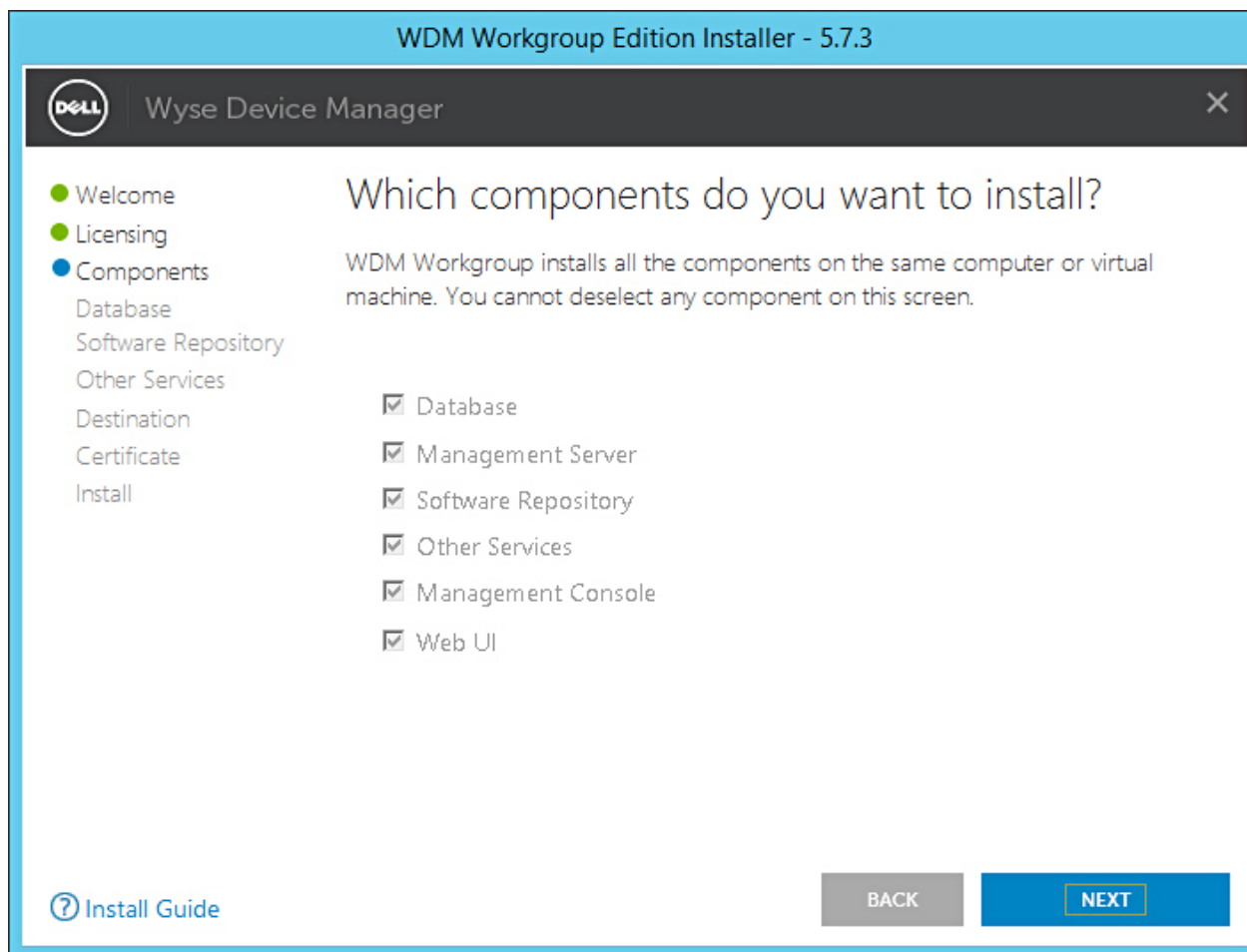


Figura 3. Pantalla Components (Componentes)

- Haga clic en **NEXT** (Siguiente).

NOTA: Todos los componentes están seleccionados de manera predeterminada y no se puede anular ninguna selección.

Se muestra la pantalla **Configure Database** (Configurar base de datos).

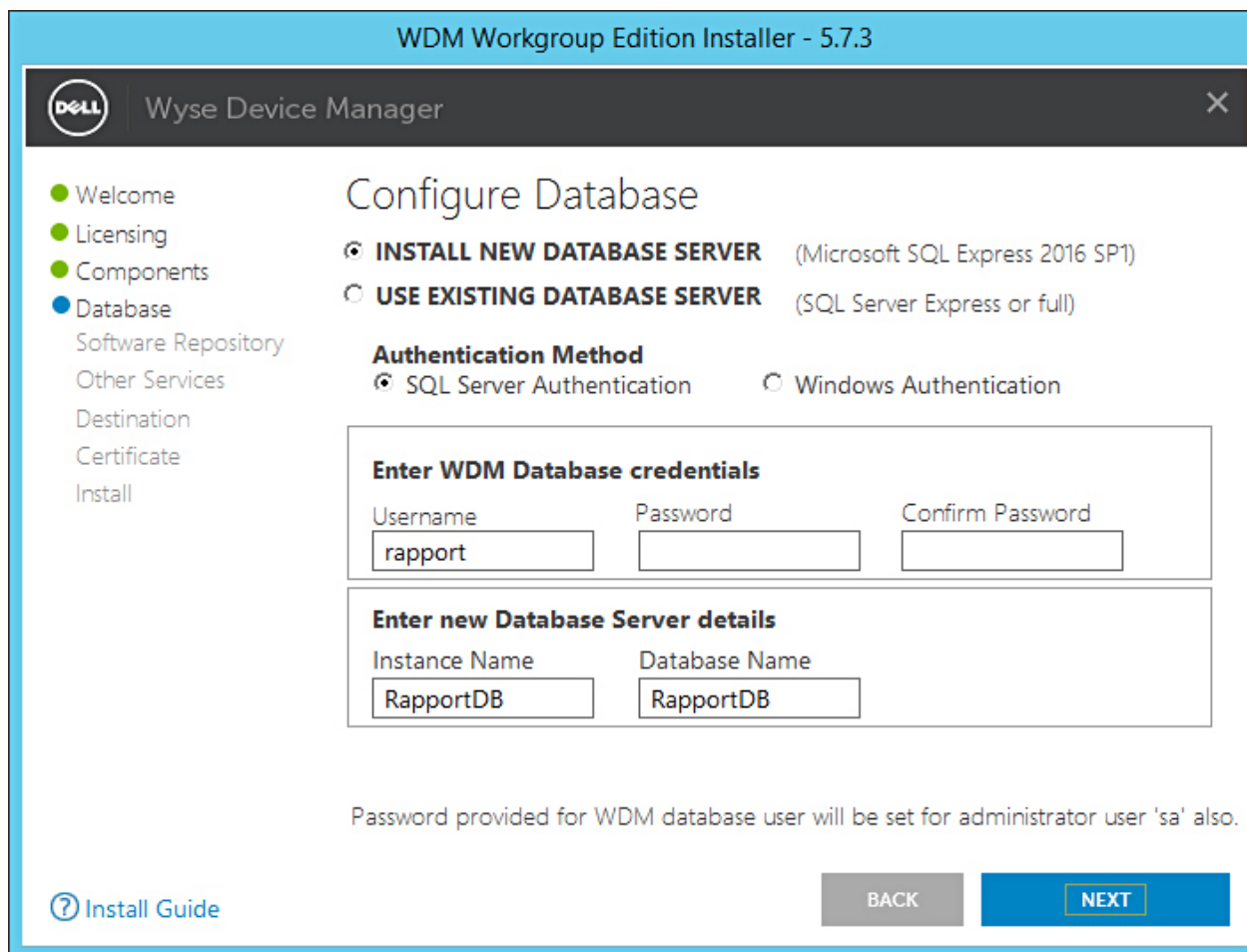


Figura 4. Pantalla Configure Database (Configurar base de datos)

- 6 En la pantalla **Configure Database** (Configurar base de datos), seleccione una de las siguientes opciones:
 - **Install New Database Server (Microsoft SQL Express 2016 SP1)** (Instalar nuevo servidor de base de datos [Microsoft SQL Express 2016 SP1]): seleccione esta opción si no tiene ninguna versión compatible de Microsoft SQL Server instalada en el sistema, y continúe con el paso 8.
 - **Use Existing Database Server (SQL Server Express or full)** (Usar servidor de base de datos existente [SQL Server Express o completo]): seleccione esta opción si ya ha instalado una versión compatible de Microsoft SQL Server en el sistema. Si selecciona esta opción, asegúrese de que el servidor de base de datos existente esté en el mismo sistema en el que instalará WDM Workgroup Edition, y continúe con el paso 9.
- 7 Si seleccionó la primera opción en el paso 7, seleccione el método de autenticación.

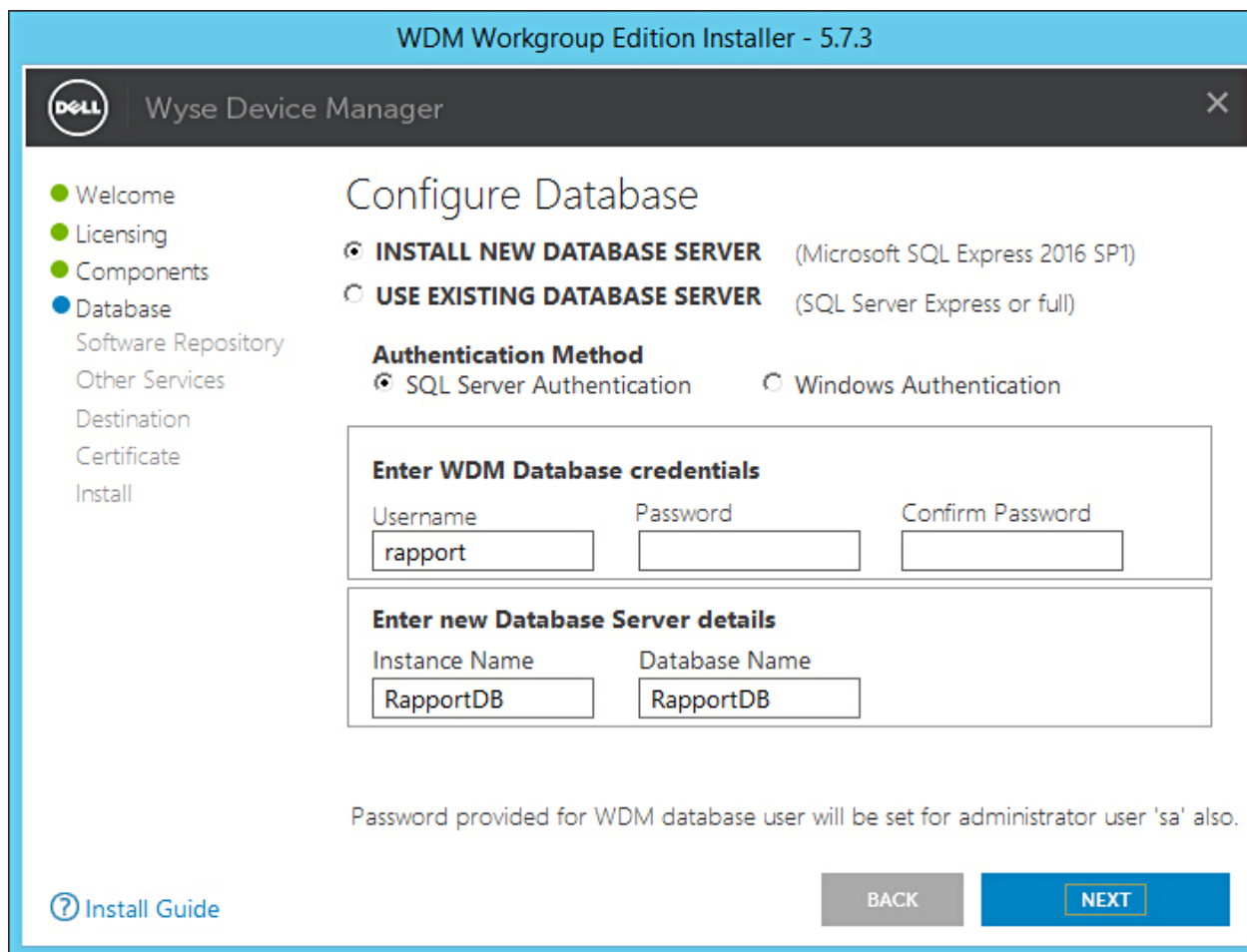


Figura 5. Opción Install New Database Server (Instalar nuevo servidor de base de datos)

- **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:
 - 1 Ingrese las credenciales de la base de datos de WDM.
 - 2 Ingrese las nuevas credenciales de la base de datos. Puede ingresar el nombre de la instancia y el nombre de la base de datos en los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.
- **Windows Authentication (Autenticación de Windows)**: ingrese los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.

NOTA:

- Seleccione **Windows Authentication** (Autenticación de Windows) si desea conectarse a la base de datos de WDM con sus credenciales de inicio de sesión de Windows.
- La contraseña debe cumplir con las reglas de complejidad del sistema operativo Windows.

8 Si seleccionó la segunda opción en el paso 7, seleccione el método de autenticación.

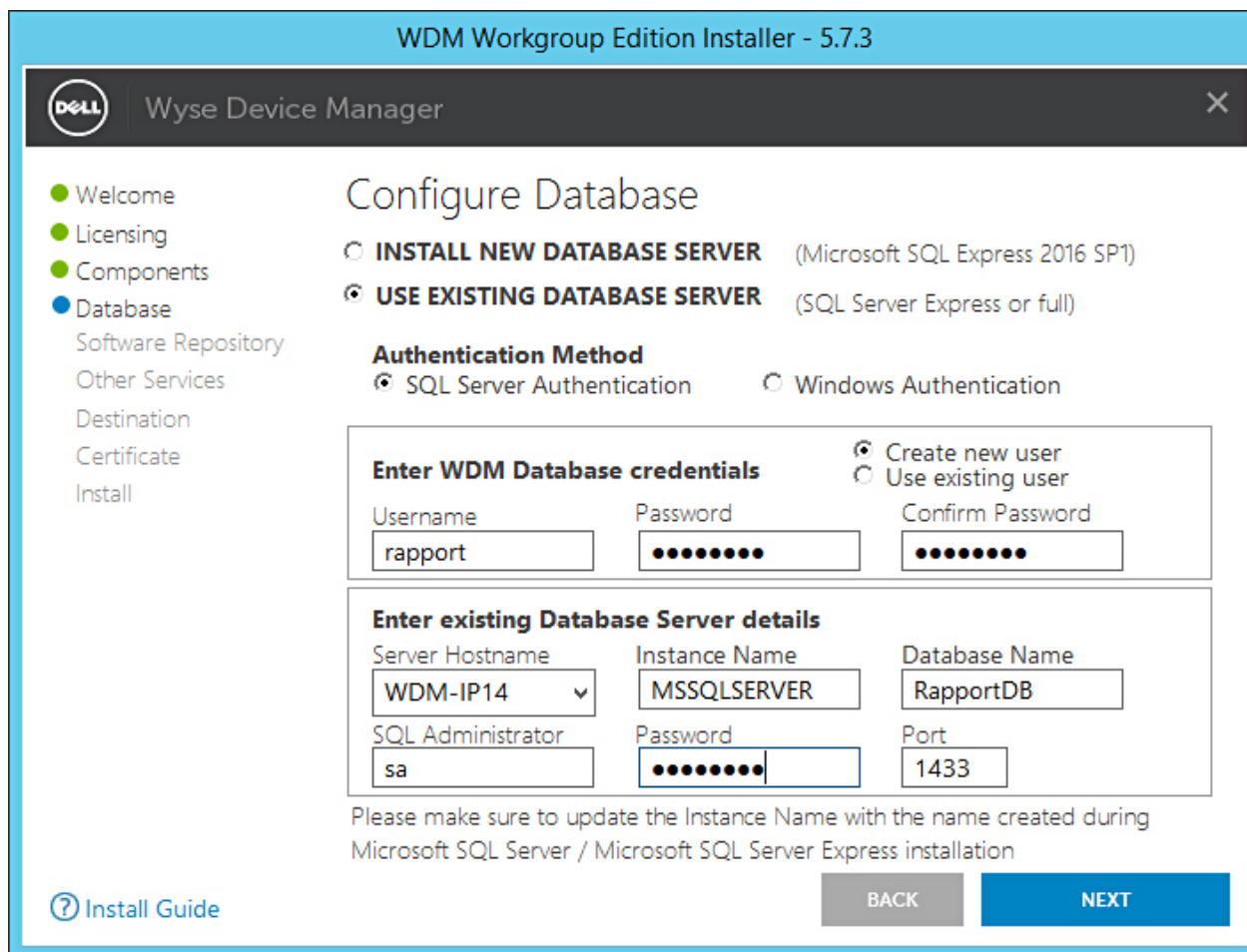


Figura 6. Opción Use Existing Database Server (Usar servidor de base de datos existente)

- **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:
 - 1 Seleccione la opción de Create New User (Crear nuevo usuario) o Use the existing user (Usar un usuario existente) y, a continuación, ingrese las credenciales de la base de datos de WDM.
 - 2 Ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL. El número de puerto predeterminado es 1433.
 - **Windows Authentication (Autenticación de Windows)**: ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL.
- 9 Haga clic en **NEXT** (Siguiente).
 Se muestra la pantalla **Configure Software Repository Server** (Configurar el servidor de repositorio del software).

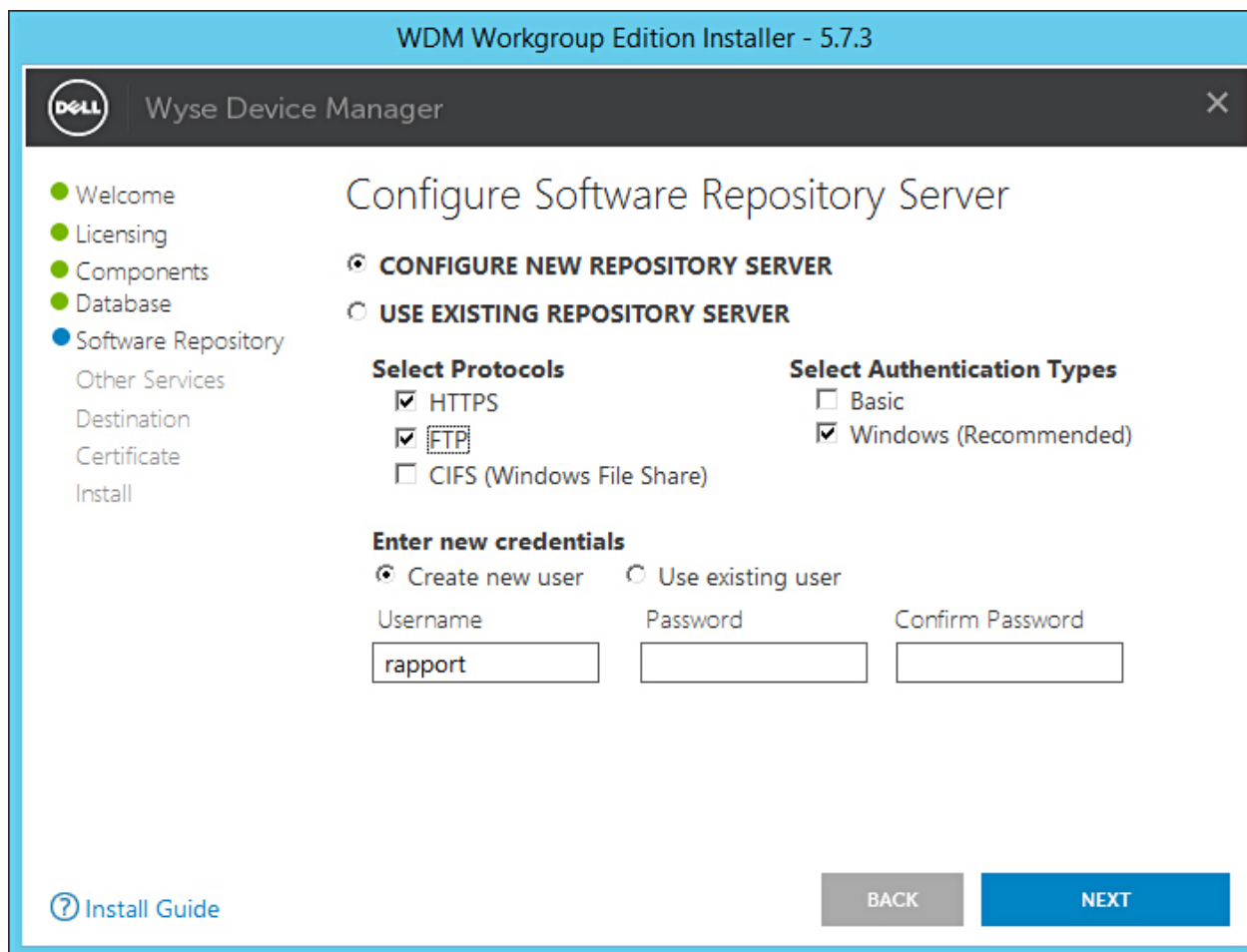


Figura 7. Pantalla Configure Software Repository Server (Configurar el servidor de repositorio del software)

- 10 En la pantalla **Configure Software Repository Server** (Configurar el servidor de repositorio del software), puede elegir una de las siguientes opciones:
- **CONFIGURE NEW REPOSITORY SERVER** (Configurar nuevo servidor de repositorio): seleccione esta opción si desea que el instalador configure un nuevo servidor de repositorio. Para configurar un nuevo servidor de repositorio:
 - Seleccione el protocolo y la configuración para distribuir el software a los dispositivos administrados. **HTTPS** aparece seleccionado de manera predeterminada. También puede seleccionar **FTP** para ThreadX 4.x y **CIFS** para ThreadX 5.x.
 - Seleccione el tipo de autenticación. **Windows** aparece seleccionado de manera predeterminada.
 - **NOTE: Se requiere la autenticación básica para Linux.**
 - Cree nuevas credenciales de usuario o use las credenciales existentes.
 - **USE EXISTING REPOSITORY SERVER** (Usar servidor de repositorio existente): seleccione esta opción si desea que el instalador configure un servidor de repositorio existente. Para configurar el servidor de repositorio existente:
 - Seleccione el protocolo y la configuración para distribuir el software a los dispositivos administrados. **HTTPS** aparece seleccionado de manera predeterminada. También puede seleccionar **FTP** para ThreadX 4.x y **CIFS** para ThreadX 5.x.
 - Seleccione el tipo de autenticación. **Windows** aparece seleccionado de manera predeterminada.
 - Ingrese las credenciales del servidor. La opción de dirección IP del servidor aparece atenuada y el nombre de usuario predeterminado es rapport.
- 11 Haga clic en **NEXT** (Siguiente).
- 12 Seleccione los servicios que desea instalar y haga clic en **NEXT** (Siguiente).

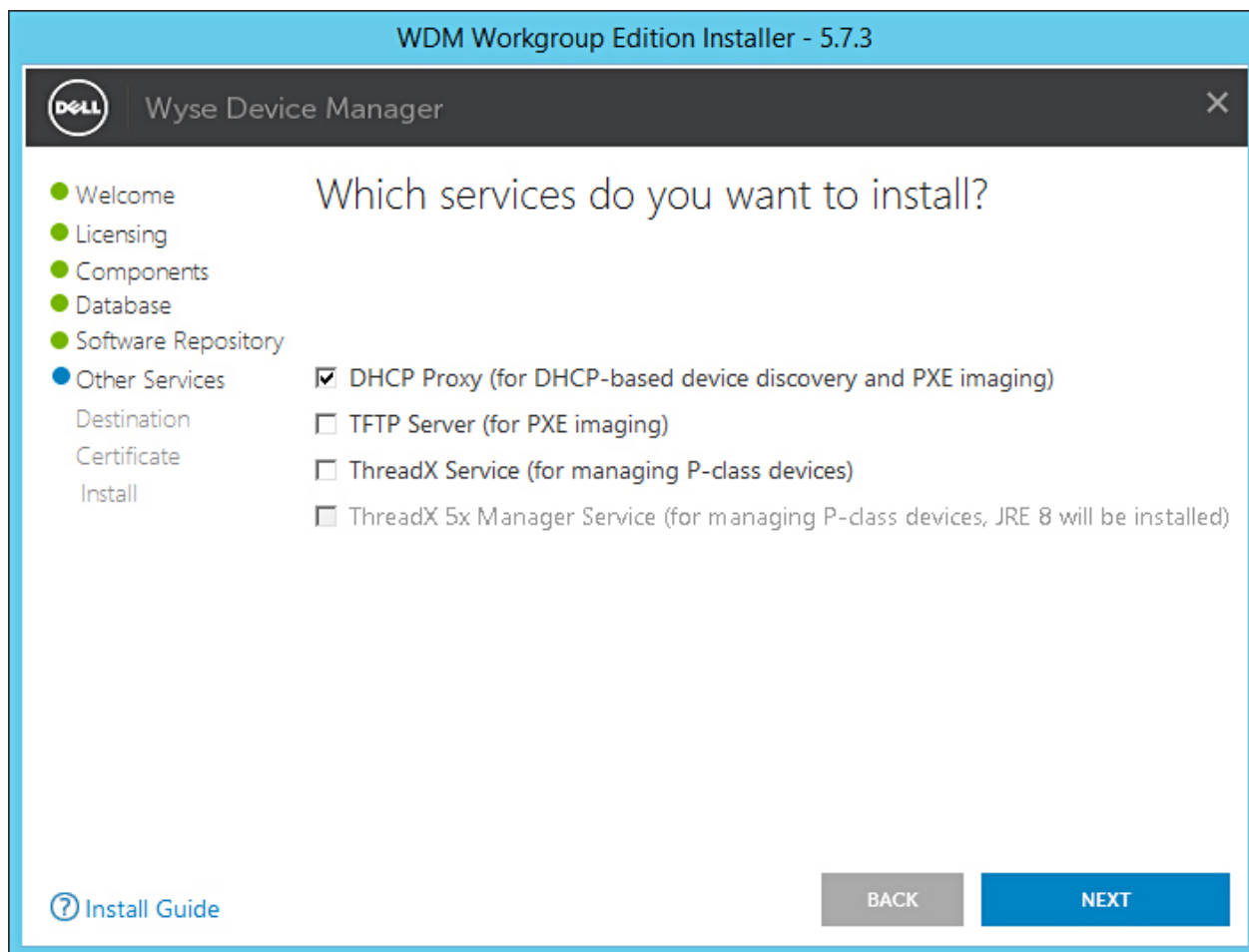


Figura 8. Pantalla Other Services (Otros servicios)

NOTA: Proxy DHCP aparece seleccionado de manera predeterminada.

13 Ingrese la ruta de instalación y haga clic en **NEXT** (Siguiente).

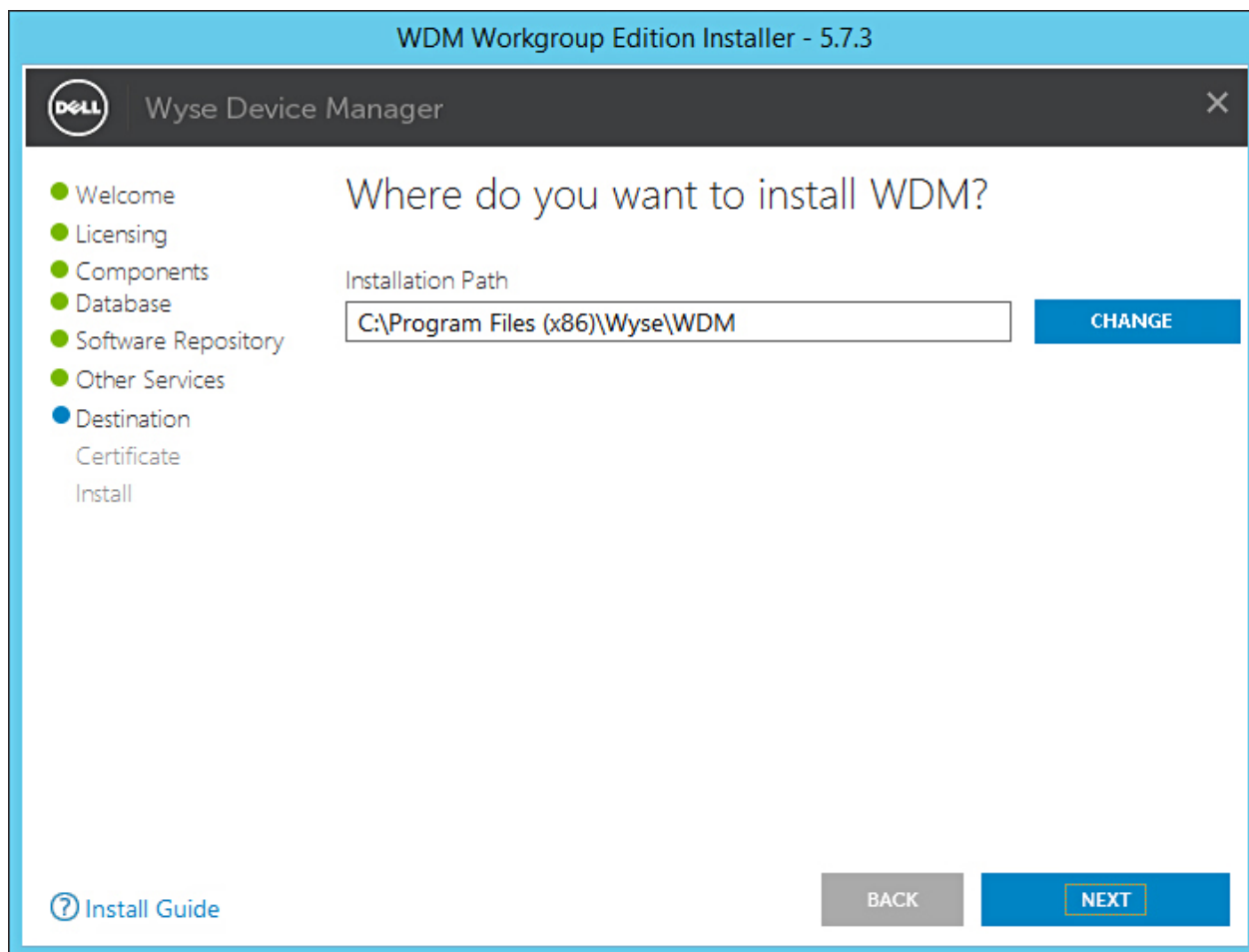


Figura 9. Pantalla Destination (Destino)

- 14 Seleccione e importe el certificado para iniciar la instalación.

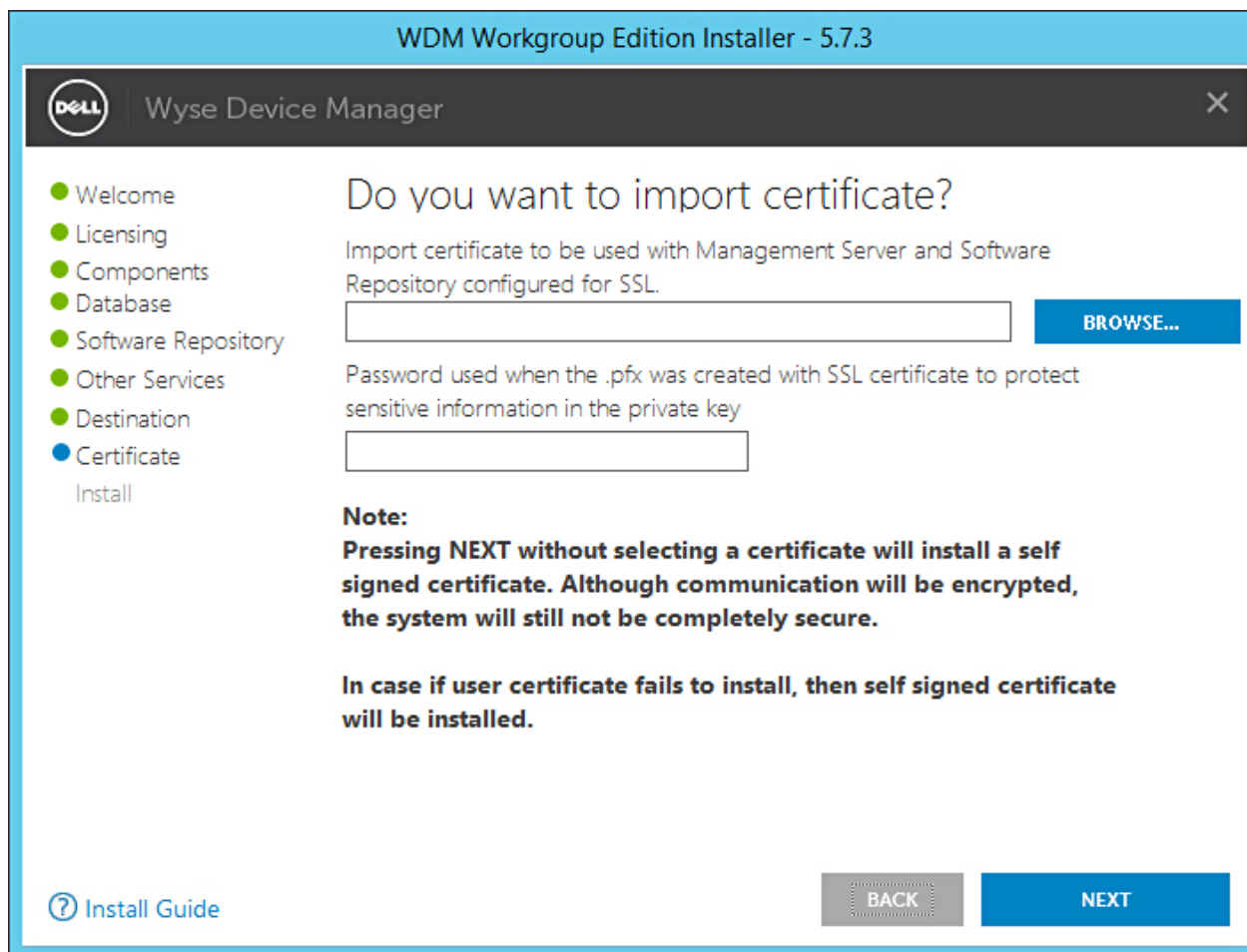


Figura 10. Pantalla Certificate (Certificado)

NOTA: Si hace clic en NEXT (Siguiente) sin seleccionar un certificado, el instalador instalará un certificado autofirmado. Las comunicaciones estarán cifradas, pero el sistema no está completamente seguro. El certificado debe estar en el formato de archivo .pfx.

El progreso de la instalación se muestra en la pantalla. Una vez finalizada la instalación, se le pedirá que reinicie el sistema.

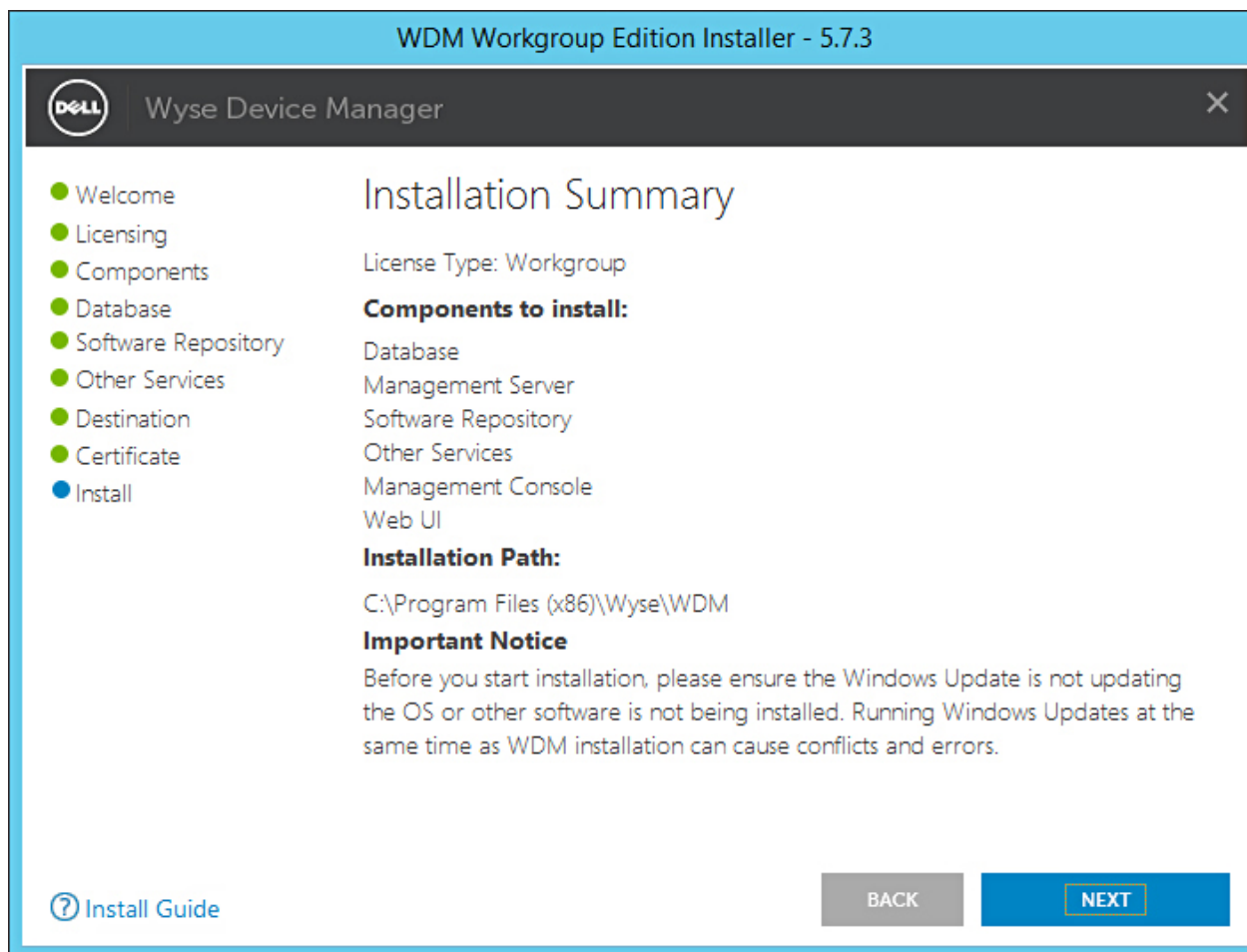


Figura 11. Pantalla Installation summary (Resumen de instalación)

15 Reinicie el sistema para que se efectúe el cambio.

Siguiente paso

Después de la instalación, asegúrese de que se cumplan las siguientes listas de verificación:

- WDM está instalado en `<drive C>\inetpub\ftproot path` y se creó la carpeta Rapport.
- Se creó un ícono de WebUI de WyseDeviceManager 5.7.3 en el escritorio.
- En IIS, se creó la aplicación HApi en la carpeta del servidor Rapport HTTP.
- En IIS, se creó la aplicación MyWDM en la carpeta del servidor Rapport HTTP.
- En IIS, se creó la aplicación WebUI en la carpeta del servidor Rapport HTTP.

NOTA: Después de la instalación, asegúrese de que la base de datos se haya creado con los nombres de la instancia y de la base de datos proporcionados.

Instalar WDM Enterprise Edition

- 1 Extraiga el contenido del instalador de WDM en el sistema en donde desea instalar WDM.
- 2 Vaya a la carpeta en la que extrajo el instalador y ejecute `setup.exe`.
Si el servidor no tiene .Net Framework, se instalará automáticamente.

Se muestra la pantalla de **Welcome** (Bienvenida).



Figura 12. Pantalla de bienvenida

- 3 Haga clic en **NEXT** (Siguiente).
- 4 En el tipo de licencia, seleccione **ENTERPRISE**.

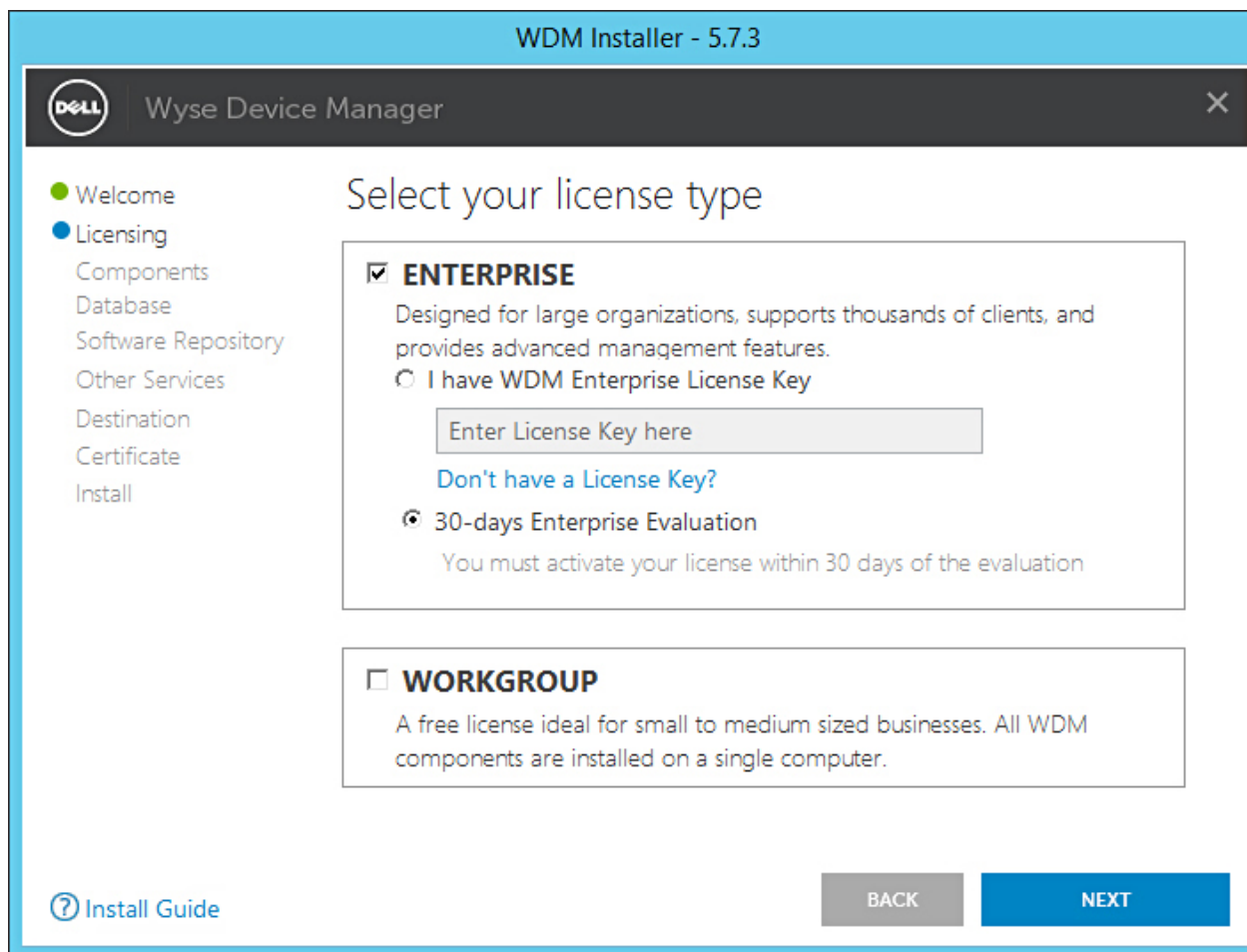


Figura 13. Tipo de licencia Enterprise

- a Si tiene la clave de licencia de WDM, seleccione la opción **I have WDM Enterprise License Key** (Tengo clave de licencia de WDM) e ingrésela en el espacio que se proporciona.
 - b Si no tiene la clave de licencia, seleccione la opción **30-days Enterprise Evaluation** (Evaluación de 30 días de Enterprise).
La clave de licencia se ingresa de forma predeterminada. Sin embargo, después del período de evaluación de 30 días, debe obtener la clave de licencia y agregarla a WDM. Para obtener más información sobre cómo agregar la clave de licencia, consulte la *Dell Wyse Device Manager Administrator's Guide (Guía del administrador de Dell Wyse Device Manager)*.
- 5 Haga clic en **NEXT** (Siguiente).
 - 6 Seleccione los componentes que desea instalar y haga clic en **NEXT** (Siguiente).

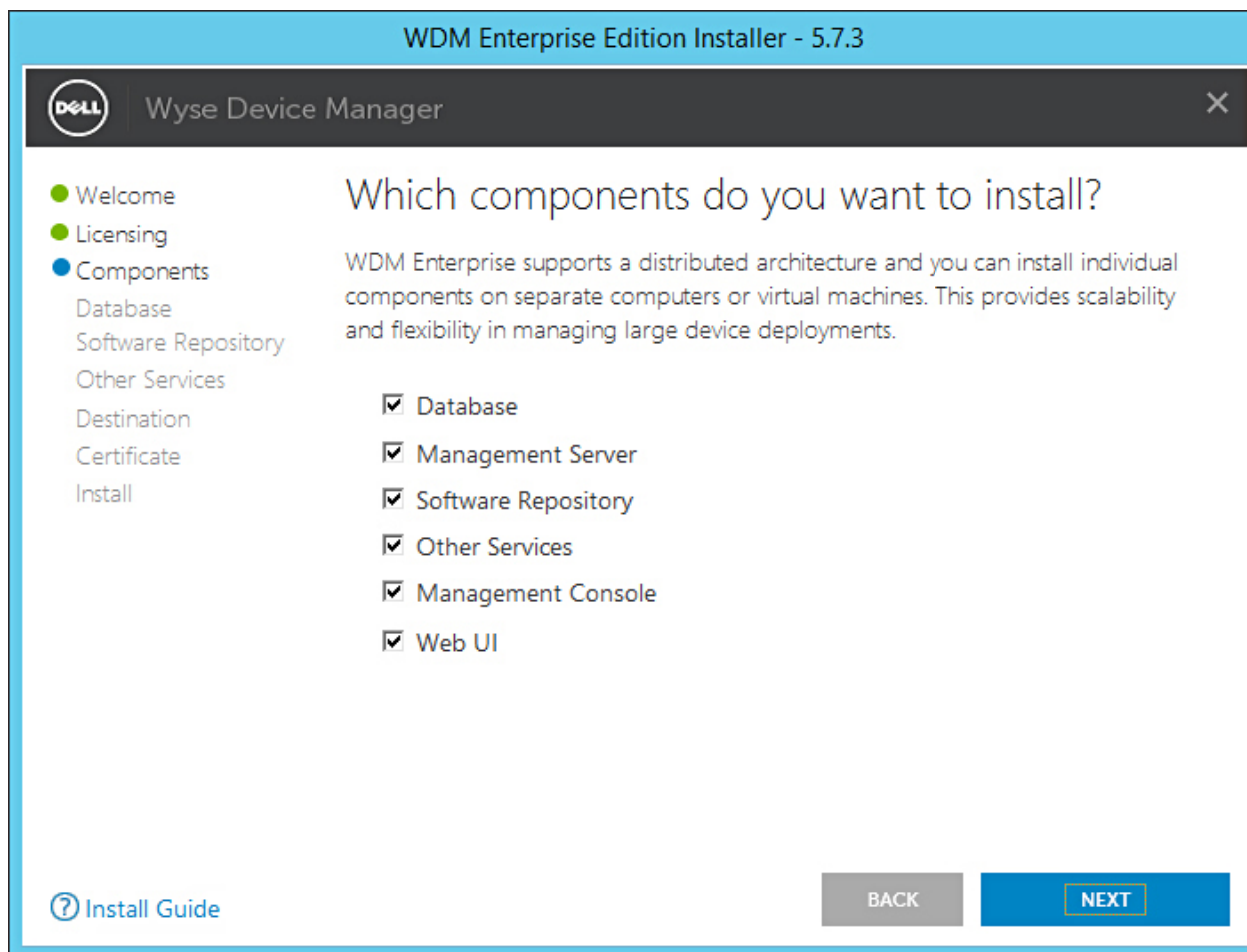


Figura 14. Pantalla Components (Componentes)

Puede instalar todos los componentes en el mismo sistema o cada componente en un sistema diferente.

NOTA: Si va a instalar los componentes por separado en diferentes sistemas, asegúrese de instalar la base de datos primero. Si no instala la base de datos, no podrá instalar los componentes restantes.

- 7 En la pantalla **Configure Database** (Configurar base de datos), seleccione una de las siguientes opciones:

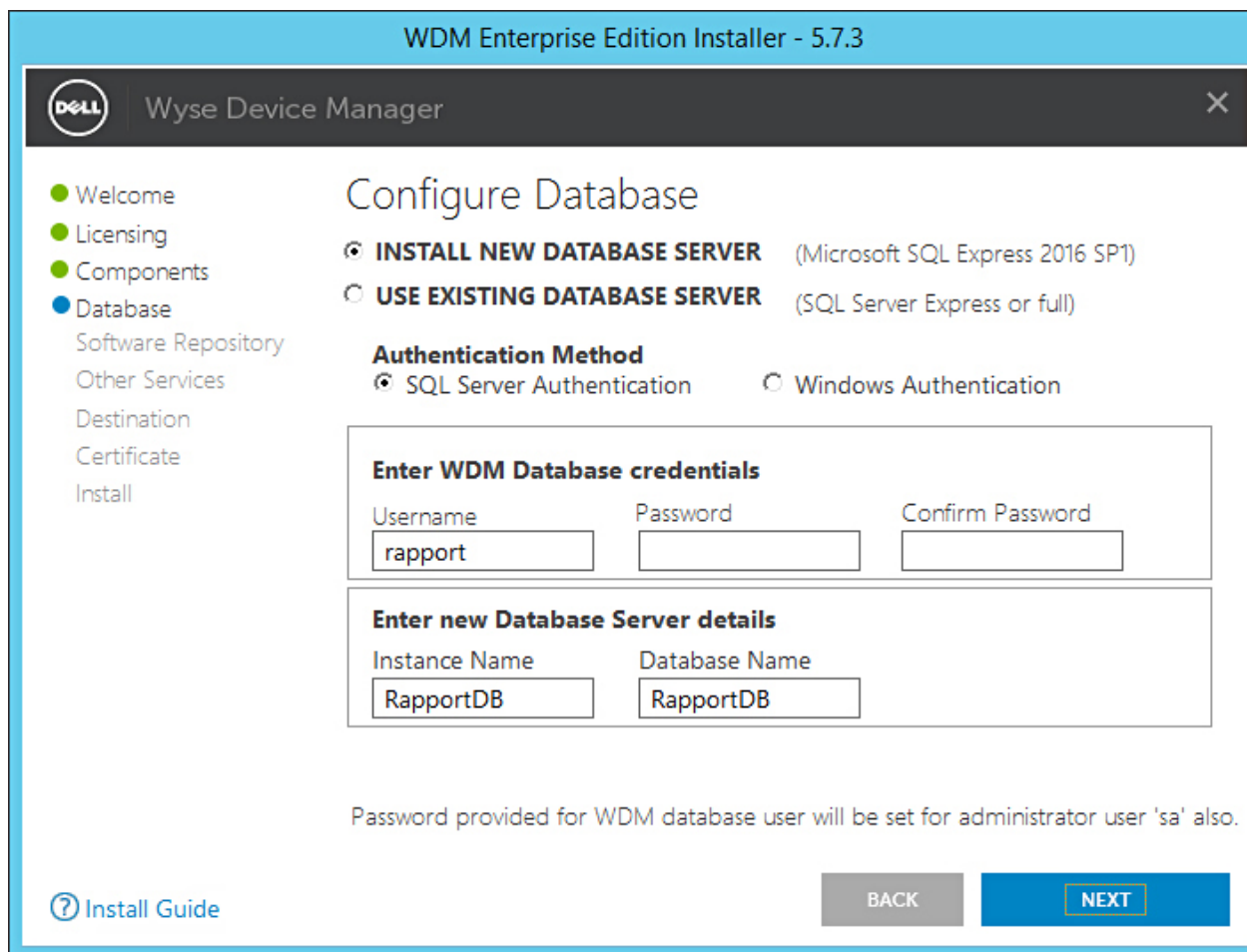


Figura 15. Pantalla Configure Database (Configurar base de datos)

- **Install New Database Server (Microsoft SQL Express 2016 SP1)** (Instalar nuevo servidor de base de datos [Microsoft SQL Express 2016 SP1]): seleccione esta opción si no tiene ninguna versión compatible de Microsoft SQL Server instalada en el sistema, y continúe con el paso 8.
 - **Use Existing Database Server (SQL Server Express or full)** (Usar servidor de base de datos existente [SQL Server Express o completo]): seleccione esta opción si ya ha instalado una versión compatible de Microsoft SQL Server en el sistema. Si selecciona esta opción, asegúrese de que el servidor de base de datos existente esté en el mismo sistema en el que instalará WDM Workgroup Edition, y continúe con el paso 9.
- 8 Si seleccionó la primera opción en el paso 7, seleccione el método de autenticación.

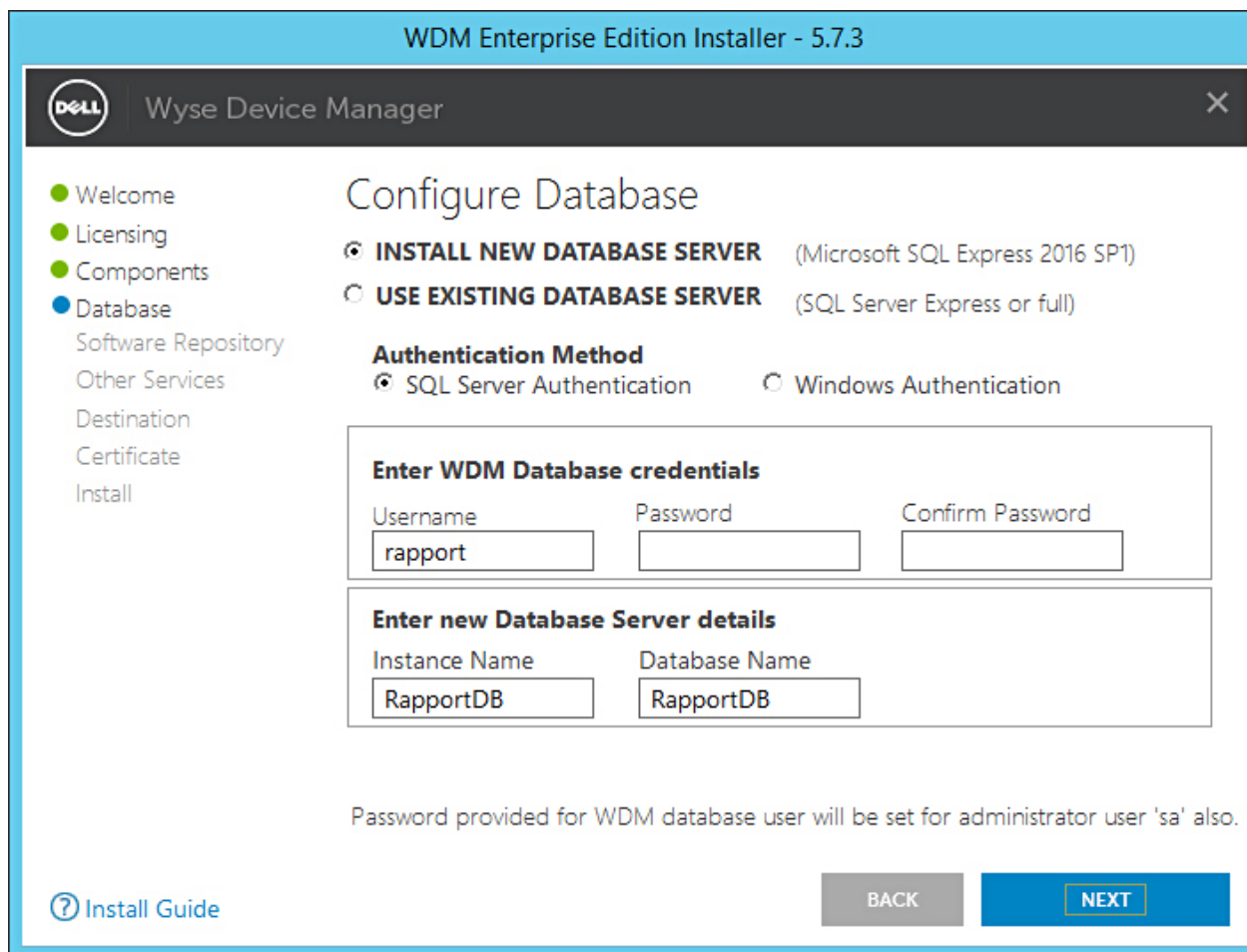


Figura 16. Opción Install New Database Server (Instalar nuevo servidor de base de datos)

- **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:
 - 1 Ingrese las credenciales de la base de datos de WDM.
 - 2 Ingrese las nuevas credenciales de la base de datos. Puede ingresar el nombre de la instancia y el nombre de la base de datos en los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.
 - ① **NOTA:** Incluso si elige la autenticación de Windows, la instalación de WDM requiere la autenticación de SQL para acceder a la base de datos de SQL. En una instalación independiente, después de completar la instalación de la base de datos de WDM, el instalador se encarga de asignar el usuario de Active Directory a la base de datos y el mismo usuario se utiliza para instalar los servicios de WDM.
 - **Windows Authentication (Autenticación de Windows):** ingrese los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.
 - ① **NOTA:**
 - Seleccione **Windows Authentication** (Autenticación de Windows) si desea conectarse a la base de datos de WDM con sus credenciales de inicio de sesión de Windows.
 - La contraseña debe cumplir con las reglas de complejidad del sistema operativo Windows.
- 9 Si seleccionó la segunda opción en el paso 7, seleccione el método de autenticación.

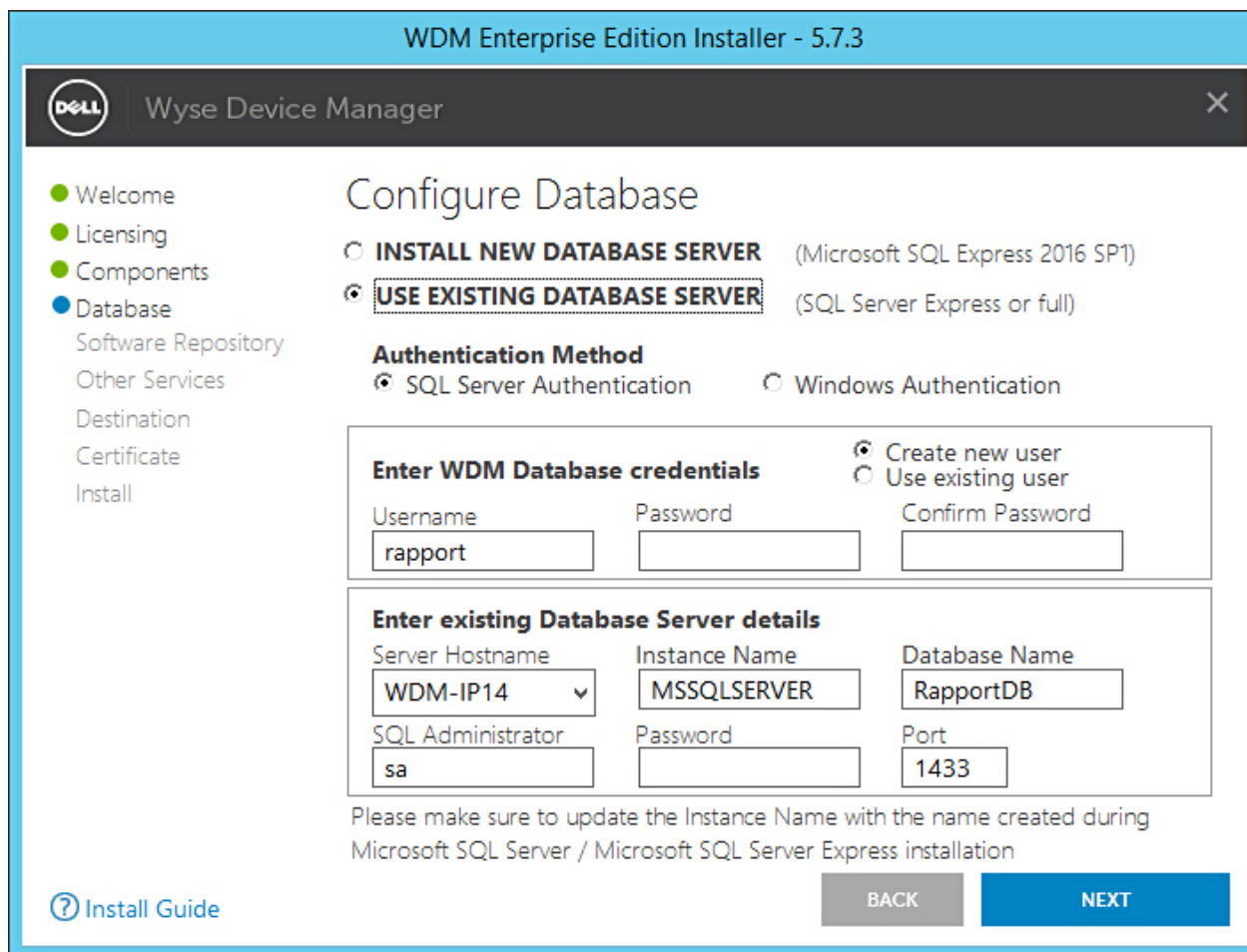


Figura 17. Opción Use Existing Database Server (Usar servidor de base de datos existente)

- **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:
 - 1 Seleccione la opción de Create New User (Crear nuevo usuario) o Use the existing user (Usar un usuario existente) y, a continuación, ingrese las credenciales de la base de datos de WDM.
 - 2 Ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL.
- **Windows Authentication (Autenticación de Windows)**: ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL.

NOTA: El número de puerto predeterminado es 1433. Dell recomienda ingresar manualmente el número de puerto, ya que es dinámico. El rango de puerto dinámico para TCP/UDP es entre 49152 y 65535.

10 Haga clic en **NEXT** (Siguiente).

Se muestra la pantalla **Configure Software Repository Server** (Configurar el servidor de repositorio del software).

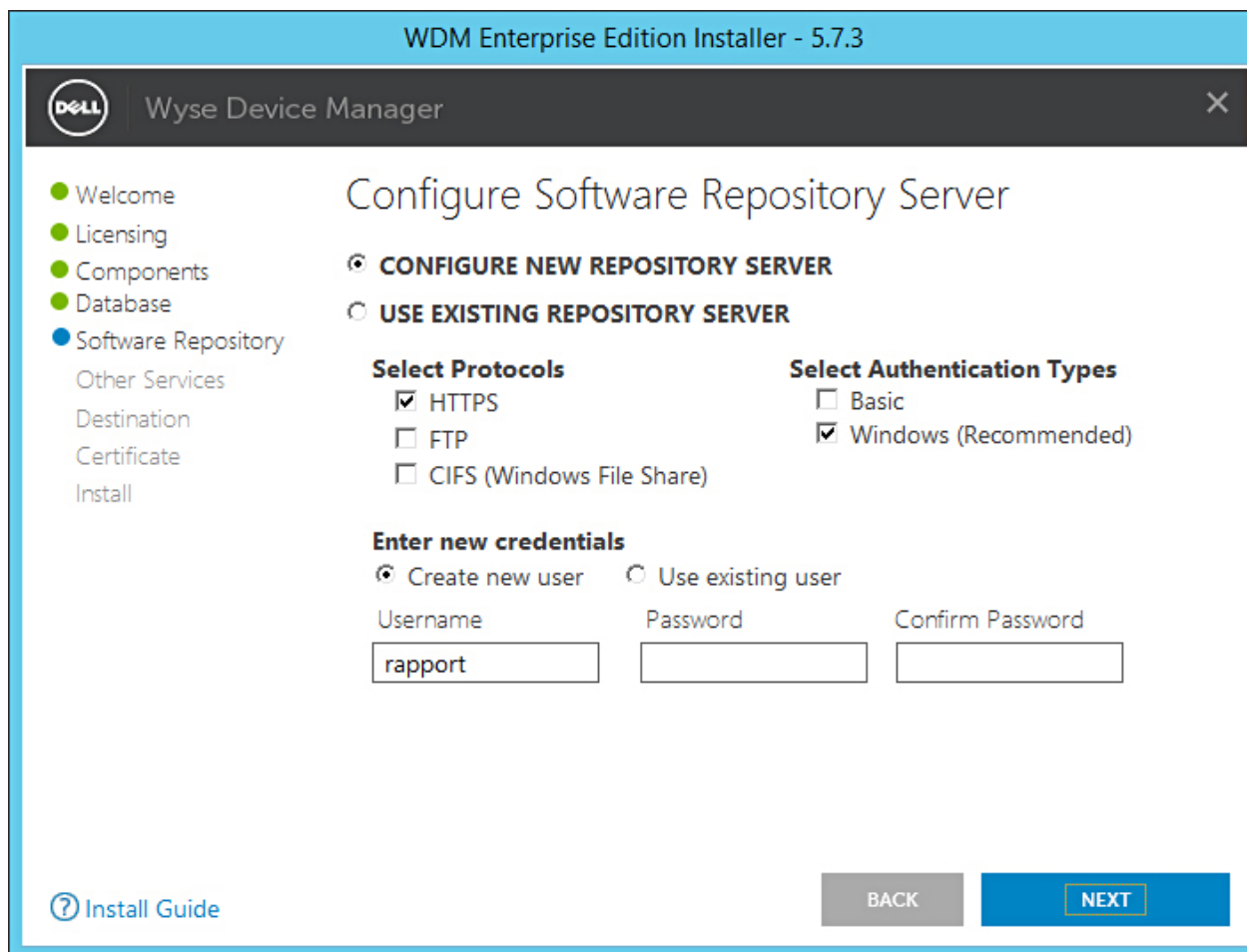


Figura 18. Pantalla Configure Software Repository Server (Configurar el servidor de repositorio del software)

- 11 En la pantalla **Configure Software Repository Server** (Configurar el servidor de repositorio del software), puede elegir una de las siguientes opciones:
- **CONFIGURE NEW REPOSITORY SERVER** (Configurar nuevo servidor de repositorio): seleccione esta opción si desea que el instalador configure un nuevo servidor de repositorio. Para configurar un nuevo servidor de repositorio:
 - Seleccione el protocolo y la configuración para distribuir el software a los dispositivos administrados. **HTTPS** aparece seleccionado de manera predeterminada. También puede seleccionar **FTP** para ThreadX 4.x y **CIFS** para ThreadX 5.x.
 - Seleccione el tipo de autenticación. **Windows** aparece seleccionado de manera predeterminada.
- NOTA:** Se requiere la autenticación básica para Linux.
- Cree nuevas credenciales de usuario o use las credenciales existentes.

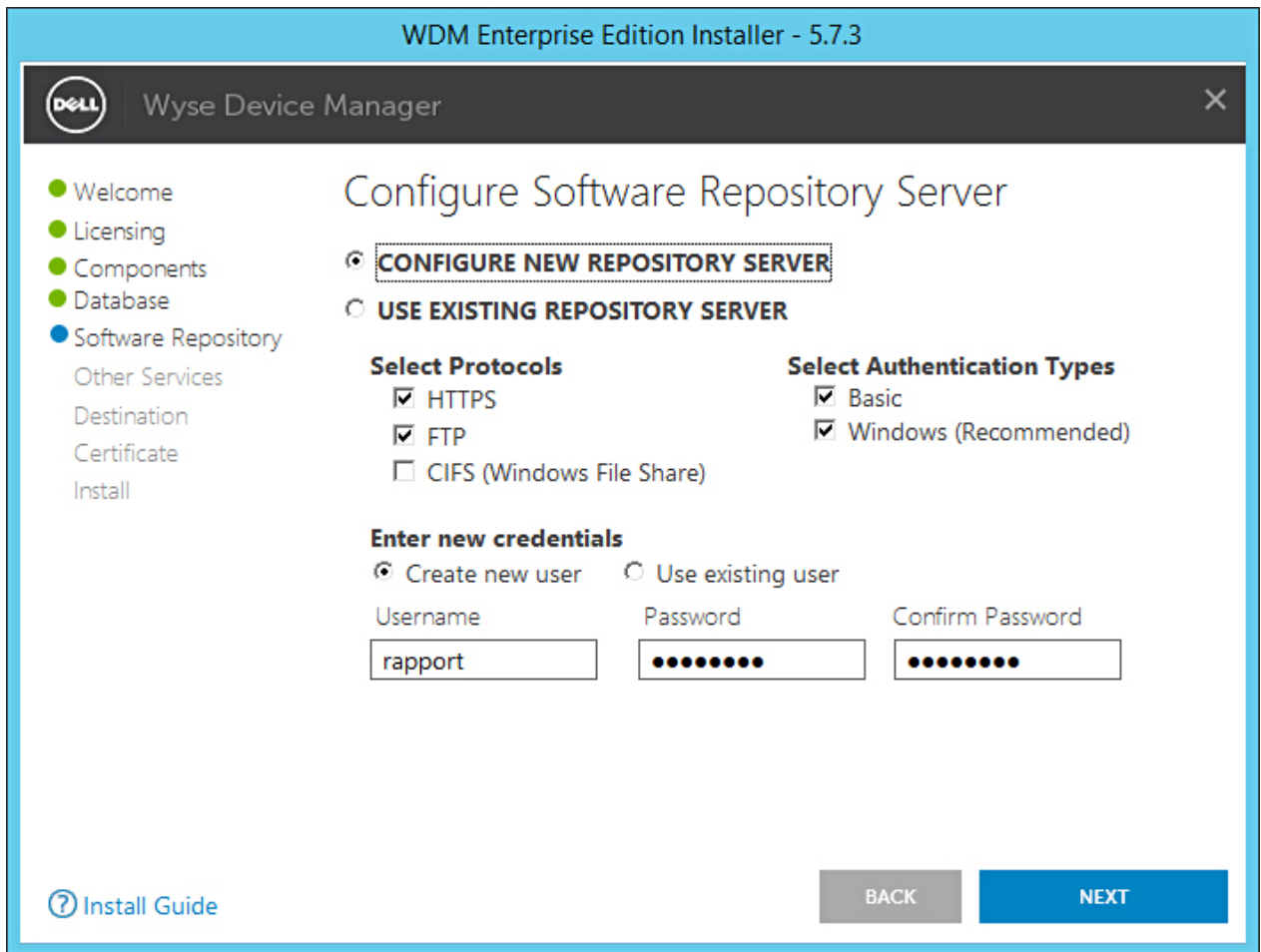


Figura 19. Opción CONFIGURE NEW REPOSITORY SERVER (Configurar nuevo servidor de repositorio)

- **USE EXISTING REPOSITORY SERVER** (Usar servidor de repositorio existente): seleccione esta opción si desea que el instalador configure un servidor de repositorio existente. Para configurar el servidor de repositorio existente:
 - Seleccione el protocolo y la configuración para distribuir el software a los dispositivos administrados. **HTTPS** aparece seleccionado de manera predeterminada. También puede seleccionar **FTP** para ThreadX 4.x y **CIFS** para ThreadX 5.x.
 - Seleccione el tipo de autenticación. **Windows** aparece seleccionado de manera predeterminada.
 - Ingrese las credenciales del servidor. La opción de dirección IP del servidor aparece atenuada y el nombre de usuario predeterminado es rapport.

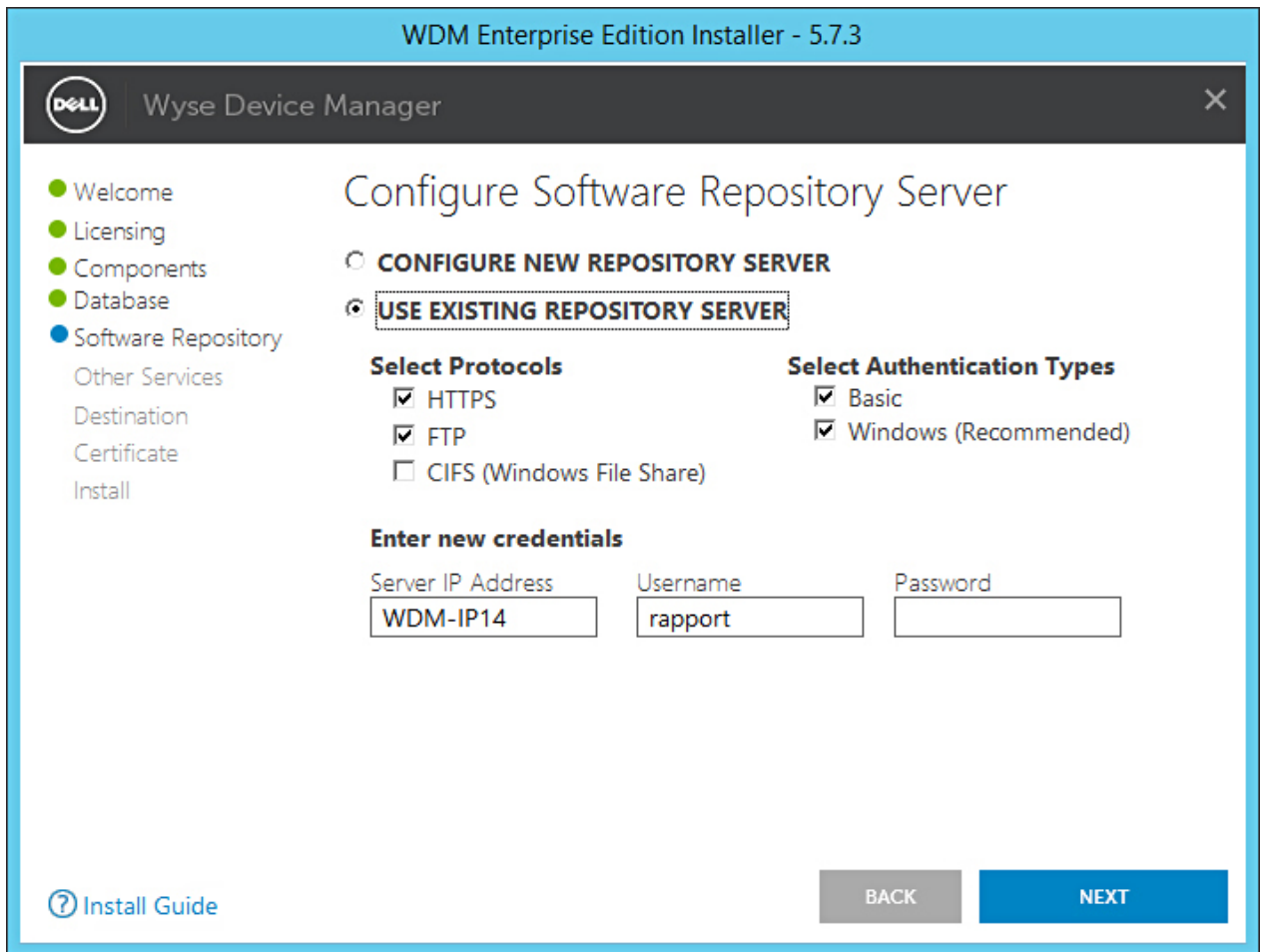


Figura 20. Opción USE EXISTING REPOSITORY SERVER (Usar servidor de repositorio existente)

- 12 Haga clic en **NEXT** (Siguiente).
- 13 Seleccione los servicios que desea instalar y haga clic en **NEXT** (Siguiente).

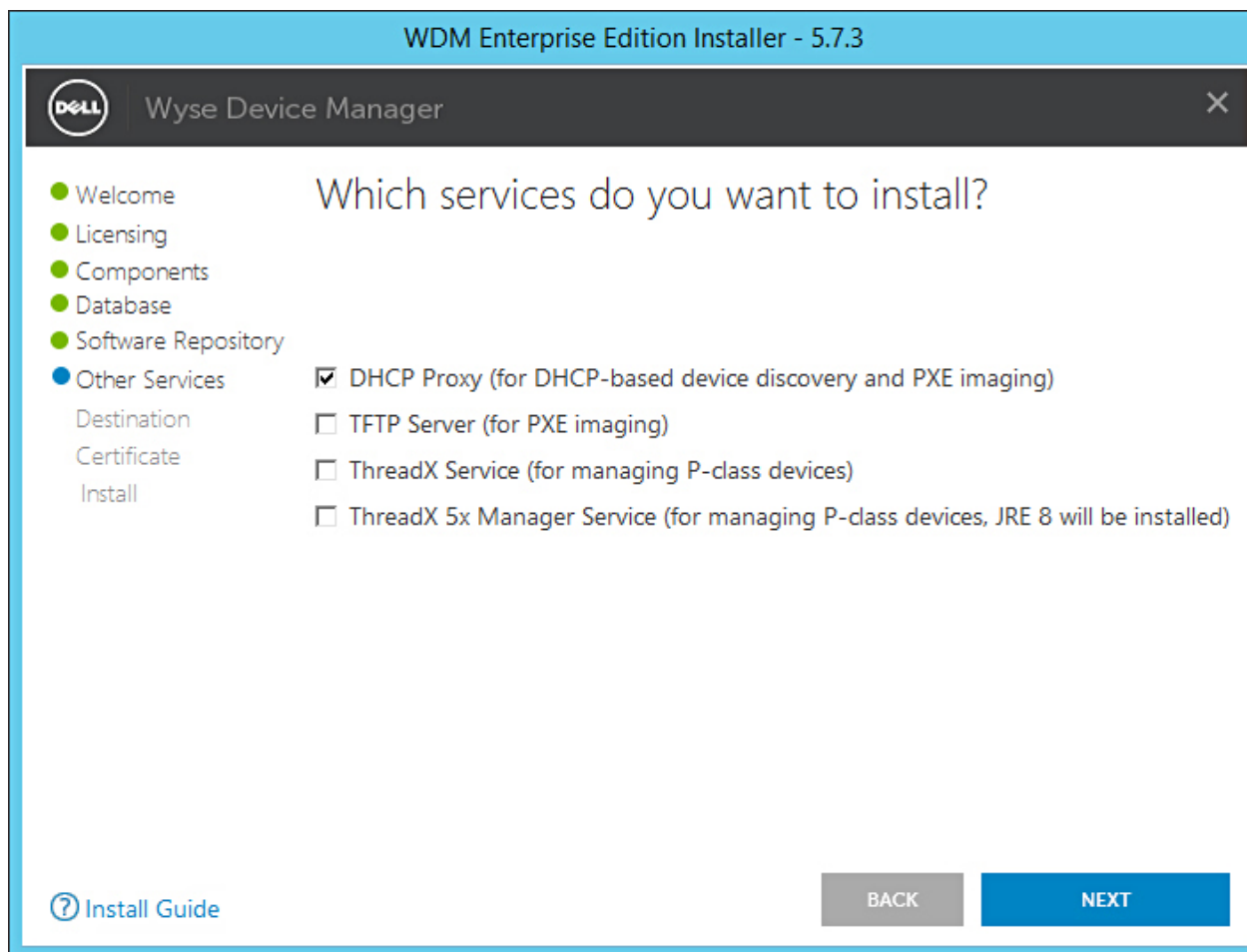


Figura 21. Pantalla Other Services (Otros servicios)

NOTA: Proxy DHCP aparece seleccionado de manera predeterminada.

14 Ingrese la ruta de instalación y haga clic en **NEXT** (Siguiente).

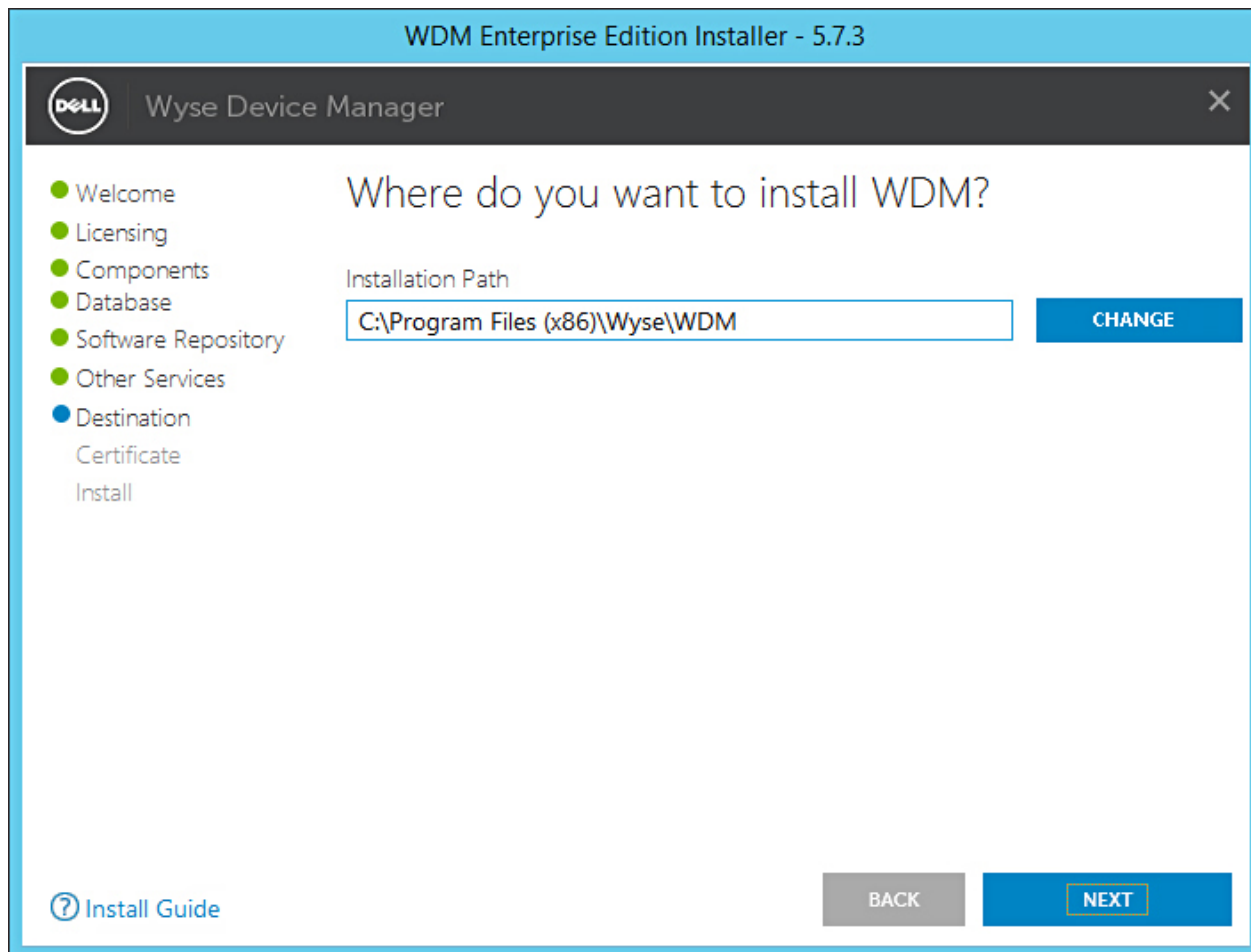


Figura 22. Pantalla Destination (Destino)

- 15 Seleccione e importe el certificado para iniciar la instalación.

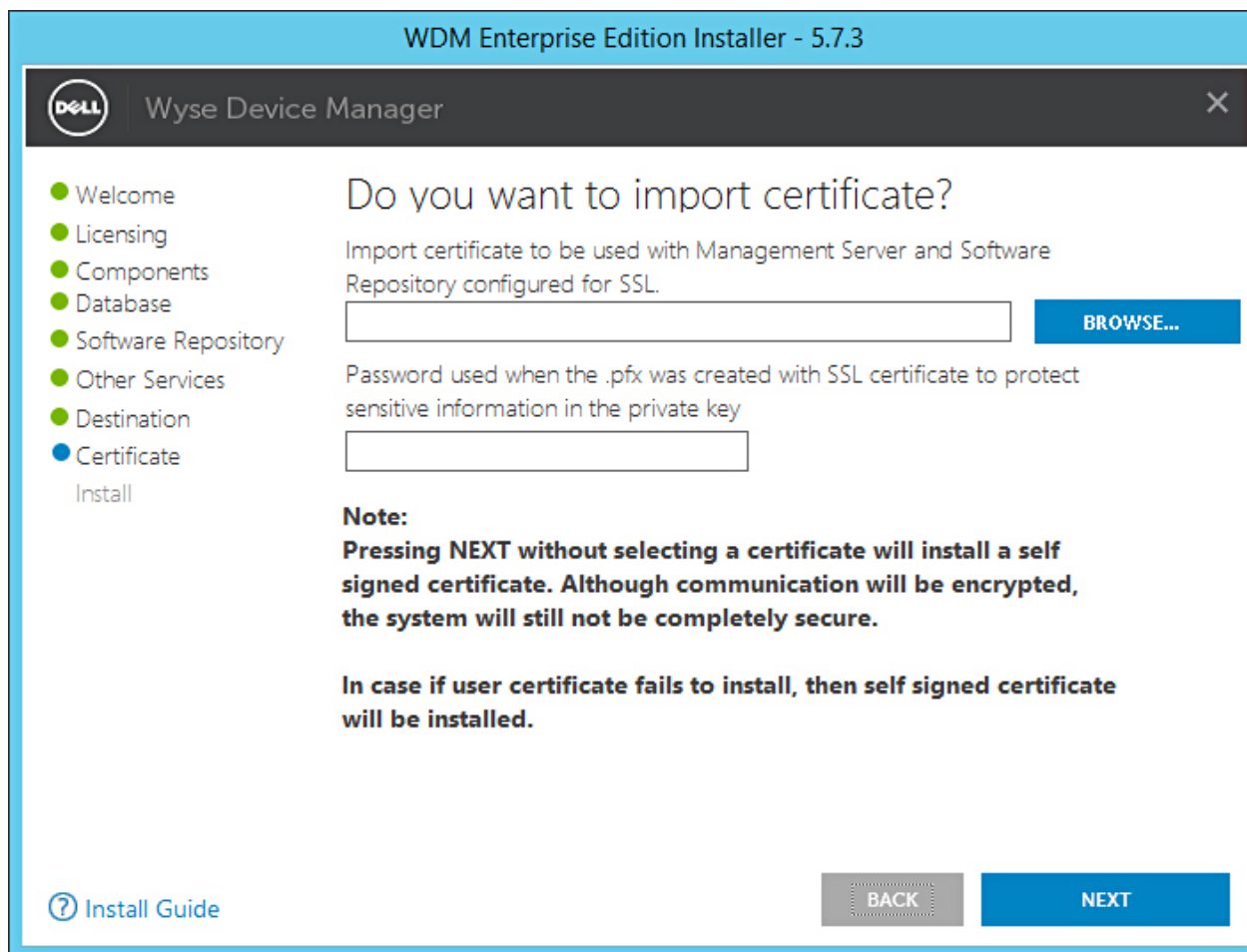


Figura 23. Pantalla Certificate (Certificado)

NOTA: Si hace clic en NEXT (Siguiente) sin seleccionar un certificado, el instalador instalará un certificado autofirmado. Las comunicaciones estarán cifradas, pero el sistema no está completamente seguro. El certificado debe estar en el formato de archivo .pfx.

El progreso de la instalación se muestra en la pantalla. Una vez finalizada la instalación, se le pedirá que reinicie el sistema.

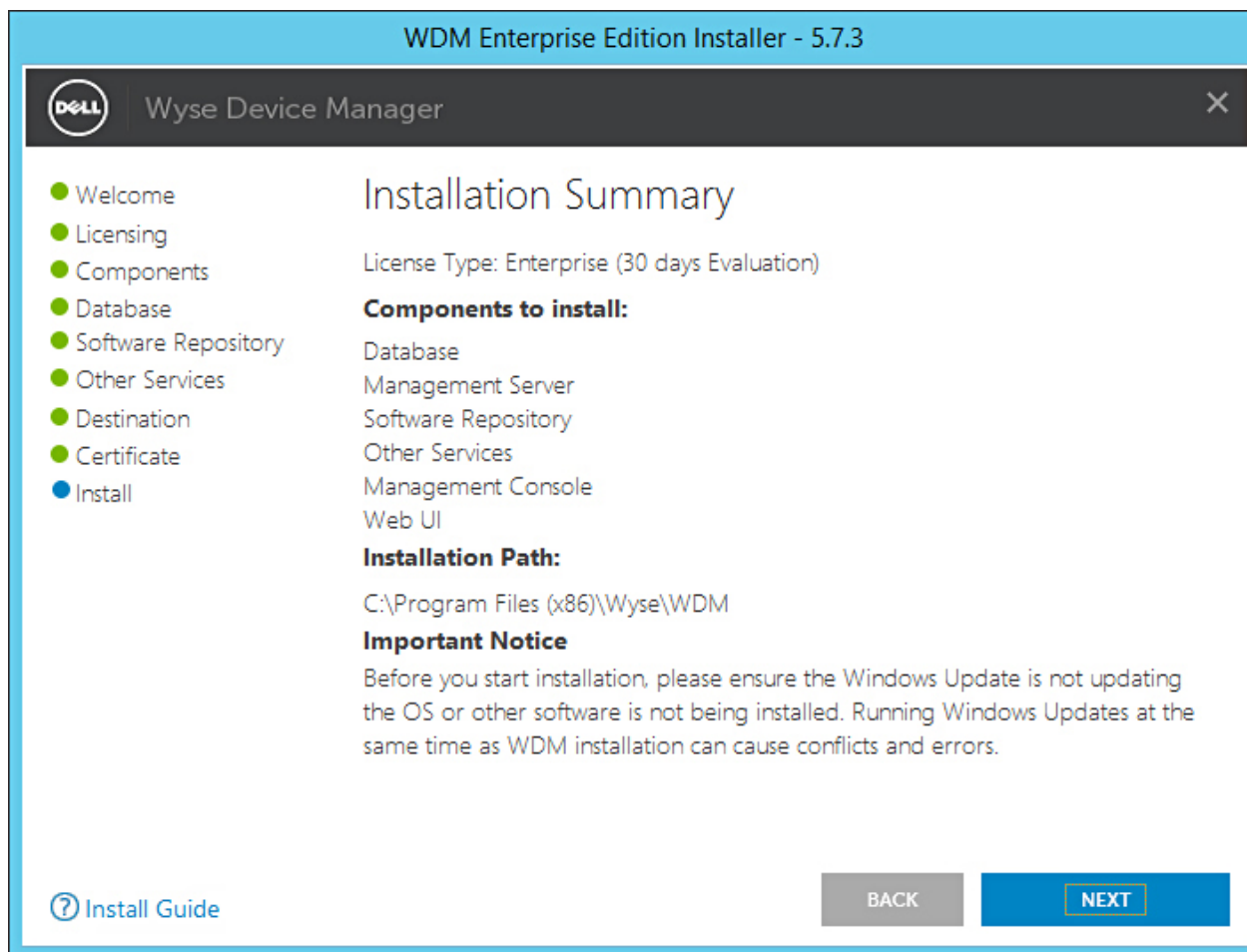


Figura 24. Pantalla Installation summary (Resumen de instalación)

16 Reinicie el sistema para que se efectúe el cambio.

Instalar WDM en un ambiente de nube

Acerca de esta tarea

Para instalar WDM en un ambiente de nube, debe instalar Enterprise Edition.

Pasos

- 1 Extraiga el contenido del instalador de WDM en el sistema en donde desea instalar WDM.
- 2 Vaya a la carpeta en la que extrajo el instalador y ejecute **setup.exe**.
Si el servidor no tiene .Net Framework, se instalará automáticamente.

Se muestra la pantalla de **Welcome** (Bienvenida).

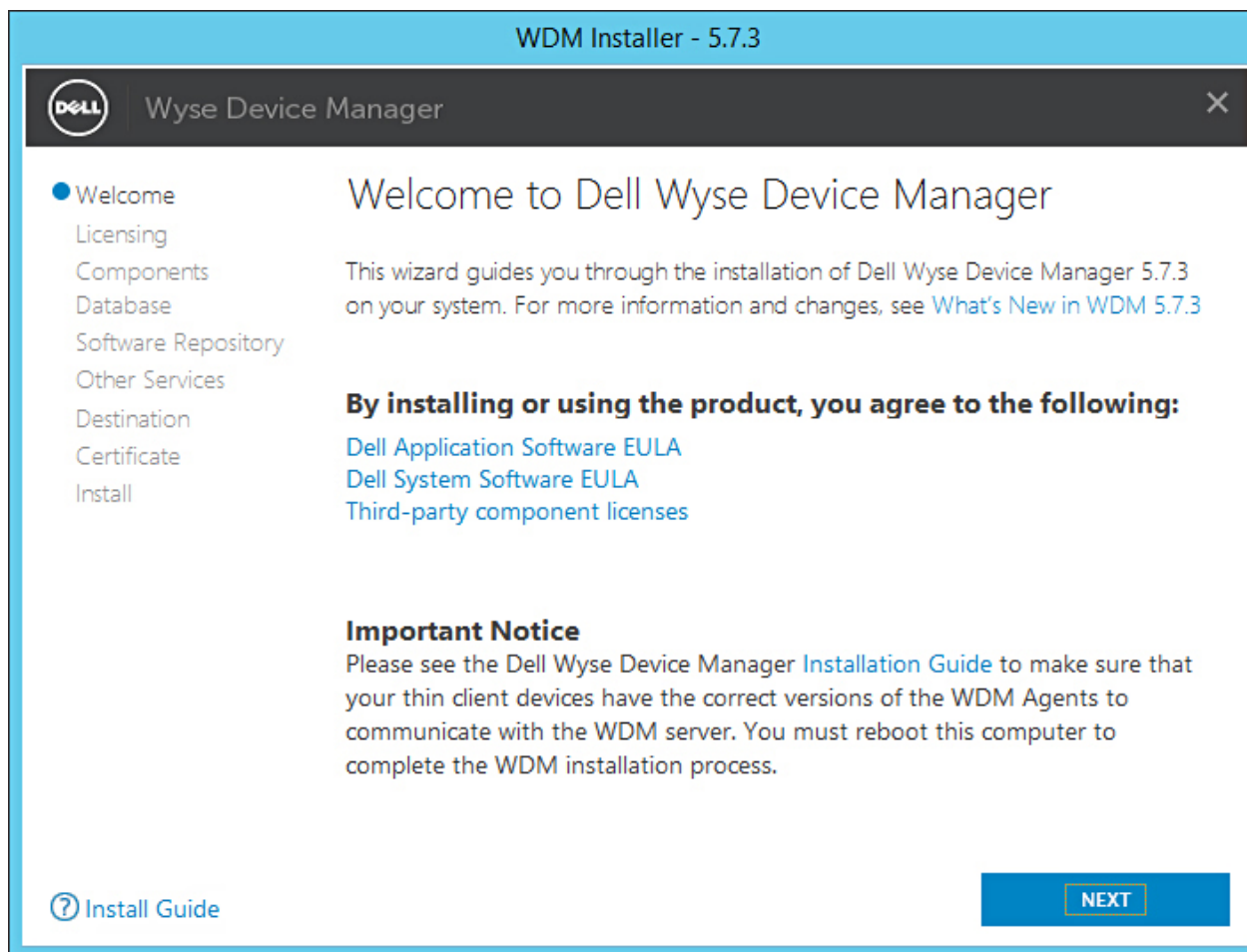


Figura 25. Pantalla de bienvenida

- 3 Haga clic en **NEXT** (Siguiente).
- 4 En el tipo de licencia, seleccione **ENTERPRISE**.

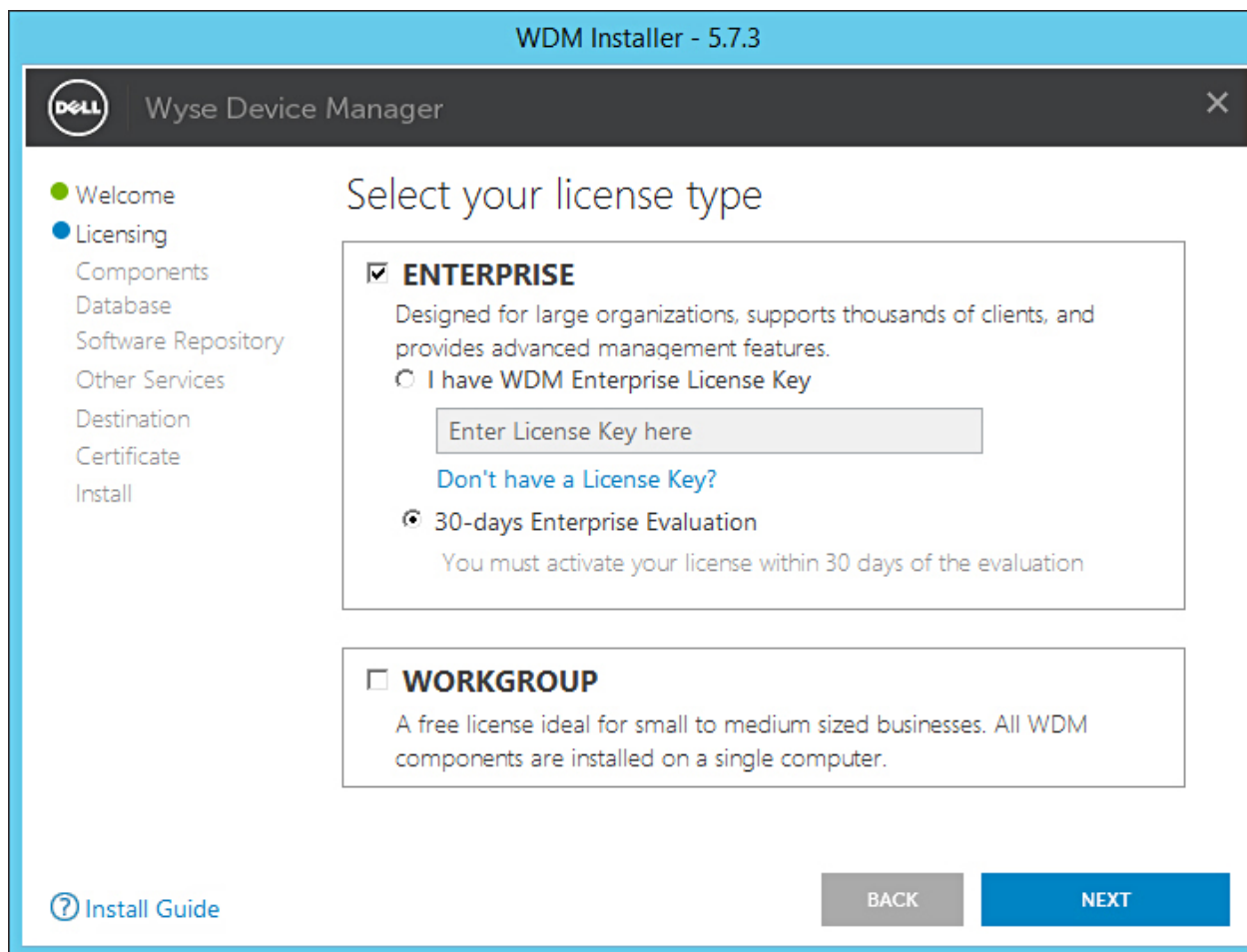


Figura 26. Tipo de licencia Enterprise

- a Si tiene la clave de licencia de WDM, seleccione la opción **I have WDM Enterprise License Key** (Tengo clave de licencia de WDM) e ingrésela en el espacio que se proporciona.
 - b Si no tiene la clave de licencia, seleccione la opción **30-days Enterprise Evaluation** (Evaluación de 30 días de Enterprise).
La clave de licencia se ingresa de forma predeterminada. Sin embargo, después del período de evaluación de 30 días, debe obtener la clave de licencia y agregarla a WDM. Para obtener más información sobre cómo agregar la clave de licencia, consulte la *Dell Wyse Device Manager Administrator's Guide (Guía del administrador de Dell Wyse Device Manager)*.
- 5 Haga clic en **NEXT** (Siguiente).
 - 6 Seleccione los componentes que desea instalar y haga clic en **NEXT** (Siguiente).

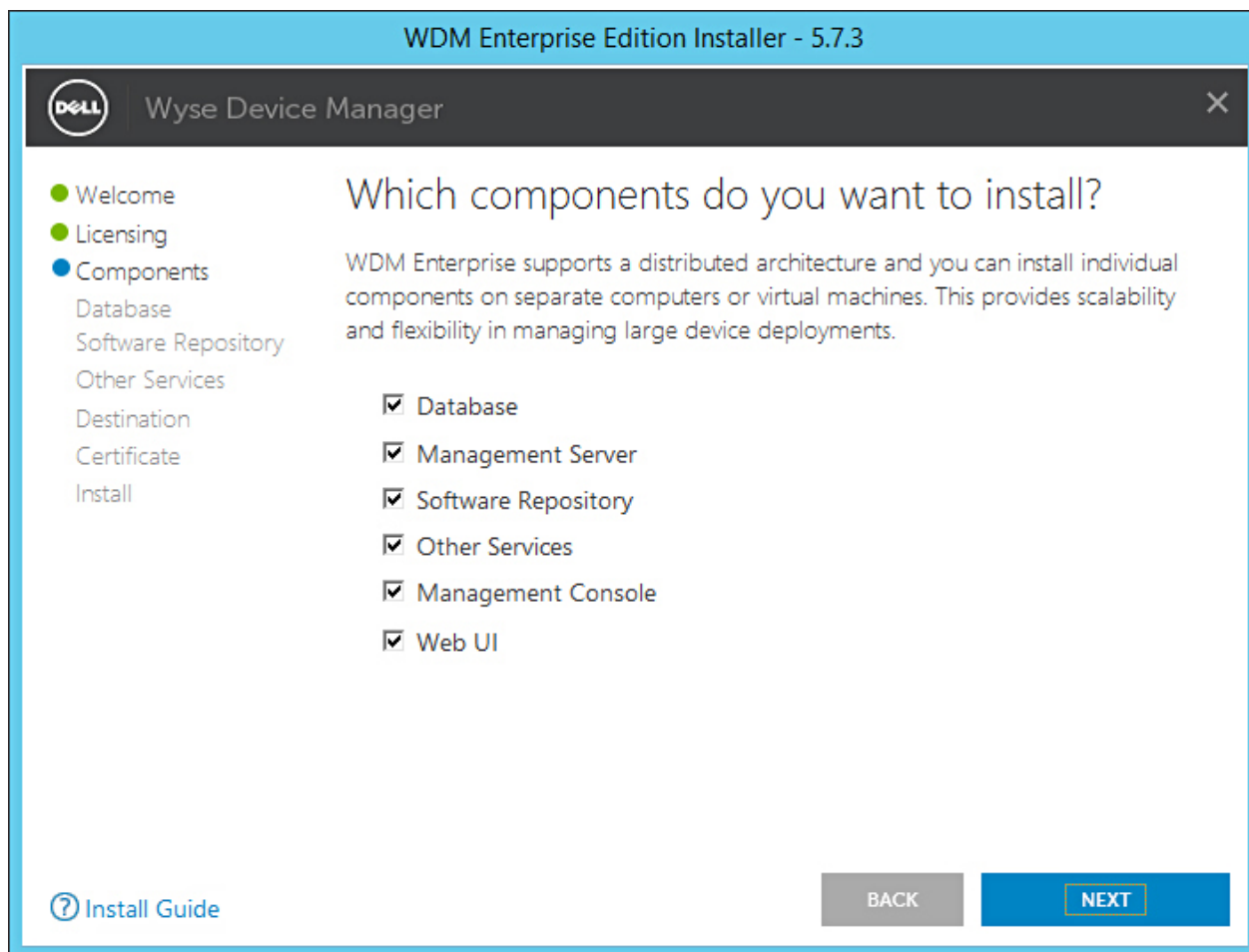


Figura 27. Pantalla Components (Componentes)

Puede instalar todos los componentes en el mismo sistema o cada componente en un sistema diferente.

NOTA: Si va a instalar los componentes por separado en diferentes sistemas, asegúrese de instalar la base de datos primero. Si no instala la base de datos, no podrá instalar los componentes restantes.

- 7 En la pantalla **Configure Database** (Configurar base de datos), seleccione una de las siguientes opciones:

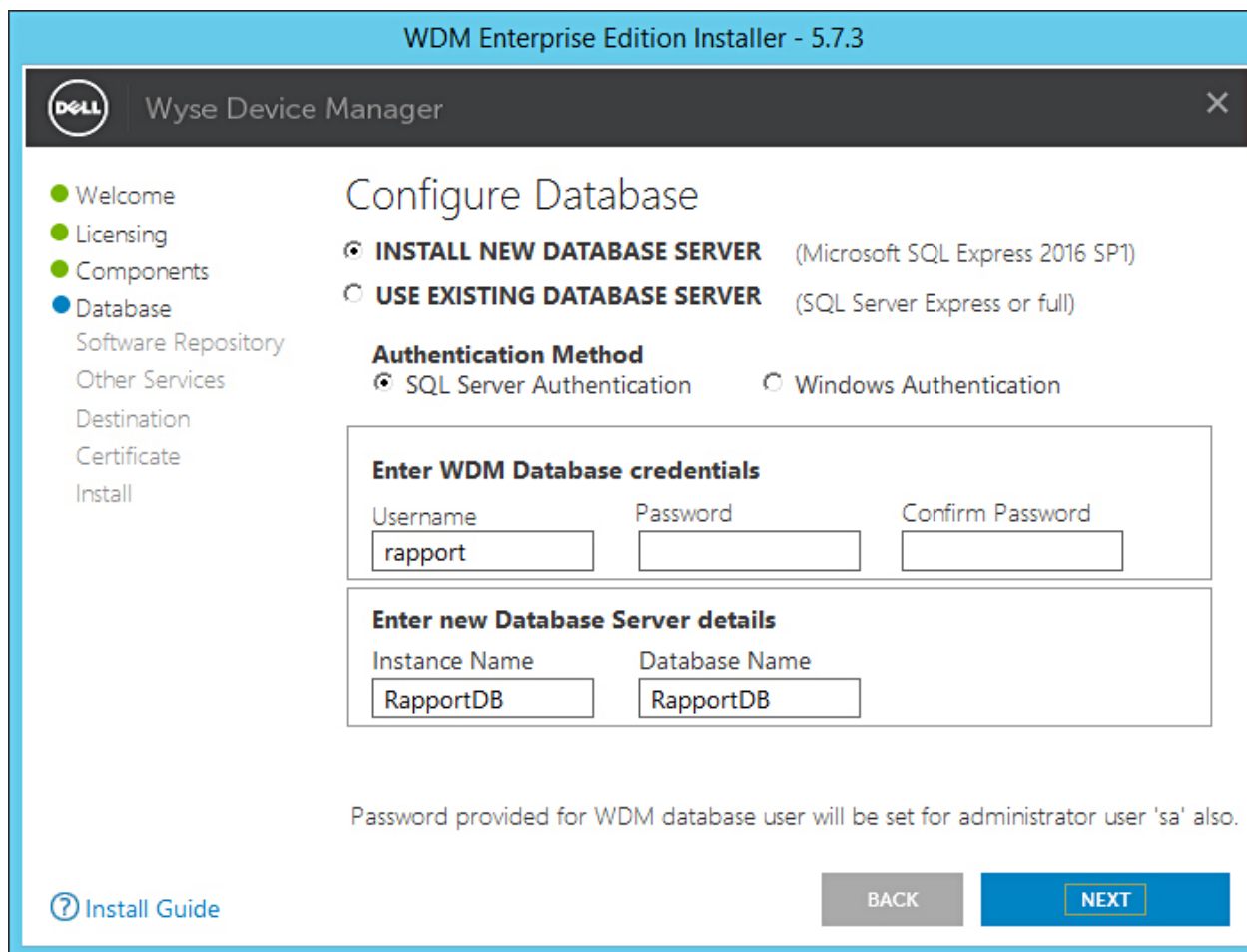


Figura 28. Pantalla Configure Database (Configurar base de datos)

- **Install New Database Server (Microsoft SQL Express 2016 SP1)** (Instalar nuevo servidor de base de datos [Microsoft SQL Express 2016 SP1]): seleccione esta opción si no tiene ninguna versión compatible de Microsoft SQL Server instalada en el sistema, y continúe con el paso 8.
 - **Use Existing Database Server (SQL Server Express or full)** (Usar servidor de base de datos existente [SQL Server Express o completo]): seleccione esta opción si ya ha instalado una versión compatible de Microsoft SQL Server en el sistema. Si selecciona esta opción, asegúrese de que el servidor de base de datos existente esté en el mismo sistema en el que instalará WDM Workgroup Edition, y continúe con el paso 9.
- 8 Si seleccionó la primera opción en el paso 7, seleccione el método de autenticación.

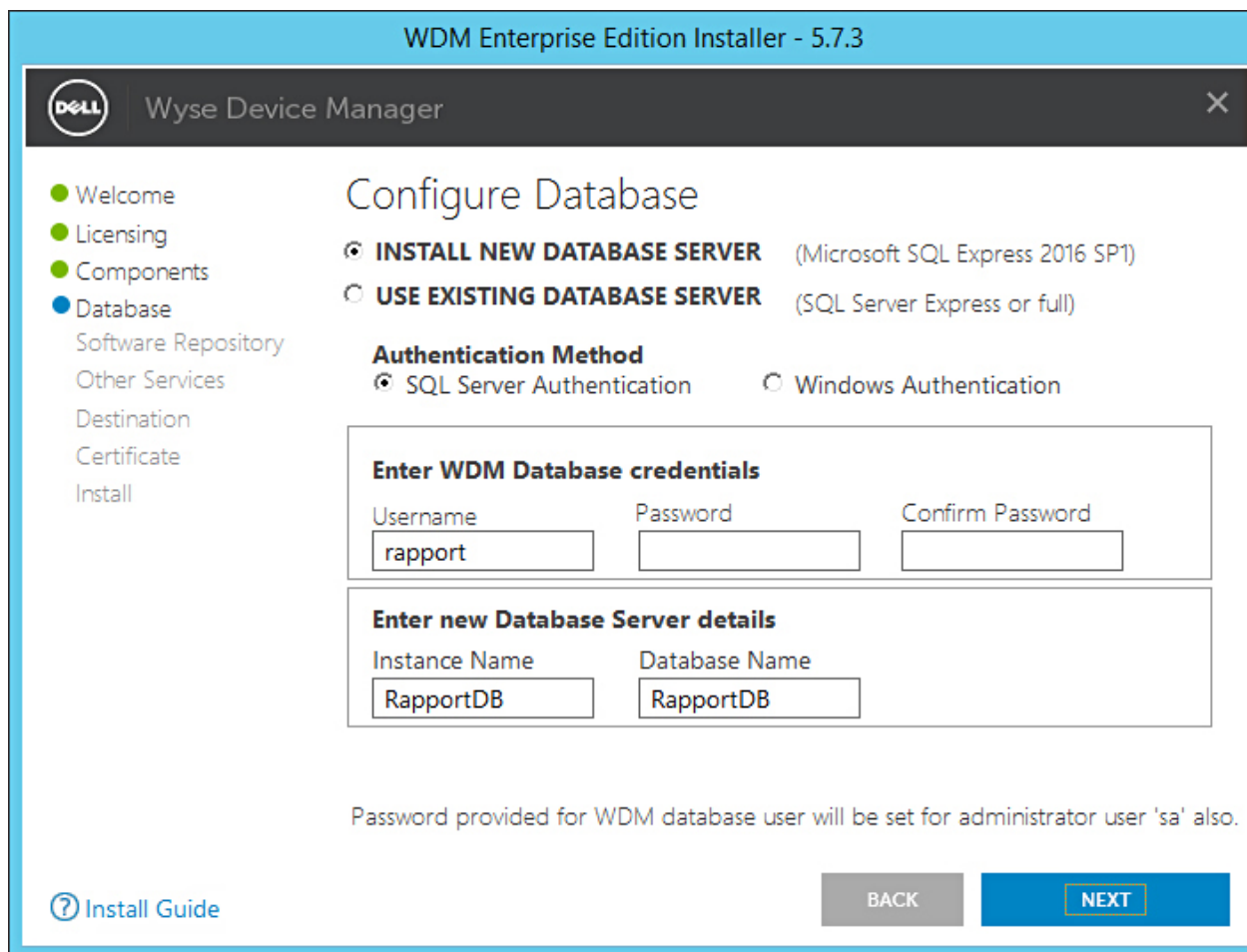


Figura 29. Opción Install New Database Server (Instalar nuevo servidor de base de datos)

- **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:
 - 1 Ingrese las credenciales de la base de datos de WDM.
 - 2 Ingrese las nuevas credenciales de la base de datos. Puede ingresar el nombre de la instancia y el nombre de la base de datos en los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.
 - ① **NOTA:** Incluso si elige la autenticación de Windows, la instalación de WDM requiere la autenticación de SQL para acceder a la base de datos de SQL. En una instalación independiente, después de completar la instalación de la base de datos de WDM, el instalador se encarga de asignar el usuario de Active Directory a la base de datos y el mismo usuario se utiliza para instalar los servicios de WDM.
 - **Windows Authentication (Autenticación de Windows):** ingrese los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.
 - ① **NOTA:**
 - Seleccione **Windows Authentication** (Autenticación de Windows) si desea conectarse a la base de datos de WDM con sus credenciales de inicio de sesión de Windows.
 - La contraseña debe cumplir con las reglas de complejidad del sistema operativo Windows.
- 9 Si seleccionó la segunda opción en el paso 7, seleccione el método de autenticación.

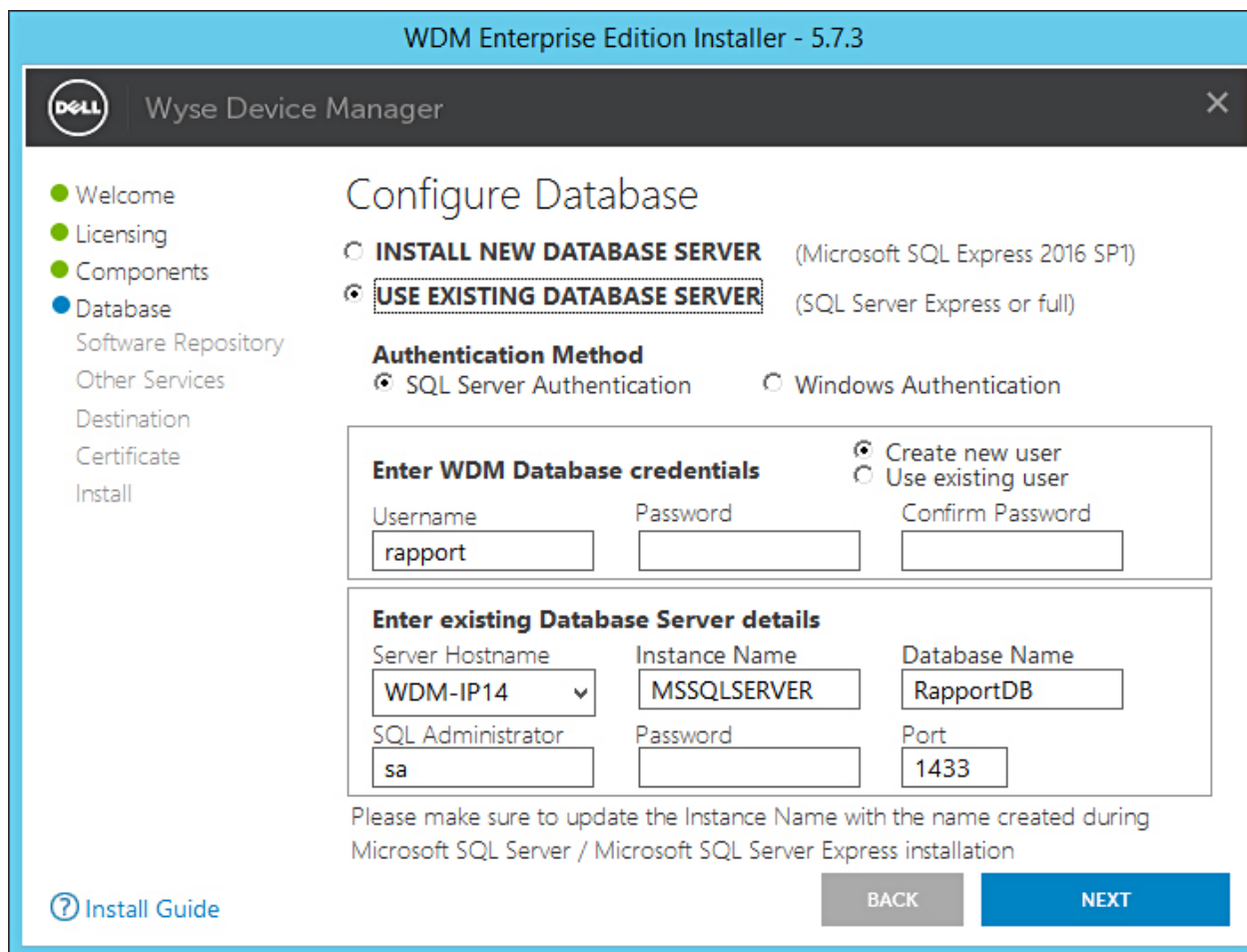


Figura 30. Opción Use Existing Database Server (Usar servidor de base de datos existente)

- **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:
 - 1 Seleccione la opción de Create New User (Crear nuevo usuario) o Use the existing user (Usar un usuario existente) y, a continuación, ingrese las credenciales de la base de datos de WDM.
 - 2 Ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL.
- **Windows Authentication (Autenticación de Windows)**: ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL.

NOTA: El número de puerto predeterminado es 1433. Dell recomienda ingresar manualmente el número de puerto, ya que es dinámico. El rango de puerto dinámico para TCP/UDP es entre 49152 y 65535.

10 Haga clic en **NEXT** (Siguiente).

Se muestra la pantalla **Configure Software Repository Server** (Configurar el servidor de repositorio del software).

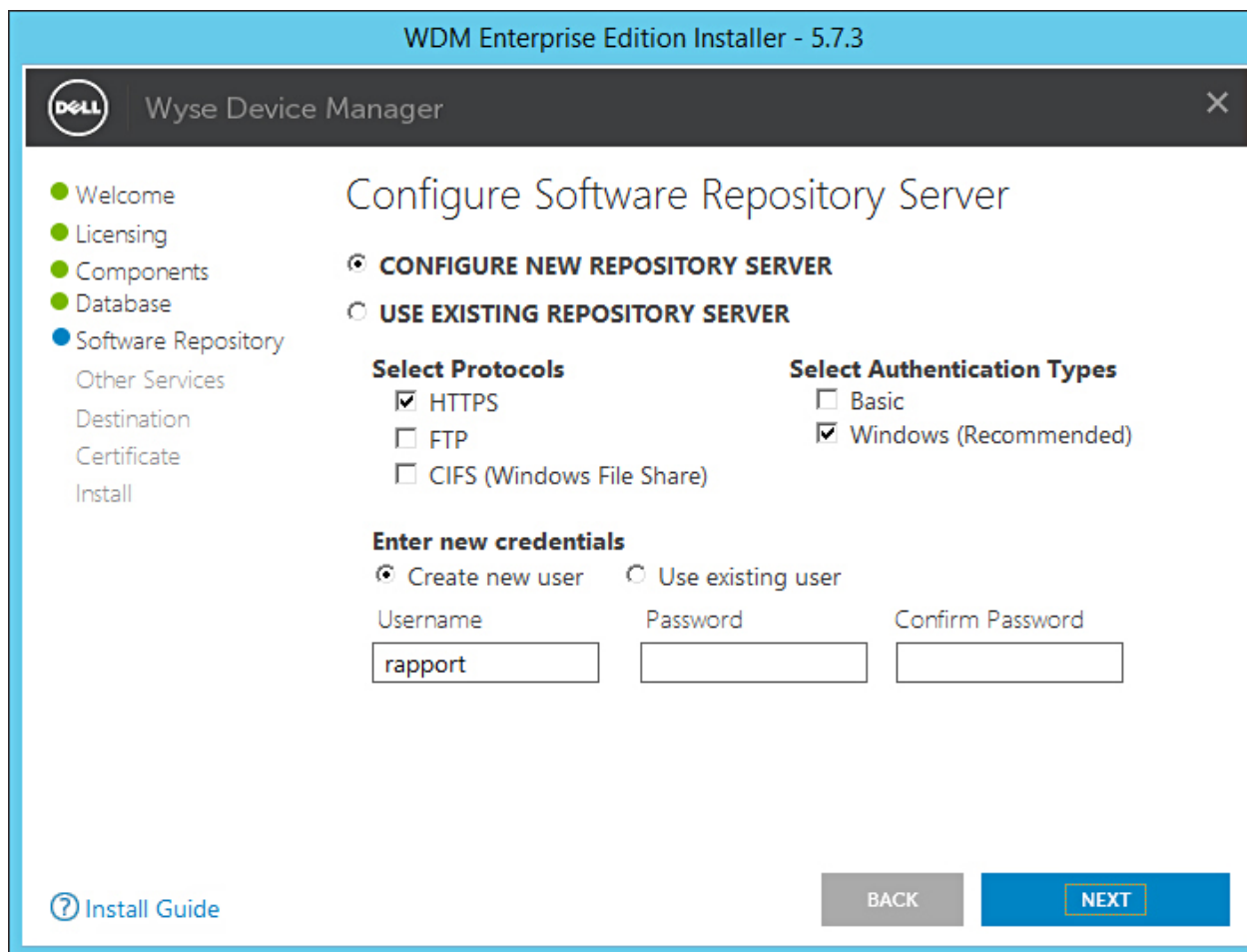


Figura 31. Pantalla Configure Software Repository Server (Configurar el servidor de repositorio del software)

- 11 En la pantalla **Configure Software Repository Server** (Configurar el servidor de repositorio del software), puede elegir una de las siguientes opciones:
- **CONFIGURE NEW REPOSITORY SERVER** (Configurar nuevo servidor de repositorio): seleccione esta opción si desea que el instalador configure un nuevo servidor de repositorio. Para configurar un nuevo servidor de repositorio:
 - Seleccione el protocolo y la configuración para distribuir el software a los dispositivos administrados. **HTTPS** aparece seleccionado de manera predeterminada. También puede seleccionar **FTP** para ThreadX 4.x y **CIFS** para ThreadX 5.x.
 - Seleccione el tipo de autenticación. **Windows** aparece seleccionado de manera predeterminada.
- NOTA: Se requiere la autenticación básica para Linux.**
- Cree nuevas credenciales de usuario o use las credenciales existentes.

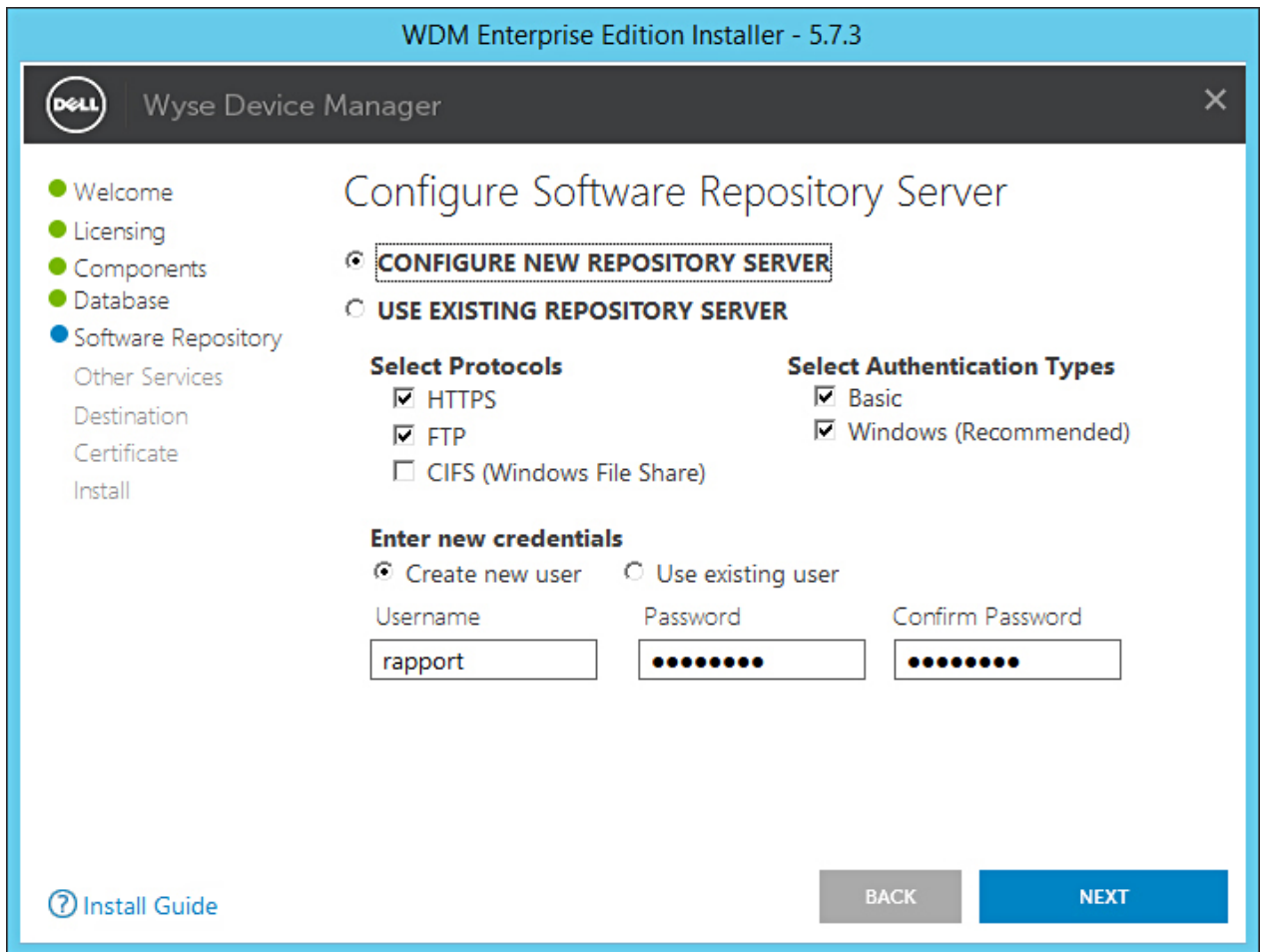


Figura 32. Opción CONFIGURE NEW REPOSITORY SERVER (Configurar nuevo servidor de repositorio)

- **USE EXISTING REPOSITORY SERVER** (Usar servidor de repositorio existente): seleccione esta opción si desea que el instalador configure un servidor de repositorio existente. Para configurar el servidor de repositorio existente:
 - Seleccione el protocolo y la configuración para distribuir el software a los dispositivos administrados. **HTTPS** aparece seleccionado de manera predeterminada. También puede seleccionar **FTP** para ThreadX 4.x y **CIFS** para ThreadX 5.x.
 - Seleccione el tipo de autenticación. **Windows** aparece seleccionado de manera predeterminada.
 - Ingrese las credenciales del servidor. La opción de dirección IP del servidor aparece atenuada y el nombre de usuario predeterminado es rapport.

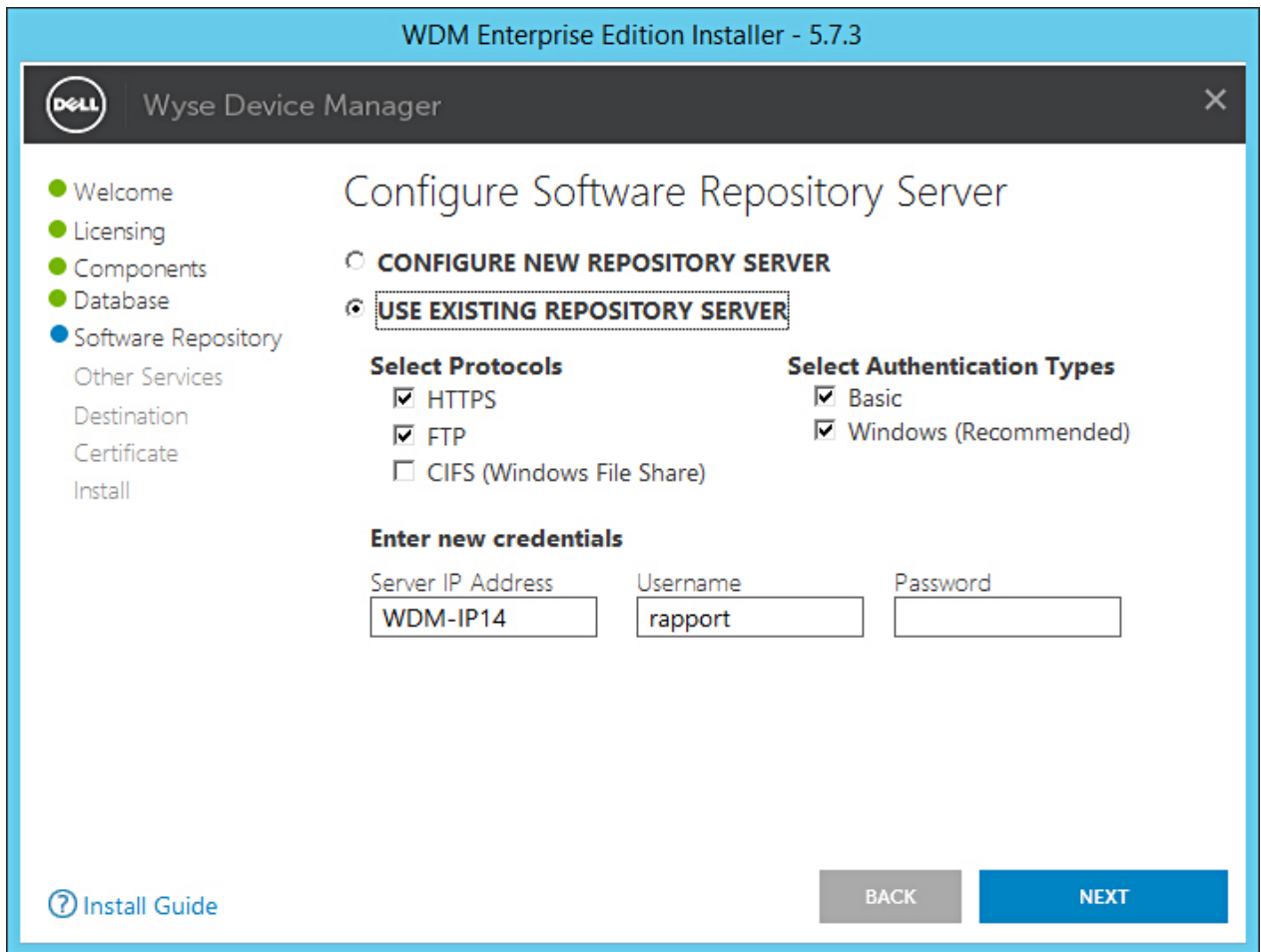


Figura 33. Opción USE EXISTING REPOSITORY SERVER (Usar servidor de repositorio existente)

- 12 Haga clic en **NEXT** (Siguiente).
- 13 Seleccione los servicios que desea instalar y haga clic en **NEXT** (Siguiente).

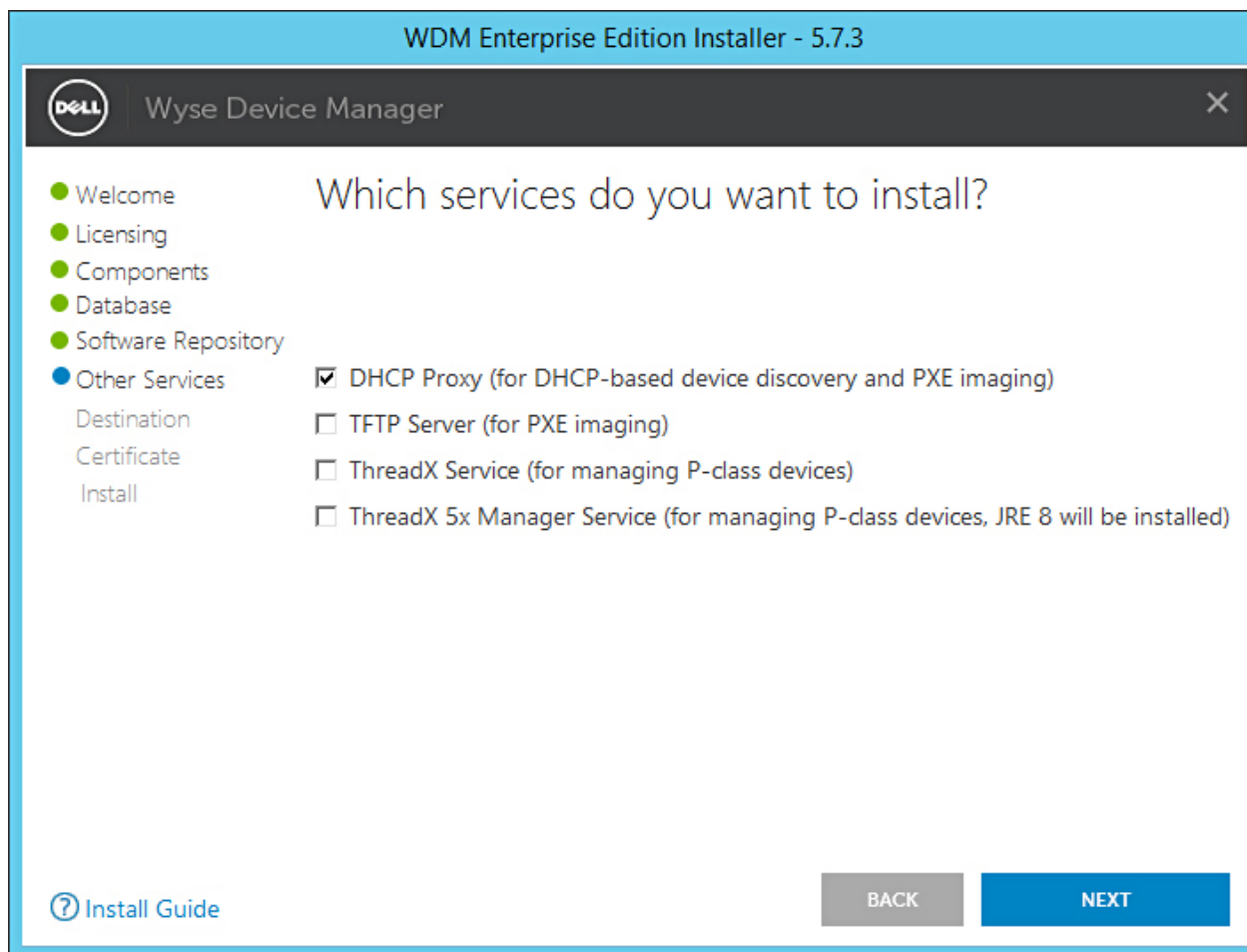


Figura 34. Pantalla Other Services (Otros servicios)

NOTA: Proxy DHCP aparece seleccionado de manera predeterminada.

14 Ingrese la ruta de instalación y haga clic en **NEXT** (Siguiendo).

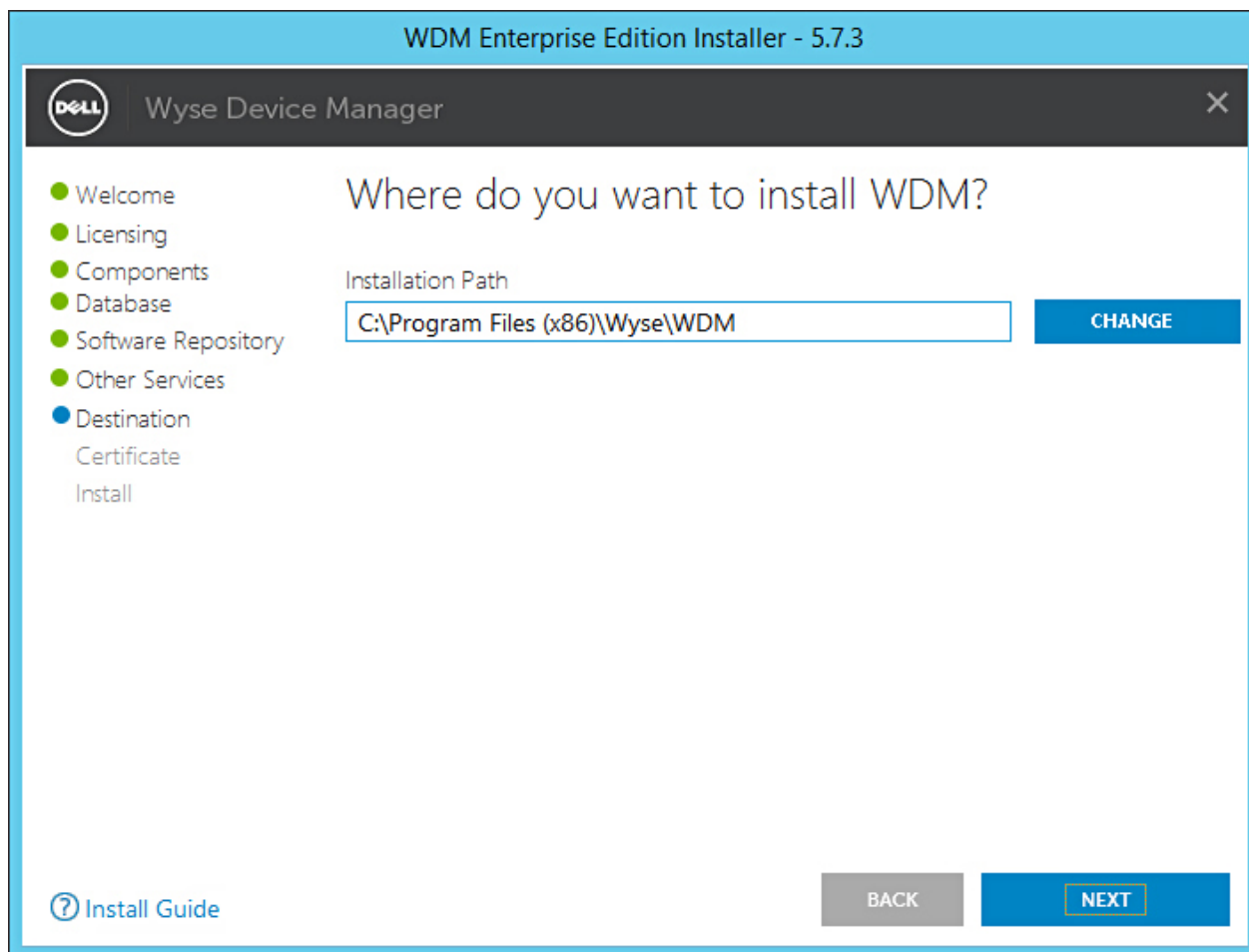


Figura 35. Pantalla Destination (Destino)

- 15 Seleccione e importe el certificado para iniciar la instalación.

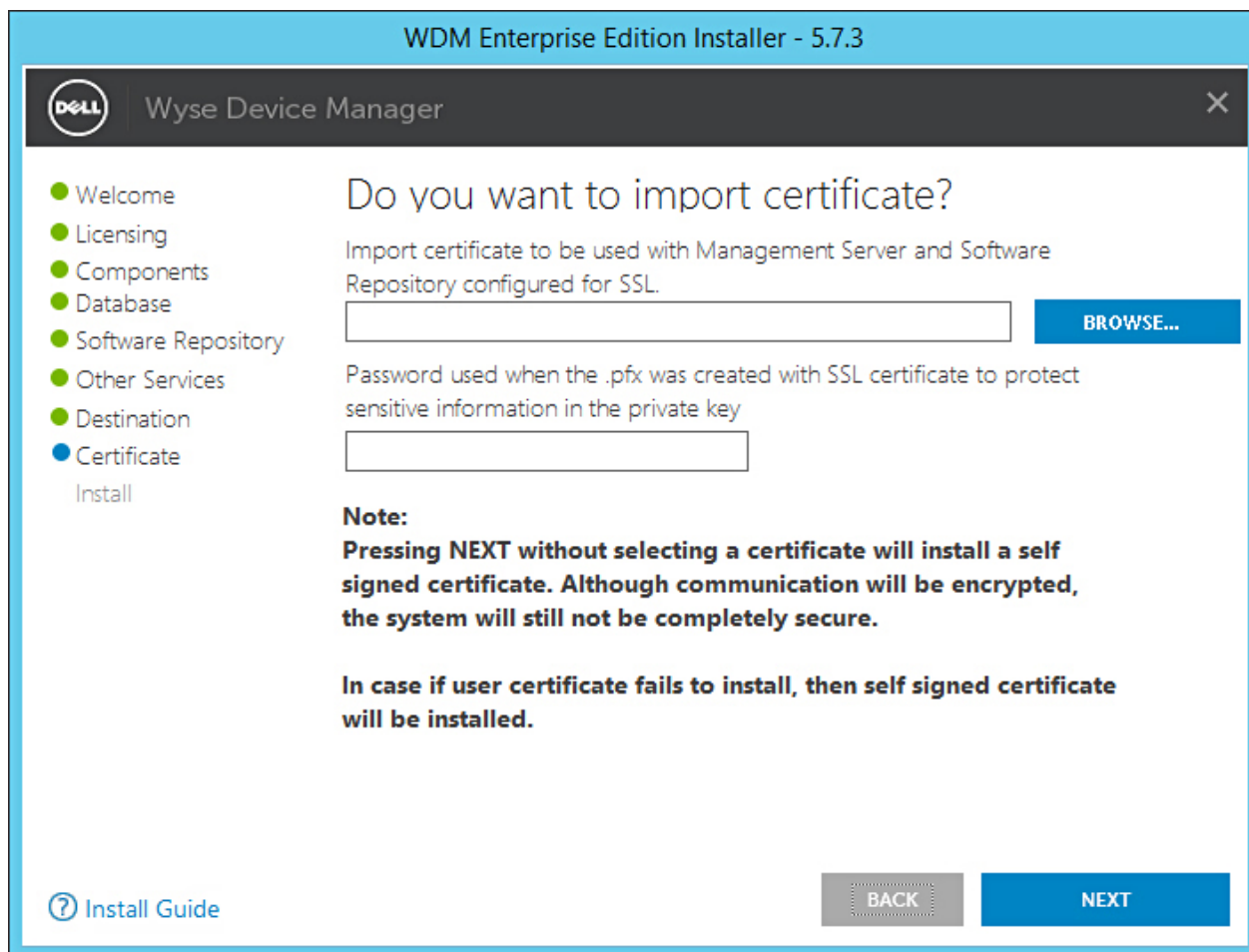


Figura 36. Pantalla Certificate (Certificado)

NOTA: Si hace clic en NEXT (Siguiente) sin seleccionar un certificado, el instalador instalará un certificado autofirmado. Las comunicaciones estarán cifradas, pero el sistema no está completamente seguro. El certificado debe estar en el formato de archivo .pfx.

El progreso de la instalación se muestra en la pantalla. Una vez finalizada la instalación, se le pedirá que reinicie el sistema.

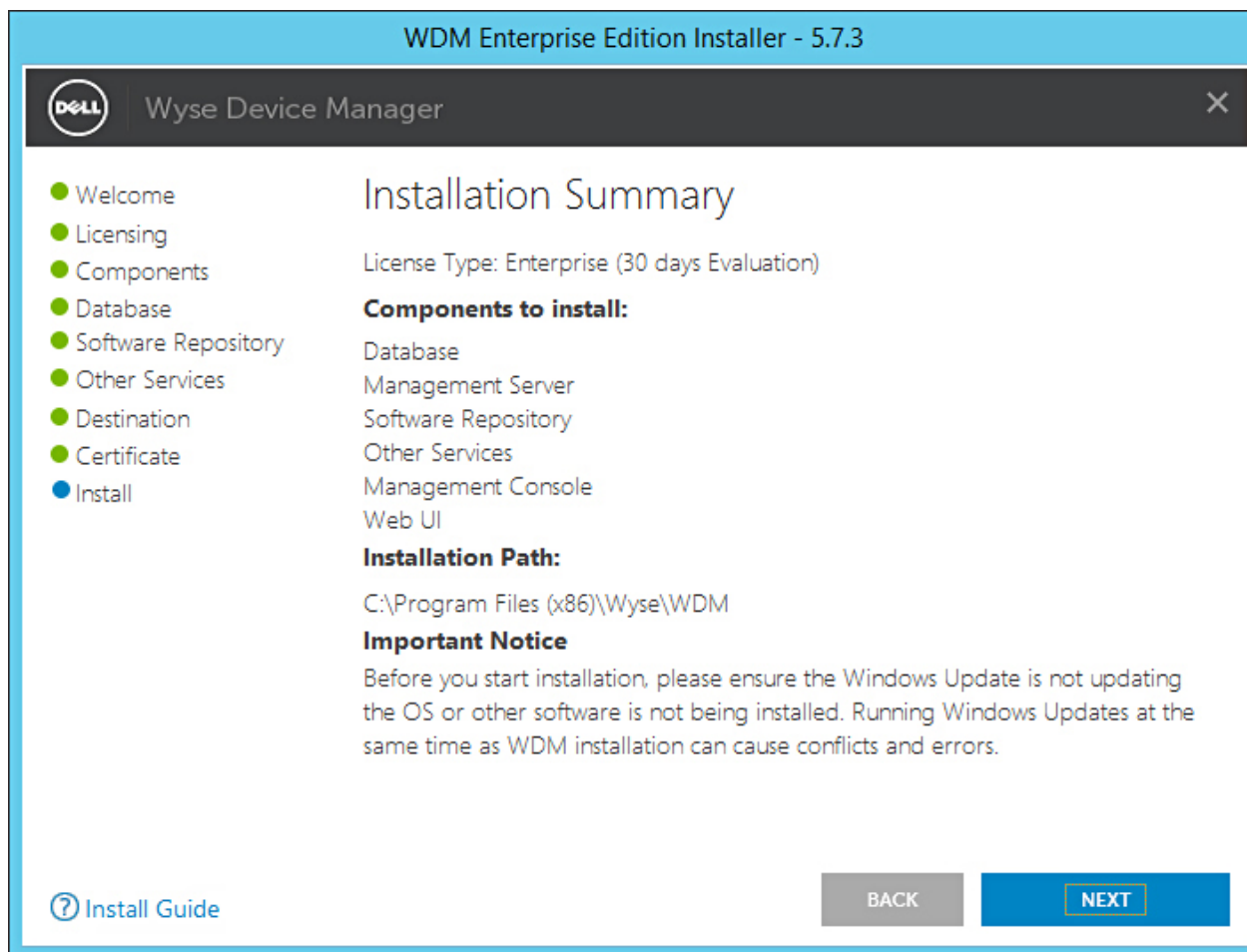


Figura 37. Pantalla Installation summary (Resumen de instalación)

16 Reinicie el sistema para que se efectúe el cambio.

Instalar WDM en una configuración distribuida

Puede dividir los componentes de WDM e instalarlos en diferentes sistemas. Esta configuración se denomina una configuración distribuida de WDM. Lo ideal sería que dividiera los componentes como se indica a continuación:

- Base de datos de WDM
- Servidor de administración de WDM, consola de administración de WDM y otros servicios
- Repositorio de software de WDM
- Web UI

También puede tener múltiples instancias de servidores de administración y otros servicios de WDM instalados en diferentes sistemas para activar el equilibrio de carga. Para obtener más información, consulte [Configurar la función de equilibrio de carga](#).

La instalación de WDM en una configuración distribuida es más adecuada en una gran empresa, en la que administre una gran cantidad de dispositivos. En esta sección se describe en detalle lo siguiente:

- [Instalar la base de datos de WDM](#).
- [Instalar el servidor de administración y la WebUI](#).
- [Instalar el repositorio de software](#).

Instalar la base de datos de WDM

Prerequisito

Antes de instalar la base de datos de WDM en un sistema o una máquina virtual (VM), asegúrese de haber instalado la versión compatible de Microsoft SQL Server. Si no tiene SQL Server en el sistema, puede instalar Microsoft SQL Express 2016 SP1, el que se suministra con el instalador de WDM.

NOTA:

Si va a instalar la base de datos de WDM en una base de datos de SQL Server existente, asegúrese de que el puerto 1433 esté disponible en el sistema.

Para instalar la base de datos de WDM, debe seleccionar **Database** (Base de datos) en la pantalla **Components** (Componentes) y, a continuación, continúe con el proceso de instalación.

Pasos

1 Extraiga el contenido del instalador de WDM en el sistema en donde desea instalar WDM.

2 Vaya a la carpeta en la que extrajo el instalador y ejecute **setup.exe**.

Si el servidor no tiene .Net Framework, se instalará automáticamente.

Se muestra la pantalla de Welcome (Bienvenida).

3 Haga clic en **NEXT** (Siguiente).

4 En el tipo de licencia, seleccione **ENTERPRISE**.

a Si tiene la clave de licencia de WDM, seleccione la opción **I have WDM Enterprise License Key** (Tengo clave de licencia de WDM) e ingrésela en el espacio que se proporciona.

b Si no tiene la clave de licencia, seleccione la opción **30–days Enterprise Evaluation** (Evaluación de 30 días de Enterprise).

La clave de licencia se ingresa de forma predeterminada. Sin embargo, después del período de evaluación de 30 días, debe obtener la clave de licencia y agregarla a WDM. Para obtener más información sobre cómo agregar la clave de licencia, consulte la *Dell Wyse Device Manager Administrator's Guide (Guía del administrador de Dell Wyse Device Manager)*.

5 Haga clic en **NEXT** (Siguiente).

6 Seleccione el componente de la **Database (base de datos)**.

7 En la pantalla **Configure Database** (Configurar base de datos), seleccione una de las siguientes opciones:

• **Install New Database Server (Microsoft SQL Express 2016 SP1)** (Instalar nuevo servidor de base de datos [Microsoft SQL Express 2016 SP1]): seleccione esta opción si no tiene ninguna versión compatible de Microsoft SQL Server instalada en el sistema, y continúe con el paso 8.

• **Use Existing Database Server (SQL Server Express or full)** (Usar servidor de base de datos existente [SQL Server Express o completo]): seleccione esta opción si ya ha instalado una versión compatible de Microsoft SQL Server en el sistema. Si selecciona esta opción, asegúrese de que el servidor de base de datos existente esté en el mismo sistema en el que instalará WDM Workgroup Edition, y continúe con el paso 9.

8 Si seleccionó la primera opción en el paso 7, seleccione el método de autenticación.

• **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:

1 Ingrese las credenciales de la base de datos de WDM.

2 Ingrese las nuevas credenciales de la base de datos. Puede ingresar el nombre de la instancia y el nombre de la base de datos en los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.

NOTA: Incluso si elige la autenticación de Windows, la instalación de WDM requiere la autenticación de SQL para acceder a la base de datos de SQL. En una instalación independiente, después de completar la instalación de la base de datos de WDM, el instalador se encarga de asignar el usuario de Active Directory a la base de datos y el mismo usuario se utiliza para instalar los servicios de WDM.

• **Windows Authentication (Autenticación de Windows):** ingrese los detalles del nuevo servidor de base de datos. Los nombres de la instancia y la base de datos predeterminados se muestran como RapportDB.

NOTA:

- Seleccione **Windows Authentication** (Autenticación de Windows) si desea conectarse a la base de datos de WDM con sus credenciales de inicio de sesión de Windows.
- La contraseña debe cumplir con las reglas de complejidad del sistema operativo Windows.

- 9 Si seleccionó la segunda opción en el paso 7, seleccione el método de autenticación.
- **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, haga lo siguiente:
 - 1 Seleccione la opción de **Create New User** (Crear nuevo usuario) o **Use the existing user** (Usar un usuario existente) y, a continuación, ingrese las credenciales de la base de datos de WDM.
 - 2 Ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL.
 - **Windows Authentication (Autenticación de Windows)**: ingrese los detalles del servidor de base de datos existente, tales como el nombre del host del servidor, el nombre de la instancia, el nombre de la base de datos, el número de puerto, y el nombre y la contraseña del administrador de SQL.

NOTA: El número de puerto predeterminado es 1433. Dell recomienda ingresar manualmente el número de puerto, ya que es dinámico. Es posible agregar un puerto personalizado de cinco dígitos para TCP/UDP en el rango entre 49152 y 65535.

- 10 Haga clic en **NEXT** (Siguiente).
- 11 Ingrese la ruta de instalación y haga clic en **NEXT** (Siguiente).
Se muestra la pantalla **Installation Summary** (Resumen de instalación).
- 12 Haga clic en **NEXT** (Siguiente).
El progreso de la instalación se muestra en la pantalla. Una vez finalizada la instalación, se le pedirá que reinicie el sistema.
- 13 Reinicie el sistema para que se efectúe el cambio.

Para la instalación manual de la base de datos de WDM por medio de scripts, consulte [Instalación manual de la base de datos de WDM por medio de scripts](#).

Instalar los servicios de administración

Acerca de esta tarea

Puede instalar el servidor de administración, la consola de administración y la interfaz para el usuario web (WebUI) en el mismo sistema o en diferentes sistemas.

Pasos

- 1 Extraiga el contenido del instalador de WDM en el sistema en donde desea instalar WDM.
- 2 Vaya a la carpeta en la que extrajo el instalador y ejecute **setup.exe**.
Si el servidor no tiene .Net Framework, se instalará automáticamente.

Se muestra la pantalla de **Welcome** (Bienvenida).
- 3 Haga clic en **NEXT** (Siguiente).
- 4 En el tipo de licencia, seleccione **ENTERPRISE**.
 - a Si tiene la clave de licencia de WDM, seleccione la opción **I have WDM Enterprise License Key** (Tengo clave de licencia de WDM) e ingrésela en el espacio que se proporciona.
 - b Si no tiene la clave de licencia, seleccione la opción **30-days Enterprise Evaluation** (Evaluación de 30 días de Enterprise).
La clave de licencia se ingresa de forma predeterminada. Sin embargo, después del período de evaluación de 30 días, debe obtener la clave de licencia y agregarla a WDM. Para obtener más información sobre cómo agregar la clave de licencia, consulte la *Dell Wyse Device Manager Administrator's Guide (Guía del administrador de Dell Wyse Device Manager)*.
- 5 Haga clic en **NEXT** (Siguiente).
- 6 Seleccione **Management Server** (Servidor de administración), **Other Services** (Otros servicios), **Management Console** (Consola de administración) y **WebUI**.

NOTA: Si va a instalar cada componente en un sistema diferente, puede seleccionarlos uno por uno siguiendo los pasos 1 al 5.

- 7 En la pantalla **Configure Database** (Configurar base de datos), seleccione una de las siguientes opciones:
 - **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, ingrese las credenciales del servidor de base de datos de WDM
 - **Windows Authentication (Autenticación de Windows)**: ingrese los detalles del servidor de base de datos de WDM como, por ejemplo, nombre del servidor, nombre de la instancia, nombre de la base de datos, contraseña y número de puerto. El campo **Username** (Nombre de usuario) está atenuado.

NOTA:

- El número de puerto predeterminado es 1433. Dell recomienda ingresar manualmente el número de puerto, ya que es dinámico. Es posible agregar un puerto personalizado de cinco dígitos para TCP/UDP en el rango entre 49152 y 65535.
- Seleccione **Windows Authentication** (Autenticación de Windows) si desea conectarse a la base de datos de WDM con sus credenciales de inicio de sesión de Windows.

- 8 Haga clic en **NEXT** (Siguiente).
- 9 Seleccione los servicios que desea instalar y haga clic en **NEXT** (Siguiente).

NOTA: Proxy DHCP aparece seleccionado de manera predeterminada.

- 10 Ingrese la ruta de instalación y haga clic en **NEXT** (Siguiente).
- 11 Seleccione e importe el certificado para iniciar la instalación.

NOTA: Si hace clic en NEXT (Siguiente) sin seleccionar un certificado, el instalador instalará un certificado autofirmado. Las comunicaciones estarán cifradas, pero el sistema no es seguro. El certificado debe estar en el formato de archivo .pfx.

El progreso de la instalación se muestra en la pantalla. Una vez finalizada la instalación, se le pedirá que reinicie el sistema.

- 12 Reinicie el sistema para que se efectúe el cambio.

NOTA: En un ambiente distribuido, la WebUI se puede instalar en varias consolas.

Instalar el repositorio de software

Prerequisito

El repositorio de software es otro componente importante de WDM. Los paquetes que se van a implementar en los sistemas del cliente se guardan y almacenan en el repositorio de software. Antes de instalar el repositorio de software, asegúrese de haber instalado y configurado la base de datos de WDM.

Pasos

- 1 Extraiga el contenido del instalador de WDM en el sistema en donde desea instalar WDM.
- 2 Vaya a la carpeta en la que extrajo el instalador y ejecute **setup.exe**.
Si el servidor no tiene .Net Framework, se instalará automáticamente.

Se muestra la pantalla de **Welcome** (Bienvenida).
- 3 Haga clic en **NEXT** (Siguiente).
- 4 En el tipo de licencia, seleccione **ENTERPRISE**.
 - a Si tiene la clave de licencia de WDM, seleccione la opción **I have WDM Enterprise License Key** (Tengo clave de licencia de WDM) e ingrésela en el espacio que se proporciona.
 - b Si no tiene la clave de licencia, seleccione la opción **30-days Enterprise Evaluation** (Evaluación de 30 días de Enterprise).
La clave de licencia se ingresa de forma predeterminada. Sin embargo, después del período de evaluación de 30 días, debe obtener la clave de licencia y agregarla a WDM. Para obtener más información sobre cómo agregar la clave de licencia, consulte la *Dell Wyse Device Manager Administrator's Guide (Guía del administrador de Dell Wyse Device Manager)*.
- 5 Haga clic en **NEXT** (Siguiente).
- 6 Seleccione el componente **Software Repository** (Repositorio de software).
- 7 En la pantalla **Configure Database** (Configurar base de datos), seleccione una de las siguientes opciones:
 - **SQL Server Authentication** (Autenticación de SQL Server): esta opción está seleccionada de manera predeterminada. Para configurar la autenticación de SQL Server, ingrese las credenciales del servidor de base de datos de WDM

- **Windows Authentication (Autenticación de Windows):** ingrese los detalles del servidor de base de datos de WDM como, por ejemplo, nombre del servidor, nombre de la instancia, nombre de la base de datos, contraseña y número de puerto. El campo **Username** (Nombre de usuario) está atenuado.

NOTA:

- El número de puerto predeterminado es 1433. Dell recomienda ingresar manualmente el número de puerto, ya que es dinámico. Es posible agregar un puerto personalizado de cinco dígitos para TCP/UDP en el rango entre 49152 y 65535.
- Seleccione **Windows Authentication** (Autenticación de Windows) si desea conectarse a la base de datos de WDM con sus credenciales de inicio de sesión de Windows.

- 8 Haga clic en **NEXT** (Siguiente).
- 9 Seleccione los servicios que desea instalar y haga clic en **NEXT** (Siguiente).

NOTA: Proxy DHCP aparece seleccionado de manera predeterminada.

- 10 Ingrese la ruta de instalación y haga clic en **NEXT** (Siguiente).
- 11 Seleccione e importe el certificado para iniciar la instalación.

NOTA: Si hace clic en NEXT (Siguiente) sin seleccionar un certificado, el instalador instalará un certificado autofirmado. Las comunicaciones estarán cifradas, pero el sistema no es seguro. El certificado debe estar en el formato de archivo .pfx.

El progreso de la instalación se muestra en la pantalla. Una vez finalizada la instalación, se le pedirá que reinicie el sistema.

- 12 Reinicie el sistema para que se efectúe el cambio.

NOTA: En un ambiente distribuido, la WebUI se puede instalar en varias consolas.

Actualizar WDM

Requisitos previos

La versión actual de WDM es compatible con una actualización de la versión 5.7.2/5.7.2 hotfix. No se puede actualizar de ninguna otra versión. Si se ejecuta una versión anterior de WDM, primero debe actualizar a la versión 5.7.2/5.7.2 hotfix y, a continuación, actualizar a la versión más reciente.

NOTA: Después de actualizar WDM a la versión 5.7.3, debe actualizar todos los dispositivos con los paquetes de agentes más recientes disponibles para asegurarse de que se puedan administrar con WDM. Para obtener más información, consulte *WDM 5.7.3 Release Notes (Notas de la versión WDM 5.7.3)* en support.dell.com.

Tarea

- 1 Extraiga el contenido del instalador de WDM en el sistema donde tenga instalada la versión WDM 5.7.2 /5.7.2 hotfix.
- 2 Vaya a la carpeta en la que extrajo el instalador y ejecute **setup.exe**.

Se muestra la pantalla de **Welcome** (Bienvenida).

- 3 Haga clic en **Next** (Siguiente).
Se muestra la pantalla **Upgrade Information** (Información de actualización).
- 4 Haga clic en **Next** (Siguiente). Se muestra la pantalla **User Credentials** (Credenciales de usuario).
- 5 Ingrese la contraseña.

IMPORTANTE: En el caso de la autenticación de SQL, el campo Password (Contraseña) está desactivado. Es necesario que ingrese la contraseña solo para autenticación de Windows.

- 6 Haga clic en **Next** (Siguiente).
Se muestra la pantalla **Important Information** (Información importante).
- 7 Lea la **Important Information (información importante)** y haga clic en **Next** (Siguiente).

Comienza el proceso de actualización.

- Una vez terminado el proceso de actualización, haga clic en **Restart Now** (Reiniciar ahora) para que los cambios se apliquen al sistema antes de empezar a utilizar WDM.

NOTA: ThreadX 5.x se instala automáticamente si ThreadX 4.x ya está instalado en el sistema con Windows 2012 y versiones anteriores.

Configurar comunicaciones seguras

Configurar comunicaciones seguras mediante SSL:

Existen diferentes formas de instalar SSL en IIS 6.0 e IIS 7.0. Los procedimientos necesarios para configurar SSL en IIS 6.0 e IIS 7.0 se proporcionan a continuación.

Configurar SSL en IIS 7.0 en Windows Server 2008 R2

Para configurar SSL en IIS 7.0:

- Descargue la utilidad **SelfSSL7** desde el vínculo [SelfSSL.exe](#).
- Nombre esta utilidad como **SelfSSL7.exe** con los parámetros mencionados a continuación:

```
SelfSSL7.exe /Q /N cn=Certificate_Name /I /S Web_Site_Name. e.g. SelfSSL7.exe /Q /N  
cn="TestCert.TestLab.com" /I /S "Default Web Site"
```

Configurar comunicaciones seguras mediante la autoridad de certificación raíz

Instalar la autoridad de certificación raíz en IIS 7 en Windows Server 2008 R2

Use las siguientes pautas:

Para instalar el certificado, debe seguir dos pasos:

- Instale el certificado en el servidor **Domain Controller** (Controlador de dominio).
- Instale el certificado en el servidor **WDM**.

Instalar el certificado en el servidor Controlador de dominio

Use las siguientes pautas:

- Vaya al **Server Manager (Administrador del servidor)**.
- En el panel de árbol, seleccione **Roles->Add Roles** (Roles-> Agregar roles).
- En el asistente **Add Roles** (Agregar roles), seleccione **Server Roles** (Roles del servidor) desde el panel de árbol.
- En la ventana para seleccionar **Server Roles** (Roles del servidor), marque **Active Directory Certificate Service** (Servicio de certificación de Active Directory) en **Roles (Roles)**.
- Haga clic en **Next->Next** (Siguiente-> Siguiente). A continuación, en **Role Services** (Servicios de rol), seleccione las opciones **Certification Authority** (Autoridad de certificación) y **Certificate Authority Web Enrolment** (Registro web de autoridad de certificación).
- Tras seleccionar la opción **Certificate Authority Web Enrolment** (Registro web de autoridad de certificación), si IIS no está instalado en el servidor, se mostrará otra ventana bajo el nombre **Add Required Role Services** (Agregar servicios de rol requeridos).
- En la ventana anterior, haga clic en el botón **Add Required Role Services** (Agregar servicios de rol requeridos) y haga clic en **Next** (Siguiente) para invocar la ventana **Specify Setup Type** (Especificar tipo de configuración).
- En la ventana anterior, según el requisito, seleccione el botón de opción **Enterprise** o **Standalone** (Independiente) y, a continuación, haga clic en **Next** (Siguiente) para abrir la ventana **Specify CA Type** (Especificar tipo de autoridad de certificación).
- En la ventana **Specify CA Type** (Especificar tipo de autoridad de certificación), según el requisito, seleccione el botón de opción **Root CA** (Autoridad de certificación raíz) o **Subordinate CA** (Autoridad de certificación subordinada) y, a continuación, haga clic en **Next** (Siguiente) para abrir la ventana **Setup Private Key** (Configurar clave privada).
- En la ventana **Setup Private Key** (Configurar clave privada), según el requisito, seleccione el botón de opción **Create a new private key** (Crear una nueva clave privada) o **Use existing private key** (Utilizar clave privada existente) y, a continuación, haga clic en **Next** (Siguiente) para abrir la ventana **Configure Cryptography for CA** (Configurar criptografía para la autoridad de certificación).
- En la ventana **Configure Cryptography for CA** (Configurar criptografía para la autoridad de certificación), según el requisito, seleccione el valor para el campo **Select a cryptography service provider (CSP)** (Seleccionar proveedor de servicios criptográficos).

[CPS]) en el cuadro combinado, proporcione la **Key character length (Longitud de caracteres de la clave)** en el cuadro combinado, seleccione el valor para el campo **Select the Hash algorithm for signing certificate issued by this CA** (Seleccionar algoritmo hash para el certificado de firma emitido por esta autoridad de certificación); además, seleccione o deseleccione el cuadro de verificación **Allow administrator interaction when the private key is accessed by the CA** (Permitir interacción de administrador cuando la autoridad de certificación accede a la clave privada) y, a continuación, haga clic en el botón **Next (Siguiente)** para abrir la ventana **Configure CA Name** (Configurar nombre de autoridad de certificación).

ⓘ | NOTA: El nombre común del certificado debe coincidir con el nombre de la computadora del servidor WDM.

- 12 En la ventana **Configure CA Name** (Configurar nombre de autoridad de certificación), proporcione los valores de los campos **Common name for this CA** (Nombre común de esta autoridad de certificación) y **Distinguished name suffix** (Sufijo del nombre distintivo), y haga clic en **Next** (Siguiente) para abrir la ventana **Set Validity Period** (Establecer período de validez).
- 13 En la ventana **Set Validity Period** (Establecer período de validez), seleccione el período de validez del certificado generado para esta autoridad de certificación y haga clic en **Next** (Siguiente) para abrir la ventana **Configure Certificate Database** (Configurar base de datos del certificado).
- 14 En la ventana **Configure Certificate Database** (Configurar base de datos del certificado), seleccione la **Certificate database location (Ubicación de la base de datos del certificado)** y la **Certificate database log location (Ubicación del registro de la base de datos del certificado)** y, a continuación, haga clic en **Next** (Siguiente) para abrir la ventana **Add Roles Wizard** (Asistente para agregar roles).
- 15 Seleccione los valores predeterminados y haga clic en **Next-> Install** (Siguiente-> Instalar).
- 16 Se instalarán los **Active Directory Certificate Services (Servicios de certificación de Active Directory)**, el **Web Server (IIS) (Servidor web [IIS])** y las **Remote Server Administration Tools (Herramientas de administración remota del servidor)**.
- 17 Una vez que haya instalado el certificado, vaya al **Internet Information Services Manager (Administrador de servicios de información de Internet)** del controlador del dominio.
- 18 En el panel de árbol **Server Manager** (Administrador del servidor), expanda **Roles (Roles)** y, a continuación, haga clic en **Web Server (IIS)-> Internet Information Services (IIS) Manager** (Servidor web [IIS]-> Administrador de servicios de información de Internet [IIS]) para abrir la ventana **IIS Manager** (Administrador de IIS).
- 19 En el panel de árbol, seleccione el **Server (Servidor)** y en el panel de la derecha, haga doble clic en **Server Certificates** (Certificados del servidor).
- 20 En el panel derecho de **Server Certificates** (Certificados del servidor), haga doble clic en **Create Domain Certificate...** (Crear certificado de dominio...) para empezar a crear un certificado.
- 21 Rellene la información solicitada en la ventana **Create Certificate** (Crear certificado) y haga clic en **Next** (Siguiente) para abrir **Online Certification Authority** (Autoridad de certificación en línea).
- 22 En **Online Certification Authority** (Autoridad de certificación en línea), haga clic en **select** (Seleccionar) para **Specify Online Certification Authority** (especificar la autoridad de certificación en línea) y proporcione un **Friendly Name** (nombre descriptivo) para la misma; a continuación, haga clic en **Finish** (Terminar).
- 23 Ahora que está lista la instalación del certificado en el servidor del controlador de dominio, vaya a la instalación del certificado en el servidor WDM.

Instalar el certificado en el servidor WDM

Use las siguientes pautas:

- 1 En la barra de tareas, haga clic en **Start->Administrative Tools->Internet Information Services (IIS) Manager** (Iniciar-> Herramientas administrativas-> Administrador de servicios de información de Internet [IIS]) para abrir la ventana **IIS Manager** (Administrador de IIS).
- 2 En el panel de árbol, haga clic en el **Server (Servidor)** y, en el panel derecho, haga doble clic en **Server Certificates** (Certificados del servidor) para abrir la ventana **Server Certificates** (Certificados del servidor).
- 3 Rellene la información solicitada en la ventana **Create Certificate** (Crear certificado) y haga clic en **Next** (Siguiente) para abrir **Online Certification Authority** (Autoridad de certificación en línea).
- 4 En **Online Certification Authority** (Autoridad de certificación en línea), haga clic en **select** (Seleccionar) para **Specify Online Certification Authority** (especificar la autoridad de certificación en línea) y proporcione un **Friendly Name** (nombre descriptivo) para la misma; a continuación, haga clic en **Finish** (Terminar).
- 5 Ahora está lista la instalación del certificado en el servidor WDM.
- 6 Después de instalar el certificado, examine **Server ->Web Sites->Rapport HTTP Server** (Servidor -> Sitios web-> Servidor HTTP Rapport) y haga clic en **Bindings...** (Vinculaciones...) en el panel que está más a la derecha para abrir la ventana **Site Bindings** (Vinculaciones de sitio).
- 7 En la ventana **Site Bindings** (Vinculaciones de sitio), haga clic en **Add** (Agregar) para **Add Site Binding** (Agregar vinculación de sitio).
- 8 En **Add Site Binding** (Agregar vinculación de sitio), seleccione el certificado creado recientemente desde el cuadro combinado **SSL Certificate** (Certificado SSL) y haga clic en el botón **OK** (Aceptar).

- 9 Para iniciar solo la comunicación HTTPS, seleccione **SSL Settings** (Configuración de SSL) en **Server->Web Sites->Report HTTP Server** (Servidor-> Sitios web-> Servidor HTTP Report).
- 10 En **SSL Settings** (Configuración de SSL), seleccione la casilla de verificación **Require SSL** (Requerir SSL) y haga clic en **Apply** (Aplicar) para aplicar el ajuste.

Instalar la autoridad de certificación raíz en IIS 7 en Windows Server 2012 R2

Use las siguientes pautas:

- Para instalar el certificado, debe seguir dos pasos:
 - Instalar el certificado en el servidor Controlador de dominio
 - Instalar el certificado en el servidor WDM

Instalar el certificado en el servidor Controlador de dominio:

Use las siguientes pautas:

- 1 Vaya al Administrador del servidor.
- 2 En el **Dashboard (Panel)** >> seleccione la opción 2 **Add Roles and features** (Agregar roles y funciones).
- 3 En el asistente Add Roles and Features (Agregar roles y funciones), seleccione Installation Type as >> Role-based or feature-based installation (Tipo de instalación como>> Instalación basada en roles o basada en funciones).
- 4 En Server Selection >> (Selección de servidor>>) seleccione un servidor del grupo de servidores (de forma predeterminada estará seleccionado el servidor local).
- 5 A continuación, en la ventana Server Role (Rol del servidor), seleccione Active Directory Certificate Services' Role (Rol de los servicios de certificación de Active Directory).
- 6 Si selecciona Active Directory Certificate Services Role (Rol de los servicios de certificación de Active Directory), iniciará el asistente Add Role and Features (Agregar roles y funciones), que automáticamente iniciará las subfunciones>> haga clic en el botón Add Features (Agregar funciones).
- 7 Haga clic en Next->Next (Siguiente-> Siguiente). A continuación, en la ventana Features (Funciones), deje los valores predeterminados tal como están y haga clic en Next (Siguiente).
- 8 A continuación, se mostrará la ventana Servicios de certificación de Active Directory; haga clic en el botón Next (Siguiente).
- 9 En la ventana Role Service (Servicios de rol), seleccione las opciones Certification Authority (Autoridad de certificación) y Certificate Authority Web Enrolment (Registro web de autoridad de certificación).
- 10 Después de seleccionar la opción Registro web de autoridad de certificación, si IIS no está instalado en el servidor, se mostrará otra ventana Add Features (Agregar funciones) para aquellas que requiere la subventana Certification Authority Web Enrollment (Registro web de autoridad de certificación).
- 11 En la ventana anterior, haga clic en el botón Add Feature (Agregar función) y haga clic en Next (Siguiente) para ver la ventana de confirmación.
- 12 A continuación, haga clic en el botón "Install" (Instalar) para instalar el rol del certificado de AD.
- 13 En la ventana "Results" (Resultados) puede ver el progreso de la instalación de funciones.
- 14 Después de la instalación correcta del rol de la autoridad de certificación de AD, haga clic en el botón "Close" (Cerrar).
- 15 A continuación, en "Server Manager>> Dashboard console" (Administrador del servidor>> Consola del panel), en Notifications (Notificaciones), encontrará el mensaje de configuración después de la implementación.
- 16 En el mensaje de configuración después de la implementación, haga clic en el vínculo "Configure Active Directory Certificate Services on the local server" (Configurar servicios de certificación de Active Directory en el servidor local).
- 17 A continuación, se abrirá la ventana AD CS Configuration (Configuración de autoridad de certificación de AD)>> Credentials (Credenciales); en esta ventana, ingrese las credenciales correctas y haga clic en el botón "Next" (Siguiente).
- 18 Luego, en Role Services>> (Servicios de rol) seleccione las opciones Certification Authority (Autoridad de certificación) y Certificate Authority Web Enrolment (Registro web de autoridad de certificación) y, a continuación, haga clic en botón "Next" (Siguiente).
- 19 Ahora, en la ventana Setup Type (Tipo de configuración), según el requisito, seleccione el botón de opción Enterprise o Standalone (Independiente) y, a continuación, haga clic en Next (Siguiente) para abrir la ventana CA Type (Tipo de autoridad de certificación).
- 20 En la ventana CA Type (Tipo de autoridad de certificación), según el requisito, seleccione el botón de opción Root CA (Autoridad de certificación raíz) o Subordinate CA (Autoridad de certificación subordinada) y, a continuación, haga clic en Next (Siguiente) para abrir la ventana Private Key (Clave privada).
- 21 En la ventana Private Key (Clave privada), según el requisito, seleccione el botón de opción Create a new private key (Crear una nueva clave privada) o Use existing private key (Utilizar clave privada existente) y, a continuación, haga clic en Next (Siguiente) para abrir la ventana Configure Cryptography for CA (Configurar criptografía para la autoridad de certificación).

- 22 En la ventana Configure Cryptography for CA (Configurar criptografía para la autoridad de certificación):
 - Según el requisito, seleccione el valor para el campo Select a cryptographic service provider (CSP) (Seleccionar proveedor de servicios criptográficos [CPS]) en el cuadro combinado.
 - Proporcione la longitud de la clave desde el siguiente cuadro combinado
 - Seleccione el valor para el campo Select the Hash algorithm (Seleccionar algoritmo hash) para el certificado de firma emitido por esta autoridad de certificación.
 - A continuación, seleccione o deseleccione el cuadro de verificación "Allow administrator interaction when the private key is accessed by the CA" (Permitir interacción de administrador cuando la autoridad de certificación accede a la clave privada).
 - Finalmente, haga clic en el botón Next (Siguiente) para abrir la ventana Configure CA Name (Configurar nombre de autoridad de certificación). NOTA: El nombre común del certificado debe coincidir con el nombre de la computadora del servidor WDM.
- 23 En la ventana CA Name (Nombre de autoridad de certificación), proporcione los valores de los campos Common name for this CA (Nombre común de esta autoridad de certificación) y Distinguished name suffix (Sufijo del nombre distintivo), y haga clic en Next (Siguiente) para abrir la ventana Validity Period (Período de validez).
- 24 En la ventana Validity Period (Período de validez), seleccione el período de validez del certificado generado para esta autoridad de certificación y haga clic en Next (Siguiente) para abrir la ventana Certificate Database (Base de datos del certificado).
- 25 En la ventana Certificate Database (Base de datos del certificado), seleccione la ubicación de la base de datos del certificado y la ubicación del registro de la base de datos del certificado y, a continuación, haga clic en Next (Siguiente) para abrir la ventana de confirmación.
- 26 A continuación, en la ventana "Confirmation " (Confirmación), haga clic en botón Configure button which will launch the progress (Configurar para iniciar la ventana de progreso).
- 27 Luego, en la ventana "Results" (Resultados), se mostrará el mensaje "Certification Authority and Certification Authority Web Enrollment Configuration succeeded" (Configuración de la autoridad de certificación y el registro web de la autoridad de certificación se realizó correctamente).
- 28 Haga clic en el botón Close (Cerrar) para terminar la configuración de los servicios de certificación de AD.
- 29 Ahora que está lista la instalación del certificado en el servidor del controlador de dominio, vaya a la instalación del certificado en el servidor WDM.

Instalar el certificado en el servidor WDM:

Use las siguientes pautas:

- 1 En la barra de tareas, haga clic en Start->Administrative Tools->Internet Information Services (IIS) Manager (Iniciar-> Herramientas administrativas-> Administrador de servicios de información de Internet [IIS]) para abrir la ventana IIS Manager (Administrador de IIS).
- 2 En el panel de árbol, haga clic en el servidor y, en el panel derecho, haga doble clic en Server Certificates (Certificados del servidor) para abrir la ventana Server Certificates (Certificados del servidor).
- 3 Haga clic en el vínculo Create Domain Certificate (Crear certificado de dominio) en el panel que está más a la derecha y rellene la información solicitada en la ventana Create Certificate (Crear certificado) y, a continuación, haga clic en Next (Siguiente) para abrir Online Certification Authority (Autoridad de certificación en línea).
- 4 En Online Certification Authority (Autoridad de certificación en línea), haga clic en seleccionar para Specify Online Certification Authority (Especificar la autoridad de certificación en línea) (creada en su máquina controladora de AD o en su configuración) y proporcione un nombre descriptivo para la misma; a continuación, haga clic en Finish (Terminar).
- 5 Ahora está lista la instalación del certificado en el servidor WDM.
- 6 Después de instalar el certificado, examine Server ->Sites->Rapport HTTP Server (Servidor -> Sitios-> Servidor HTTP Rapport) y haga clic en Bindings... (Vinculaciones...) en el panel que está más a la derecha para abrir la ventana Site Bindings (Vinculaciones de sitio).
- 7 En la ventana Site Bindings (Vinculaciones de sitio), haga clic en Add (Agregar) para Add Site Binding (Agregar vinculación de sitio).
- 8 En Add Site Binding (Agregar vinculación de sitio), seleccione Type as HTTPS (Tipo como HTTPS) y seleccione la autoridad de certificación en la dirección IP; seleccione el certificado creado recientemente desde el cuadro combinado desplegable SSL Certificate (Certificado SSL) y haga clic en el botón OK (Aceptar).
- 9 Para iniciar solo la comunicación HTTPS, seleccione SSL Settings (Configuración de SSL) en Server->Web Sites->Rapport HTTP Server (Servidor-> Sitios web-> Servidor HTTP Rapport).
- 10 En SSL Settings (Configuración de SSL), seleccione la casilla de verificación Require SSL (Requerir SSL) y el botón de opción "Require" (Requerir) para el certificado de cliente, y aplique los ajustes.

Desinstalar la instalación independiente de WDM

Acerca de esta tarea

Si tiene una instalación independiente de WDM, donde todos los componentes están instalados en el mismo sistema, puede llevar a cabo los siguientes pasos para desinstalar WDM.

Pasos

- 1 Vaya a **Start (Iniciar) > Control Panel (Panel de control)**.
- 2 Haga clic en **Programs (Programas) > Uninstall a program (Desinstalar un programa)**.
- 3 Seleccione **WDM 5.7.3** de la lista de programas, y haga clic en **Uninstall** (Desinstalar).
Se mostrará la pantalla **Uninstallation** (Desinstalación).
- 4 Haga clic en **Next** (Siguiente) en la pantalla de **Welcome** (Bienvenida).
- 5 Ingrese las credenciales para acceder a la base de datos de WDM.
Tendrá que especificar las credenciales de inicio de sesión de SQL Server o SQL Express, según la ubicación donde tenga instalada la base de datos de WDM.

Si especifica las credenciales incorrectas, se mostrará el mensaje de error **Unable to connect to database** (No se puede conectar a la base de datos).
- 6 Haga clic en **Next** (Siguiente).
Una vez que haya desinstalado los componentes, se le pedirá que reinicie el sistema.
- 7 Haga clic en **Restart Now** (Reiniciar ahora) para completar el proceso de desinstalación.

Siguiente paso

Después de desinstalar, asegúrese de que cumple con las siguientes listas de verificación:

- Debe eliminar el ícono de **WebUI** de Wyse Device Manager 5.7.3 del escritorio.
- En IIS, la aplicación HAPI debe eliminarse bajo Rapport HTTP Server.
- En IIS, la aplicación MyWDM debe eliminarse bajo Rapport HTTP Server.
- En IIS, la aplicación WebUI debe eliminarse bajo Rapport HTTP Server.

Desinstalar WDM en una configuración distribuida

Acerca de esta tarea

Si instaló WDM en una configuración distribuida, debe desinstalar los componentes uno por uno en los sistemas donde los haya instalado.

NOTA: Antes de desinstalar la base de datos de WDM, debe desinstalar todos los otros componentes en los sistemas donde los haya instalado.

Pasos

- 1 Inicie sesión en el sistema o los sistemas donde haya instalado el servidor de administración, la consola de administración, otros servicios, el repositorio de software y la WebUI.
- 2 Vaya a **Start (Iniciar) > Control Panel (Panel de control)**.
- 3 Haga clic en **Programs (Programas) > Uninstall a program (Desinstalar un programa)**.
- 4 Seleccione **WDM 5.7.3** de la lista de programas, y haga clic en **Uninstall** (Desinstalar).
Se mostrará la pantalla **Uninstallation** (Desinstalación).
- 5 Haga clic en **Next** (Siguiente) en la pantalla de **Welcome** (Bienvenida).
- 6 Haga clic en **Next** (Siguiente) para iniciar el proceso de desinstalación.
- 7 Inicie sesión en el sistema donde haya instalado la base de datos de WDM.

- 8 Repita los pasos 2 al 5.
- 9 Ingrese las credenciales para acceder a la base de datos de WDM.
Tendrá que especificar el ID de inicio de sesión de SQL Server o SQL Express, según la ubicación donde tenga instalada la base de datos de WDM.

Si especifica las credenciales incorrectas, el programa mostrará el siguiente mensaje de error *Unable to connect to database* (No se puede conectar a la base de datos). Asegúrese de ingresar las credenciales correctas.
- 10 Haga clic en **Next** (Siguiete) para iniciar el proceso de desinstalación.
- 11 Una vez que haya desinstalado la base de datos, reinicie el sistema cuando se le solicite.

Configurar agrupación en clústeres de bases de datos de alta disponibilidad para WDM

Los clústeres de alta disponibilidad (también conocidos como clústeres de HA o clústeres de conmutación por error) son grupos de computadoras que son compatibles con las aplicaciones de servidor que se pueden utilizar con confianza con un mínimo tiempo de inactividad. Funcionan mediante el aprovechamiento de computadoras redundantes en grupos o clústeres que proporcionan servicio continuo cuando fallan los componentes del sistema.

Si un servidor que está ejecutando una aplicación específica colapsa, sin tener clústeres, la aplicación no estará disponible hasta que el error se haya corregido. Los clústeres de alta disponibilidad solucionan esta situación, ya que detectan las fallas de hardware y software, e inmediatamente reinician la aplicación en otro sistema sin requerir intervención administrativa. Este proceso se conoce como **failover (conmutación por error)**.

Los clústeres de alta disponibilidad, por lo general, utilizan una conexión de red privada de latido para monitorear la condición y el estado de cada nodo del clúster.

El tamaño más habitual de un clúster de alta disponibilidad es de dos nodos.

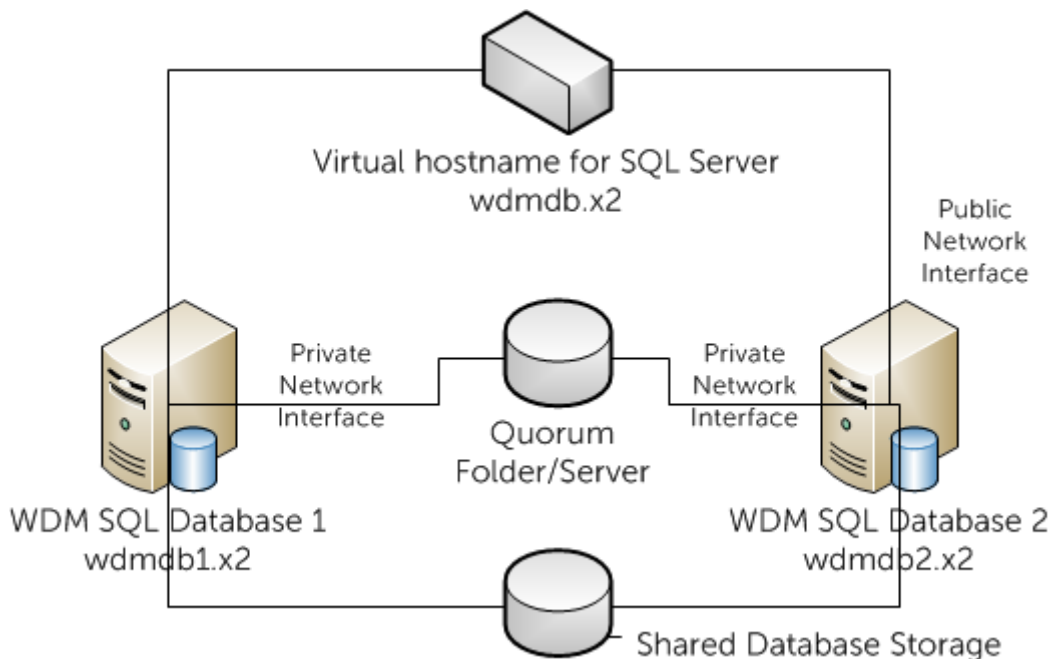


Figura 38. Agrupación en clústeres de base de datos de alta disponibilidad de WDM

En esta sección se proporcionan los pasos para configurar la agrupación en clústeres de base de datos de alta disponibilidad (HA) de Dell Wyse Device Manager (WDM) versión 5.0 y superiores.

Temas:

- [Componentes necesarios para agrupación en clústeres de bases de datos](#)

- Requisitos previos para la agrupación en clústeres de bases de datos
- Configurar las máquinas virtuales principal y secundaria
- Crear un clúster en el nodo principal
- Implementar un nodo y cuórum de mayoría de recursos compartidos
- Instalar .NET Framework en los nodos principal y secundario
- Instalar SQL Server en los nodos principal y secundario
- Procedimiento después de la agrupación en clústeres
- Ejecutar la utilidad de configuración de HA
- Agregar una licencia en WDM

Componentes necesarios para agrupación en clústeres de bases de datos

El ambiente de alta disponibilidad para WDM consta de los siguientes componentes:

- **Primary Server or Primary Node (Servidor principal o nodo principal):** esta es una de las cuatro máquinas virtuales (VM) en las que debe instalar la base de datos de Microsoft SQL Server 2012. Debería haber dos adaptadores de red, uno configurado para la red pública y otro configurado para la red privada.
- **Secondary Server or Secondary Node (Servidor secundario o nodo secundario):** esta es la segunda VM y garantiza una alta disponibilidad cuando el servidor principal falla. También debería haber dos adaptadores de red, uno configurado para la red pública y otro configurado para la red privada.
- **Server for the Quorum folder (Servidor para la carpeta de cuórum):** esta es la tercera de las cuatro máquinas virtuales y es necesaria para crear la carpeta de cuórum.
- **WDM Server (Servidor WDM):** esta es la cuarta máquina virtual en la que necesita instalar WDM.

Requisitos previos para la agrupación en clústeres de bases de datos

La agrupación en clústeres de la base de datos requiere lo siguiente:

- Cuatro máquinas virtuales VMware (VM) de las cuales dos deben contener dos adaptadores de red cada una.
- Versión compatible de la base de datos Microsoft SQL Server (versión independiente). Para obtener más información sobre las bases de datos compatibles, consulte [Información de soporte](#).

① | NOTA: Los pasos para la agrupación en clústeres de la base de datos analizados en esta guía se realizan en Microsoft SQL Server 2012. Sin embargo, la agrupación en clústeres es compatible con otras versiones de SQL Server.

Todas las VM deben estar conectadas a un dominio de Active Directory (AD).

- Las cuatro máquinas virtuales deben tener instalado Windows Server 2008 R2 Enterprise.

① | NOTA: No se puede utilizar SQL Server Express para la agrupación en clústeres de la base de datos.

Configurar las máquinas virtuales principal y secundaria

Después de crear las máquinas virtuales en el servidor, debe configurarlas para que sean compatibles con la agrupación en clústeres. Debe configurar tanto el nodo principal como el secundario siguiendo los pasos que se indican a continuación.

Acerca de esta tarea

Para configurar las máquinas virtuales principal y secundaria

Pasos

- 1 Inicie el cliente de vSphere en cualquier sistema de la red y seleccione la máquina virtual.
 - 2 Haga clic con el botón secundario y seleccione **Edit Settings** (Editar configuración). Haga clic en **Add** (Agregar) para agregar un adaptador de red adicional (también conocido como nodo).
 - 3 En la pantalla **Add Hardware** (Agregar hardware), seleccione **Ethernet Adapter** (Adaptador Ethernet) y haga clic en **Next** (Siguiente).
 - 4 Seleccione la subred en la lista desplegable **Network label** (Etiquetas de red) y haga clic en **Next** (Siguiente).
 - 5 Haga clic en **Finish** (Terminar).
 - 6 En la pantalla **VM Properties** (Propiedades de VM), compruebe que haya dos nodos.
 - 7 Inicie la pantalla de **Network Connections** (Conexiones de red) desde **Control Panel** (Panel de control) → **Network and Internet** (Redes e Internet) → **Network Connections** (Conexiones de red) y cambie el nombre de las conexiones de red a **Private** (Privada) y **Public** (Pública).
- NOTA:** Debe haber dos subredes para dos tarjetas de red, es decir, una subred para la red pública (PDB) y una subred para la red privada (PDB), y la misma para las dos tarjetas de red en el servidor SDB
- 8 Asegúrese de que la opción **Public Network** (Red pública) sea la primera en el orden de la ventana **Advanced Settings** (Configuración avanzada).
 - 9 Para iniciar la ventana **Advanced Settings** (Configuración avanzada), presione la tecla Alt para acceder al menú **Advanced** (Avanzado), en la pantalla **Network Connections** (Conexiones de red) y seleccione la opción **Advanced Settings** (Configuración avanzada).
 - 10 En la pantalla **Network Connections** (Conexiones de red), seleccione **Public** (Pública), haga clic con el botón derecho del mouse y seleccione **Properties** (Propiedades).
 - 11 En la ventana **Advanced Settings** (Configuración avanzada), seleccione **IPv4** y haga clic en **Properties** (Propiedades).
 - 12 Ingrese la **IP address** (Dirección IP), la **Subnet mask** (Máscara de subred), la **Default gateway** (Puerta de enlace predeterminada) y el **Preferred DNS server** (Servidor DNS preferido). Haga clic en OK (Aceptar).
 - 13 Repita los pasos 10 y 11 para la red privada.
 - 14 Asegúrese de que la red privada contenga solo la dirección IP y la máscara de subred. La puerta de enlace predeterminada o los servidores DNS no deben estar definidos.
 - 15 Asegúrese de que los servidores puedan comunicarse en esta red de forma que los nodos puedan comunicarse entre sí a través de dicha red.
 - 16 Inicie el "Server Manager" (Administrador del servidor) en **Start** (Iniciar) → **Administrative Tools** (Herramientas administrativas). Seleccione **Features** (Funciones).
 - 17 Haga clic en **Add Features** (Agregar funciones) para ver el asistente **Add Features** (Agregar funciones).
 - 18 Seleccione **Failover Clustering** (Clúster de conmutación por error) y haga clic en **Next** (Siguiente).
 - 19 Asegúrese de que la opción **Failover Clustering** (Clúster de conmutación por error) aparezca en la pantalla **Confirm Installation Selections** (Confirmar selecciones de instalación). Haga clic en **Install** (Instalar). Se muestra el progreso de la instalación.
 - 20 Una vez finalizada la instalación, compruebe los resultados de la instalación y haga clic en **Close** (Cerrar).

Siguiente paso

Después de completar la instalación del Failover Clustering (Clúster de conmutación por error), reinicie el servidor.

Validar una configuración

Acerca de esta tarea

Después de instalar el clúster de conmutación por error, debe validar la configuración en el nodo principal. Para validar la configuración:

Pasos

- 1 Inicie el "Server Manager" (Administrador del servidor) del nodo principal desde **Start** → **Administrative Tools** (Iniciar → Herramientas administrativas).
- 2 Seleccione **Failover Cluster Manager** (Administrador de clústeres de conmutación por error) en **Features** (Funciones).
- 3 Haga clic en **Validate a Configuration** (Validar una configuración) para iniciar el asistente.
- 4 Haga clic en **Next** (Siguiente) para agregar los nodos principal y secundario.
- 5 Ingrese el nombre de host del nodo principal.

- 6 Haga clic en **Add** (Agregar) para seleccionar los servidores. En la pantalla se muestra el siguiente mensaje al agregar los servidores: "The operation is taking longer than expected" (La operación está tardando más tiempo de lo normal). Tiene que esperar unos minutos para que los servidores se agreguen.
- 7 Una vez que los servidores estén seleccionados, se mostrarán en "Selected Servers" (Servidores seleccionados). Haga clic en **Next** (Siguiente).
- 8 No se necesita un clúster de múltiples sitios para aprobar la validación de almacenamiento. Para omitir el proceso de validación de almacenamiento, haga clic en Run only the tests I select (Ejecutar solo las pruebas que yo seleccione) y, a continuación, haga clic en **Next** (Siguiente).
- 9 En la pantalla **Test Selection** (Selección de prueba), deseleccione la opción **Storage** (Almacenamiento) y haga clic en **Next** (Siguiente) para continuar.
Se muestra la pantalla de confirmación.
- 10 Haga clic en **Next** (Siguiente) para comenzar a ejecutar las pruebas de validación en los nodos principal y secundario (en este caso, clúster1 y clúster2). El estado de las pruebas de validación se mostrará en la pantalla.
- 11 Revise el resumen de validación y haga clic en **Finish** (Terminar).

Crear un clúster en el nodo principal

Acerca de esta tarea

Después de instalar y validar la función **Failover Cluster Manager** (Administrador de clúster de conmutación por error) en el nodo principal, podrá crear un clúster.

Para crear un clúster en el nodo principal:

Pasos

- 1 Inicie el "Server Manager" (Administrador del servidor) en el nodo principal, seleccione **Failover Cluster Manager** (Administrador de clúster de conmutación por error) en **Features** (Funciones), y haga clic en **Create a Cluster** (Crear un clúster).
- 2 Haga clic en **Next** (Siguiente) del asistente.
- 3 Haga clic en **Next** (Siguiente) para continuar y, en la pantalla **Select Servers** (Seleccionar servidores), ingrese el nombre de host del nodo principal y haga clic en **Add** (Agregar) para agregar el servidor.
- 4 Escriba el nombre del nodo secundario y haga clic en **Add** (Agregar).
- 5 Una vez que haya agregado los servidores, haga clic en **Next** (Siguiente) para continuar. Se le pedirá que valide el clúster. Seleccione **No** puesto que su clúster está validado.
- 6 Seleccione la segunda opción en la pantalla y haga clic en **Next** (Siguiente) para continuar.
- 7 Proporcione un nombre para el clúster y un IP para administrarlo. El nombre que proporcione es para administrar el clúster. Este no debe ser el mismo que el nombre del recurso de clúster de SQL que creará más adelante. Ingrese **WINCLUSTER** como el nombre del clúster e ingrese la dirección IP. Haga clic en **Next** (Siguiente) para continuar.

NOTA: Este es también el nombre de la computadora a la que debe proporcionar permiso para el cuórum de mayoría de recursos compartidos, que se describe más adelante en este documento. Para obtener más información, consulte [Cómo implementar un nodo y un cuórum de mayoría de recursos compartidos](#).

- 8 Confirme y haga clic en **Next** (Siguiente).
El progreso de la formación de clúster se muestra en la pantalla. Si realizó todos los pasos correctamente, la formación de clúster se habrá realizado de manera correcta. Si aparece el símbolo de aviso amarillo en la pantalla, esto indica que la formación de clúster se realizó correctamente, pero con advertencias.
- 9 Haga clic en **View Report** (Ver informe) para ver los avisos durante la formación del clúster. Se muestra el informe con los mensajes de aviso resaltados en amarillo.
- 10 Ignore los mensajes de aviso y haga clic en **Finish** (Terminar) para completar el proceso de formación de clúster.

Implementar un nodo y cuórum de mayoría de recursos compartidos

El cuórum es un diseño para manejar la situación cuando hay un problema de comunicación entre conjuntos de nodos del clúster, de modo que dos servidores no intenten simultáneamente ser host de un grupo de recursos y escribir en el mismo disco al mismo tiempo. Con este concepto de quórum, el clúster obligará a detener el servicio de clúster en uno de los subconjuntos de nodos para asegurarse de que haya un solo propietario verdadero de un grupo de recursos en particular. La configuración del cuórum de nodo y de la mayoría de recursos

compartidos se suelen utilizar en los clústeres de múltiples sitios. Esta configuración se utiliza cuando hay un número par de nodos en el clúster, por lo que pueden utilizarse indistintamente con el nodo y el modo de cuórum de la mayoría del disco. En esta configuración, cada nodo obtiene 1 voto y, además, 1 recurso compartido remoto obtiene 1 voto.

Acerca de esta tarea

Para configurar un cuórum del nodo y la mayoría de recursos compartidos:

Pasos

- 1 Seleccione la máquina virtual identificada para la creación de la carpeta cuórum y cree una carpeta llamada **Quorum** (Cuórum), a continuación, comparta su ubicación.
- 2 Haga clic con el botón secundario en la carpeta **Quorum** (Cuórum) y seleccione **Share with** (Compartir con) → **Specific people** (Determinadas personas).
- 3 En la ventana **File Sharing** (Uso compartido de archivos), seleccione **Everyone** (Todos). Seleccione **Read/Write permission** (Permiso de lectura/escritura) y haga clic en **Share** (Recurso compartido).
La carpeta se comparte como `\\<Name of the VM>\Quorum` (\\<Nombre de la máquina virtual>\cuórum).
- 4 Ahora debe volver a cambiar su tipo de cuórum. Inicie el **Server Manager** (Administrador del servidor) en el nodo principal y seleccione **Failover Cluster Manager** (Administrador de clúster de conmutación por error) en **Features** (Funciones).
- 5 Haga clic con el botón secundario en el clúster y seleccione **More Actions** → **Configure Cluster Quorum Settings** (Más acciones → Configurar ajustes de cuórum del clúster).
- 6 Seleccione la opción **Node and File Share Majority (for clusters with special configurations)** (Nodo y mayoría de recursos compartidos [para clústeres con configuraciones especiales]) y haga clic en **Next** (Siguiente).
- 7 Ingrese la ruta de la carpeta compartida que creó en la tercera máquina virtual y haga clic en **Next** (Siguiente).
- 8 Confirme la ubicación de la carpeta compartida y haga clic en **Next** (Siguiente).
Los ajustes de cuórum del clúster se configuraron correctamente.
- 9 Haga clic en **Finish** (Terminar) para completar el proceso y ver la configuración de cuórum del clúster.

Instalar .NET Framework en los nodos principal y secundario

Acerca de esta tarea

Microsoft .NET Framework es un prerrequisito para instalar SQL Server independiente 2012 (o cualquier otra versión compatible de SQL Server) en los nodos principal y secundario.

Para instalar .NET Framework:

Pasos

- 1 Inicie el **Server Manager (Administrador del servidor)** en las VM que haya identificado para los nodos principal y secundario.
- 2 Haga clic en **Features** (Funciones) en **Server Manager (Administrador del servidor)** para iniciar el **Add Features Wizard** (Asistente para agregar funciones) y seleccione **.NET Framework 3.5.1 Features** (Funciones de .NET Framework 3.5.1).
- 3 Haga clic en **Next** (Siguiente) y se le pedirá que instale los servicios y funciones de rol para instalar las funciones de .NET Framework 3.5.1.
- 4 Haga clic en **Add Required Role Services** (Agregar servicios de rol requeridos). La opción .NET Extensibility (Extensibilidad de .NET) está seleccionada de manera predeterminada. Haga clic en **Next** (Siguiente) para continuar.
- 5 Confirme las selecciones de instalación y haga clic en **Install** (Instalar).
- 6 Después de completar la instalación de los componentes seleccionados, se mostrarán los resultados de la instalación.
- 7 Haga clic en **Close** (Cerrar) para completar la instalación de .NET Framework.

Instalar SQL Server en los nodos principal y secundario

La instalación de SQL Server en los dos nodos y su configuración para que funcione en un clúster es un paso importante en la configuración del clúster de base de datos de alta disponibilidad. En esta sección se proporcionan los pasos para instalar y configurar SQL Server 2012 de forma independiente en los dos nodos. Si desea instalar cualquiera de las versiones compatibles de SQL Server, consulte las instrucciones de instalación proporcionadas por Microsoft.

Para instalar una versión independiente de SQL Server 2012 en ambos nodos:

- 1 Inicie el medio de instalación de SQL Server 2012.
- 2 Haga clic en **Installation** (Instalación) y seleccione **New SQL Server stand-alone installation or add features to an existing installation** (Nueva instalación independiente de SQL Server o agregar funciones a una instalación existente).
- 3 Asegúrese de que las reglas de compatibilidad de la configuración no muestren errores. Haga clic en **Next** (Siguiente) para continuar.
- 4 Ingrese la clave del producto y haga clic en **Next** (Siguiente).
- 5 Compruebe la actualización del producto y haga clic en **Next** (Siguiente).
- 6 Acepte el contrato de licencia y haga clic en **Next** (Siguiente).
- 7 Seleccione la opción **SQL Server Feature Installation** (Instalación de funciones de SQL Server) y haga clic en **Next** (Siguiente).
- 8 En la pantalla **Feature Selection** (Selección de funciones), seleccione las funciones de **Database Engine Services** (Servicios de motor de base de datos) y todas las funciones bajo esta opción.
- 9 Seleccione las herramientas de administración: función Basic (Básica) y la función que se ubica debajo de esta. Haga clic en **Next (Siguiente)**.
- 10 Asegúrese de que en la pantalla **Installation Rules** (Reglas de instalación) no se muestren fallas. Haga clic en **Next** (Siguiente).
- 11 En la pantalla **Instance Configuration** (Configuración de instancia), asegúrese de que la opción **Default instance** (Instancia predeterminada) esté activada.
- 12 Haga clic en **Next** (Siguiente) para ver los requisitos de espacio en el disco.
- 13 Haga clic en **Next** (Siguiente) para ver la configuración del servidor.
- 14 Ingrese las credenciales de dominio para la configuración del servidor y haga clic en **Next** (Siguiente).
- 15 En la pantalla de configuración del motor de base de datos, seleccione **Mixed Mode** (Modo mixto) e ingrese la contraseña de administrador de SQL, y haga clic en **Add Current User** (Agregar usuario actual).
- 16 Haga clic en **Next** (Siguiente) en la ventana **Error Reporting** (Informes de error).
- 17 Haga clic en **Next** (Siguiente) y asegúrese de que las reglas de configuración de instalación no muestren errores.
- 18 Haga clic en **Install** (Instalar) para iniciar el proceso de instalación.
- 19 Una vez que finaliza la instalación, se muestra el estado de esta. Vea el estado y haga clic en **Close** (Cerrar) para completar la instalación.

ⓘ **NOTA:** Si se encuentra con un aviso de firewall de Windows cuando instala SQL Server, puede ignorarlo y continuar con la instalación. Si es necesario, puede agregar el puerto 1433 a la excepción de firewall de SQL Server.

Instalar un clúster de conmutación por error de SQL Server en el nodo principal

Después de haber finalizado la instalación de SQL Server 2012 en los nodos principal y secundario, deberá configurar ambos nodos para que sean compatibles con el clúster de conmutación por error.

Para instalar el clúster de conmutación por error de SQL Server 2012 en el nodo principal:

- 1 Inicie el medio de instalación de SQL Server 2012.
- 2 Haga clic en **Installation** (Instalación) y seleccione **New SQL Server failover cluster installation** (Nueva instalación de clúster de conmutación por error de SQL Server).
- 3 Asegúrese de que en la pantalla **Setup Support Rules** (Reglas de soporte de configuración) no se muestren errores. Haga clic en **OK** (Aceptar).
- 4 Ingrese la clave del producto y haga clic en **Next** (Siguiente).
- 5 Acepte los términos de licencia y haga clic en **Next** (Siguiente).
- 6 Compruebe las actualizaciones del producto y haga clic en **Next** (Siguiente).

- 7 Asegúrese de que en la pantalla **Setup Support Rules** (Reglas de soporte de configuración) no se muestren fallas o errores. Ignore los avisos y haga clic en **Next** (Siguiente).
- 8 Seleccione la opción **SQL Server Feature Installation** (Instalación de funciones de SQL Server) en la pantalla **Setup Role** (Configurar rol) y haga clic en **Next** (Siguiente).
- 9 Seleccione todas las opciones en **Instance Features → Database Engine Services** (Funciones de instancia → Servicios de motor de base de datos), y **Shared Features → Client Tools Connectivity** (Funciones compartidas → Conectividad de herramientas de cliente) en la pantalla **Feature Selection** (Selección de funciones). Haga clic en **Next** (Siguiente).
- 10 Asegúrese de que en la pantalla **Feature Rules** (Reglas de función) no se muestren fallas. Haga clic en **Next** (Siguiente).
- 11 En la pantalla **Instance Configuration** (Configuración de instancia), ingrese los siguientes detalles:
 - **SQL Server Network Name (Nombre de red de SQL Server):** WDMCLUSTER
 - **Named Instance (Instancia con nombre):** WDMCLUST
 - **Instance ID (ID de instancia):** WDMCLUSTHaga clic en **Next** (Siguiente).
- 12 Compruebe los **Disk Space Requirements (Requisitos de espacio en el disco)** y haga clic en **Next** (Siguiente).
- 13 Deje la configuración predeterminada en la pantalla **Cluster Resource Group** (Grupo de recursos del clúster) y haga clic en **Next** (Siguiente).
- 14 Dado que configuró una agrupación en clústeres de **File Share Majority (Mayoría de recursos compartidos)**, no es necesario que seleccione un disco. Haga clic en **Next** (Siguiente) en la pantalla **Cluster Disk Selection** (Selección de disco para clúster).
- 15 En la pantalla **Cluster Network Configuration** (Configuración de red del clúster), habilite **IP4** y proporcione la dirección IP para el clúster de conmutación por error de SQL, a continuación, haga clic en **Next** (Siguiente) para continuar a la pantalla **Server Configuration** (Configuración del servidor).
- 16 Ingrese las credenciales de dominio del Agente de SQL Server y el motor de la base de datos de SQL Server, a continuación, haga clic en **Next** (Siguiente).
- 17 En la pantalla **Database Engine Configuration** (Configuración del motor de la base de datos), seleccione la opción **Mixed Mode** (Modo mixto) (autenticación de SQL Server y autenticación de Windows) e ingrese la contraseña de administrador de SQL.
- 18 Haga clic en **Add Current User** (Agregar usuario actual) para agregar el usuario administrador y haga clic en **Next** (Siguiente).
- 19 Se le pedirá que instale un clúster de conmutación por error de SQL. Haga clic en **Yes** (Sí) cuando esto ocurra.
- 20 Haga clic en la pestaña **Data Directories** (Directorios de datos) en la pantalla **Database Engine Configuration** (Configuración del motor de la base de datos). En la ubicación del directorio raíz de los datos, ingrese `\\<Name of the Quorum VM>\quorum` (\<Nombre de la máquina virtual de cóorum>\quorum). Haga clic en **Next** (Siguiente).
- 21 Verifique la pantalla **Error Reporting** (Informes de errores) y haga clic en **Next** (Siguiente). Puede ignorar los avisos.
- 22 Asegúrese de que no haya fallas en la pantalla **Cluster Installation Rules** (Reglas de instalación del clúster). Haga clic en **Next** (Siguiente).
- 23 Haga clic en **Install** (Instalar) para comenzar la instalación.
- 24 En la pantalla **Installation Progress** (Progreso de la instalación) puede ver el progreso de la instalación. Haga clic en **Next** (Siguiente) cuando la operación haya finalizado.
- 25 Haga clic en **Close** (Cerrar) para completar la instalación. Debe mostrarse **Failover Cluster Manager** (Administrador de clústeres de conmutación por error) en el **Server Manager (Administrador del servidor)** bajo **Features** (Funciones).

Procedimiento después de la agrupación en clústeres

Acerca de esta tarea

En esta sección, se analizan los diversos pasos que debe realizar una vez que haya completado la configuración del clúster. Estas medidas permiten que el clúster funcione sin problemas.

Siga los pasos que se indican a continuación:

Pasos

- 1 En los dos nodos del clúster, asegúrese de que los servicios de servidor de SQL se inicien con las credenciales de dominio.
- 2 Inicie **SQL Server Configuration Manager** (Administrador de configuración de SQL Server) y seleccione **SQL Server Services → SQL Server** (Servicios de SQL Server → SQL Server). Haga clic con el botón secundario y seleccione **Properties** (Propiedades).
- 3 Compruebe las credenciales de dominio y haga clic en **OK** (Aceptar).
- 4 Haga clic en la pestaña **AlwaysOn High Availability** (Alta disponibilidad AlwaysOn) en ambos nodos y seleccione **Enable AlwaysOn Availability Groups** (Activar grupos de disponibilidad AlwaysOn). Haga clic en **OK** (Aceptar).
- 5 Instale la base de datos de WDM en las VM que haya identificado como los nodos principal y secundario del clúster.
- 6 Ejecute el siguiente script en la base de datos:

```
Use RapportDB
GO
Update Install set ServerName='NEWCLUSTER01' where Module='Rapport4DB'
```
- 7 Cuando instale los componentes de WDM sin la base de datos, asegúrese de proporcionar el nombre del clúster de la base de datos de SQL en el campo Server IP Address (Dirección IP del servidor).
- 8 Cree la misma estructura de directorios apuntando a la ubicación de la base de datos, tanto en el nodo principal como el secundario. Por ejemplo, si la base de datos está presente en **C:\Program Files\WYSE\WDM\Database**, en el nodo principal, cree la misma estructura también en el servidor secundario.
- 9 Inicie SQL Server Management Studio en el nodo principal. Inicie sesión con el nombre de usuario y la contraseña predeterminados de SQL.
- 10 Haga clic con el botón secundario en la base de datos **RapportDB** y seleccione **Properties** (Propiedades).
- 11 En la pantalla **Database Properties** (Propiedades de la base de datos), cambie el **Recovery Model** (Modelo de recuperación) a **Full** (Completo).
- 12 Haga clic con el botón secundario en RapportDB y seleccione **Tasks → Backup** (Tareas → Respaldo) para realizar una copia de seguridad de RapportDB.
- 13 Deje los valores predeterminados en la pantalla **Backup Database** (Base de datos de respaldo) y haga clic en **OK** (Aceptar).
- 14 Haga clic con el botón secundario en **AlwaysOn High Availability** (Alta disponibilidad AlwaysOn) en el explorador de objetos y seleccione **New Availability Group Wizard** (Asistente de nuevo grupo de disponibilidad).
- 15 Haga clic en **Next** (Siguiente) en la pantalla **New Availability Group Wizard** (Asistente de nuevo grupo de disponibilidad).
- 16 Proporcione un nombre para el grupo de disponibilidad como, por ejemplo, **Rapport_cluster** y haga clic en **Next** (Siguiente).
- 17 Seleccione la base de datos y haga clic en **Next** (Siguiente).
- 18 Haga clic en **Add Replica** (Agregar réplica) y seleccione las casillas de verificación **Automatic Failover (up to 2)** (Conmutación por error automática [hasta 2]) y **Synchronous commit (up to 3)** (Confirmación sincrónica [hasta 3]).
Repita el procedimiento en el nodo secundario.
- 19 Haga clic en **Next (Siguiente)**.
- 20 Seleccione la opción **Full** (Completo) y especifique la ubicación de la carpeta compartida como **\\<Name of the Quorum Machine>\quorum** (\\<Nombre de la máquina de cuórum>\quorum). Haga clic en **Next** (Siguiente).
- 21 Asegúrese de que en la pantalla de **Validation** (Validación) no se muestren fallas. Haga clic en **Next** (Siguiente).
- 22 Si ve algún aviso en la pantalla, puede ignorarlo y continuar con la instalación.
- 23 Haga clic en **Finish** (Terminar) para completar la instalación del **New Availability Group (Nuevo grupo de disponibilidad)**.
- 24 En la ventana de progreso se muestra el progreso de la instalación. Haga clic en **Next** (Siguiente) cuando se complete la instalación.
- 25 Vea los resultados y haga clic en **Close** (Cerrar).
- 26 Se muestran los nodos principal y secundario en SQL Server Management Studio.
- 27 Apague el nodo secundario y realice una comprobación para asegurarse de que el nodo principal se esté ejecutando en el clúster.
- 28 Inicie SQL Server Management Studio en el nodo principal. Inicie sesión con el nombre de usuario y la contraseña predeterminados de SQL.
- 29 Haga clic en el nodo **Security** (Seguridad), seleccione **Login** (Inicio de sesión), haga clic con el botón secundario y seleccione **New Login** (Nuevo inicio de sesión) para crear el usuario de Rapport. Este paso es importante para que WDM funcione mientras está creando el usuario de autenticación de SQL Server.
- 30 Seleccione **Server Roles** (Roles del servidor), marque la casilla de verificación **admins** y haga clic en **OK** (Aceptar).
- 31 Vea el usuario de **Rapport** en **SQL Server Management Studio**.
- 32 Repita los pasos 28 al 31 en el nodo secundario.

Siguiente paso

① **NOTA:** Si hay una conmutación por error desde la base de datos principal a la secundaria, debe reiniciar la interfaz de usuario de WDM.

Ejecutar la utilidad de configuración de HA

Acerca de esta tarea

WDM necesita conectarse al clúster para funcionar dentro de este; además, debe asegurarse de que no haya tiempo de inactividad.

La Utilidad de configuración de alta disponibilidad estará disponible después de instalar WDM en un nodo independiente, que no sean el nodo principal ni el secundario.

Pasos

- 1 Inicie sesión en el sistema donde haya instalado WDM.
- 2 Inicie la **HAConfigureUtility (Utilidad de configuración de alta disponibilidad)** desde **Start (Iniciar) > All Programs (Todos los programas) > Dell Wyse Device Manager > Utilities (Utilidades)**.
- 3 Especifique los siguientes detalles.
 - **Configure Setup As (Ajustar configuración como):** seleccione **Cluster (Clúster)** en la lista desplegable.
 - **Database Name (Nombre de la base de datos):** esta se muestra de manera predeterminada y no puede ser editada.
 - **Database Server (Servidor de base de datos):** especifique el nombre del host del clúster de la base de datos. Por ejemplo, **WDMCLUSTER**.
 - **Database User Name (Nombre de usuario de la base de datos):** especifique **rapport** como el usuario de la base de datos.
 - **Database Password (Contraseña de la base de datos):** especifique la contraseña del usuario rapport.
- 4 Haga clic en **Configure (Configurar)**.
Los detalles de conexión se muestran en el panel inferior de la utilidad.

Agregar una licencia en WDM

Acerca de esta tarea

WDM necesita una licencia para funcionar. El código de licencia se genera en función de la base de datos. WDM normalmente se instala una base de datos independiente y, a continuación, se transfiere a un clúster. Por lo tanto, cuando haya completado la configuración del clúster, nuevamente deberá generar el código de licencia para este.

Para agregar una licencia en WDM para el servidor WDM:

Pasos

- 1 Inicie Wyse Device Manager (WDM). Se muestra el siguiente mensaje de error: *"Application Function: Scopeltems_Expand: 13 Type mismatch"* (Función de la aplicación: Scopeltems_Expand: discrepancia de tipo 13).
- 2 Haga clic en **OK (Aceptar)** y agregue la licencia de la consola de WDM.
- 3 Para iniciar la conmutación por error, apague la base de datos en el nodo principal y reinicie la consola de WDM.

Configurar el equilibrio de carga

Cuando se utiliza WDM para administrar dispositivos de thin client en un gran ambiente empresarial, es posible que un único servidor de administración de WDM no tenga la capacidad de administrar un gran número de dispositivos. Podría haber problemas o retrasos en los registros de clientes, la ejecución de programaciones o la ejecución de comandos en tiempo real.

El equilibrio de carga ayuda a solucionar estos problemas en gran medida. En esta configuración, puede instalar y ejecutar varias instancias de servidores de administración de WDM en diferentes sistemas y configurar la función de equilibrio de carga entre ellas. WDM utiliza la solicitud de enrutamiento de aplicaciones (ARR) de Microsoft para que la función IIS 7 realice un equilibrio de carga entre los servidores de administración. En esta sección se describe cómo instalar y configurar el equilibrio de carga.

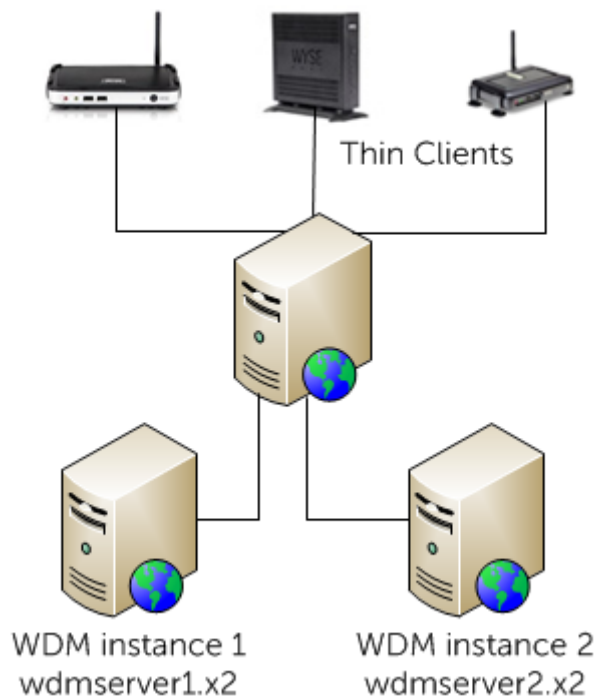


Figura 39. Configuración del equilibrio de carga de WDM

Temas:

- [Configurar el servidor proxy de ARR](#)
- [Instalar los componentes de WDM](#)
- [Configurar el equilibrio de carga de los dispositivos ThreadX 4.x](#)
- [Configurar el equilibrio de carga de los dispositivos ThreadX 5.x](#)

Configurar el servidor proxy de ARR

El servidor proxy de la solicitud de enrutamiento de aplicaciones (ARR) es el componente más importante del equilibrio de carga. Este servidor recibe las solicitudes de los sistemas de thin client y las enruta a los diferentes servidores de administración de WDM.

Prerrequisitos

Antes de configurar el servidor proxy de ARR, asegúrese de lo siguiente:

- La configuración completa debe estar en Windows 2008 Server R2 o superior.
- Instale todos los componentes de WDM en un servidor.
- Instale solo el servidor de administración de WDM y el servicio ThreadX 4.x en otro servidor.

ⓘ **NOTA:** Puede configurar el servidor proxy de ARR y los servidores de administración de WDM en distintas subredes del mismo dominio.

Acerca de esta tarea

La configuración del servidor proxy de ARR consta de los siguientes pasos:

Pasos

- 1 [Instalar IIS.](#)
- 2 [Instalar el módulo ARR.](#)
- 3 [Configurar el proceso de grupo de aplicaciones para ARR.](#)
- 4 [Crear una granja de servidores de administración de WDM.](#)
- 5 [Configurar SSL](#)
- 6 [Configurar las propiedades de la granja de servidores para ARR.](#)
- 7 [Configurar el filtrado de solicitudes](#)
- 8 [Configurar el FQDN del proxy en Preferencias de WDM.](#)

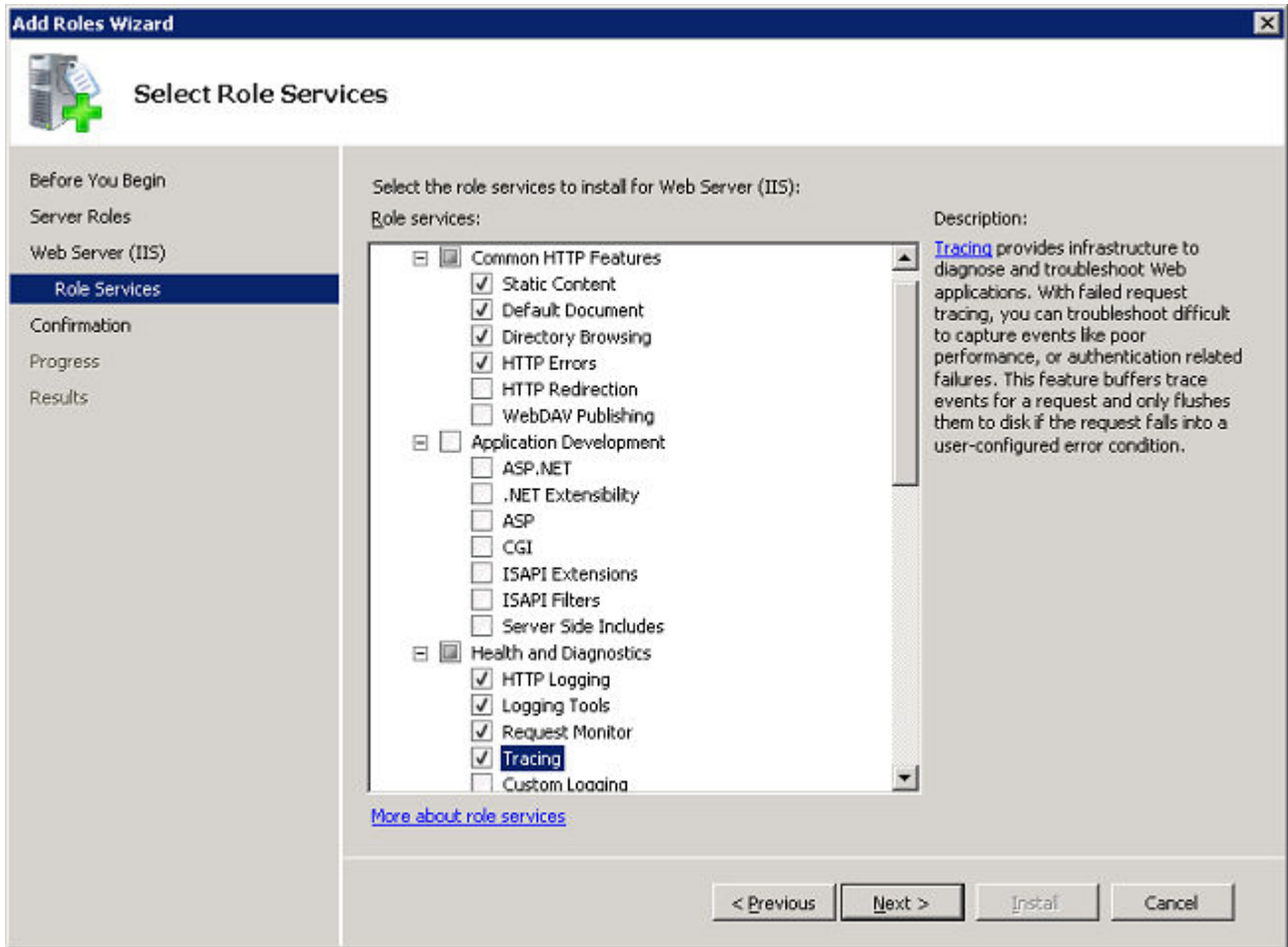
Instalar los servicios de información de Internet (IIS)

Acerca de esta tarea

Instale Windows 2008 Server R2 en cualquiera de los sistemas que haya identificado para ser el servidor proxy de ARR.

Pasos

- 1 Inicie la sesión como administrador y ejecute el **Server Manager** (Administrador del servidor).
- 2 Seleccione **Roles** (Roles) en el Administrador del servidor y haga clic en **Add Roles** (Agregar roles) en el panel de la derecha. Se muestra el **Add Roles Wizard** (Asistente para agregar roles).
- 3 Seleccione **Server Roles** (Roles del servidor), seleccione **Web Server (IIS)** (Servidor web [IIS]) y haga clic en **Next** (Siguiente).



4 Seleccione las siguientes opciones:

Opción	Subopciones
Common HTTP Features (Características HTTP comunes)	<ul style="list-style-type: none"> Static Content (Contenido estático) Default Document (Documento predeterminado) HTTP Errors (Errores HTTP) Directory Browsing (Exploración de directorios)
Health and Diagnostics (Condición y diagnóstico)	<ul style="list-style-type: none"> HTTP Logging (Registro HTTP) Request Monitor (Monitor de solicitudes) Logging Tools (Herramientas de inicio de sesión) Tracing (Seguimiento)
Management Tools (Herramientas de administración)	Seleccione todas las subopciones.

5 Haga clic en **Next** (Siguiete) para ver el resumen.

6 Haga clic en **Install** (Instalar) para instalar IIS.

Instalar el módulo ARR

Debe instalar la versión 3.0 de la solicitud de enrutamiento de aplicaciones en el sistema que haya identificado para ser el servidor proxy de ARR. El instalador está disponible en el sitio de descargas de Microsoft <https://www.microsoft.com/en-us/download/details.aspx?id=47333>. Descargue el archivo **ARRv3_0.exe** e instálelo.

Configurar el proceso de grupo de aplicaciones para ARR

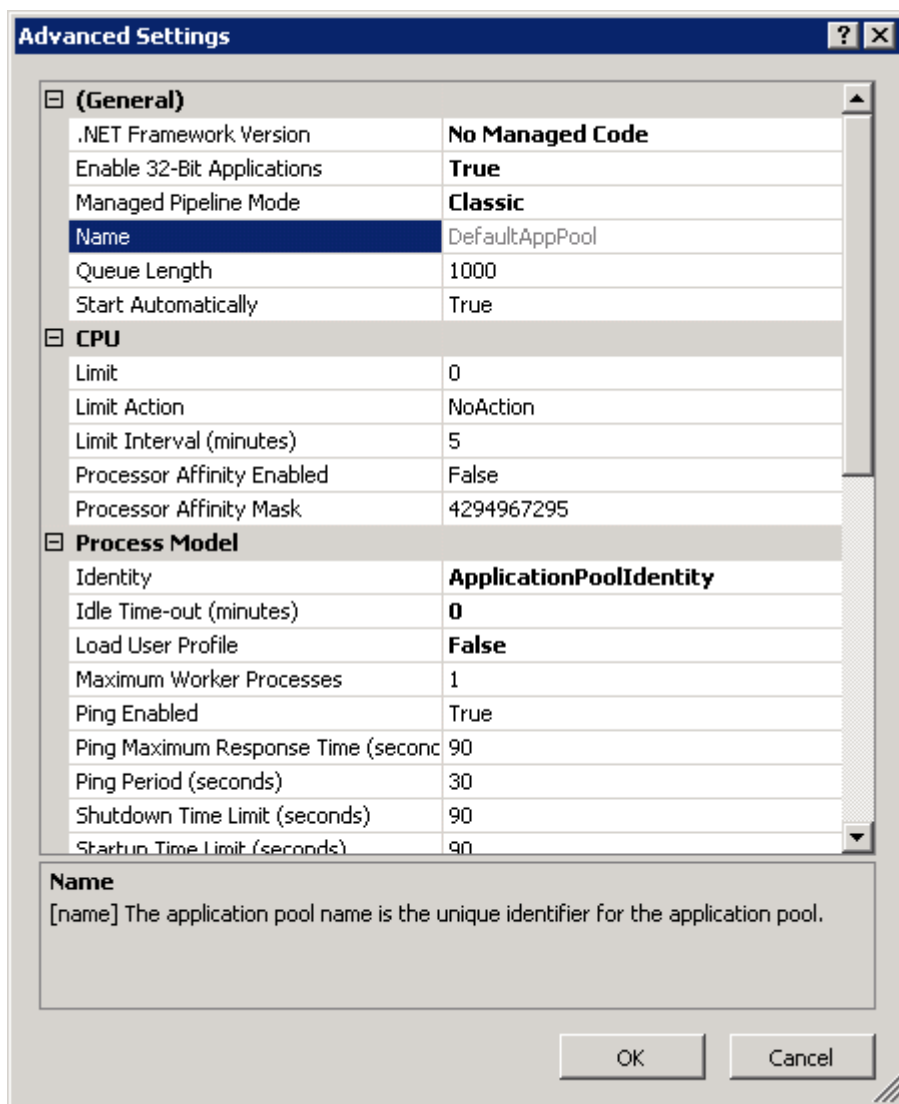
Todas las solicitudes y respuestas HTTP para los sitios de contenido pasan por la solicitud de enrutamiento de aplicaciones. Para que esto funcione correctamente, debe asegurarse de que el proceso de trabajo del sitio web predeterminado en ARR siempre esté en ejecución.

Acerca de esta tarea

Para configurar el proceso del grupo de aplicaciones:

Pasos

- 1 Inicie sesión en el servidor proxy de ARR e inicie el Administrador de IIS.
- 2 Seleccione **Application Pools** (Grupos de aplicaciones) en el nodo raíz.
En el panel de la derecha se muestra **DefaultAppPool** como el grupo de aplicaciones para el sitio web predeterminado.
- 3 Seleccione **DefaultAppPool** y, a continuación, haga clic en **Edit Application Pool** (Editar grupo de aplicaciones) en el panel de **Action (Acciones)**.
- 4 Seleccione **Advanced Settings** (Configuración avanzada) para ver la ventana **Advanced Settings** (Configuración avanzada).



- 5 En **Process Model** (Modelo de proceso), cambie el valor de **Identity** (Identidad) de **LocalSystem** a **ApplicationPoolIdentity**.
- 6 Cambie **Idle Time-out (minutes)** (Tiempo de espera en inactividad [minutos]) a 0 para desactivar la configuración. Haga clic en **OK (Aceptar)** para guardar los cambios.

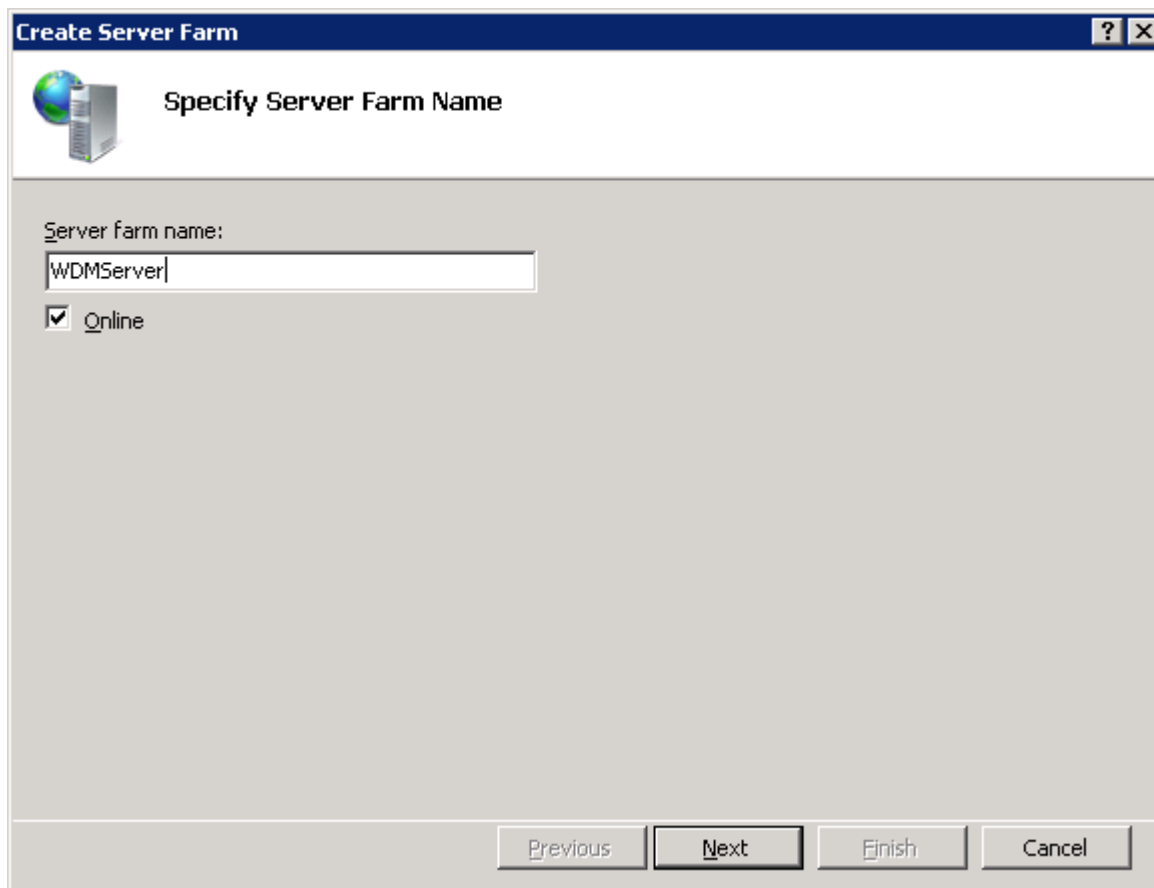
Crear una granja de servidores de administración de WDM

Acerca de esta tarea

Para crear y definir una granja de servidores:

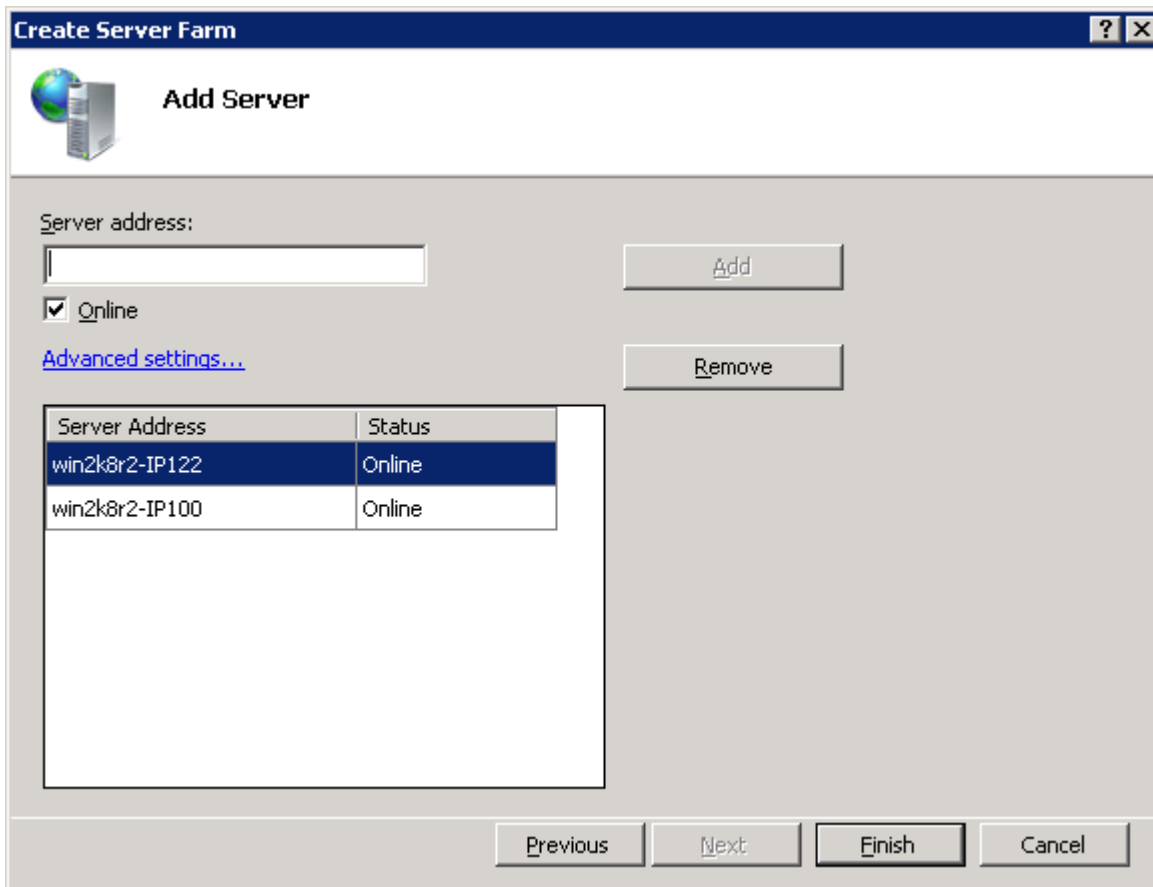
Pasos

- 1 Inicie sesión en el sistema del servidor proxy de ARR e inicie el Administrador de IIS.
- 2 Seleccione **Server Farms** (Granjas de servidores) en el nodo raíz. Esta opción solo está disponible después de instalar el módulo proxy de ARR.
- 3 Haga clic con el botón secundario y seleccione **Create Server Farm** (Crear granja de servidores) en el menú.
Se muestra la pantalla **Create Server Farm** (Crear granja de servidores).



The screenshot shows a Windows-style dialog box titled "Create Server Farm". The main heading inside is "Specify Server Farm Name". There is a small icon of a server tower on the left. Below the heading, there is a text input field labeled "Server farm name:" containing the text "WDMServer". Underneath the text field is a checkbox labeled "Online" which is checked. At the bottom of the dialog, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

- 4 Ingrese un nombre para la granja de servidores. Por ejemplo, **WDMServerFarm**. Haga clic en **Next** (Siguiente) para agregar los servidores de administración de WDM.



- 5 Escriba el nombre de host del servidor WDM y haga clic en **Add** (Agregar). Puede agregar todos los servidores donde instaló el servidor de administración de WDM.
- 6 Haga clic en **Finish** (Terminar) para agregar todos los servidores a la granja.
Una vez que haya agregado los servidores y creado la granja de servidores, se le mostrará un mensaje para que reescriba las reglas de enrutamiento, de modo que todas las solicitudes se dirijan automáticamente a la granja de servidores.
- 7 Haga clic en **Yes** (Sí) para que el Administrador de IIS cree una URL para reescribir reglas, a fin de enrutar todas las solicitudes entrantes a esta granja de servidores.

Configurar SSL

Una de las funciones en ARR es la **SSL off-loading** (Descarga de SSL). Se trata de una función en la que las comunicaciones entre los clientes y el servidor proxy de ARR se realizan a través de SSL, y las comunicaciones entre el servidor proxy de ARR y los servidores de administración de WDM se realizan a través de texto no cifrado. Si se habilita esta función, puede ayudar a aumentar los recursos de los servidores de administración de WDM.

Prerequisito

Primero debe crear el Certificado SSL en el servidor proxy de ARR.

Acerca de esta tarea

Para crear y configurar el Certificado SSL:

Pasos

- 1 Inicie sesión en el servidor proxy de ARR e inicie el Administrador de IIS.
- 2 Seleccione el nodo raíz y abra la página **Server Certificates** (Certificados del servidor) en el panel de la derecha.
- 3 Haga clic en **Create Domain Certificate** (Crear certificado de dominio) en el panel de acciones.
- 4 Proporcione el nombre del servidor proxy de ARR en el asistente **Create Certificate** (Crear certificado).
- 5 Haga clic en **Next** (Siguiente) para completar la creación del certificado.
- 6 Seleccione **Default Web Site** (Sitio web predeterminado) en **Sites** (Sitios), y haga clic en **Bindings** (Vinculaciones) en el panel de acciones.

- 7 Asigne el certificado a la vinculación **HTTPS**.
- 8 Vaya a **Server Farm** (Granja de servidores) y haga doble clic en **Created Farm** (Granja creada).
- 9 Haga doble clic en **Routing Rules** (reglas de enrutamiento) y seleccione la opción **Enable SSL offloading** (Activar descarga de SSL) si desea que la comunicación entre los servidores proxy de ARR y los servidores de administración de WDM se realice en texto sin formato. También es necesario que agregue los puertos HTTP y HTTPS a las vinculaciones del sitio web predeterminado en los sistemas particulares de servidores de administración de WDM.

NOTA:

Si desea que la comunicación entre el servidor proxy de ARR y los servidores de administración de WDM también esté en el protocolo HTTPS, debe deshabilitar la función **SSL off-loading** (Descarga de SSL) y configurar SSL en cada servidor de administración de WDM por separado. Si utiliza un certificado autofirmado para configurar SSL en el servidor de administración de WDM, importe este certificado a **Trusted Root Certificate Authorities store** (Almacenamiento de autoridades de certificado raíz confiable) en una computadora local en el servidor proxy de ARR, siguiendo los pasos disponibles en el sitio web de Microsoft: http://technet.microsoft.com/en-us/library/cc754841.aspx#BKMK_addlocal

Configurar las propiedades de la granja de servidores para ARR

Después de crear y definir la granja de servidores, deberá establecer propiedades adicionales para administrar el comportamiento de ARR.

- 1 Inicie sesión en el servidor proxy de ARR e inicie el Administrador del servidor IIS.
- 2 Seleccione la granja de servidores que creó. Se muestran las siguientes opciones en el panel de la derecha:
 - Caching (Almacenamiento en caché)
 - Health Test (Prueba de condición)
 - Load Balance (Compensación de carga)
 - Monitoring and Management (Monitoreo y administración)
 - Proxy
 - Routing Rules (Reglas de enrutamiento)
 - Server Affinity (Afinidad del servidor)
- 3 Seleccione **Caching** (Almacenamiento en caché).
 - a Deseleccione la opción **Enable disk cache** (Activar caché en disco) para deshabilitar el almacenamiento en caché.
 - b Establezca **Memory cache duration** (Duración de la memoria caché) en 0.
- 4 Seleccione **Health Test** (Prueba de condición).
 - a Ingrese el nombre de dominio completo (FQDN) del servidor proxy de ARR en el campo **URL**. El valor debe ser: **http(s)/<FQDNProxy>/hserver.dll? &V93**. Esta es la dirección URL que utiliza ARR para enviar solicitudes al servidor de administración de WDM a fin de comprobar la condición de una determinada granja de servidores.
 - b Establezca el período de intervalo después del cual la Prueba de condición de ARR repetirá este control. El valor predeterminado es 30 segundos. Puede establecerlo en 180 segundos.
 - c Establezca el período de espera de la URL especificada. Este es el período durante el que, si el servidor no responde, se marcará como **Unhealthy** (En mal estado).
 - d Establezca **Acceptable Status codes** (Códigos de estado aceptables) en **200-399**. Si la URL de la condición devuelve un código de estado que no coincide con el valor de **Acceptable Status codes** (Códigos de estado aceptables), ARR marcará a este servidor como en mal estado.
 - e Establezca el valor de texto **Server Healthy** (Servidor en buen estado) en el campo **Response Match** (Coincidencia de respuesta). El texto de **Response Match** (Coincidencia de respuesta) se verifica contra la entidad de respuesta de cada servidor y, si la respuesta de un servidor no contiene la cadena especificada en la coincidencia de respuesta, se marca el servidor como en mal estado.
 - f Haga clic en **Verify URL** (Verificar URL). Tiene que aprobarse para todos los servidores de administración de WDM de la granja de servidores.
- 5 Cambie el algoritmo **Load Balance** (Equilibrio de carga).
 - a Seleccione **Weighted Round Robin** (Round-robin medido) en la lista desplegable **Load balance algorithm** (Algoritmo de equilibrio de carga).
 - b Seleccione **Even distribution** (Distribución igualitaria) en la lista desplegable **Load distribution** (Distribución de carga).
 - c Haga clic en **Apply** (Aplicar).
- 6 Haga doble clic en la opción **Monitoring and Management** (Monitoreo y administración) para ver el estado de la condición del servidor de administración de WDM y otras estadísticas.

- 7 Haga doble clic en **Proxy** para configurar el proxy:
 - a Cambie el valor de **Response buffer threshold** (Umbral de búfer de respuesta) a 0.
 - b Deseleccione la opción **Keep Alive** (Mantener activo).
 - c Cambie la versión **HTTP** a **HTTP/1.1**.
 - d Seleccione la opción **Reverse rewrite host in response headers** (Revertir reescritura de host en encabezados de respuesta).
- 8 Haga doble clic en **Routing Rules** (Reglas de enrutamiento).
 - a Haga clic en **URL Rewrite** (Reescribir URL) en el panel de **Actions (Acciones)**.
 - b En la página **Edit Inbound Rule** (Editar regla de entrada), establezca **Pattern** (Patrón) en ***hserver.dll***.

Este paso garantiza que el servidor proxy de ARR enviará solo las solicitudes de URL que se dirijan del servidor de administración de WDM a la granja de servidores.

Ya están configuradas las propiedades de la granja de servidores.

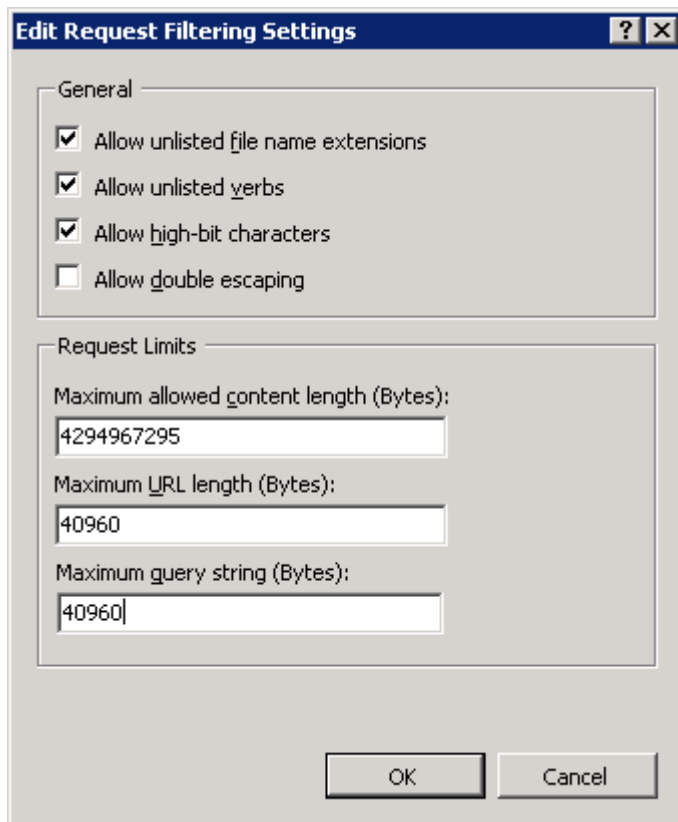
Configurar el filtrado de solicitudes

Acerca de esta tarea

Para configurar el filtrado de solicitudes:

Pasos

- 1 Inicie sesión en el servidor proxy de ARR e inicie el Administrador de IIS.
- 2 Seleccione **Default Web Site** (Sitio web predeterminado) en **Sites** (Sitios) y, en el panel de la derecha, haga doble clic en **Request Filtering** (Filtrado de solicitudes).
- 3 Haga clic en **Edit Feature Settings** (Editar configuración de función).
- 4 Establezca los **Request Limits (Límites de solicitud)** como se muestra a continuación:



- 5 Haga clic en **OK** (Aceptar) para aplicar la configuración.

Configurar el FQDN del proxy en Preferencias de WDM

Para completar la configuración del equilibrio de carga, deberá especificar los detalles del servidor proxy en WDM.

Acerca de esta tarea

Para configurar el FQDN del proxy en WDM:

Pasos

- 1 Inicie sesión en el sistema donde haya instalado WDM e inicie la consola WebUI de WDM.
- 2 Seleccione **System (Sistema) > Console (Consola)**.
- 3 En el nombre de alias del administrador del servidor, ingrese el FQDN del servidor proxy de ARR.
- 4 Haga clic en **Save** (Guardar) para guardar la configuración.

El servidor proxy de ARR ahora está registrado en la base de datos de WDM y con ello se completa la configuración del equilibrio de carga.

Instalar los componentes de WDM

La configuración del equilibrio de carga necesita varias instalaciones de servidores de administración de WDM. Sin embargo, debe asegurarse de que uno de los sistemas en esta configuración tenga la instalación completa de WDM. En este caso, puede instalar solo el servidor de administración y el servicio ThreadX en los otros sistemas. Para obtener más información sobre cómo instalar solo los componentes seleccionados, consulte [Instalar el servidor de administración](#)

Configurar el equilibrio de carga de los dispositivos ThreadX 4.x

Cuando desee administrar un gran número de dispositivos PCoIP (ThreadX), es posible que solo un servicio de administrador de ThreadX no tenga la capacidad de administrarlos todos. Si configura el equilibrio de carga de los dispositivos ThreadX, podrá administrar una gran cantidad de esos dispositivos.

Prerrequisitos

Antes de configurar el equilibrio de carga de los dispositivos ThreadX, primero debe identificar un sistema Windows 2008 R2 e instalar el servidor de nombre de dominio (DNS) en el sistema.

Para obtener más información sobre cómo instalar el DNS en un servidor de Windows 2008, vaya a <http://technet.microsoft.com/en-us/library/cc725925.aspx>.

El mecanismo del equilibrio de carga utiliza el método "Round-robin" del DNS para compartir y distribuir las cargas de recursos en la red.

Acerca de esta tarea

Para configurar el Round-robin del DNS:

Pasos

- 1 Inicie sesión en el servidor DNS e inicie el Administrador de DNS.
- 2 Seleccione el nombre del servidor en el árbol del panel izquierdo, haga clic con el botón secundario y seleccione **Properties** (Propiedades) en el menú.
Aparece la ventana **Properties** (Propiedades).
- 3 Haga clic en la pestaña **Advanced** (Avanzado) de la ventana **Properties** (Propiedades).
- 4 En el panel **Server Options** (Opciones del servidor), asegúrese de que las opciones **Enable round robin** (Activar Round-robin) y **Secure cache against pollution** (Proteger caché contra la contaminación) estén seleccionadas.
- 5 Si necesita ordenar las máscaras de red, seleccione la opción **Enable netmask ordering** (Activar orden de máscaras de red). Esta función intenta dar prioridad a los recursos locales para los clientes.
- 6 Haga clic en el menú **View** (Ver), en el Administrador de DNS, y seleccione la opción **Advanced** (Avanzado).
- 7 Expanda el nodo de **Domain (Dominio)** y, en **Forward Lookup Zones** (Reenviar zonas de búsqueda), seleccione el dominio. Por ejemplo, **WDMSQA11.com**.
- 8 Haga clic con el botón secundario y seleccione **New Host (A or AAAA)... (Nuevo host [A o AAAA]...**
Se abre la ventana **New Host** (Nuevo host).

- 9 Ingrese el nombre del host virtual de la granja de servidores de ThreadX que participará en el equilibrio de carga. Por ejemplo, ThreadXServidor1.
El FQDN del servidor aparecerá automáticamente.
- 10 Ingrese la dirección IP del servidor.
- 11 Haga clic en **Add Host** (Agregar hosts).
- 12 Repita los pasos **8 al 11** para agregar tantos servidores ThreadX como desee.
- 13 Seleccione el nodo de **Domain (Dominio)** en el **DNS Manager (Administrador de DNS)**; haga clic con el botón secundario y seleccione **Other New Records** (Otros registros nuevos).
- 14 En el cuadro de diálogo **Resource Record Type** (Tipo de registro de recurso), seleccione **SRV Location** (Ubicación SRV) y haga clic en **Create Record** (Crear registro).
- 15 En el cuadro de diálogo New Resource Record (Nuevo registro de recurso), ingrese los siguientes valores:
 - **Service Name** (Nombre del servicio): _PCOIP-broker
 - **Protocol** (Protocolo): _tcp
 - **Port Number** (Número de puerto): 50000.
 - **Host Offering this Service** (Host que ofrece este servicio): ingrese el nombre de host de la granja de servidores ThreadX.
- 16 Repita los pasos **13 al 15** para agregar el registro SRV **_PCOIP-tool**.
- 17 Configure el almacenamiento en caché del DNS:
 - a En el Administrador de DNS, expanda el nodo de **Domain (Dominio)** y, debajo de este, seleccione el nodo **_tcp**.
 - b Seleccione **_PCOIP-tool** en el panel derecho, haga clic con el botón secundario y seleccione **Properties** (Propiedades).
 - c En la ventana **Properties** (Propiedades), compruebe el valor de **Time to live (TTL)** (Tiempo de vida [TTL]). El intervalo del almacenamiento en caché se denomina **Maximum TTL value (Máximo valor TTL)** y el valor predeterminado es 1 hora. Puede cambiarlo si lo desea.
El campo TTL se muestra solo si seleccionó **Advanced View** (Vista avanzada) en el menú **View** (Ver) del servidor DNS.

El equilibrio de carga ahora está configurado para dispositivos ThreadX y puede usar los servidores de administración de WDM para administrar un gran número de este tipo de dispositivos.

Configurar el equilibrio de carga de los dispositivos ThreadX 5.x

Cuando WDM se utiliza para administrar dispositivos ThreadX 5.x en un gran ambiente empresarial, un único servidor proxy para dispositivos Teradici, que se usa para administrar dispositivos Threadx 5x desde WDM, no tiene la capacidad de administrar más de 18.000 dispositivos. Podría haber problemas o retrasos en los registros de clientes, la ejecución de programaciones o la ejecución de comandos en tiempo real.

El equilibrio de carga ayuda a solucionar estos problemas en gran medida. En esta configuración, puede instalar y ejecutar múltiples instancias de servidores proxy para dispositivos Teradici en diferentes sistemas, además de equilibrar la carga entre ellos utilizando un proxy como se describe a continuación.

Los componentes del equilibrador de carga son los siguientes:

- Servidor proxy para dispositivos Teradici
- Servidor proxy de alta disponibilidad

WDM utiliza el servidor proxy de alta disponibilidad alojado en el servidor Ubuntu 16.04.1 LTS para equilibrar la carga entre los servidores proxy para dispositivos Teradici. El servidor proxy de alta disponibilidad es un proxy equilibrador de carga que también pueden proporcionar alta disponibilidad en función de cómo esté configurado. Se trata de un popular software de código abierto para equilibradores de carga TCP/HTTP, y una solución de proxy que se puede ejecutar en Linux. El uso más común es mejorar el rendimiento y la confiabilidad de un ambiente de servidores mediante la distribución de la carga de trabajo en varios servidores.

En esta sección se describe cómo configurar y ajustar el equilibrio de carga del servidor proxy de alta disponibilidad.

Pasos para crear un registro DNS_SRV:

Firmware 5.x utiliza un registro DNS_SRV además del registro de texto que contiene la huella digital del certificado SSL para utilizarlo en la consola de administración.

WDM 5.7.3 es compatible con el firmware Teradici 5.x con funciones completas.

- 1 El primer registro requerido es un registro DNS_SRV para `_pcoip-bootstrap`. El registro debe apuntar al nombre del proxy para dispositivos Teradici (proxy de alta disponibilidad).

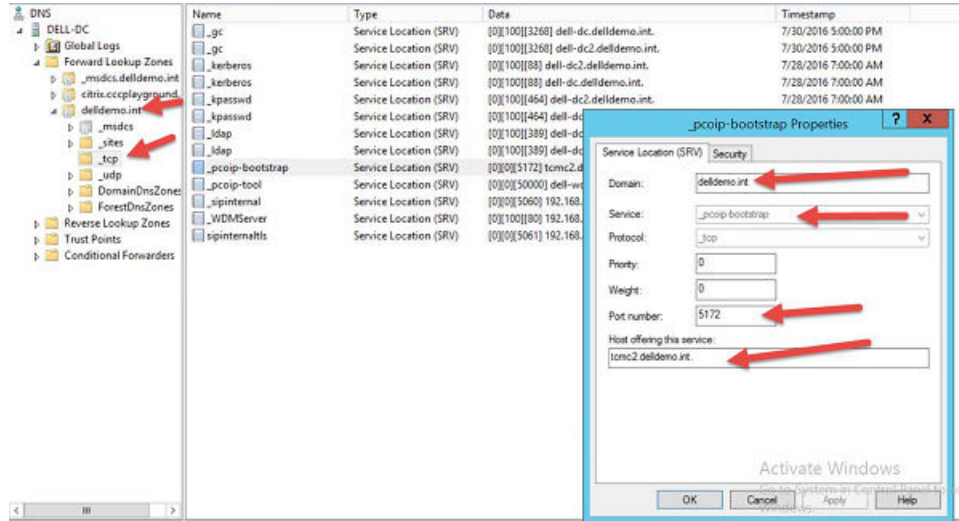


Figura 40. Registro DNS_SRV para `_pcoip-bootstrap`

- 2 El segundo registro requerido es un registro A que apunta al nombre que se utiliza en el campo **Host offering this service** (Host que ofrece este servicio).

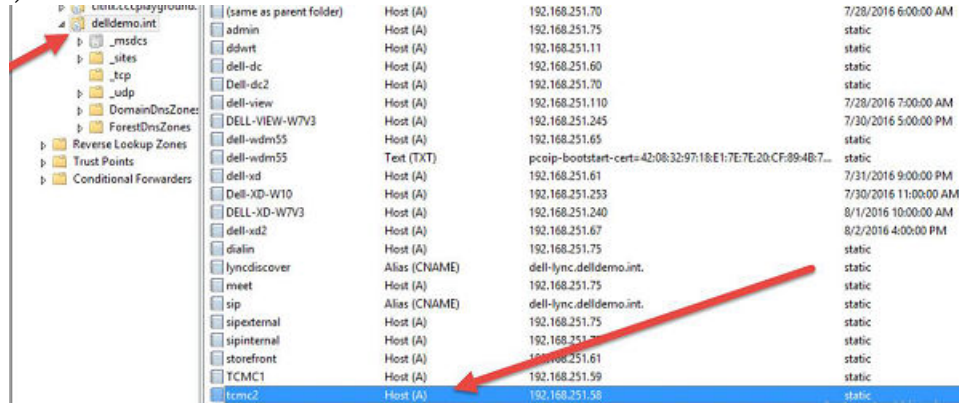


Figura 41. Registro de host

- 3 El tercer registro requerido es un registro txt. El registro txt es la huella digital del certificado SSL que usa la consola de administración. Realice los pasos siguientes para crear un registro A para host, así como un registro txt:

- 1 Haga clic en el nodo de dominio (delldemo.int) y seleccione **Other New Records** (Otros registros nuevos) y, a continuación, seleccione Host (A o AAAA), donde el nombre es el registro A de la consola de administración.

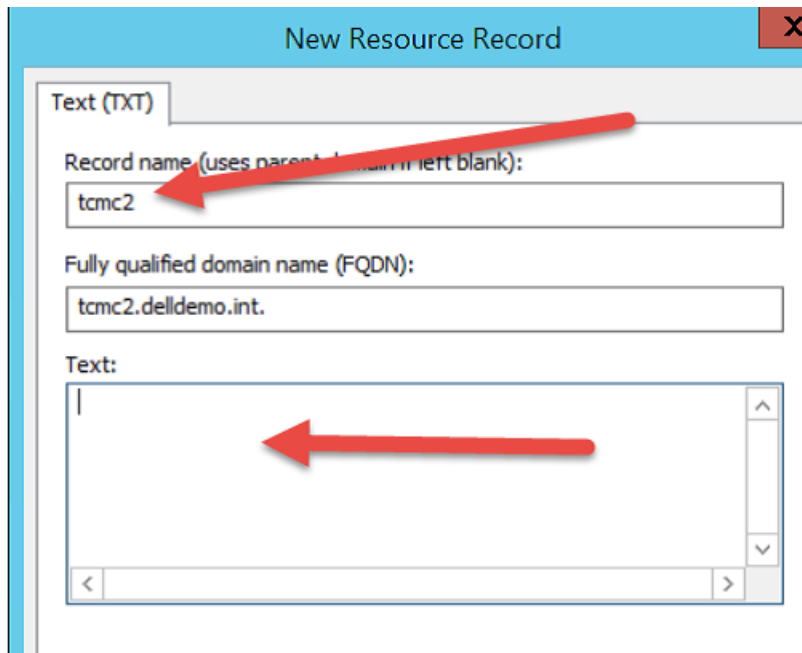


Figura 43. Nuevo registro de recursos

La huella digital SHA-256 puede obtenerse con el navegador Firefox.

Para obtener la huella digital cuando Wyse Device Manager (WDM) se instala con Teradici 5x:

- 1 Debe abrir el navegador Firefox desde el dispositivo en el que está instalado el componente Teradici 5.x. Después de abrir el navegador, pulse la tecla **Alt + T** para abrir las herramientas.
- 2 En la lista desplegable, seleccione **Options** (Opciones).

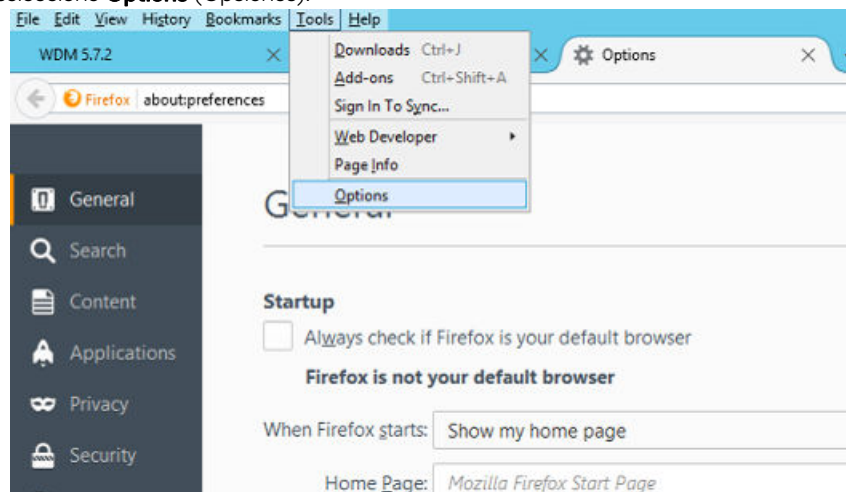


Figura 44. Pestaña general

- 3 En el panel izquierdo de la página **Options** (Opciones), haga clic en la pestaña **Advanced** (Avanzado) y, a continuación, haga clic en la opción **Certificates** (Certificados).

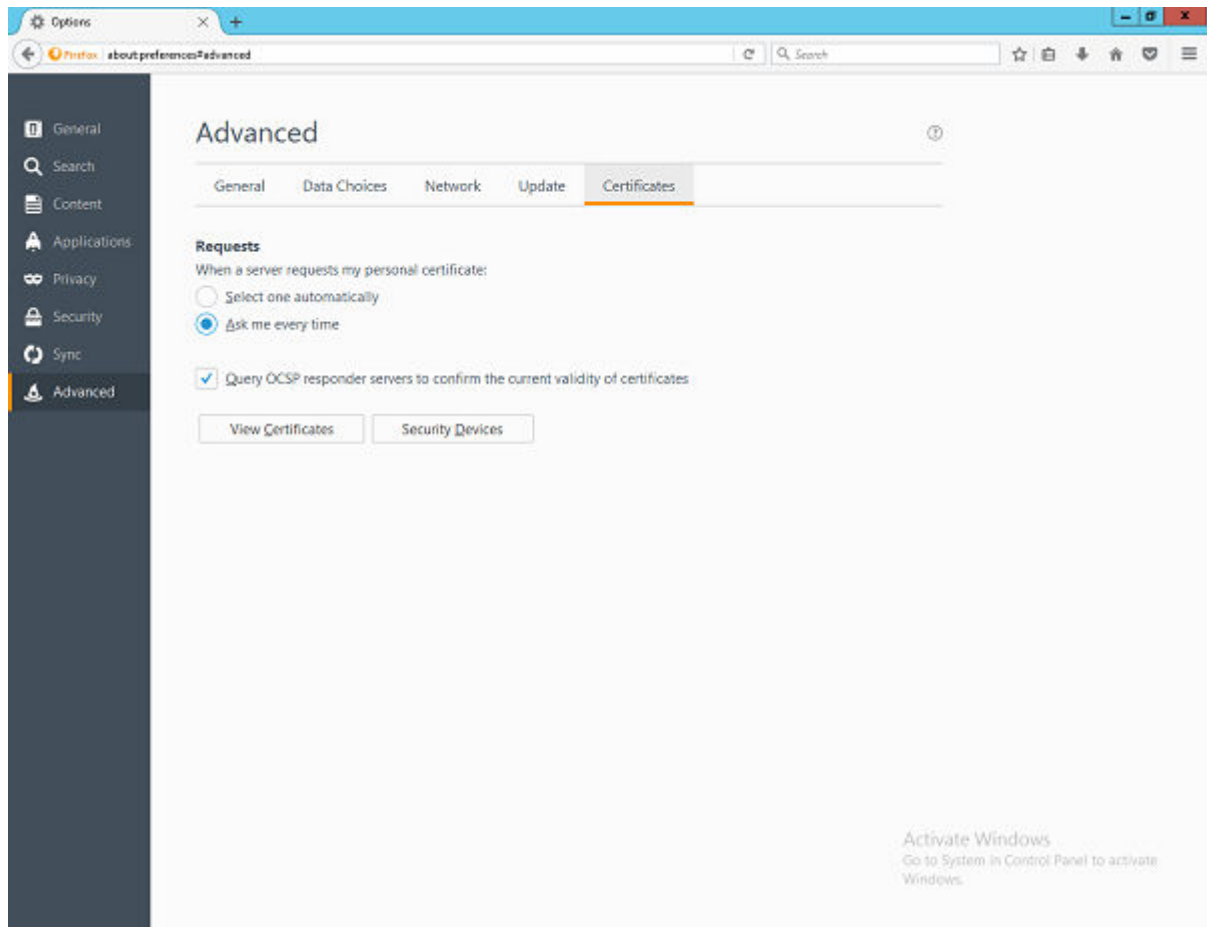


Figura 45. Avanzado

- 4 Haga clic en **View Certificates** (Ver certificados) para abrir la ventana del administrador de certificados.
- 5 Seleccione la pestaña **Authorities** (Autoridades) en la ventana **Certificate Manager** (Administrador de certificados) y haga clic en **Import** (Importar).

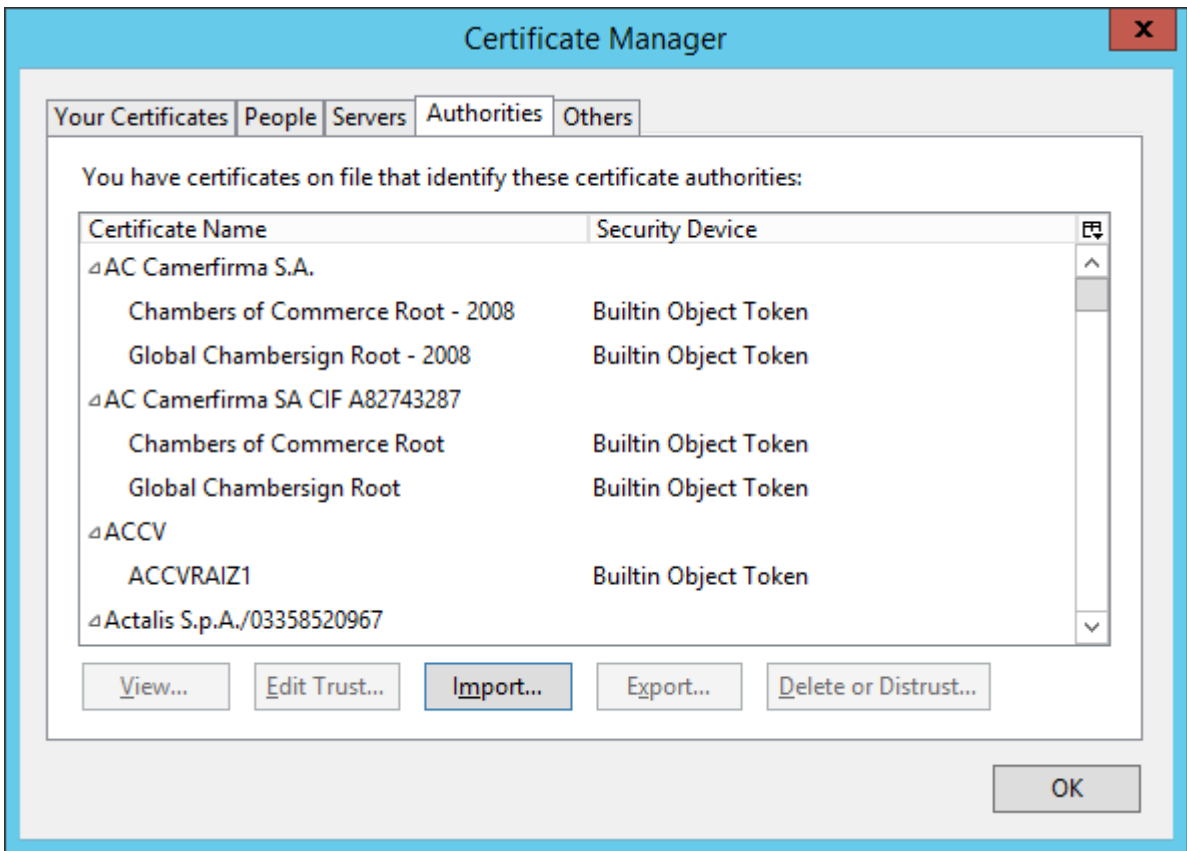


Figura 46. Administrador de certificados

- 6 En el diálogo de explorador de archivos, vaya a la ubicación donde está instalado WDM, por ejemplo: `\\Wyse\WDM\Teradici`, donde la ruta raíz puede ser `C:\Program Files (x86)` basado en el sistema operativo y la ruta de instalación.

NOTA: En algunos casos, si los componentes de Teradici se instalan de una manera personalizada o se configuran manualmente, se deben seguir los pasos descritos anteriormente en el mismo dispositivo, y es posible que no sea aplicable la ruta del instalador estándar. En tal caso, vaya a la ruta raíz correspondiente donde está disponible la carpeta Teradici.

- 7 Seleccione el archivo con el nombre **cert.pem** y, a continuación, haga clic en **Open** (Abrir).
- 8 Ahora haga clic en el botón **View** (Ver) en la ventana **Downloading Certificate** (Descargar certificado).

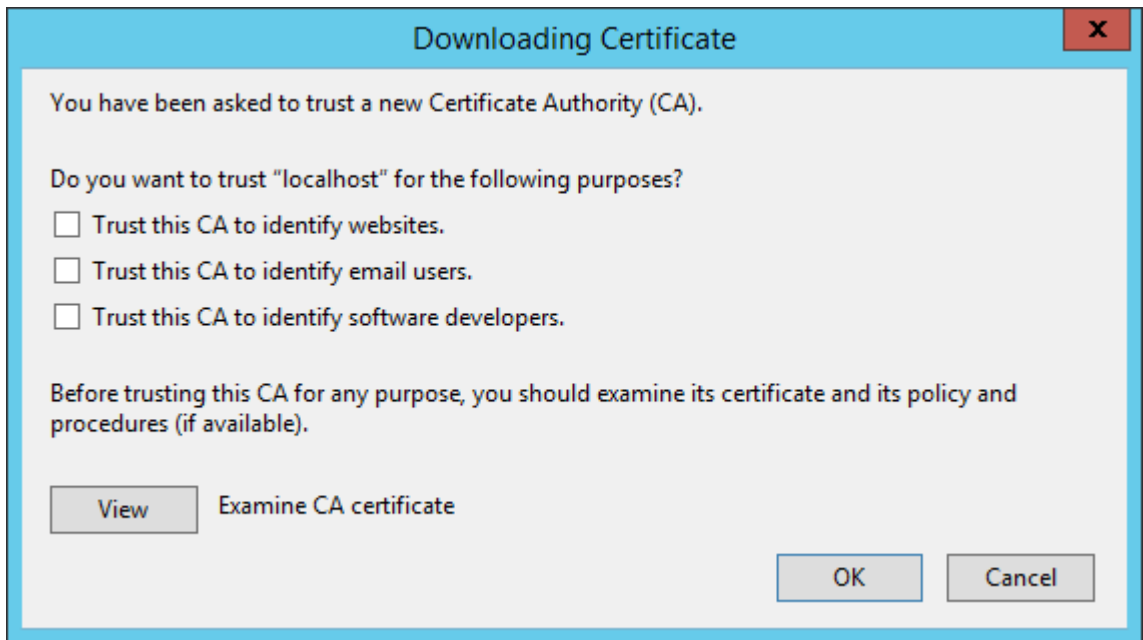


Figura 47. Descargar certificado

- 9 Copie el valor de huella digital sha256. Haga clic en **Close** (Cerrar) y cancele todas las ventanas de Firefox.

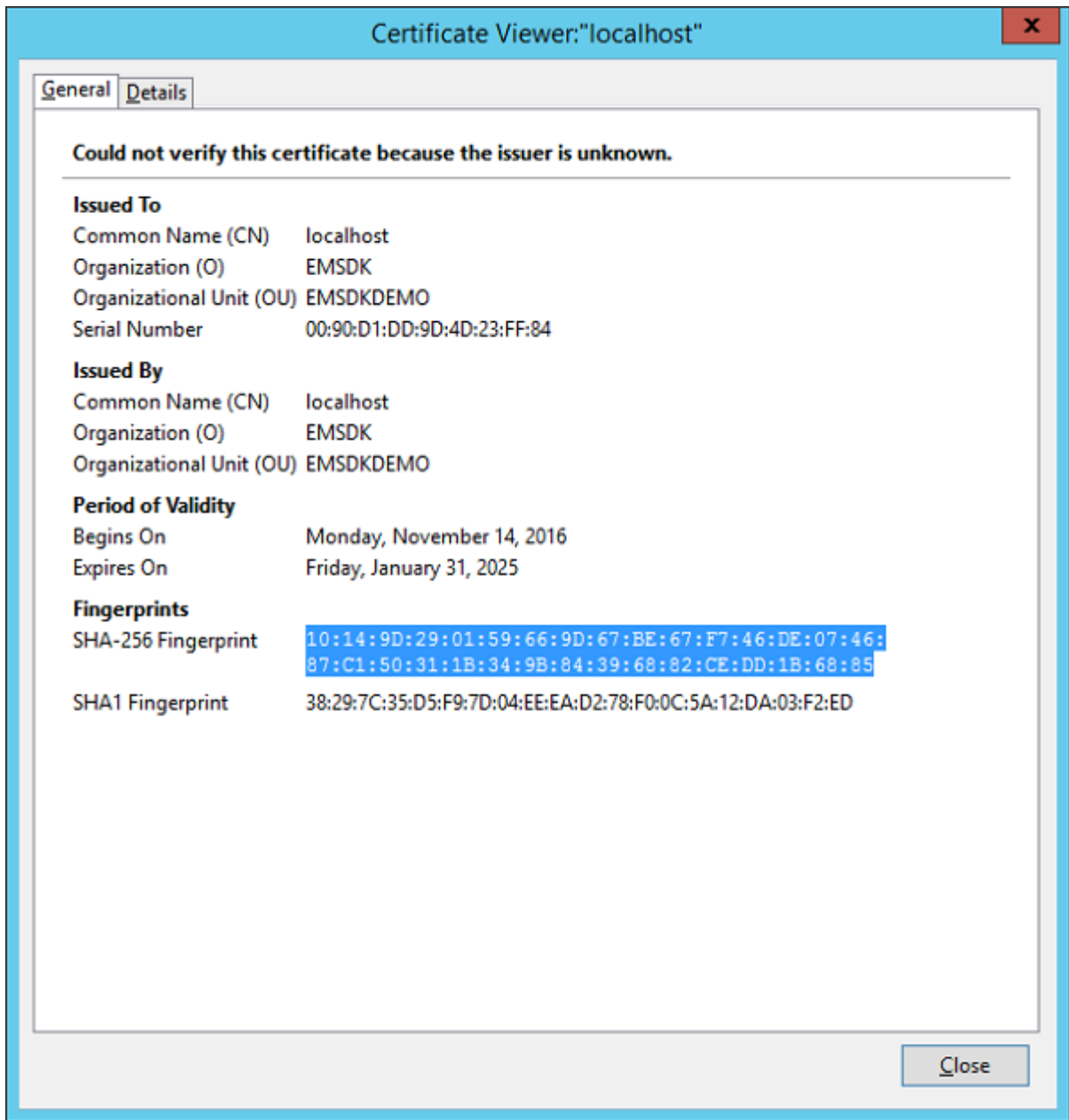


Figura 48. Visor de certificados

① **NOTA:** En el campo de texto, el texto debe tener el prefijo `pcoip-bootstrap-cert=` antes de la huella digital sha256, la que ya se obtuvo.

Después de copiar la huella de certificado, complete los siguientes pasos en el servidor DNS:

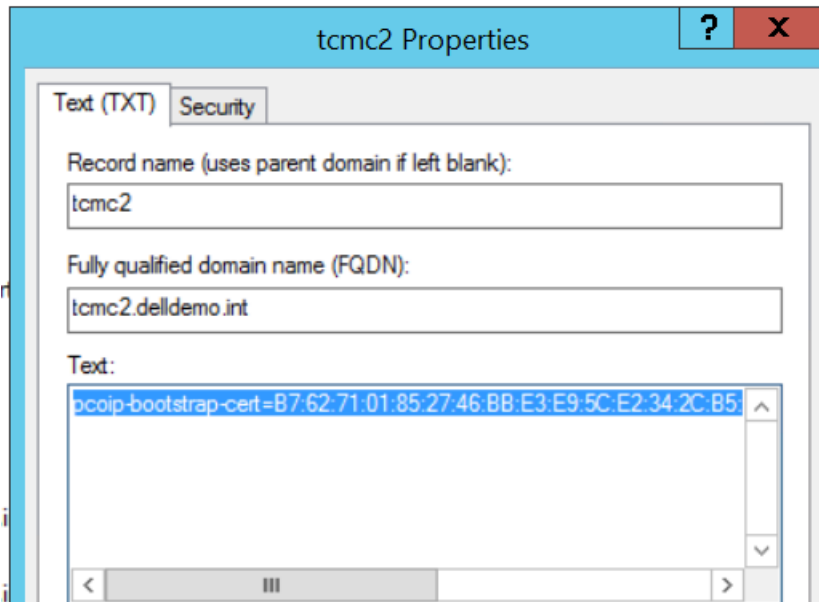


Figura 49. Propiedades de tcmc2

- 10 El cuarto y último registro es un registro PTR inverso para el host de administración.

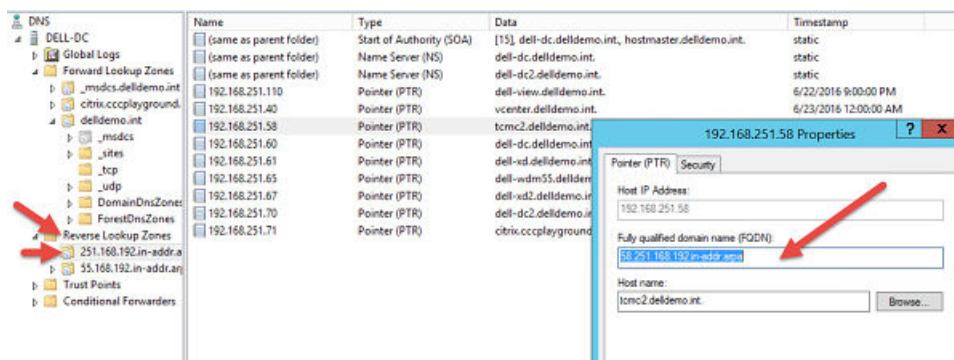


Figura 50. Registro PTR

- 11 La zona debe coincidir con la subred donde está el host y el registro es la dirección IP asignada al proxy para dispositivos Teradici (proxy de alta disponibilidad).

Instalar y configurar el proxy de alta disponibilidad

El proxy de alta disponibilidad, que es el equilibrador de carga de los dispositivos ThreadX 5x, se configura en Linux Ubuntu versión 16.04.1 con HAProxy versión 1.6.

Siga los pasos para instalar y configurar el proxy de alta disponibilidad en la máquina Ubuntu Linux:

Vínculo de referencia: <https://haproxy.debian.net/#?distribution=Ubuntu&release=precise&version=1.6>

- 1 Inicie sesión en la máquina Ubuntu ingresando las credenciales de usuario que utilizó durante la instalación del sistema operativo Ubuntu.
- 2 Abra el terminal y ejecute los siguientes comandos para instalar el proxy de alta disponibilidad:
 - `sudo apt-get install software-properties-common`
 - `sudo add-apt-repository ppa:vbernat/haproxy-1.6`

- `sudo apt-get update`
 - `sudo apt-get install haproxy`
- 3 Ejecute los siguientes comandos para configurar el proxy de alta disponibilidad:
- Respalde la configuración original antes de editar, con el comando `sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.original`
 - Ahora, edite el archivo de configuración con el comando `sudo nano /etc/haproxy/haproxy.cfg`
 - En el archivo de configuración, edite las siguientes secciones según se requiera:
 - Sección global: Maxconn <número máximo de conexiones>
 - Front-end tcp-in: vínculo <IP del servidor proxy de alta disponibilidad>:5172
 - Servidores back-end: servidor <nombre de alias del servidor> <IP del servidor proxy para dispositivos Teradici>:5172
 - Maxconn <número máximo de conexiones por servidor proxy para dispositivos Teradici>

NOTA: Para lograr una alta disponibilidad, el administrador puede agregar más servidores back-end, más allá de la capacidad total de clientes, para tener recuperación óptima.

- Después de editar la configuración, guárdela con el comando `Ctrl + O`
- La muestra de configuración del proxy de alta disponibilidad se proporciona como se indica a continuación:

```
global
log /dev/log local0
log /dev/log local1 notice
chroot /var/lib/haproxy
daemon
#maxconn is maximum allowed connections
maxconn 50000
defaults
log global
mode tcp
timeout connect 5000ms
timeout client 50000ms
timeout server 50000ms
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http
frontend tcp-in
#reemplace la IP con la IP de su máquina proxy Linux
```

vínculo 10.150.99.102:5172

servidores default_backend

servidores de backend

#Agregue su IP de máquina Windows con varios back-end con el puerto 5172

maxconn representa el número de conexión: vuelva a colocar 10 con límite # (por debajo de 20000)

server1 (servidor1) y server2 (servidor2) son solo nombres y no palabras clave

```
server server1 10.150.99.107:5172 maxconn 10
```

```
server server2 10.150.99.107:5172 maxconn 10
```

- 4 Ahora, valide el archivo de configuración del proxy de alta disponibilidad con el comando **sudo haproxy -f /etc/haproxy/haproxy.cfg -c**

Si la configuración es válida, se mostrará el mensaje a continuación:

Configuration file is valid (El archivo de configuración es válido)

- 5 Ahora inicie el servicio del proxy de alta disponibilidad con el siguiente comando:

```
Sudo service haproxy restart
```

- 6 **Comando para detener el servicio del proxy de alta disponibilidad**

```
Sudo service haproxy stop
```

- 7 **Comando para verificar la versión del proxy de alta disponibilidad**

```
Sudo haproxy -f
```

- 8 **Comando para desinstalar el proxy de alta disponibilidad**

```
Sudo apt-get remove haproxy
```

o

```
Sudo apt-get purge --auto-remove haproxy
```

Instalar los servidores proxy de dispositivos Teradici

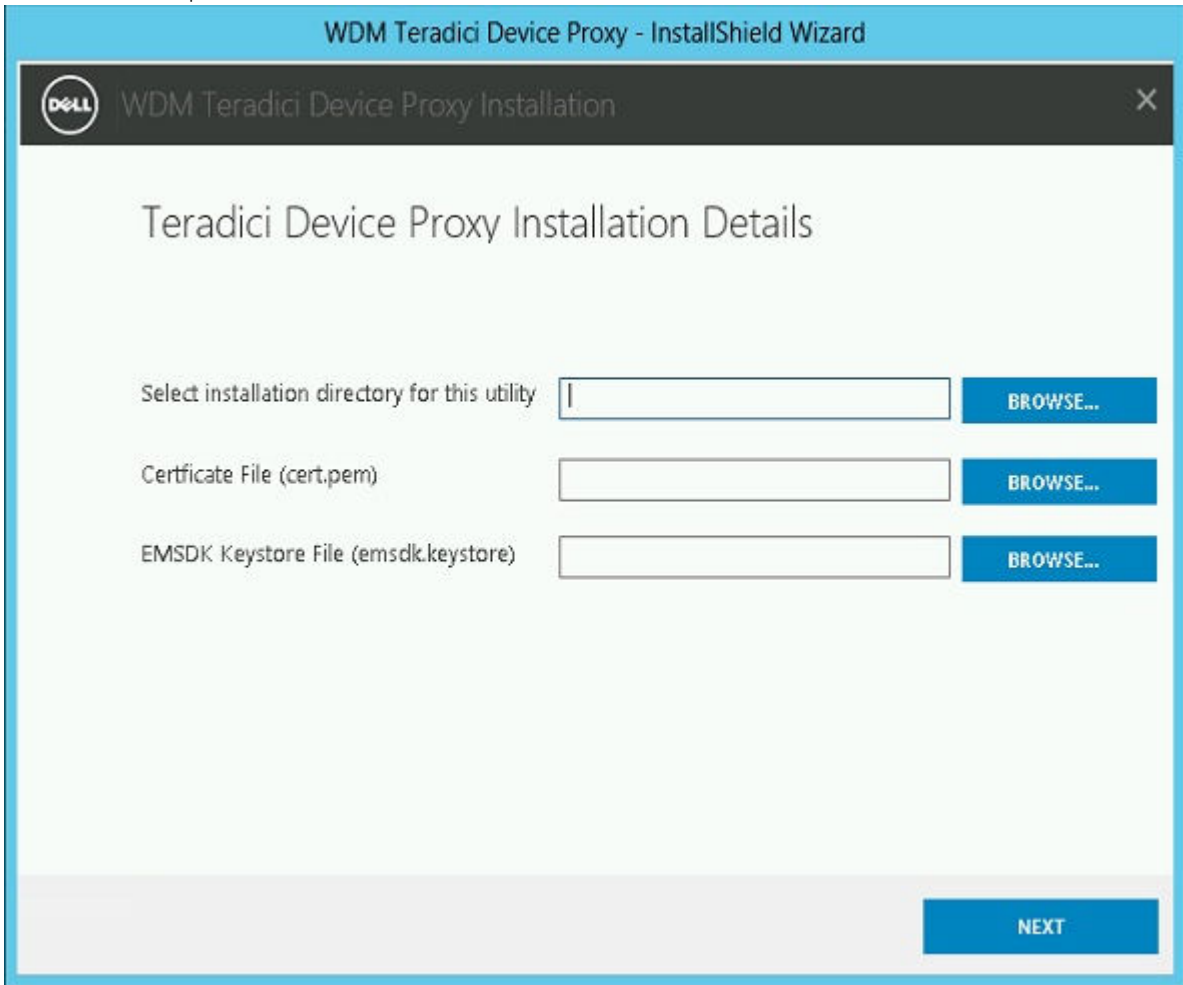
Los servidores proxy de los dispositivos Teradici pueden instalarse en los servidores que ejecutan los siguientes sistemas operativos:

- Windows 2012
- Windows 2012 R2
- Windows 2008 R2 de 64 bits
- Windows Server 2016

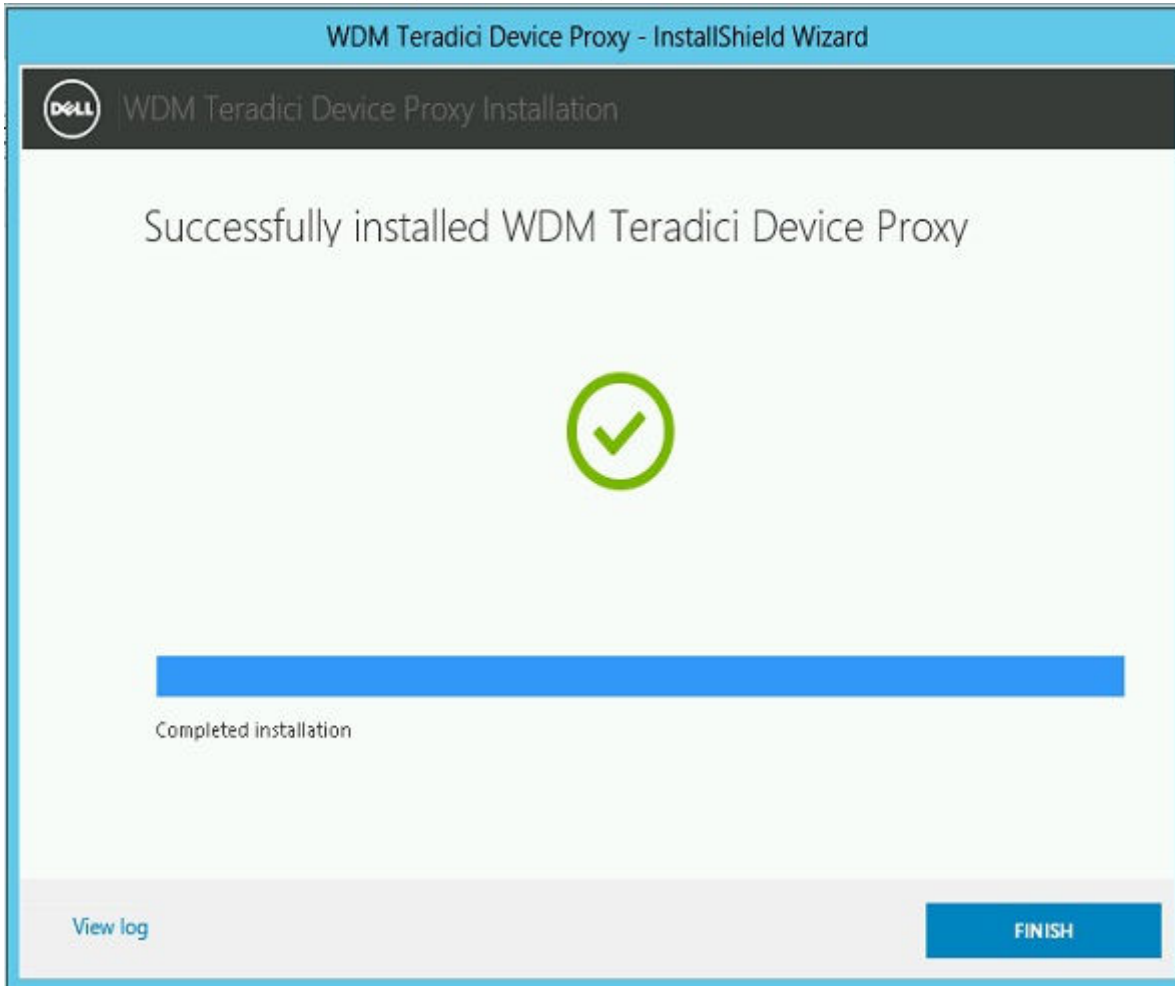
Siga los pasos que se proporcionan para instalar el servicio proxy para dispositivos Teradici:

- 1 Inicie sesión en el sistema como administrador.
- 2 Copie la carpeta **WDM installer** (Instalador de WDM) en la máquina de destino.
- 3 Vaya a la carpeta **TeradiciDeviceProxy**.
- 4 Haga doble clic en el archivo **WDMTeradiciDeviceProxy.exe** para iniciar la instalación.
- 5 Proporcione los siguientes detalles:
 - a Seleccione la ruta donde desea instalar el proxy para dispositivos Teradici y sus componentes relacionados.

- b Seleccione el archivo **Cert.pem** en la carpeta **<WDM installed location>\Teradici (<Ubicación de instalación de WDM>\Teradici)**, en la máquina donde está seleccionado el componente **ThreadX 5X** cuando instale WDM.
- c Seleccione el archivo **emsdk.keystore** en la carpeta **<WDM installed location>\Teradici\EMSDK\config (<Ubicación de instalación de WDM>\Teradici\EMSDK\config)**, en la máquina donde está seleccionado el componente **ThreadX 5X** se selecciona un componente al instalar WDM.



- 6 Proporcione las entradas necesarias y haga clic en **Next** (Siguiente).



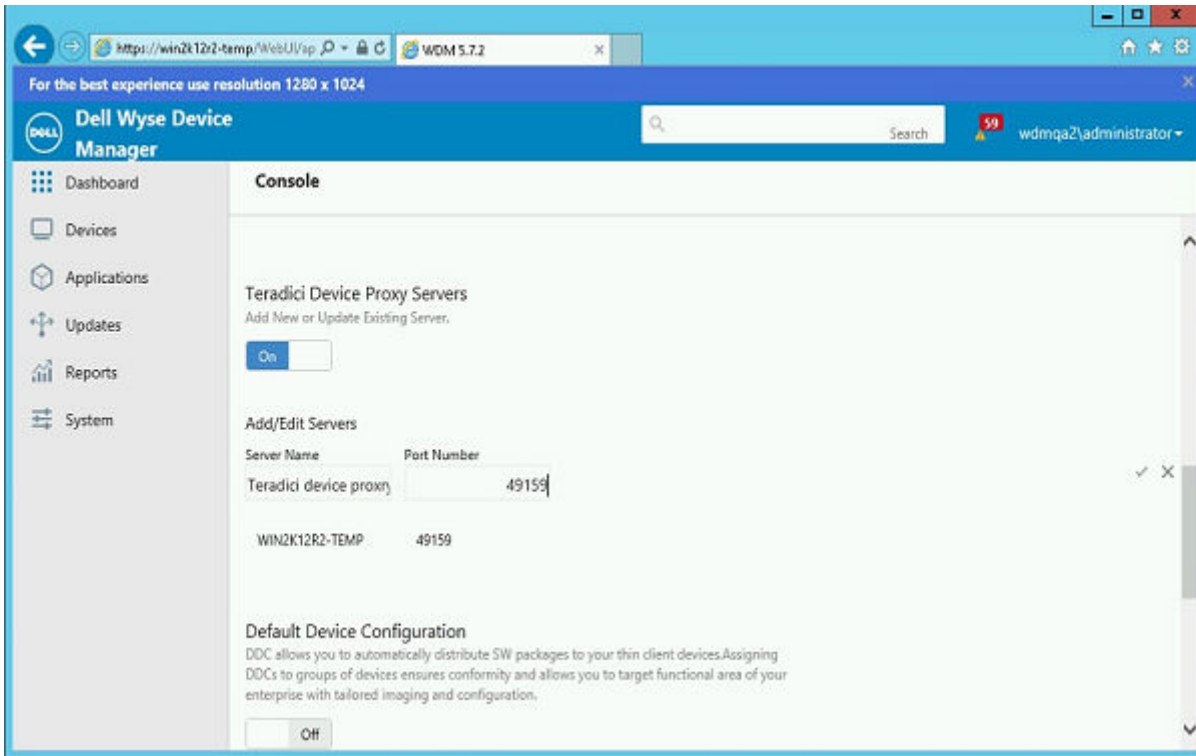
- 7 Haga clic en **Finish** (Terminar).
- 8 Se creará el registro de instalación en <EMSDK Installed location>\Teradici\Detail_TeradiciDeviceProxy.log (<Ubicación de instalación de EMSDK>\Teradici\Detail_TeradiciDeviceProxy.log).
- 9 Vaya a **Start (Iniciar) > Administrative Tools (Herramientas administrativas) > Services (Servicios)**.
- 10 Compruebe que el servicio de Windows del Administrador de ThreadX 5x está instalado y se está ejecutando.

Agregar servidores proxy de dispositivos Teradici a WDM

Tareas

- 1 Abra la WebUI de WDM e inicie sesión como administrador.
- 2 Vaya a **System (Sistema) > Console (Consola)** y active la opción **Teradici Device Proxy servers** (Servidores proxy para dispositivos Teradici).
- 3 Haga clic en **Add Server** (Agregar servidor).
- 4 Agregue el nombre del servidor proxy para dispositivos Teradici en el campo **Server Name** (Nombre del servidor) y coloque el número de puerto del servicio proxy para dispositivos Teradici en el campo **Port Number** (Número de puerto). El valor predeterminado es 49159.

NOTA: Si el número de puerto predeterminado se cambia, debe actualizarse en WDM. Para obtener más información, consulte la *Wyse Device Manager 5.7.3 Administrator's guide (Guía del administrador de Wyse Device Manager 5.7.3)*.



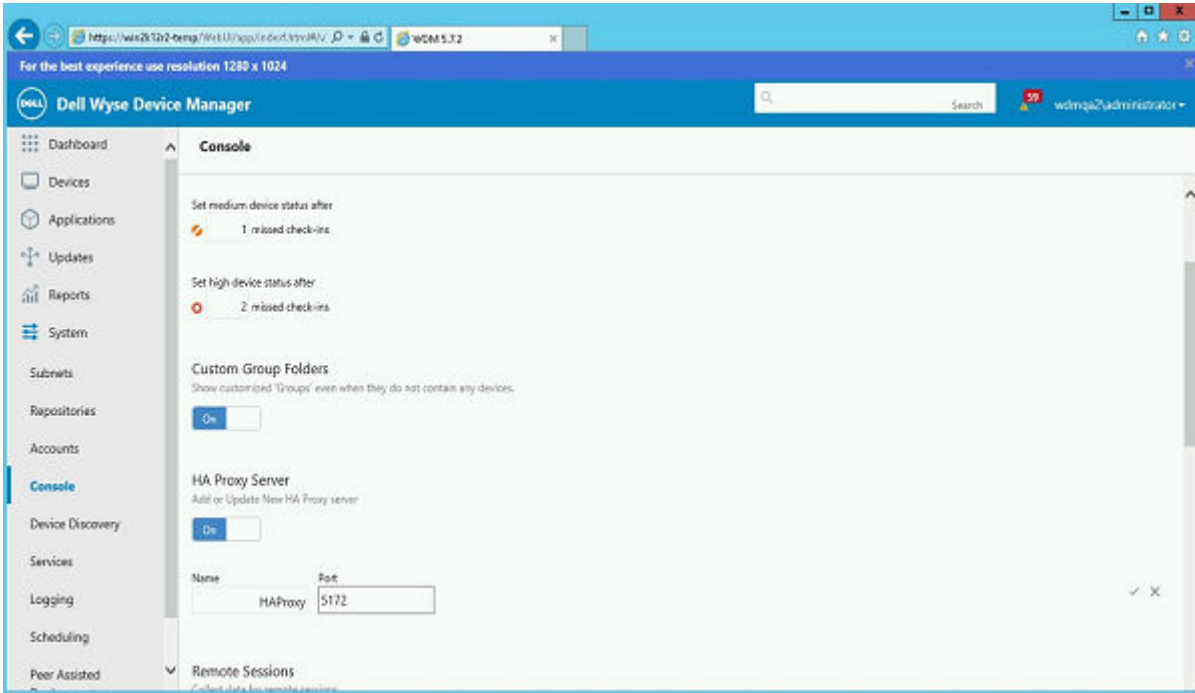
- 5 Haga clic en la marca de verificación, en la parte derecha de los cuadros de texto, para guardar los valores.

Agregar proxy de alta disponibilidad a WDM

Siga los pasos a continuación para agregar el proxy de alta disponibilidad a WDM:

- 1 Inicie sesión en la WebUI de WDM como administrador.
- 2 Vaya a página de la consola y active la opción **HAProxy Server** (Servidor proxy de alta disponibilidad).
- 3 Haga clic en **Add Server** (Agregar servidor).
- 4 Agregue el nombre del servidor proxy de alta disponibilidad en el campo correspondiente y otorgue el número de puerto 5172.

- Haga clic en **Add Server** (Agregar servidor) nuevamente.



- Haga clic en la marca de verificación, en la parte derecha de los cuadros de texto, para guardar los valores.

Reiniciar API de Threadx

Siga los pasos que se muestran a continuación para reiniciar ThreadX API:

- Inicie sesión en el servidor donde está instalado el componente ThreadX 5x de WDM.
- Haga clic en **Start menu (Menú de inicio) > Administrative tools (Herramientas administrativas) > Internet information service (IIS) manager (Administrador de servicios de información de Internet [ISS])**.
- Expanda el nodo raíz (nombre de host del servidor) y seleccione **Application pools (Grupos de aplicaciones) > ASP .Net v4.0**.
- Haga clic con el botón derecho del mouse en **AASP .Net v4.0** y seleccione **Stop** (Detener).
- Nuevamente haga clic con el botón derecho del mouse en **ASP .Net v4.0** y seleccione **Start** (Iniciar).
- Abra la WebUI de WDM e inicie sesión como administrador.
- Verifique el estado utilizando el panel.

Verifique el estado en el panel

- Haga clic en el panel y seleccione Teradici Servers (Servidores Teradici).
- Compruebe que Thread 5x, proxy de alta disponibilidad de Teradici y el servidor proxy para dispositivos Teradici estén en línea.

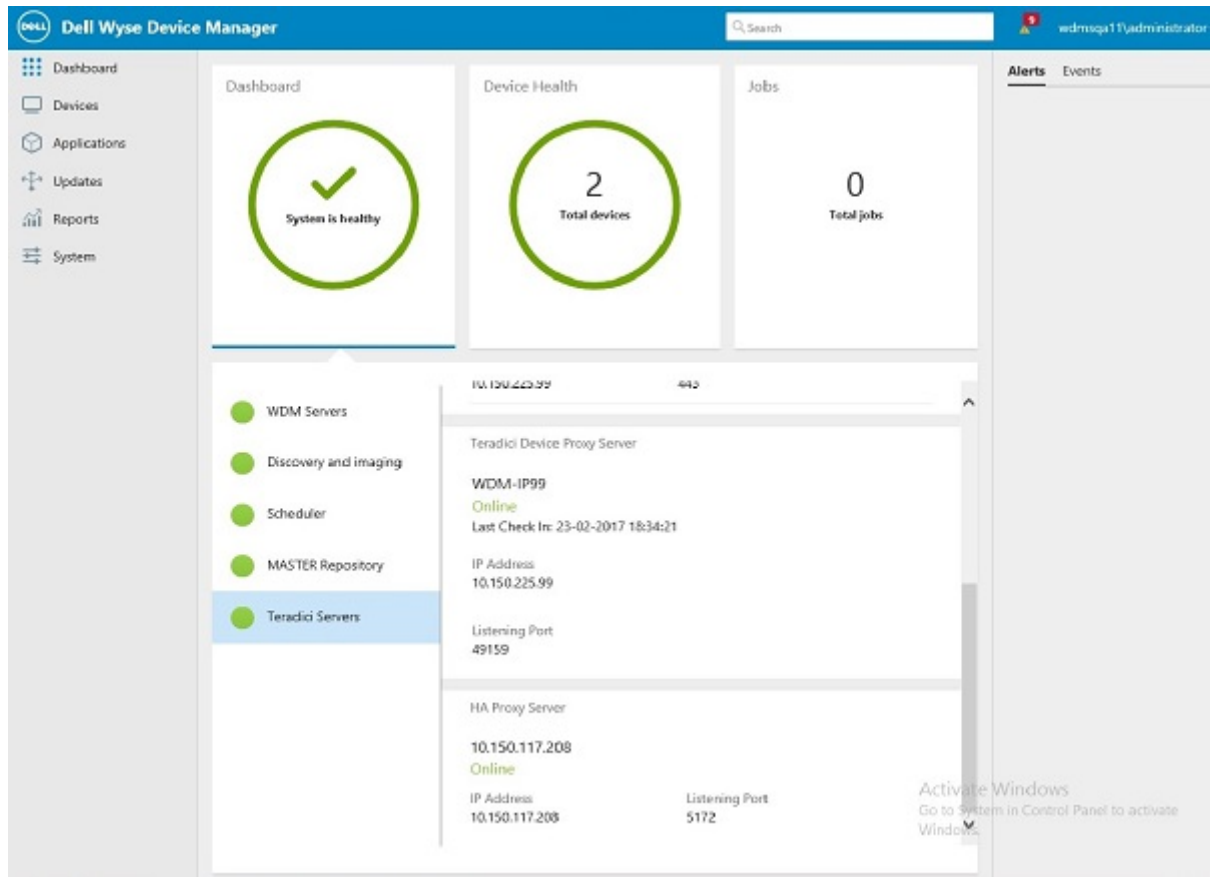


Figura 51. Estado en el panel

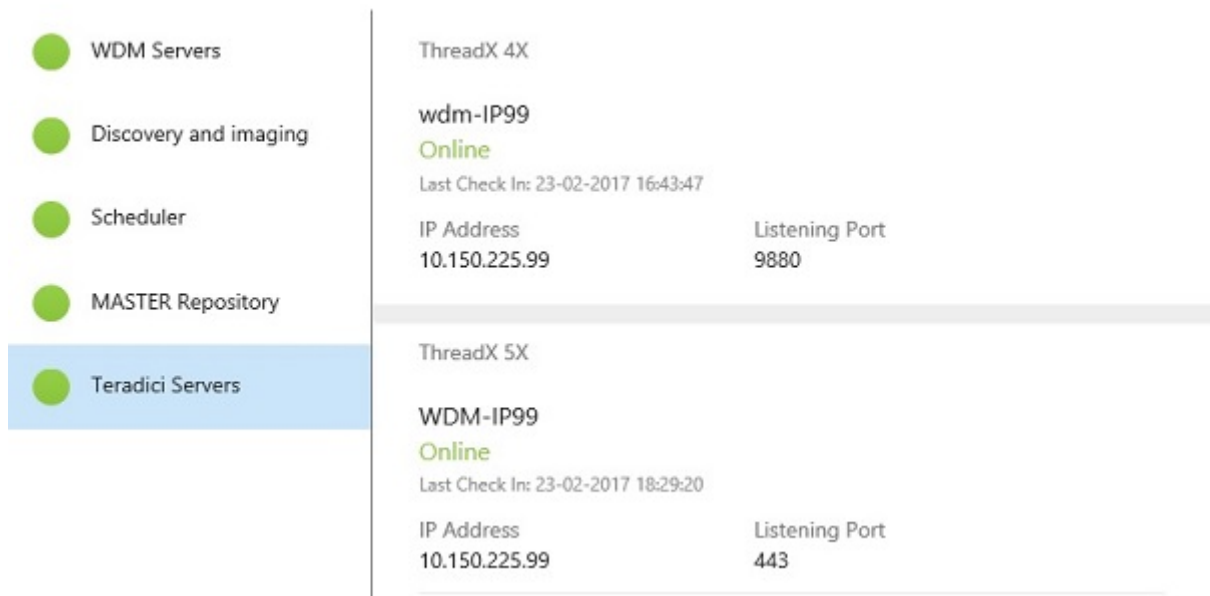


Figura 52. Estado en el panel

Teradici Device Proxy Server

WDM-IP99

Online

Last Check In: 23-02-2017 18:34:21

IP Address

10.150.225.99

Listening Port

49159

HA Proxy Server

10.150.117.208

Online

IP Address

10.150.117.208

Listening Port

5172

Active
Go to
Window

Figura 53. Estado en el panel

Configurar la alta disponibilidad del servicio WebUI

Cuando hay una sola instancia de servicio WebUI, y si ese servidor deja de funcionar, no podrá administrar WDM desde la WebUI. Por esta razón, se recomienda utilizar alta disponibilidad (HA) del servicio WebUI.

Puede utilizar el proxy equilibrador de carga como proxy inverso de ARR donde haya que configurar para lograr la compatibilidad de la alta disponibilidad del servicio WebUI.

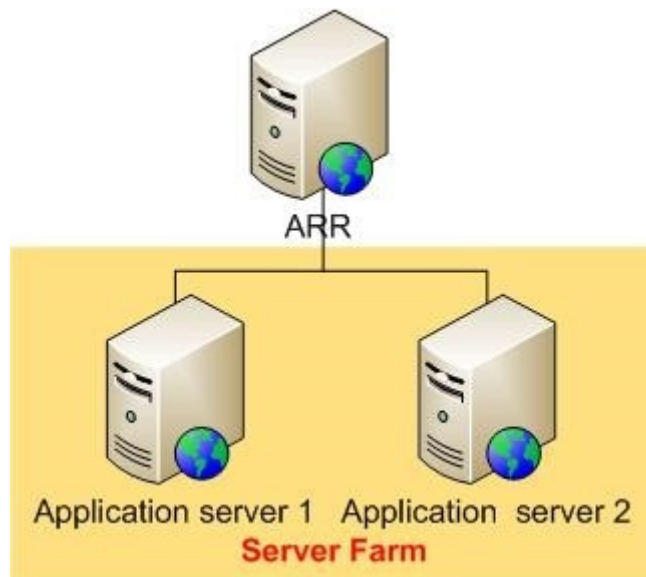


Figura 54. Alta disponibilidad (HA) del servicio WebUI

Temas:

- Configurar el servidor proxy de ARR
- Instalar los servicios de información de Internet (IIS)
- Instalar el módulo ARR
- Cambiar el modelo de proceso del grupo de aplicaciones para la solicitud de enrutamiento de aplicaciones
- Crear una granja de servidores WebUI
- Configurar SSL en el servidor proxy
- Configurar las propiedades de la granja de servidores para la solicitud de enrutamiento de aplicaciones
- Iniciar sesión en el navegador del WebUI

Configurar el servidor proxy de ARR

El servidor proxy de la solicitud de enrutamiento de aplicaciones (ARR) es el componente más importante del equilibrio de carga. Este servidor recibe las solicitudes de los sistemas de thin client y las enruta a los diferentes servidores de administración de WDM.

Prerequisito

Debe tener instalado IIS 7.0 o una versión posterior en Windows 2008 (cualquier SKU) o una versión posterior.

Acerca de esta tarea

La configuración del servidor proxy de ARR consta de los siguientes pasos:

Pasos

- 1 Instalar IIS.
- 2 Instalar el módulo ARR.
- 3 Cambiar el modelo de proceso del grupo de aplicaciones por la solicitud de enrutamiento de aplicaciones.
- 4 Crear una granja de servidores WebUI.
- 5 Configurar SSL en el servidor proxy.
- 6 Configurar las propiedades de la granja de servidores para la solicitud de enrutamiento de aplicaciones.

Instalar los servicios de información de Internet (IIS)

- 1 Inicie sesión como administrador.
- 2 Vaya a **Control Panel (Panel de control) > Programs and Features (Programas y características) > Turn Windows features on or off (Activar o desactivar funciones de Windows)**.
- 3 Seleccione las opciones según se muestra en la siguiente captura de pantalla.

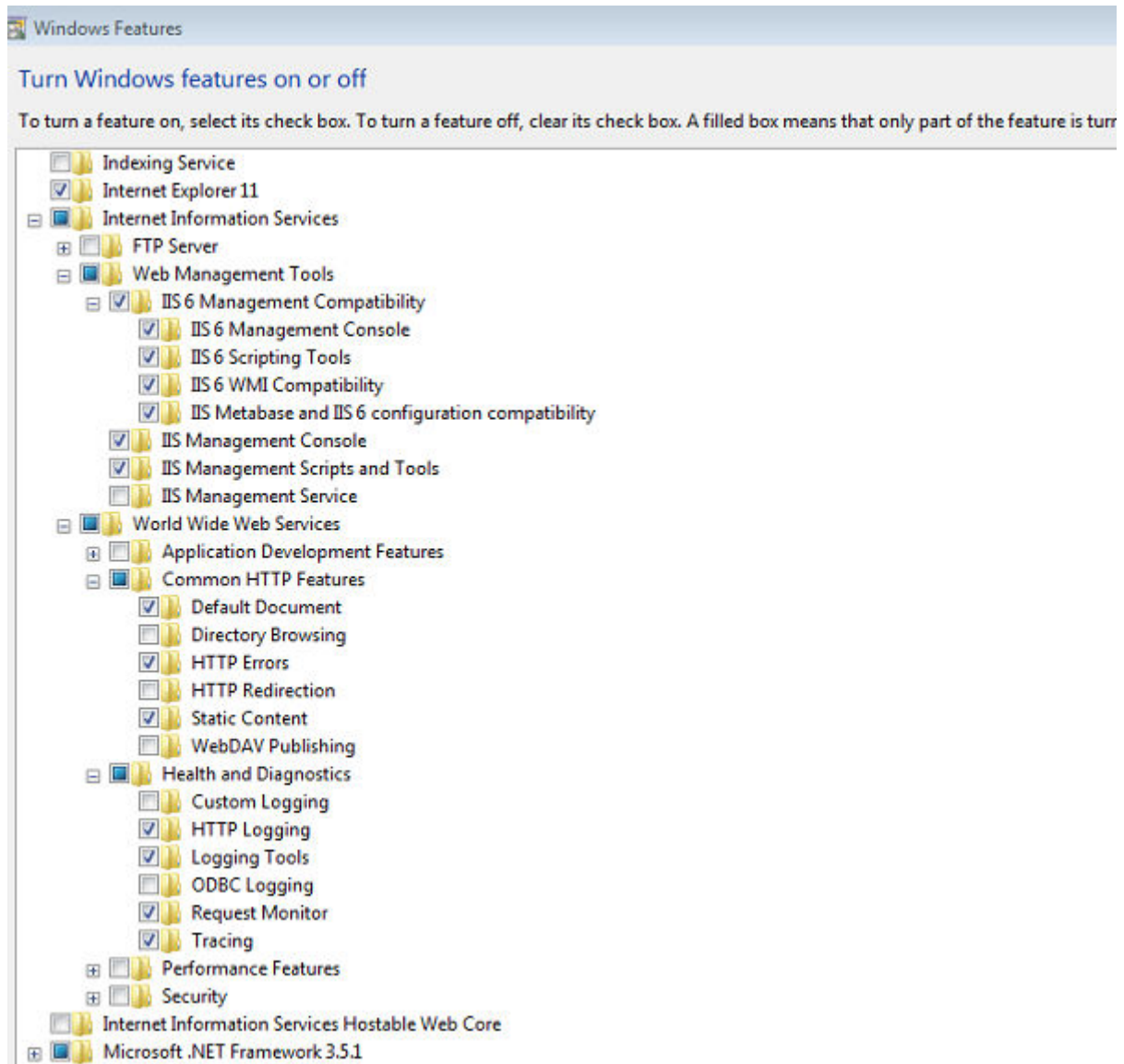


Figura 55. Funciones de Windows

4 Haga clic en **OK** (Aceptar).

Instalar el módulo ARR

Debe instalar la versión 3.0 de la solicitud de enrutamiento de aplicaciones en el sistema que haya identificado para ser el servidor proxy de ARR. El instalador está disponible en el sitio de descargas de Microsoft en support.microsoft.com. Descargue el archivo **ARRv3_0.exe** e instálelo.

Cambiar el modelo de proceso del grupo de aplicaciones para la solicitud de enrutamiento de aplicaciones

Acerca de esta tarea

Todas las solicitudes y respuestas HTTP para los sitios de contenido pasan por la solicitud de enrutamiento de aplicaciones. El proceso de trabajo del sitio web predeterminado en la solicitud de enrutamiento de aplicaciones siempre debe estar en ejecución, independientemente de si los procesos de trabajo de algunos de los sitios se estén ejecutando o no.

Debe deshabilitar el tiempo de espera en inactividad, en el modelo del proceso de grupos para el sitio web predeterminado.

Pasos

- 1 Inicie el Administrador de IIS.
- 2 Seleccione **Application Pools** (Grupos de aplicaciones).

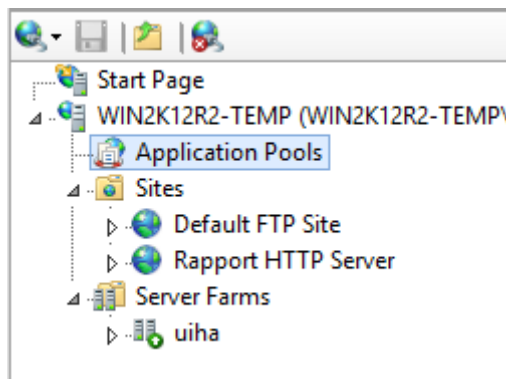


Figura 56. Grupos de aplicaciones

- 3 Seleccione **DefaultAppPool**.
- 4 Vaya a **Actions (Acciones) > Edit Application Pool (Editar grupos de aplicaciones) > Advanced Settings (Configuración avanzada)**.
- 5 Cambie el **Idle Time-out (minutes)** (Tiempo de espera en inactividad [minutos]) a 0.

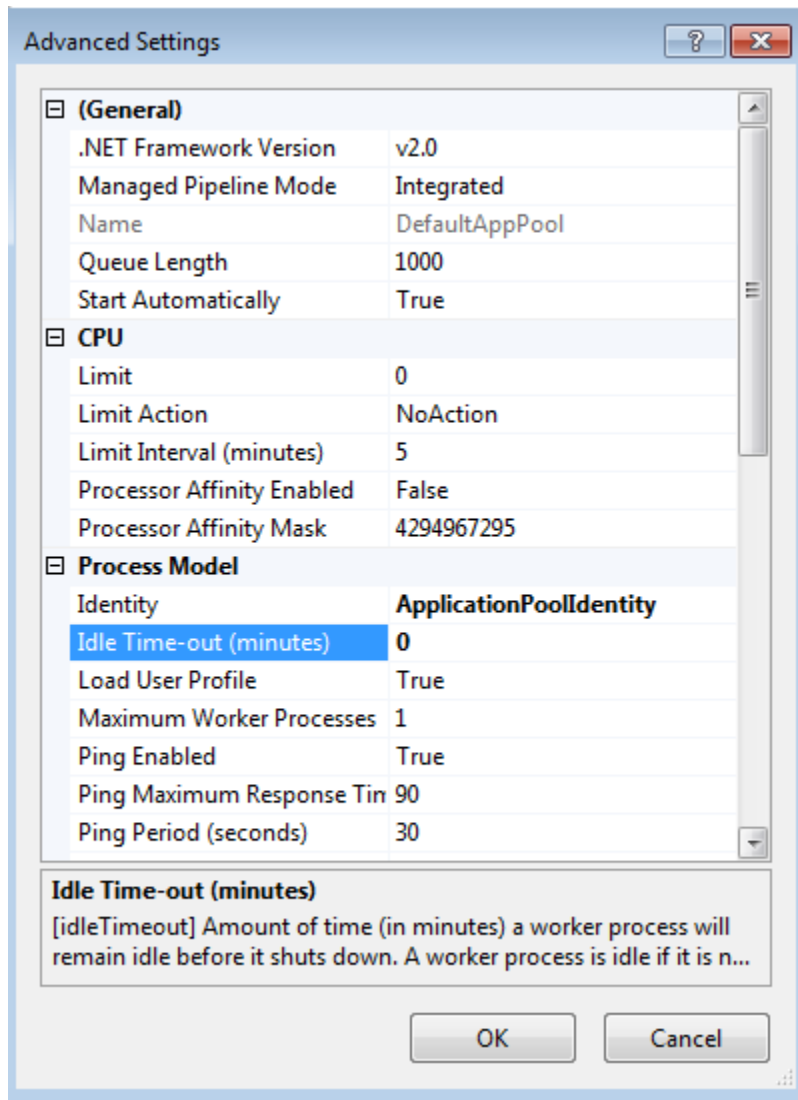


Figura 57. Configuración avanzada

- Haga clic en **OK** (Aceptar) para guardar los cambios.

Crear una granja de servidores WebUI

- Inicie el Administrador de IIS.
- Haga clic con el botón derecho del mouse en **Server Farms** (Centros de datos) y seleccione **Create Server Farm** (Crear granja de servidores).

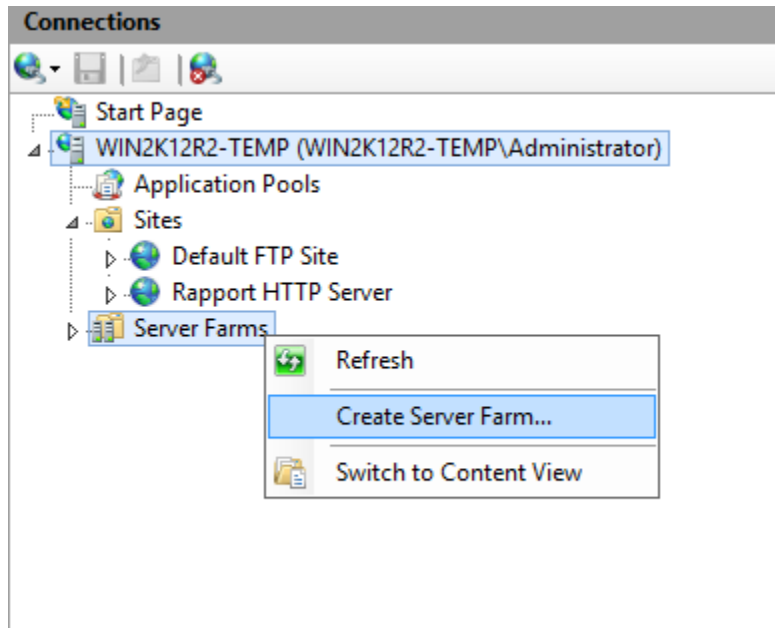


Figura 58. Granjas de servidores

- 3 Ingrese un nombre para la granja de servidores.

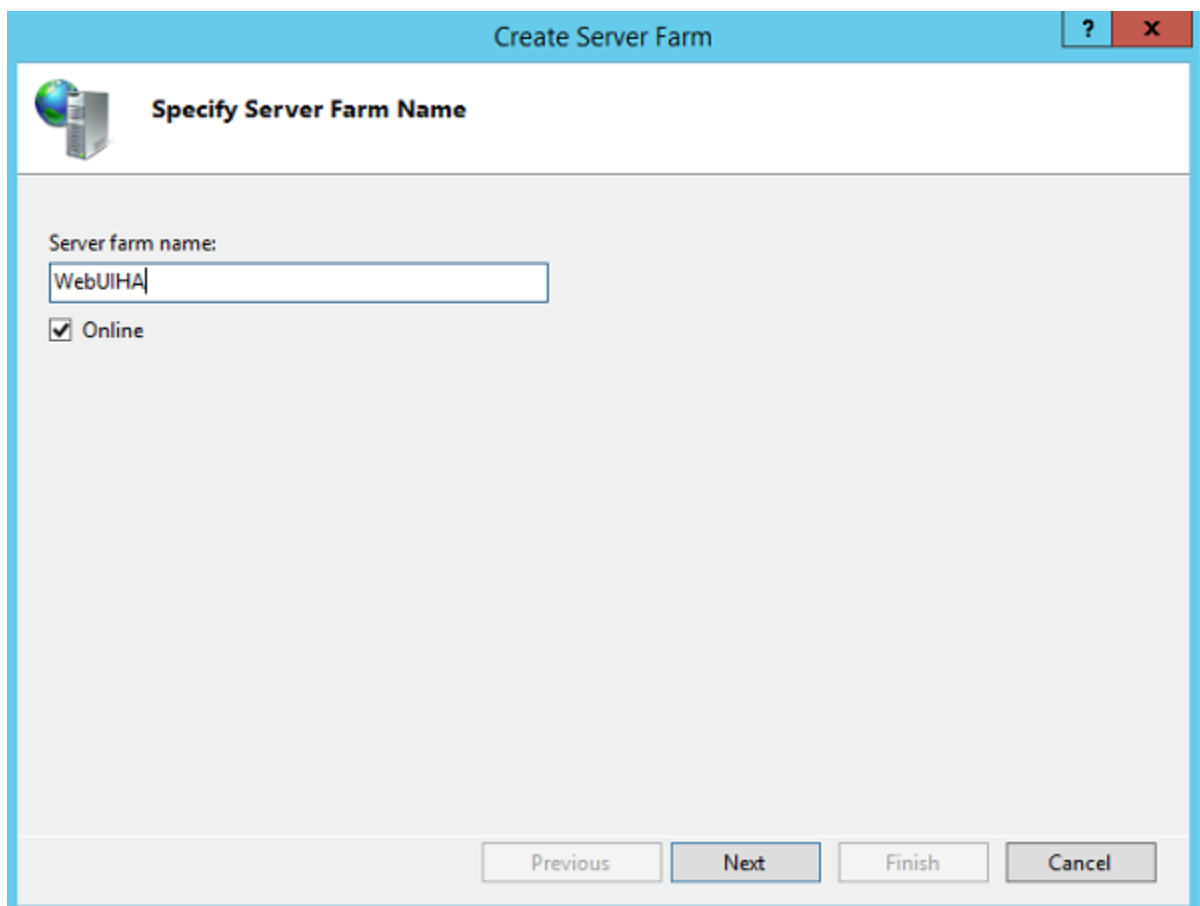


Figura 59. Crear granja de servidores

- 4 Haga clic en **Next** (Siguiete).

- 5 En la página **Add Server** (Agregar servidor), agregue los servidores de aplicaciones (servidores WebUI).

Server Address	Status
10.150.101.6	Online

Figura 60. Agregar servidor

- 6 Haga clic en **Finish** (Terminar) para crear la granja de servidores, de la que los servidores de aplicaciones ingresados son miembros. Se muestra la ventana **Rewrite Rules** (Reescribir reglas).

Server Farms

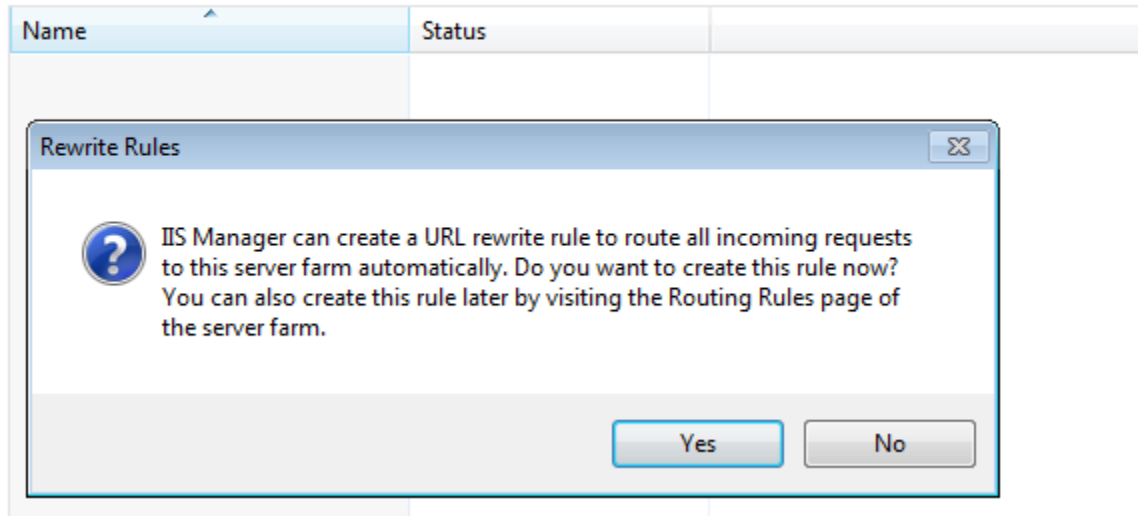


Figura 61. Reescribir reglas

- 7 Haga clic en **Yes** (Sí) para que el Administrador de IIS cree una URL para reescribir reglas, a fin de enrutar todas las solicitudes entrantes a esta granja de servidores.

Configurar SSL en el servidor proxy

Para configurar SSL en el proxy de ARR, cree un certificado de dominio para el servidor proxy. Asigne este certificado a la vinculación https para el sitio web y habilite SSL.

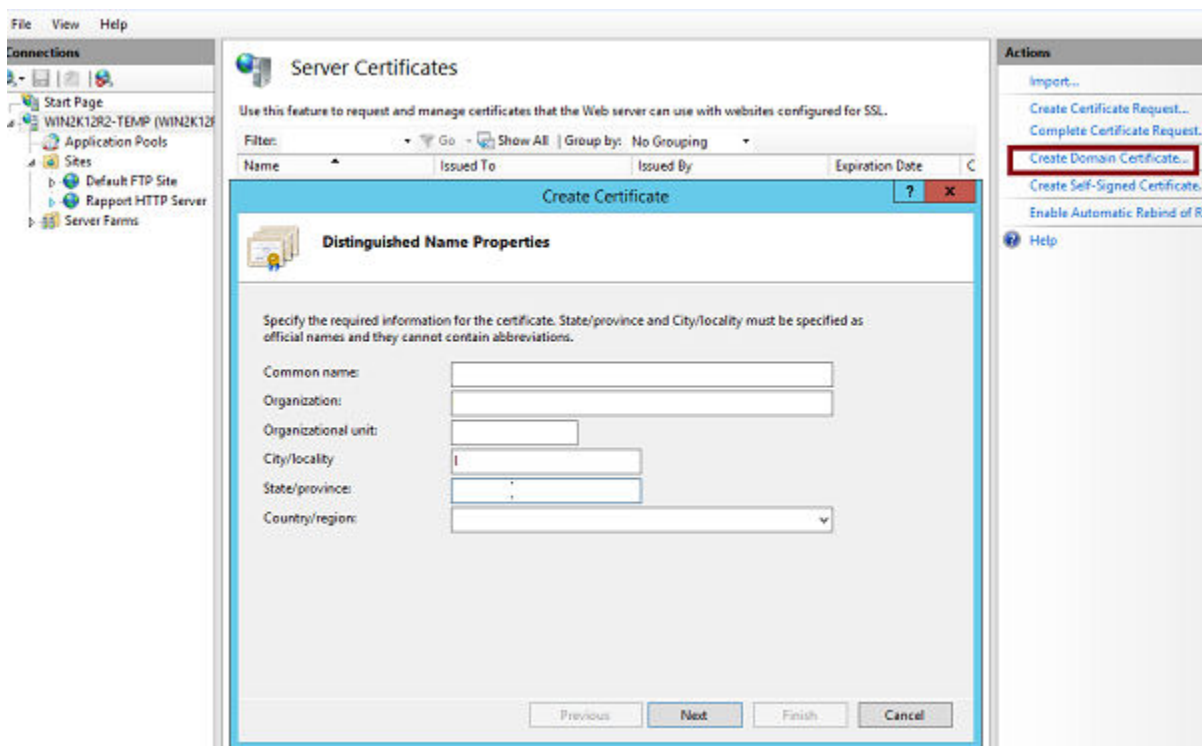


Figura 62. Certificados de servidor

La comunicación entre el servidor proxy de ARR y los servidores de administración de WDM debe realizarse en el protocolo HTTPS. Por lo tanto, debe desactivar la función de descarga de-SSL y configurar SSL en cada servidor de administración de WDM por separado. Si utiliza un certificado autofirmado para configurar SSL en el servidor de administración de WDM, importe este certificado al Almacenamiento de autoridades de certificado raíz confiable de una computadora local en el servidor proxy de ARR, siguiendo los pasos disponibles en el sitio web de Microsoft: support.microsoft.com. ARR de IIS requiere que haya un certificado de confianza entre ARR y el servidor de backend; de lo contrario, devolverá un error de seguridad y se rehusará a enrutar hacia el servidor de backend.

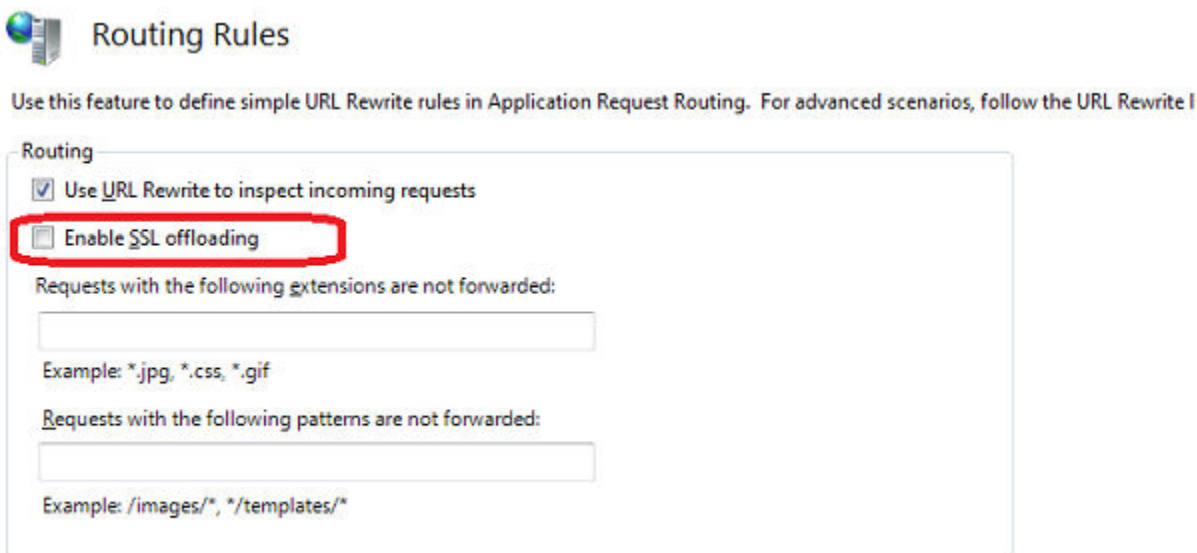


Figura 63. Reglas de enrutamiento

Configurar las propiedades de la granja de servidores para la solicitud de enrutamiento de aplicaciones

Después de crear y definir la granja de servidores, deberá establecer propiedades adicionales para administrar el comportamiento de ARR.

- 1 Inicie sesión en el servidor proxy de ARR e inicie el Administrador del servidor IIS.
- 2 Seleccione la granja de servidores que creó. Se muestran las siguientes opciones en el panel de la derecha:
 - Caching (Almacenamiento en caché)
 - Health Test (Prueba de condición)
 - Load Balance (Compensación de carga)
 - Monitoring and Management (Monitoreo y administración)
 - Proxy
 - Routing Rules (Reglas de enrutamiento)
 - Server Affinity (Afinidad del servidor)
- 3 Seleccione **Caching** (Almacenamiento en caché).
 - a Deseleccione la opción **Enable disk cache** (Activar caché en disco) para deshabilitar el almacenamiento en caché.
 - b Establezca **Memory cache duration** (Duración de la memoria caché) en 0.
- 4 Seleccione **Health Test** (Prueba de condición).
 - a Ingrese el nombre de dominio completo (FGDN) del servidor proxy de ARR en el campo **URL**. El valor debe ser: **https://<IP del proxy>[FGDN]/hapi/ping**. Esta es la dirección URL que utiliza ARR para enviar solicitudes al servidor de administración de WDM a fin de comprobar la condición de una determinada granja de servidores.
 - b Establezca el período de intervalo después del cual la Prueba de condición de ARR repetirá este control. El valor predeterminado es 30 segundos. Puede establecerlo en 180 segundos.
 - c Establezca el período de espera de la URL especificada. Este es el período durante el que, si el servidor no responde, se marcará como **Unhealthy** (En mal estado).

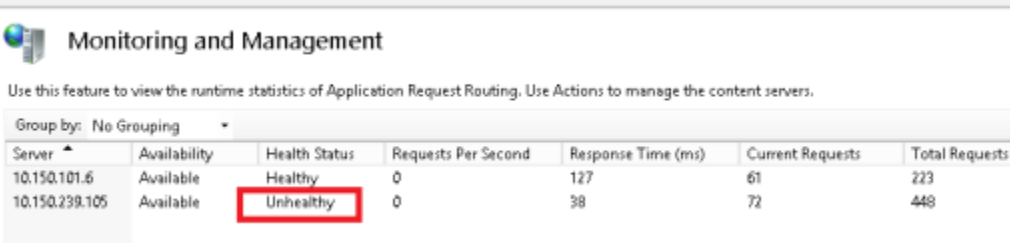
- d Establezca **Acceptable Status codes** (Códigos de estado aceptables) en **200-399**. Si la URL de la condición devuelve un código de estado que no coincide con el valor de **Acceptable Status codes** (Códigos de estado aceptables), ARR marcará a este servidor como en mal estado.
 - e Establezca el valor de texto **Server Healthy** (Servidor en buen estado) en el campo **Response Match** (Coincidencia de respuesta). El texto de **Response Match** (Coincidencia de respuesta) se verifica contra la entidad de respuesta de cada servidor y, si la respuesta de un servidor no contiene la cadena especificada en la coincidencia de respuesta, se marca el servidor como en mal estado.
 - f Haga clic en **Verify URL** (Verificar URL). Tiene que aprobarse para todos los servidores de administración de WDM de la granja de servidores.
- 5 Cambie el algoritmo **Load Balance** (Equilibrio de carga).
 - a Seleccione **Server variable hash** (Hash variable del servidor) en la lista desplegable **Load balance algorithm** (Algoritmo de equilibrio de carga).
 - b Ingrese el valor **Server Variable** (Variable del servidor) `HTTP_WDM_X_USER`.
 - c Haga clic en **Apply** (Aplicar).
 - 6 Haga doble clic en la opción **Monitoring and Management** (Monitoreo y administración) para ver el estado de la condición del servidor de administración de WDM y otras estadísticas. Puede definir el estado a Healthy (En buen estado) manualmente.
 - 7 Haga doble clic en **Proxy** para configurar el proxy:
 - a Cambie el valor de **Response buffer threshold** (Umbral de búfer de respuesta) a 0.
 - b Deseleccione la opción **Keep Alive** (Mantener activo).
 - c Cambie la versión **HTTP** a **HTTP/1.1**.
 - d Seleccione la opción **Reverse rewrite host in response headers** (Revertir reescritura de host en encabezados de respuesta).
 - 8 Haga doble clic en **Routing Rules** (Reglas de enrutamiento).
 - a Haga clic en **URL Rewrite** (Reescribir URL) en el panel de **Actions (Acciones)**.
 - b En la página **Edit Inbound Rule** (Editar regla de entrada), establezca **Pattern** (Patrón) en `(webui|hapi)/*`.

Este paso garantiza que el servidor proxy de ARR enviará solo las solicitudes de URL que se dirijan del servidor de administración de WDM a la granja de servidores.

Ya están configuradas las propiedades de la granja de servidores.

Iniciar sesión en el navegador del WebUI

- 1 Inicie sesión en la WebUI mediante la IP o FQDN del proxy en la URL del navegador.
- 2 Cuando el servidor en el que inició sesión se encuentra en mal estado según la prueba de condición mencionada anteriormente, la sesión de WebUI se cerrará.



Server	Availability	Health Status	Requests Per Second	Response Time (ms)	Current Requests	Total Requests
10.150.101.6	Available	Healthy	0	127	61	223
10.150.239.105	Available	Unhealthy	0	38	72	448

Figura 64. Monitoreo y administración

- 3 Vuelva a iniciar sesión para conectarse al otro servidor en buen estado de backend.

Instalar manualmente la base de datos de WDM por medio de scripts

En esta sección se indican los scripts de base de datos compatibles con Wyse Device Manager (WDM) y los detalles de funcionalidad relacionados.

Temas:

- [Requisitos](#)
- [Forma sugerida de instalar la base de datos de WDM](#)
- [Archivos de script](#)

Requisitos

Soporte para la base de datos de WDM existente

La instalación de WDM es compatible con SQL Server 2008. La base de datos contiene todos los objetos de SQL Server como tablas, vistas, procedimientos almacenados, etc. El instalador de WDM almacena la base de datos en la carpeta correspondiente (el valor predeterminado es: `C:\Program Files (x86)\Wyse\WDM\Database`) y se conecta a la misma máquina del servidor donde debe instalar WDM.

A continuación, el instalador actualiza los detalles del servidor, los detalles de usuario, los detalles de configuración del repositorio de software, etc., en la máquina del servidor.

Forma sugerida de instalar la base de datos de WDM

Se utilizan scripts para instalar base de datos de la versión WDM 5.7.3.

Requisito previo: antes de ejecutar los scripts, se debe crear la carpeta de ruta de la base de datos y se debe desactivar el firewall en el servidor de la base de datos.

ⓘ **NOTA:** Se deben ejecutar los siguientes scripts en el mismo orden en el que se mencionan. Si no es así, debe eliminar la base de datos y repetir todo el proceso de nuevo.

Archivos de script

Se utilizarán los siguientes archivos de script de base de datos para instalar la base de datos de WDM 5.7.3:

- `CreateDatabase.sql`
- `Schema&User.sql`
- `Tables.sql`
- `Userdefinedtables.sql`
- `Views.sql`
- `Stored_Procedures.sql`
- `Default_Table_Data.sql`

· CustomizeScript.sql

CreateDatabase.sql

Para crear la base de datos manualmente, ejecute el siguiente script:

ⓘ | NOTA: Aquí se mencionan los scripts de base de datos con el propósito de personalización.

```
CREATE DATABASE [RapportDB]
ON PRIMARY
(NAME = N'Rapport_dat', FILENAME = N'C:\Program Files (x86)\Wyse\WDM\Database\Rapport4.MDF',
SIZE = 42496KB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%)
LOG ON
(NAME = N'Rapport_log', FILENAME = N'C:\Program Files (x86)\Wyse\WDM\Database\Rapport4.LDF',
SIZE = 768KB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%)
GO
```

- 1 El archivo de script contiene una base de datos RapportDB que crea scripts.
- 2 El usuario o el administrador pueden cambiar la ruta de archivo. La ruta predeterminada del archivo es C:\Program Files (x86)\Wyse\WDM\Database.

ⓘ | NOTA: Compruebe la carpeta mencionada anteriormente para verificar el paso. Esta carpeta debe contener Rapport4.mdf y Rapport4.ldf.

Schema&User.sql

Para crear una cuenta de usuario, ejecute el script. Puede agregar y asignar permisos a cualquier cuenta de usuario.

- 1 El archivo de script contiene los detalles acerca de la creación del esquema y el rol del usuario.
- 2 Los valores predeterminados son esquema rapport y usuario rapport. Si desea cambiar el usuario de acceso de WDM, puede hacerlo desde aquí.

Tables.sql

Este archivo de script contiene scripts para todos los objetos y las limitaciones de la tabla.

ⓘ | NOTA: Los cambios personalizados no están incluidos en este archivo.

Userdefinedtables.sql

Este archivo de script contiene scripts para todos los objetos de la tabla definidos por el usuario.

ⓘ | NOTA: Los cambios personalizados no están incluidos en este archivo.

Views.sql

Este archivo de script contiene scripts para todos los objetos de visualización.

ⓘ | NOTA: Los cambios personalizados no están incluidos en este archivo.

Stored_Procedures.sql

Este archivo de script contiene scripts para todos los objetos de procedimientos almacenados.

ⓘ | NOTA: Los cambios personalizados no están incluidos en este archivo.

Default_Table_Data.sql

Este archivo de script contiene scripts para todos los valores de datos predeterminados de la tabla, como el SO, la plataforma, el tipo de administración, los grupos predeterminados, los paquetes de software predeterminados, los detalles de Parm, etc.

ⓘ | NOTA: Los cambios personalizados no están incluidos en este archivo.

CustomizeScript.sql

Este archivo de script contiene scripts para los valores de datos personalizados.

Proporcione el nombre del servidor de la base de datos mientras ejecuta el siguiente script. Si no ingresa el nombre del servidor, se mostrará un mensaje de error.

ⓘ | NOTA:

---- Customize Script (Personalizar script)

```
Use RapportDB
Go
SET IDENTITY_INSERT [dbo].[License] ON
INSERT [dbo].[License]
([LicenseID], [Sales], [UnActivated], [Code], [License], [Utilize], [NumberOfClients],
[VendorID])
VALUES
(1, N'7V931PHY08K01LZHYXWKKP6GQ1', N'BR69T51SSP500PFW9W4R0Z0TL5', NULL, NULL, NULL, NULL, NULL)
SET IDENTITY_INSERT [dbo].[License] OFF
GO
SET IDENTITY_INSERT [dbo].[sysHash] ON
INSERT [dbo].[sysHash] ([ID], [Hash]) VALUES (2,
0x4458473935334D31513034525254524643475338343442485836)
SET IDENTITY_INSERT [dbo].[sysHash] OFF
Go
Begin
Declare @DBServerName varchar(200) = ''
Set @DBServerName = ''
If (@DBServerName is null or @DBServerName = '')
Begin
RAISERROR(N'Database Server Name Should not be Empty...', 16, 1)
End
Else
Begin
SET IDENTITY_INSERT [dbo].[Install] ON
INSERT [dbo].[Install]
([InstallID], [Module], [ServerName], [UserName], [Installed], [Status], [Information],
[RegKey], [RegName], [RegValue], [LatestHFID], [SiteID], [SiteName])
VALUES
(0, N'Rapport4DB', @DBServerName, N'administrator', GetDate(), N'MASTER', NULL, NULL, NULL,
NULL, N'00HF05070001516', 0, NULL)
SET IDENTITY_INSERT [dbo].[Install] OFF
End
End
Go
```


Solución de problemas

En esta sección se describe cómo solucionar los problemas que pueden surgir cuando instale o actualice WDM.

Temas:

- [Error de instalación de .NET Framework en Windows 2012 y Windows Server 2016](#)
- [Falla al conectar la base de datos](#)
- [Error al instalar la base de datos de WDM en una configuración distribuida](#)
- [Falla de instalación de la base de datos después de la desinstalación manual de SQL Server Express 2014](#)
- [Después de actualizar de WDM 5.5.1 a WDM 5.7, el repositorio de software no es seguro](#)
- [Solución de problemas después de la implementación](#)
- [Solución de problemas del equilibrio de carga](#)
- [Problema de configuración del ambiente de nube](#)
- [Error en la instalación de WDM en la configuración de actualización](#)

Error de instalación de .NET Framework en Windows 2012 y Windows Server 2016

Problema: la instalación de .NET Framework 3.5 arroja un error en Windows Server 2012 y Windows Server 2016 con el código de error 0x800F0906

Resolución:

Método 1:

- 1 Inicie sesión en el sistema donde instaló Windows Server 2012 y Windows Server 2016, e inicie el Administrador de servidores.
- 2 Instale las funciones de .NET Framework 3.5 utilizando el asistente **Add Roles and Features** (Agregar roles y funciones) en el Administrador de servidores.
- 3 Durante la instalación, especifique una ruta de origen alternativa mediante el vínculo ubicado en la parte inferior del asistente.

Método 2:

Desde el símbolo del sistema, utilice el DISM para especificar el parámetro de ruta de los archivos de origen:

Por ejemplo, si **D:** fuera el medio de DVD de Windows Server, la ruta de los archivos de origen sería: `DISM/Online/Enable-Feature/FeatureName:NetFx3ServerFeatures/FeatureName:NetFx3/Source:D:\Sources\sxs`

Método 3:

- 1 Inicie sesión en el sistema donde instaló Windows Server 2012 y Windows Server 2016, e inicie el Administrador de servidores.
- 2 Instale **Server Role Windows Server Update Services (WSUS) (Windows Server Update Service [WSUS] del rol del servidor)** mediante el asistente **Add Roles and Features** (Agregar roles y funciones) del Administrador del servidor.
- 3 Desde el símbolo del sistema, utilice el DISM para especificar el parámetro de ruta de los archivos de origen: `DISM/Online/Enable-Feature/FeatureName:NetFx3ServerFeatures/FeatureName:NetFx3`

- 4 Asegúrese de que Windows Update Service se esté ejecutando y que se pueda conectar el almacenamiento de Windows Update desde donde los componentes necesarios se pueden recuperar.

Falla al conectar la base de datos

Problema: falla al conectar la base de datos en Windows 2012 Server, con SQL Server 2012.

Resolución:

Ejecute SQL Service 'MSSQLSERVER' utilizando la cuenta 'LocalSystem' en el sistema donde instalará WDM.

Intente de nuevo instalar WDM.

Error al instalar la base de datos de WDM en una configuración distribuida

Problema: cuando se instala la base de datos de WDM en un sistema separado que tenga instalada la versión compatible de SQL Server, es posible que se muestre el siguiente error al iniciar **Setup.exe**: *Setup was unable to initialize the required libraries* (La configuración no pudo inicializar las bibliotecas requeridas).

Solución: asegúrese de que esté instalado **Microsoft Visual C++ Redistributable 2008, versión 9.0.21022**. Deberá navegar a **Start (Iniciar) > Control Panel (Panel de control) > Programs (Programas)** para ver si está instalada la versión Redistributable. Si no está instalada, debe instalarla manualmente, mediante la ejecución del **vcredist_x86.exe** disponible en la carpeta **Prereq** (Prerrequisitos) del instalador de WDM.

Falla de instalación de la base de datos después de la desinstalación manual de SQL Server Express 2014

Problema: la instalación de la base de datos de WDM falla una vez que desinstala manualmente el SQL Server Express 2014 existente, y utiliza la opción **Install New Database** (Instalar nueva base de datos) en el instalador.

Resolución: para resolver este problema:

- 1 Desinstale SQL Server Express 2014 R2 desde Add\Remove Programs (Agregar o quitar programas).
- 2 Inicie la ventana **Services** (Servicios) desde **Control Panel (Panel de control) > Administrative Tools (Herramientas administrativas)**.
- 3 Elimine el servicio **MSSQL\$RapportDb**.
- 4 Elimine **MSSQL12.RAPPORTDB** de la carpeta de instalación de SQL Server Express.
- 5 Elimine la entrada del registro **RapportDB** desde **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names\SQL**.
- 6 Elimine la entrada del registro **MSSQL10_50.RAPPORTDB** desde **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server**.
- 7 Elimine la entrada del registro **RAPPORTDB** desde **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server**.
- 8 Reinicie el instalador de WDM.

Después de actualizar de WDM 5.5.1 a WDM 5.7, el repositorio de software no es seguro

Problema: si selecciona WEBUI durante la actualización, el servidor de administración estará configurado para Https, pero el instalador no configurará el repositorio de software de WDM.

Solución: configure manualmente el repositorio de software a HTTPs en la interfaz gráfica de usuario de WDM. Para configurar manualmente, vaya a **Configuration Manager Software Repository** (Repositorio de software de administrador de configuración).

Solución de problemas después de la implementación

Problema: HTTP Error 404.0: no encontrado. Se agregará el Web.config de HApi con un módulo de enrutamiento si este está ausente:

Solución: agregue el Web.config de HApi con un módulo de enrutamiento de URL como se indica a continuación:

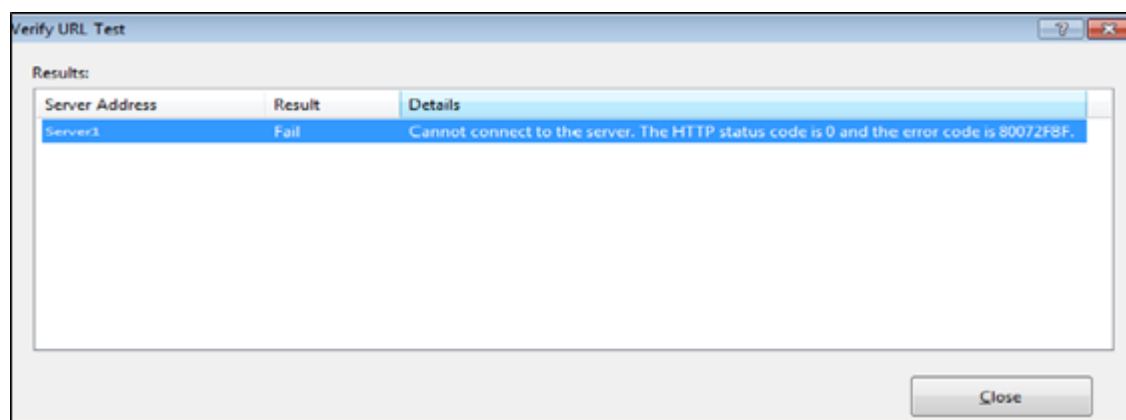
```
<system.webserver>
<modules>
<remove name= "urlroutingmodule-4.0"/>
<add name= "urlroutingmodule-4.0" type="system.web.Routing.urlroutingmodule" precondition="" />
</modules>
```

Solución de problemas del equilibrio de carga

En esta sección se describe cómo solucionar algunos problemas que pueden surgir en la configuración del equilibrio de carga.

Falla de la función de prueba de condición en el proxy de ARR con SSL

Problema: si el proxy de ARR no confía en el certificado digital del servidor de backend, es posible que falle la prueba de condición con el código de error 80072F8F.



Solución: importe el certificado que se utiliza para configurar SSL en el servidor de administración de WDM al **Trusted Root Certificate Authorities store for a local computer (Almacenamiento de autoridades de certificado raíz confiable de una computadora local)** en el sistema proxy de ARR; para ello puede consultar technet.microsoft.com.

El proxy de ARR arroja el código de error HTTP 502.3

Problema: el proxy de ARR devuelve el código de error HTTP 502.3 a los agentes de WDM de versiones anteriores (HAgents) que no envían la etiqueta **HTTPHEADSUPP=2** cuando se registran. Si el HAgent no envía la etiqueta **HTTPHEADSUPP=2** durante el proceso de registro, el servidor de administración no enviará el encabezado del código de estado HTTP (200 es correcto) en la respuesta; este es el motivo por el cual se produce el error. Solo los clientes que envían el valor **2** son compatibles en la configuración del equilibrador de carga.

Solución: puede ejecutar la siguiente consulta en la base de datos de WDM y leer el valor:

```
SELECT [HttpHeadSupp]
FROM [ClientNetwork]
where [MAC] = <ClientMac>
```

El proxy de ARR arroja el código de error HTTP 502.4

Problema: el servidor proxy de ARR puede devolver el código de error HTTP 502.4 cuando cualquiera de los servidores de administración (HServers) no está disponible. El estado de la condición de todos los HServers de la **granja de servidores** se puede establecer **Unhealthy** (En mal estado), debido a que las pruebas de condición configuradas han fallado.

Solución: para corregirlo:

- 1 Inicie sesión en el servidor proxy de ARR e inicie el Administrador del servidor IIS.
- 2 Seleccione la granja de servidores que creó y, en el panel derecho, seleccione **Monitoring and Management** (Monitoreo y administración).
- 3 Seleccione el HServer y, en el panel de **Action (Acciones)**, seleccione **Set Server as Healthy** (Establecer servidor como en buen estado).
- 4 Si la carga del HServer es alta, intente aumentar los valores de **interval** (intervalo) y **time-out** (tiempo de espera) en la función **Health Test** (Prueba de estado).

Activar la descarga de SSL en el proxy

El equilibrio de carga solo es compatible en la configuración de HTTPS. Para efectuar la depuración de errores, si desea consultar la respuesta del servidor de administración (HServer) en una captura de **Wireshark**, puede cambiar la comunicación del proxy del HServer a HTTP.

- 1 Inicie sesión en el servidor proxy de ARR e inicie el Administrador de IIS.
- 2 Haga doble clic en la función **Routing Rules** (Reglas de enrutamiento) y seleccione la configuración **Enable SSL offloading** (Activar la descarga de SSL).
- 3 Active las vinculaciones de HTTP y HTTPS en el sitio web, en las máquinas del HServer, y no seleccione **Require SSL** (Requerir SSL) en la **SSL Settings** (Configuración de SSL).

..

Transición indefinida durante la instalación

Problema: el proceso se efectúa indefinidamente cuando instala Microsoft Visual C++ Redistributable o Microsoft SQL Express 2008. Los sistemas operativos compatibles son Windows 2012 Standard y Windows 2012 R2.

Solución: abra el Administrador de tareas y compruebe si el proceso "**Windows Modules Installer Worker**" (Trabajo del instalador de módulos de Windows) se está ejecutando en su thin client o no. Si este proceso se está ejecutando, debe finalizarlo para reanudar la instalación. Debe reiniciar el thin client después de haber finalizado la instalación.

Problema del equilibrador de carga

Problema: el servidor proxy no responde si la dirección IP V6 está activada.

Solución: desactive la dirección IP V6 en la configuración del equilibrador de carga.

Actualizar WDM en Windows 2008 SP2 de 32 bits

Problema: para actualizar WDM 5.7 en Windows 2008 SP2 (32 bits), active el servicio de actualización de Windows.

Solución: para actualizar WDM 5.7 en Windows 2008 SP2 (32 bits), active el servicio de actualización de Windows para instalar la actualización KB980368. Después de instalar la actualización KB980368, desactive el servicio de actualización de Windows para instalar WDM 5.7.

Error en la instalación de la actualización de WDM

Problema: la instalación de actualización de WDM falla cuando se conecta al repositorio de software.

Solución: uno de los motivos de este problema puede ser el nombre de la computadora, ya que la configuración tiene más de 16 caracteres. Esto produce una discrepancia entre el nombre de la computadora y el de NetBIOS (truncado para 15 caracteres) para la configuración. Para confirmar este problema, verifique si las variables del sistema mencionadas son diferentes. Si es así, instale WDM en una configuración que tenga un nombre de host de un máximo de 15 caracteres y, a continuación, vuelva a ejecutar el instalador de la actualización.

Problema de configuración del ambiente de nube

Problema: se muestra un mensaje de error en forma intermitente cuando se ejecuta el archivo `setup.exe` durante la instalación de WDM en el ambiente de nube.

Solución

- **Escenario 1: solo se muestra el mensaje de error**

Cierre el cuadro de diálogo del mensaje de error y, a continuación, ejecute el archivo `setup.exe` otra vez.

- **Escenario 2: se muestra un mensaje de error junto con la pantalla de bienvenida que se ejecuta en segundo plano**

Cierre el cuadro de diálogo del mensaje de error y la pantalla de bienvenida y, a continuación, ejecute el archivo `setup.exe` otra vez.

Error en la instalación de WDM en la configuración de actualización

Problema: durante la instalación de WDM, si utiliza usuarios de la base de datos distintos al usuario predeterminado, no podrá continuar con la instalación de WDM en la configuración de actualización. Se muestra el mensaje de error **Unable to proceed with the installation, aborting installation** (No es posible continuar con la instalación, anulando la instalación).

Solución:

- Abra la interfaz gráfica de usuario de WDM.
- Haga clic con el botón secundario en **Configuration Manager** (Administrador de configuración) y seleccione **Utilities (Utilidades) > Database Credential Manager (Administrador de credenciales de bases de datos)**.
- Aparece un mensaje de aviso. Haga clic en **OK** (Aceptar).
- Ingrese el nombre de usuario y la contraseña que utilizó cuando instaló WDM. Haga clic en **OK** (Aceptar) para continuar.
- Ahora cierre la interfaz gráfica de usuario de WDM y continúe con la instalación.
- Después de la instalación, ejecute nuevamente **Database Credential Manager** (Administrador de credenciales de base de datos) disponible en la ruta de instalación (C:\Program Files (X86)\Wyse\WDM\Utilities\Database).
- Proporcione su nombre de usuario y la contraseña que utilizó al instalar WDM y, a continuación, reinicie el servidor.