HITACHI
Inspire the Next

Hitachi IT Operations Analyzer

Guía de introducción: Apéndice de configuración de dispositivos

ENLACES FASTFIND

Hitachi Data Systems

MK-90IOS006ES-12

Contenido

Prólogo

Esta guía es un apéndice a la Guía de introducción de Hitachi IT Operations Analyzer. Le ayudará con las tareas de preinstalación para configurar los componentes de red que pretende supervisar en su sitio.

Este prólogo incluye la siguiente información:

Destinatarios

Este documento está destinado a los administradores de sistemas y otros usuarios responsables de configurar y utilizar Hitachi IT Operations Analyzer.

Versión del producto

Esta revisión de documento se aplica a IT Operations Analyzer versión 3.3.1.

Nivel de revisión del documento

Esta sección ofrece un historial de las revisiones llevadas a cabo en este documento.

Revisión	Fecha	Descripción
MK-90IOS006ES-00	Marzo de 2010	Versión inicial
MK-90IOS006ES-01	Octubre de 2010	Revisión 1, reemplaza a la MK-90IOS006ES-00
MK-90IOS006ES-02	Abril de 2011	Revisión 2, reemplaza a la MK-90IOS006ES-01
MK-90IOS006ES-03	Enero de 2012	Revisión 3, reemplaza a la MK-90IOS006ES-02
MK-90IOS006ES-04	Marzo de 2013	Revisión 4, reemplaza a la MK-90IOS006ES-03
MK-90IOS006ES-12	Julio de 2013	Revisión 12, reemplaza a la MK-90IOS006ES-04

Documentos relacionados

- *Guía de introducción de Hitachi IT Operations Analyzer: Apéndice de configuración de dispositivos*, MK-90IOS006ES
- Ayuda de Hitachi IT Operations Analyzer
- Notas de la versión, RN-99IOS004

Convenciones del documento

Los siguientes símbolos se utilizan para advertirle de información importante.

Símbolo	Significado	Descripción
	Consejo	Los consejos ofrecen información útil, instrucciones y sugerencias para realizar tareas de forma más eficaz.
	Nota	Las notas resaltan o complementan puntos importantes del texto principal.

En este documento se utilizan las siguientes convenciones tipográficas:

Convención	Descripción
Negrita	Indica el texto en una ventana (excepto el título de la misma), incluidos los menús, las opciones de menú, los botones, los campos y las etiquetas. Ejemplo: Haga clic en **Aceptar**.
Cursiva	Indica una variable, que es un marcador de posición del texto real proporcionado por el usuario o el sistema. En el caso de la información de versión, la x cursiva representa todas las versiones siguientes. Ejemplos: • Copie *archivo-origen archivo-destino*. • Kernel versión 2.6.*x*. **Nota**: las llaves angulares (< >) también se utilizan para indicar variables.
Código de pantalla	Indica texto mostrado en pantalla o introducido por el usuario. Ejemplo: `# pairdisplay -g oradb`
Llaves angulares	Indica una variable, que es un marcador de posición del texto real proporcionado por el usuario o el sistema. Ejemplo: `# pairdisplay -g` <group> **Nota**: la cursiva también se utiliza para indicar variables.

Referencias de productos

En este documento se hace referencia a productos VMware®.
Dichas referencias se tratan como se indica a continuación:

- Referencia al producto cuando el tipo o la versión son específicos; por ejemplo: VMware ESX 3, VMware ESX 3i, VMware ESX 4.0, etc.
- Referencia al servidor del producto cuando el tipo o la versión del servidor no son específicos: Servidor ESX.

Obtención de ayuda

Si ha adquirido este producto y tiene un acuerdo de soporte para el producto actual, recopile la siguiente información:

- El nombre de producto y el número de versión
- El nombre del sistema operativo y la revisión o número de paquete de servicio
- El número de serie de la licencia para la que está solicitando ayuda
- El contenido de los mensajes de error mostrados
- Las circunstancias del error o fallo
- Una descripción del problema y qué se ha hecho para intentar resolverlo

Tras recopilar estos datos, póngase en contacto con el centro de ayuda de Hitachi Data Systems.

A continuación encontrará un enlace al sitio Web de Hitachi Data Systems, donde puede obtener números de teléfono actualizados y otra información de contacto para el centro de ayuda de Hitachi Data Systems:

https://portal.hds.com

NOTA: Si está utilizando una versión de prueba del producto, consulte el material de autoservicio que se encuentra en el portal de IT Operations Software: http://www.itoperations.com

Comentarios

Envíenos sus comentarios acerca de este documento a: doc.comments@hds.com. Incluya el título, el número y la revisión del documento y consulte las secciones y párrafos específicos siempre que sea posible.

Gracias. (Todos los comentarios pasan a ser propiedad de Hitachi Data Systems Corporation).

1

Descripción general

Antes de instalar IT Operations Analyzer o de utilizar el Asistente de detección, es importante comprobar y preparar el entorno. Esto incluye verificar la configuración que se utiliza en su entorno y recopilar la información que será necesaria más adelante, durante los procedimientos de configuración.

Preparación del entorno

La Tabla 1-1 describe las tareas necesarias y las recomendadas u opcionales en función del entorno y los objetivos de supervisión.

Cada tarea incluye la referencia al capítulo que contiene los detalles.

Tabla 1-1: Preparaciones del entorno

Tareas requeridas	
Tarea	**Detalles**
En el servidor de gestión (el equipo en el que está instalado IT Operations Analyzer), compruebe la configuración de DCOM para WMI.	Se evitan errores de conexión remota WMI porque la ejecución remota de DCOM no está permitida. Consulte el Capítulo 2, Preparación de WMI para servidores Windows.
Si el sitio utiliza alguno de los objetivos de supervisión siguientes, deberá configurarlos:	Los objetivos de supervisión son los servidores, el almacenamiento y los conmutadores que el sitio pretende supervisar.
• Conmutadores IP	IT Operations Analyzer utiliza SNMP para supervisar conmutadores IP. • Activar SNMP • Obtener la cadena de comunidad de SNMP • Obtener la dirección IP Consulte el Capítulo 5, Preparación de SNMP para conmutadores IP.
• Hitachi 9500V	IT Operations Analyzer supervisa Hitachi 9500V mediante el agente SMI-S de Device Manager. El rendimiento no se supervisa. Instale Device Manager 5.9 o posterior y active SMI-S. Consulte el Capítulo 6, Preparación del almacenamiento de Hitachi.
• Hitachi USP VM	IT Operations Analyzer supervisa Hitachi USP VM mediante el agente SMI-S de Device Manager. Instale Device Manager 6.2 o posterior y active SMI-S. Consulte Capítulo 6, Preparación del almacenamiento de Hitachi.

• Otros almacenamientos, conmutadores FC	IT Operations Analyzer utiliza SMI-S para detectar y supervisar otros almacenamientos y conmutadores FC. Instale el agente SMI-S y obtenga lo siguiente:
	• Dirección IP
	  • Agente SMI-S (proxy): utilice una dirección IP del servidor SMI-S para el conmutador.
	  • Agente SMI-S (integrado): utilice la misma dirección IP para el conmutador FC.
	• Identificador de usuario y contraseña
	• Número de puerto
	• Espacio de nombres
	Compruebe también el estado de SSL.
	Consulte el Capítulo 7, Revisión de la preparación de SMI-S.
	Al especificar las credenciales de la serie NetApp FAS o gestionar versiones de Linux con un agente SMI-S, recomendamos especificar **http** para la opción **SSL**, dentro del cuadro de diálogo **Añadir credencial**.

Tabla 1-1: Preparaciones del entorno

Tareas recomendadas	
Tarea	**Detalles**
Comprobar los objetivos de supervisión: • Servidores Windows	IT Operations Analyzer utiliza WMI para supervisar servidores Windows. Para acceso remoto a WMI, DCOM debe estar activo en el servidor Windows y en el servidor de gestión. Si DCOM no está activo, puede que el software no sea capaz de detectar o supervisar servidores Windows. Además, instale la plataforma Integration Service en una máquina virtual si su sitio va a supervisar una máquina virtual Hyper-V. Consulte el Capítulo 2, Preparación de WMI para servidores Windows.
• Servidores Linux/Solaris	IT Operations Analyzer utiliza SSH para detectar servidores Linux y Solaris. También utiliza la autenticación por contraseña (no la autenticación mediante certificados) para supervisarlos. Compruebe que: • El servicio SSH esté instalado y en ejecución. • La conexión SSH2 esté activa. • Se permite la autenticación de contraseña. Consulte el Capítulo 3, Preparación de SSH para servidores Linux/Solaris.
• Servidores VMware ESX	IT Operations Analyzer no puede supervisar correctamente servidores Windows o Linux en máquinas virtuales a menos que se instalen herramientas VMware. Verifique la versión admitida: • VMware ESX 3 • VMware ESX 3.5 • VMware ESX 3i • VMware ESX 3.5i • VMware ESX 4 • VMware ESX 4i • VMware ESX 4.1 • VMware ESX 4.1i • VMware ESX 5 • VMware ESX 5i • VMware ESX 5.1 • VMware ESX 5.1i Instale también herramientas VMware en máquinas virtuales. Consulte el Capítulo 4, Preparación de servidores VMware ESX.
• Hitachi AMS/WMS/SMS series y Hitachi Unified Storage series	Compruebe si la autenticación de cuenta o la protección con contraseña están activadas. Si la autenticación de cuenta o la protección con contraseña están activadas, IT Operations Analyzer necesita el identificador de usuario y la contraseña. Consulte el Capítulo 6, Preparación del almacenamiento de Hitachi.

Tabla 1-1: Preparaciones del entorno

Tareas recomendadas	
Tarea	**Detalles**
• Servidores Dell	Puede obtener información específica del servidor Dell mediante el uso del complemento integrado Dell Chassis. Podrá instalar "Dell Chassis (Windows)" como un complemento de Windows o "Dell Chassis (Linux)", como un complemento de Linux. A continuación se describen los requisitos del sistema para los servidores Dell supervisados por IT Operations Analyzer: • Las versiones 6.1.0 o 6.2.0 de Dell OpenManage Server Administrator (OMSA) deben ejecutarse en el servidor o servidores Dell supervisados. • El agente SNMP debe estar instalado y ejecutándose en el servidor o servidores Dell supervisados. • "Dell Chassis (Windows)" requiere que el servicio DSM SA Data Manager se ejecute en un servidor de Microsoft Windows. • "Dell Chassis (Linux)" requiere que el proceso dsm_sa_datamgrd o dsm_sa_datamgr32d se ejecute en un servidor Red Hat Enterprise Linux. Consulte las tareas de configuración relacionadas con los servidores Linux o Microsoft Windows, según los requisitos específicos de los sistemas operativos de los servidores Dell basados en Linux o en Windows respectivamente.
Tareas opcionales	
Tarea	**Detalles**
Comprobar los objetivos de supervisión: • Servidores Windows	IT Operations Analyzer utiliza WMI para supervisar servidores Windows. Windows 2003 debe tener FCInfo instalado para proporcionar datos de adaptador de bus anfitrión FC a través de WMI. Si sus servidores Windows utilizan un adaptador de bus anfitrión FC, instale FCInfo. Consulte el Capítulo 2, Preparación de WMI para servidores Windows.
• Conmutadores IP	Permita el envío de capturas SNMP. IT Operations Analyzer puede recibir capturas SNMP de conmutadores IP. Esta tarea es opcional porque IT Operations Analyzer puede supervisar conmutadores IP sin capturas, utilizando el sondeo. Consulte el Capítulo 5, Preparación de SNMP para conmutadores IP.

2

Preparación de Hyper-V y WMI para servidores Windows

IT Operations Analyzer utiliza WMI para supervisar servidores Windows. Para acceso remoto a WMI, DCOM debe estar activo en el servidor Windows y en el servidor de gestión. Si DCOM no está activo, puede que el software no sea capaz de detectar o supervisar servidores Windows. Este capítulo describe la preparación de los entornos Hyper-V y WMI.

Preparación de Hyper-V

Si el sitio planea supervisar un servidor Windows o Linux instalado en la máquina virtual Hyper-V, deberá instalar la plataforma "Integration Service" en el SO de la máquina virtual. De lo contrario, si la plataforma Integration Service no está instalada, no se mostrará correctamente ni el estado de la máquina virtual ni la relación entre el equipo anfitrión y el SO invitado en IT Operations Analyzer.

NOTA: La configuración de la máquina anfitriona Hyper-V es parecida a las preparaciones del servidor Windows. Como referencia, consulte la siguiente sección.
También, si KB2264080 no se aplica a Windows Server 2008 R2 para el sistema operativo anfitrión del destino de gestión, no será posible conectar al sistema operativo invitado del destino de gestión Hyper-V cuando:
- existan muchas sesiones en la MV de Hyper-V.
- se transmita una gran cantidad de datos a la MV de Hyper-V.

Preparación de WMI para servidores Windows

IT Operations Analyzer detecta y supervisa los servidores Windows mediante Windows Management Instrumentation (WMI). Las siguientes secciones describen las tareas asociadas a la activación del acceso remoto a WMI y la configuración de servidores Windows 2003/2003 R2 que utilizan adaptadores de bus anfitrión (HBA) FC.

NOTA:

- Para los nodos de Microsoft Hyper-V y los de Windows Server puede obtener la información de rendimiento acerca del disco duro mediante la conexión FC, iSCSI y local. No se puede obtener información de rendimiento acerca del CD-ROM o la memoria USB. Si no se puede obtener la información de rendimiento, entonces en la ficha **Rendimiento** del módulo **Supervisión**, el icono de la métrica del rendimiento indica Desconocido.
- Para Windows Server 2003, aplique KB953955. De lo contrario, se podrían notificar valores incorrectos para el nombre de la CPU.

Preparación del servidor de gestión

Para supervisar los ordenadores Windows o servidores de almacenamiento, DCOM se debe activar en el servidor de gestión. Consulte el Cómo permitir la ejecución remota de DCOM en la página 2-4.

Preparación de ordenadores y servidores de almacenamiento de Windows

La Tabla 2-1 muestra la información necesaria para la supervisión.

Tabla 2-1: Información para la conexión a servidores Windows

Elemento	Detalles
Dirección IP	Dirección IP del servidor Windows que se va a supervisar.
Nombre de usuario	Cuenta de usuario con privilegios de administrador del servidor Windows que se va a supervisar.
Nombre de dominio	Nombre de dominio del usuario (si la cuenta de usuario descrita anteriormente es un usuario de dominio).
Contraseña	Contraseña asociada al nombre de usuario.

Para supervisar servidores Windows, DCOM debe estar validado y debe agregarse cualquier excepción de WMI al firewall de Windows. Si piensa adquirir información FC HBA mediante el uso de Windows Server 2003 o Windows Server 2003 R2, a continuación, instale la herramienta de información del canal de fibra (fcinfo).

Instalación de la herramienta de información del canal de fibra (fcinfo)

Si se utiliza un adaptador de bus anfitrión (HBA) para conectar dispositivos de disco SAN de canal de fibra al servidor que desea supervisar, se necesita la herramienta de información de canal de fibra (fcinfo). Admite la API de HBA de canal de fibra en Windows y proporciona funciones compatibles con WMI. Consulte el sitio Web de Microsoft Download Center: http://www.microsoft.com/downloads/details.aspx?FamilyID=73d7b879-55b2-4629-8734-b0698096d3b1&displaylang=en

Adición de una excepción de WMI al firewall de Windows

Puede cambiar permisos desde el símbolo del sistema de Windows o mediante el editor de directivas de grupo. Las siguientes instrucciones se aplican a Windows Server 2003. Para obtener más información sobre Windows Server 2008 o Windows Server 2012, consulte Aplicación de la configuración de Windows Server 2008 o Windows Server 2012 en la página 2-5.

Mediante el símbolo del sistema de Windows:

1. Después de iniciar sesión en el servidor, haga clic en **Inicio** y, a continuación, en **Ejecutar**.

NOTA: En Windows Server 2012, los pasos para navegar a los comandos **Inicio** y **Ejecutar** son diferentes.

2. En el símbolo del sistema, introduzca **cmd** y haga clic en **Aceptar**.
3. En el símbolo del sistema, introduzca lo siguiente y pulse **Intro**:
   `netsh firewall set service RemoteAdmin enable`

Mediante un editor de directivas de grupo:

1. Después de iniciar sesión en el servidor, haga clic en **Inicio** y, a continuación, en **Ejecutar**.

NOTA: En Windows Server 2012, los pasos para navegar a los comandos **Inicio** y **Ejecutar** son diferentes.

2. Para iniciar el editor de **directivas de grupo**, introduzca **gpedit.msc** y haga clic en **Aceptar**.
3. En **Directiva de equipo local**, amplíe la carpeta **Plantillas administrativas**.
4. Amplíe las carpetas: **Red**, **Conexiones de red** y **Firewall de Windows** y, a continuación, seleccione **Perfil de dominio**.
5. En la lista de configuración, haga clic con el botón derecho en **Firewall de Windows: permitir excepción de administración remota** y, a continuación, haga clic en **Propiedades**.
6. Haga clic en **Activado** y, a continuación, en **Aceptar**.

NOTA: Consulte el sitio Web de Microsoft Developer Center para obtener información:
http://msdn2.microsoft.com/en-us/library/aa389286(VS.85).aspx

Cómo permitir la ejecución remota de DCOM

Al ejecutar dcomcnfg.exe desde el símbolo del sistema de Windows, puede iniciar el panel Servicios de componentes y comprobar el estado de DCOM.

1. Después de iniciar sesión en el servidor, haga clic en **Inicio** y, a continuación, en **Ejecutar**.

NOTA: En Windows Server 2012, los pasos para navegar a los comandos **Inicio** y **Ejecutar** son diferentes.

2. Para iniciar **Servicios de componentes**, escriba **dcomcnfg.exe** y haga clic en **Aceptar**.
3. En **Servicios de componentes**, seleccione **Equipos** y, a continuación, **Mi PC**.
4. Haga clic con el botón derecho en **Mi PC** y seleccione **Propiedades**.
5. Haga clic en la ficha **Propiedades predeterminadas**.
6. Marque la casilla **Habilitar COM distribuido en este equipo** y, a continuación, haga clic en la ficha **Seguridad COM**.
7. Para que aparezca el cuadro de diálogo **Permisos de inicio**, haga clic en **Editar límites** para **Permisos de inicio y activación**. Si no se muestra un nombre de usuario o grupo en el cuadro **Nombres de grupos o usuarios**, haga lo siguiente:
   a. Haga clic en **Agregar**.
   b. En el cuadro de diálogo **Seleccionar usuarios, equipos o grupos**, escriba el nombre de usuario o grupo en el cuadro **Escriba los nombres de objeto que desea seleccionar**. Haga clic en **Aceptar**.
   c. En el cuadro de diálogo **Permisos de inicio**, haga clic en el usuario y grupo del área **Nombres de grupos o usuarios**. En el área **Permisos de usuario**, para **Ejecución remota**, marque la casilla de la columna **Permitir**. Haga clic en **Aceptar**.

Aplicación de la configuración de Windows Server 2008 o Windows Server 2012

Si está utilizando un servidor Windows Server 2008 o Windows Server 2012, además de la configuración de servidor de Windows descrita en las secciones anteriores, se deben cumplir todas las condiciones siguientes:

- Utilizar la cuenta de administrador incorporada
- Utilizar una cuenta de usuario de dominio
- Activar la conexión remota WMI a través de una cuenta de administrador local

Activación de cuentas de administrador local para la conexión remota de WMI

Puede cambiar la configuración del control de cuentas de usuario (UAC) desde el Panel de control del ordenador objetivo de la supervisión o aplicando métodos de configuración desde el registro.

Para cambiar el UAC desde el panel de control:

1. En el menú **Inicio**, haga clic en **Panel de control**.

NOTA: En Windows Server 2012, los pasos para navegar al menú **Inicio** son diferentes.

2. Seleccione **Cuentas de usuario** y escoja **Cambiar configuración de Control de cuentas de usuario**.
3. Configure el nivel UAC en **No notificar nunca**.
4. Reinicie el ordenador.

Como otro método de supervisión de un ordenador objetivo, registre la clave **LocalAccountTokenFilterPolicy** en el Registro, y configúrela como **1**, en el ordenador objetivo de la supervisión. A continuación, desactive la opción de **filtro por UAC**, que bloquea los privilegios de administrador local durante la conexión remota de WMI.

Mediante una cuenta de administrador local, puede gestionar tanto Windows Server 2003 como Windows Server 2008 o Windows Server 2012. Si edita el registro, se puede producir un error crítico, que puede afectar seriamente a todo el sistema. Se recomienda que realice una copia de seguridad del Registro antes de editarlo.

Para obtener más información, consulte la siguiente URL, que proporciona una descripción de UAC y de las restricciones remotas en Windows Vista: http://support.microsoft.com/kb/951016/en-us

Al configurar el Registro, utilice el:

- Editor del Registro, o bien el
- Comando “reg”

Si utiliza el Editor del Registro:

1. Haga clic en **Inicio** y, a continuación, en **Ejecutar**.

NOTA: En Windows Server 2012, los pasos para navegar a los comandos **Inicio** y **Ejecutar** son diferentes.

2. En el símbolo del sistema, introduzca **regedit** y haga clic en **Aceptar**.

   Se mostrará el **Editor del registro**.

3. Busque la siguiente subclave del Registro:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
4. Si la clave **LocalAccountTokenFilterPolicy** no existe, añádala:
   a. Desde el menú **Edición**, seleccione **Nuevo** y, a continuación, **DWORD**.
   b. Escriba **LocalAccountTokenFilterPolicy** y pulse **Intro**.
5. Si el valor de **LocalAccountTokenFilterPolicy** no es **1**, cámbielo a **1**:
   a. Haga clic con el botón derecho en **LocalAccountTokenFilterPolicy** y seleccione **Modificar**.
   b. Escriba **1** en el cuadro de diálogo de entrada y, a continuación, haga clic en **Aceptar**.
6. Cierre el **Editor del Registro**.

Si utiliza el comando reg:

1. Haga clic en **Inicio** y, a continuación, en **Ejecutar**.

NOTA: En Windows Server 2012, los pasos para navegar a los comandos **Inicio** y **Ejecutar** son diferentes.

2. En el símbolo del sistema, introduzca lo siguiente:
   reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0x1 /f
3. Haga clic en **Aceptar**.

Comprobación de la existencia de un adaptador de red duplicado en el árbol Device Manager del nodo

Si existen nombres del adaptador de red duplicados en el árbol de Device Manager del nodo, IT Operations Analyzer no podrá mostrar correctamente la siguiente información de rendimiento:

- cantidad media de recepción de paquetes en red [paquete/segundo]
- cantidad media de envío de paquetes en red [paquete/segundo].

Para comprobar si aparecen nombres de adaptador de red duplicados en Device Manager:

1. Haga clic en **Inicio** > **Mi PC** > **Ver información del sistema**. Se muestra el menú emergente **Propiedades del sistema**.

NOTA: En Windows Server 2012, los pasos para navegar al menú **Inicio** son diferentes.

2. Haga clic en la pestaña **Hardware**.
3. Haga clic en **Device Manager**.
4. Inspeccione el árbol del **Administrador de dispositivos** para ver si hay nombres duplicados en la sección **Adaptadores de red**.

NOTA: Si en la lista aparecen nombres de adaptadores de red duplicados, no podrá ver la información de rendimiento relativa a la cantidad exacta media de paquetes de red enviados [paquete/segundo]. Existirá una diferencia entre el valor real y la información de rendimiento que se muestra. Conviene comprobar con su grupo de servicios de TI la posibilidad de cambiar el nombre de los adaptadores de red para evitar cualquier duplicidad.

3

Preparación de SSH para servidores Linux/Solaris

IT Operations Analyzer utiliza SSH para detectar servidores Linux y Solaris. También utiliza la autenticación por contraseña (no la autenticación mediante certificados) para supervisarlos. Este capítulo describe cómo configurar servidores Linux y Solaris.

Instalación de los paquetes requeridos

Para CentOS, es imprescindible instalar los paquetes requeridos.

Tabla 3-1: Paquete de ejemplo para añadir a CentOS

Paquete	Comandos incluidos en el paquete que ejecuta IT Operations Analyzer
smartmontools	/usr/sbin/smartctl
nfs-utils	/usr/sbin/exportfs
pciutils	/sbin/lspci
iscsi-initiator-utils	/sbin/iscsid

Para SUSE Linux 11 SP1 y SP2, es imprescindible instalar los paquetes requeridos.

Tabla 3-2: Paquete de ejemplo para añadir a SUSE Linux 11 SP1 y SP2

Paquete	Comandos incluidos en el paquete que ejecuta IT Operations Analyzer
nfs-kernel-server	/usr/sbin/exportfs

Obtención de la configuración de conexión según el método de inicio de sesión

Existen diferentes métodos de inicio de sesión utilizando SSH con los que se puede obtener información del servidor Linux o Solaris:

- Como **usuario raíz**, puede iniciar sesión directamente utilizando SSH
- Como **usuario normal**, después de iniciar sesión utilizando SSH, ejecute el comando:
  - `su` para los privilegios raíz.
  - `sudo/pfexec` para los privilegios raíz.

Para cada método de inicio de sesión, se necesita determinada configuración de conexión. Dicha configuración se describe en las siguientes secciones.

NOTA: para los nodos Linux/Solaris, la información de rendimiento acerca del punto de montaje se puede obtener con permisos de lectura/escritura. La información de rendimiento acerca de la partición de Windows y de la unidad de CD-ROM no se puede obtener con permisos de lectura. Si no se puede obtener la información de rendimiento, entonces en la ficha **Rendimiento** del módulo **Supervisión**, el icono de la métrica del rendimiento indica Desconocido.

Configuración para el método de conexión de usuario raíz

Se requiere la configuración siguiente:

- Activar la conexión mediante SSH2
- Permitir la autenticación de contraseña de SSH
- Permitir el inicio de sesión raíz mediante SSH

Tabla 3-3: Configuración de conexión del servidor Linux/Solaris (usuarios raíz)

Configuración	Detalles
Dirección IP	Especifique la dirección IP del servidor Linux/Solaris que se va a supervisar.
Número de puerto	Especifique el número de puerto SSH del servidor Linux/Solaris que se va a supervisar.
Nombre de usuario	Especifique `root`.
Contraseña	Especifique la contraseña raíz.
contraseña raíz	Déjela en blanco.

Configuración para el método de conexión de usuario normal (comando su)

Se requiere la configuración siguiente:

- Activar la conexión mediante SSH2
- Permitir la autenticación de contraseña de SSH

Tabla 3-4: Configuración de conexión del servidor Linux/Solaris (comando su)

Configuración	Detalles
Dirección IP	Especifique la dirección IP del servidor Linux/Solaris que se va a supervisar.
Número de puerto	Especifique el número de puerto SSH del servidor Linux/Solaris que se va a supervisar.
Nombre de usuario	Especifique el identificador de usuario utilizado para el inicio de sesión.
Contraseña	Especifique la contraseña asociada al nombre de usuario.
contraseña raíz	Especifique la contraseña raíz.

Configuración para el método de conexión de usuario normal (comando sudo)

Se requiere la configuración siguiente:

- Activar la conexión mediante SSH2
- Permitir la autenticación de contraseña de SSH
- Añadir las definiciones a la configuración sudo/pfexec. Para obtener información, consulte Adición de la definición de la configuración sudo (Linux) en la página 3-7.
- Añadir las definiciones para el perfil, para Solaris. Para obtener información, consulte Adición de un perfil para pfexec (Solaris) en la página 3-9.

Tabla 3-5: Configuración de conexión del servidor Linux/Solaris (comando sudo)

Configuración	Detalles
Dirección IP	Especifique la dirección IP del servidor Linux/Solaris que se va a supervisar.
Número de puerto	Especifique el número de puerto SSH del servidor Linux/Solaris que se va a supervisar.
Nombre de usuario	Especifique el identificador de usuario utilizado para el inicio de sesión.
Contraseña	Especifique la contraseña asociada al nombre de usuario.
contraseña raíz	Déjela en blanco.

NOTA: a continuación se muestran algunas consideraciones de seguridad que debe tener en cuenta al utilizar SSH:

- Permitir el inicio de sesión raíz es la forma más fácil de realizar la configuración; sin embargo, si falta la contraseña raíz puede causar la falsificación de la configuración del servidor. Este método se debe permitir sólo si el entorno puede evitar un acceso no autorizado.
- Permitir que un usuario normal ejecute la `raíz su` con inicio de sesión raíz prohibido es más seguro que permitir un inicio de sesión raíz, excepto si el identificador de usuario normal y la contraseña se han filtrado.
- El protocolo SSH1 tiene más riesgo de examen que el protocolo SSH2; por lo tanto, se recomienda utilizar el protocolo SSH2.
- Permitir la autenticación de contraseña presenta mayor vulnerabilidad que permitir únicamente la autenticación de clave pública. Dado que IT Operations Analyzer no procesa la autenticación de clave pública, el uso de otros puertos que no sean el 22 proporciona mayor seguridad en la autenticación con contraseña.

Aplicación de la configuración de seguridad del servidor SSH

Esta sección proporciona instrucciones sobre:

- Activación de la conexión de SSH2
- Cómo permitir la autenticación de contraseña de SSH
- Cómo permitir el inicio de sesión raíz mediante SSH
- Adición de la definición de la configuración sudo (Linux)
- Adición de un perfil para pfexec (Solaris)

Antes de comenzar

- Verifique que el servicio SSH (daemon sshd) esté instalado y en ejecución.
- Si utiliza otro software de SSH, consulte el manual del software y configure los ajustes equivalentes. Linux contiene OpenSSH.
- Prepare el entorno en el que puede iniciar sesión en el servidor objetivo de supervisión y active el shell del sistema.
- Inicie sesión desde la consola del servidor o inicie sesión de forma remota utilizando SSH o telnet. Le recomendamos que inicie sesión desde una consola local para evitar fallos de reconexión (si existen errores en la configuración).
- Prepare la contraseña raíz (se necesitan privilegios raíz).
- Después de iniciar sesión como usuario raíz o usuario normal, debe obtener el privilegio raíz mediante el comando de raíz `su`.

Activación de la conexión de SSH2

1. Abra **/etc/ssh/sshd_config** con un editor.
2. En **sshd_config**, busque el archivo mediante la palabra clave **Protocol**.
   - Si no hay ninguna descripción o si no se ha incluido la palabra clave **Protocol**, se activarán SSH1 y SSH2. No es necesario realizar cambios.
   - Si se encuentra **Protocol 1**, sólo se activa SSH1. Cambie **Protocol 1** a **Protocol 1, 2**.
   - Si se encuentra **Protocol 2**, sólo se activa SSH2. No es necesario realizar cambios.
   - Si se encuentra **Protocol 1, 2**, o **Protocol 2, 1**, se activan SSH1 y SSH2. No es necesario realizar cambios.
3. Guarde el archivo y cierre el editor. Para comprobar errores de configuración, ejecute el comando apropiado:

   Linux: `/usr/sbin/sshd -t`

   Solaris: `/usr/lib/ssh/sshd -t`
   - Si no se encuentra ningún error de sintaxis o de intervalo, no se muestra nada.
   - Si se encuentra algún error de sintaxis o de intervalo, se muestra un mensaje de error.

Ejemplo de configuración de Protocol (Protocol 2, 3) incorrecta:

```
[root@linuxhost ssh]# /usr/sbin/sshd -t
ignoring bad proto spec: '3'.
```

4. Reinicie el servicio SSH ejecutando el comando apropiado:
   - Linux: `service sshd restart`
   - Solaris 9: `/etc/init.d/sshd restart`
   - Solaris 10: `svcadm restart ssh`
5. Si se muestra **OK** para **Stopping/Starting**, el servicio se está ejecutando normalmente; por ejemplo: `Stopping sshd: [ OK ]`

Cómo permitir la autenticación de contraseña de SSH

NOTA: Para obtener información sobre cómo editar **/etc/ssh/sshd_config** y reiniciar el servicio SSH, consulte la sección anterior, Activación de la conexión de SSH2.

En **/etc/ssh/sshd_config**, busque el archivo mediante la palabra clave **PasswordAuthentication**.

- Si no hay ninguna descripción o si no se ha incluido la palabra clave **PasswordAuthentication**, se activará la autenticación de contraseña. No es necesario realizar cambios.
- Si se encuentra **PasswordAuthentication no**, no estará permitida la autenticación de contraseña (se activará sólo la autenticación de clave pública). Cámbielo a **PasswordAuthentication yes**.
- Si se encuentra **PasswordAuthentication yes**, estará permitida la autenticación de contraseña. No es necesario realizar cambios.

Cómo permitir el inicio de sesión raíz mediante SSH

NOTA: Para obtener información sobre cómo editar **/etc/ssh/sshd_config** y reiniciar el servicio SSH, consulte la sección anterior, Activación de la conexión de SSH2.

En **/etc/ssh/sshd_config**, busque el archivo mediante la palabra clave **PermitRootLogin**.

- Si no hay ninguna descripción o si no se ha incluido la palabra clave **PermitRootLogin**, se activará la conexión raíz de forma predeterminada. No es necesario realizar cambios.
- Si se encuentra **PermitRootLogin no**, no estará permitida la conexión raíz (sólo se permiten usuarios normales). Cámbielo a **PermitRootLogin yes**.
- Si se encuentra **PermitRootLogin yes**, estará permitido el inicio de sesión raíz. No es necesario realizar cambios.

Adición de la definición de la configuración sudo (Linux)

La configuración de **sudo** se describe en el archivo **/etc/sudoers**. Edite el archivo sólo con el comando **visudo**, porque proporciona control de exclusión y comprobación de sintaxis.

1. Ejecute el comando **visudo**. Si se inicia de forma normal, se abre un editor.

NOTA: Si **visudo** se ejecuta simultáneamente en diferentes ubicaciones, se muestra un mensaje de error y no se iniciará el editor:

```
[root@linuxhost ssh]# visudo
visudo: sudoers file busy, try again later
```

Si se muestra el mensaje de error, pero el comando no se ha ejecutado simultáneamente, puede que haya finalizado la conexión en la ejecución anterior del comando, pero que el proceso haya continuado. En este caso, cancele el proceso **visudo**.

2. Añada líneas para permitir a los usuarios ejecutar los comandos sin contraseña.

RedHat Linux 5.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
```

RedHat Linux 6.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
/usr/sbin/exportfs
```

SUSE Linux 10:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/usr/sbin/ethtool
```

SUSE Linux 11:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/sbin/ethtool
```

SUSE Linux 11 SP1 y SP2:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/sbin/ethtool
/usr/sbin/exportfs
```

CentOS y Oracle Linux 6.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
/usr/sbin/exportfs
```

Por ejemplo, si el nombre de usuario utilizado para la conexión es **sshconn** y el nombre de servidor aplicable es **linuxhost**, entonces especifique el script siguiente /etc/sudoers de SUSE Linux 11:

```
sshconn linuxhost=NOPASSWD: /usr/sbin/dmidecode
sshconn linuxhost=NOPASSWD: /usr/sbin/smartctl
sshconn linuxhost=NOPASSWD: /bin/cat
sshconn linuxhost=NOPASSWD: /sbin/ethtool
```

3. Guarde el archivo y cierre el editor.

   Si se produce un error de sintaxis, se muestra un mensaje de error y se pospone la operación de guardado.

   - Al introducir **e**, se volverá a iniciar el editor. Modifíquelo y guarde el cambio.
   - Al introducir **x**, se descarta el cambio y puede volver al estado anterior a la ejecución de visudo.
   - Al introducir **Q**, se fuerza el almacenamiento del cambio incluso aunque sea incorrecto. Por ejemplo, si comete un error al escribir NOPASSWD, se mostrará el siguiente mensaje de error:

     ```
     Warning: undeclared Cmnd_Alias `NOOPASSWD' referenced
     near line 92
     >>> sudoers file: syntax error? line 91 <<<
     What now?
     ```

NOTA: Tenga cuidado al forzar el almacenamiento de cambios cuyo efecto no conozca. Si no está seguro del resultado, no fuerce la aplicación del cambio.

Adición de un perfil para pfexec (Solaris)

Para proporcionar una autoridad raíz mediante pfexec, añada el perfil a **/etc/security/prof_attr** y **/etc/security/exec_attr**; a continuación, asigne el perfil al usuario.

1. Ejecute `vi /etc/security/prof_attr`.
   - Si se inicia de la forma correcta, el editor se abre.
   - Si aparece un mensaje de error, pero no se ejecuta un comando al mismo tiempo, la conexión podría haber sido interrumpida cuando se ejecutó el comando por última vez, provocando la permanencia del proceso. En este caso, cancele el proceso **vi**.
2. Registre el perfil. Por ejemplo, si el nombre del perfil se ha establecido como HITOA, se indicará como: **HITOA::::**.
3. Guarde el archivo y cierre el editor.
4. Ejecute `vi /etc/security/exec_attr`. Si se inicia de la forma correcta, el editor se abre.
5. Añada las siguientes cuatro líneas para ejecutar los comandos sin ninguna contraseña:

   ```
   /sbin/ifconfig
   /usr/sbin/prtvtoc
   /usr/sbin/luxadm
   /usr/sbin/iscsiadm
   ```

   Por ejemplo, si el nombre del perfil se ha establecido como **HITOA**, la descripción será la siguiente:

   ```
   HITOA:suser:cmd:::/sbin/ifconfig:euid=0
   HITOA:suser:cmd:::/usr/sbin/prtvtoc:euid=0
   HITOA:suser:cmd:::/usr/sbin/luxadm:euid=0
   HITOA:suser:cmd:::/usr/sbin/iscsiadm:euid=0
   ```
6. Guarde el archivo y cierre el editor.
7. Asigne el perfil al usuario. Por ejemplo, si el nombre de usuario se ha establecido como **sshconn**, debería ejecutarse el comando siguiente: `usermod –P HITOA sshconn`

4

Preparación de servidores VMware ESX

IT Operations Analyzer no puede supervisar correctamente servidores Windows o Linux en máquinas virtuales a menos que se instalen herramientas VMware. Este capítulo describe cómo preparar ESX Server.

Obtención de la información de conexión de ESX Server

La siguiente tabla describe la información necesaria al conectarse a ESX Server. Tenga en cuenta que, para el proceso de detección, no se necesita ninguna credencial adicional (sólo la información del nombre de usuario y la contraseña, como se describe en la Tabla 4-1).

Tabla 4-1: Información para la conexión a servidores VMware ESX

Elemento	Detalles
Dirección IP	Utilice la dirección IP de ESX Server.
Número de puerto	Especifique el número de puerto que utilizará ESX Server.
Protocolo	Según la configuración de ESX Server, utilice http o https.
Nombre de usuario	Utilice el nombre de usuario del administrador de ESX Server.
Contraseña	Utilice la contraseña de ESX Server.

Instalación de herramientas VMware en máquinas virtuales

Si planea supervisar máquinas virtuales de servidores de Windows o Linux, debe instalar las herramientas VMWare en cada sistema operativo invitado de la máquina virtual para obtener información de ESX Server.

Si VMware Tools no se ha instalado, no se mostrará correctamente ni el estado de la máquina virtual ni la relación entre el equipo anfitrión y el SO invitado.

Tenga en cuenta que el sistema operativo invitado se gestiona como nodo individual.

Para obtener información sobre la instalación de estas herramientas, consulte el manual del producto de ESX Server (*Basic System Administration*), que está disponible en la Web:

http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_admin_guide.pdf

Si se destina una versión gratuita de ESX a tareas de gestión, es posible que IT Operations Analyzer no pueda obtener de forma precisa el estado del disco.

NOTA: IT Operations Analyzer no admite la supervisión de un servidor VMware ESX que sirve como conmutador virtual distribuido habilitado. Sin embargo, cuando IT Operations Analyzer recopila o actualiza la información de configuración de un conmutador virtual distribuido habilitado según la programación, se realizará un informe con cualquier información sobre cambios en los sucesos del NIC de kernel de la máquina virtual que pertenezcan al conmutador virtual distribuido y al NIC de consola de servicio.

5

Preparación de SNMP para conmutadores IP

IT Operations Analyzer puede recibir capturas SNMP de conmutadores IP. Este capítulo describe cómo configurar conmutadores IP.

Descripción general

IT Operations Analyzer puede supervisar los conmutadores IP del entorno proporcionado si se han configurado de la siguiente forma:

- La versión 1 de SNMP está instalada y en ejecución.
- MIB-II se puede leer si utiliza el nombre de comunidad.
- Bridge MIB se puede leer si utiliza el nombre de comunidad.

Para supervisar los conmutadores IP, la información que se muestra en Tabla 5-1 y Tabla 5-2 es necesaria.

Tabla 5-1: Información para la conexión a conmutadores IP Versión 1 o 2c de SNMP

Elemento	Detalles
Dirección IP	Dirección del nodo de conmutador IP de SNMP.
Número de puerto	Número de puerto en el que el conmutador IP de SNMP espera la comunicación (puerto 161).
Nombre de comunidad	Nombre de comunidad utilizado para conmutadores IP de SNMP.

Tabla 5-2: Información para la conexión a conmutadores IP: Versión 3 de SNMP

Elemento	Detalles
Dirección IP	Dirección del nodo de conmutador IP de SNMP.
Número de puerto	Número de puerto en el que el conmutador IP de SNMP espera la comunicación (puerto 161).
Nombre de usuario	El nombre de usuario utilizado para el conmutador IP de SNMP.
Nivel de seguridad	El nivel de seguridad utilizado para la comunicación en SNMPv3. Opciones: noAuthNoPriv, authNoPriv, authPriv
Método de autenticación	El método de autenticación utilizado para la comunicación en SNMPv3. Opciones: MD5, SHA
Contraseña de autenticación	La contraseña de autenticación utilizada para la comunicación en SNMPv3.
Método de cifrado	El método de cifrado utilizado para la comunicación en SNMPv3. Opciones: DES, AES128
Contraseña de cifrado	La contraseña de cifrado utilizada para la comunicación en SNMPv3.

Esta configuración opcional le ayudará a asegurar la precisión de la información recopilada:

- Virtual Bridge MIB se puede leer si utiliza el nombre de comunidad.
- Cisco VTP MIB se puede leer si utiliza el nombre de comunidad.
- Extreme FDB MIB se puede leer si utiliza el nombre de comunidad.
- La versión 1, 2c o 3 de SNMP está instalada y en ejecución.
- Las interfaces Group MIB se pueden leer si utiliza el nombre de comunidad.

NOTA: El conmutador IP que supervisar debe cumplir con las dos condiciones siguientes:
-RFC1213: SNMP v1 MIB-II es compatible.
-RFC1493: SNMP v1 Bridge MIB es compatible.
Para garantizar que RCA y la vista de topología funcionan correctamente, verifique que se admiten RFC2674 (Virtual Bridge MIB) (o RFC4363 (Virtual Bridge MIB) o Cisco VTP MIB. Cuando supervise conmutadores IP de Extreme Networks®, utilice ExtremeXOS® (versión 12.1.2 o posterior).

Ejemplo de procedimiento de configuración para un conmutador IP de Cisco (IOS)

Para SNMPv1 o v2c:

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `enable`. Si se le solicita, introduzca la contraseña.
   b. Escriba `configure terminal`.
   c. Escriba `snmp-server community public RO` (donde `public` es el nombre de comunidad y se puede cambiar).
   d. Escriba `end`.
   e. Escriba `show running-config` y, a continuación, confirme la configuración.
2. Desconéctese de telnet.

Para SNMPv3:

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `enable`. Si se le solicita, introduzca la contraseña.
   b. Escriba `configure terminal`.
   c. Escriba `snmp-server view allView` (donde `allView` es el nombre de la vista y se puede cambiar).
   d. Cree una vista.
   e. Escriba `snmp-server group privGroup v3 priv read allView notify allView` (donde `privGroup` es el nombre de grupo y se puede cambiar y `allView` es el nombre de la vista que especificó en el paso c).
   f. Cree un grupo.
   g. Escriba `snmp-server user Md5DesUser privGroup v3 auth md5 password1 priv des password2` (donde:
   `Md5DesUser` es un nombre de usuario y se puede cambiar.
   `privGroup` es el nombre de grupo que especificó en el paso e.
   `md5` es un método de autenticación y se puede cambiar.
   `password1` es la contraseña de autenticación y se puede cambiar.
   `des` es el método de cifrado y se puede cambiar.
   `password2` es la contraseña de cifrado y se puede cambiar).
   Establezca la contraseña y el método de autenticación/cifrado/contraseña según el nivel de seguridad.
   h. Cree un usuario.
   i. Escriba `end`.
2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador IP (IOS) de Cisco (Catalyst)

Para SNMP v3:

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `enable`. Si se le solicita, introduzca la contraseña
   b. Escriba `configure terminal`.
   c. Escriba `snmp-server view allView iso included` (donde `allView` es el nombre de la vista y se puede cambiar).
   d. Cree una vista.
   e. Escriba `snmp-server group authGroup v3 auth read allView notify allView` (donde `authGroup` es el nombre de grupo y se puede cambiar y `allView` es el nombre de vista que especificó en el paso c).
   f. Cree un grupo.
   g. Escriba `snmp-server user Md5NoneUser authGroup v3 auth md5 password1` (donde:
   `Md5NoneUser` es un nombre de usuario y se puede cambiar.
   `authGroup` es el nombre de grupo que especificó en el paso e.
   `md5` es un método de autenticación y se puede cambiar.
   `password1` es la contraseña de autenticación y se puede cambiar.
   `des` es el método de cifrado y se puede cambiar).
   Establezca la contraseña y el método de autenticación/cifrado/contraseña según el nivel de seguridad.
   h. Cree un usuario.
   i. Escriba `show vlan` y confirme la lista vlan. En ese caso, escriba `refrains from the one of enet(ethernet).`
   j. Escriba `snmp-server group authGroup v3 auth context vlan-1 read allView notify allView` y establézcalo para permitir el contexto. Tenga en cuenta que se podría producir un error de autoridad si la configuración no se aplica a todo la VLAN.
   `authGroup` es un nombre de grupo y se puede cambiar.
   `vlan-1` es el nombre de la VLAN. Configúrelo como todo VLAN restringida.
   `allView` es el nombre de la vista que especificó en el paso c.
   k. Escriba `end`.
2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador IP de HP

Para SNMPv1 o v2c:

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `configure terminal`.
   b. Escriba `snmp-server community public manager restricted` (donde: `public` es el nombre de comunidad y se puede cambiar).
   c. Escriba `show snmp-server` y después confirme la configuración.
2. Desconéctese de telnet.

Para SNMPv3:

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `configure terminal`.
   b. Escriba `snmpv3 user Md5DesUser auth md5 password1 priv password2` (donde:
   `Md5DesUser` es un nombre de usuario y se puede cambiar.
   `md5` es un método de autenticación y se puede cambiar.
   `password1` es una contraseña de autenticación y se puede cambiar.
   `password2` es una contraseña de cifrado y se puede cambiar).
   Establezca la contraseña y el método de autenticación/cifrado/contraseña según el nivel de seguridad.
   c. Cree un usuario.
   d. Escriba `snmpv3 group managerpriv user Md5DesUser sec-model ver3` (donde `managerpriv` es un nombre de grupo y se puede cambiar y `Md5DesUser` es el nombre de usuario que especificó en el paso b).
   e. Conecte el grupo con el usuario.
2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador IP de Juniper

Para SNMPv1 o v2c:

1. Utilice el explorador Web para acceder a Juniper Web Device Manager.
   a. Inicie sesión.
   b. Desde el panel de navegación, seleccione **System** (Sistema), **Management** (Gestión), **SNMP** y **Community Config** (Config. de comunidad).
   c. En el panel **Community Config**, añada o actualice la comunidad SNMP a la que acceder mediante el servidor de gestión de IT Operations Analyzer.
2. Cierre el explorador Web.

Para SNMPv3:

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `cli` y, a continuación, cambie al modo cli.
   b. Escriba `configure`.
   c. Escriba `set snmp view allView oid .1 include` (donde `allView` es un nombre de vista y se puede cambiar).
   d. Cree una vista.
   e. Escriba `set snmp v3 vacm access group privGroup default-context-prefix security-model usm security-level privacy read-view allView notify-view allView` (donde `privGroup` es un nombre de grupo y se puede cambiar y `allView` es el nombre de vista que especificó en el paso c).
   f. Cree un grupo.
   g. Escriba `set snmp v3 usm local-engine user Md5DesUser authentication-md5 authentication-password password1` (donde:
   `Md5DesUser` es un nombre de usuario y se puede cambiar.
   `authentication-md5` es un método de autenticación y se puede cambiar.
   `password1` es una contraseña de autenticación y se puede cambiar).
   Establezca el sistema o la contraseña de autenticación según el nivel de seguridad.
   h. Cree un usuario.
   i. Escriba `set snmp v3 usm local-engine user Md5DesUser privacy-des privacy-password password2` (donde:
   `Md5DesUser` es el nombre de usuario que especificó en el paso g.
   `privacy-des` es un método de cifrado y se puede cambiar.
   `password2` es una contraseña de cifrado y se puede cambiar).
   Establezca el método o contraseña de cifrado según el nivel de seguridad.
   j. Escriba `set snmp v3 vacm security-to-group security-model usm security-name Md5DesUser group privGroup` (donde "Md5DesUser" es el nombre de usuario que especificó en el paso g. "privGroup" es el nombre de grupo que especificó en el paso e).
   El usuario y el grupo están relacionados.
   k. Escriba commit.

2. Desconéctese de telnet.

Ejemplo del procedimiento de configuración para un conmutador IP Enterasys

Para SNMPv1 o v2c:

1. Utilice telnet para conectarse al conmutador IP. Inicie sesión con un modo de administrador y ejecute los siguientes comandos:
   a. `set snmp community public`.
   b. `set snmp group groupRW user public security-model v1` (donde `groupRW` y `public` son nombres que se pueden cambiar).
   c. `show snmp access groupRW` y después confirme la configuración.

2. Desconéctese de telnet.

Ejemplo del procedimiento de configuración para un conmutador IP Extreme

Para SNMPv1 o v2c:

1. Utilice el explorador Web para acceder a ExtremeXOS ScreenPlay:
   a. Inicie sesión.
   b. Desde el panel de navegación, seleccione **System** (Sistema), **Management** (Gestión), **SNMP** y **Community Config** (Config. de comunidad).
   c. En el panel **Community Config**, añada o actualice la comunidad SNMP a la que acceder mediante el servidor de gestión de IT Operations Analyzer.
2. Cierre el explorador Web.

Para SNMPv3:

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `configure snmpv3 add mib-view allView subtree 1 type included` (donde `allView` es un nombre de vista y se puede cambiar según se necesite).
   b. Cree una vista.
   c. Escriba `configure snmpv3 add access authGroup sec-model usm sec-level authnopriv read-view allView notify-view allView` (donde `authGroup` es un nombre de grupo y se puede cambiar y `allView` es el nombre de la vista que especificó en el paso a).
   d. Cree un grupo.
   e. Escriba `configure snmpv3 add user Md5NoneUser authentication md5 password1` (donde: `Md5NoneUser` es un nombre de usuario y se puede cambiar.
   `md5` es un método de autenticación y se puede cambiar.
   `password1` es una contraseña de autenticación y se puede cambiar). Establezca el método o contraseña de autenticación según el nivel de seguridad.
   f. Cree un usuario.
   g. Escriba `configure snmpv3 add group authGroup user Md5NoneUser sec-model usm` (donde `authGroup` es el nombre de grupo que especificó en el paso c y `Md5NoneUser` es el nombre de usuario que especificó en el paso e).
   h. Realice la conexión entre el usuario y el grupo.
2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador NETGEAR

Para SNMPv1 o v2c:

1. Utilice el explorador Web para acceder al conmutador NETGEAR:
   a. Inicie sesión.
   b. Desde el panel de navegación, seleccione **System** (Sistema), **Management** (Gestión), **SNMP** y **Community Config** (Config. de comunidad).
   c. En el panel **Community Config**, añada o actualice una comunidad SNMP a la que acceder mediante el servidor de gestión de IT Operations Analyzer.

2. Cierre el explorador Web.

Ejemplo de procedimiento de configuración para un conmutador IP de DELL

Para SNMPv1 o v2c:

1. Utilice el explorador Web para acceder al OpenManage Switch de DELL.
2. Administrador:
   a. Inicie sesión.
   b. Desde el panel de navegación, seleccione **System** (Sistema), **SNMP** y **Global Parameters** (Parámetros globales).
   c. En el panel **Global Parameters**, configure **SNMP Notifications** (Notificaciones SNMP) en **Enable** (Activar).
   d. En el menú de navegación, seleccione **Communities** (Comunidades).
   e. En el panel **Communities**, añada o actualice una comunidad SNMP a la que acceder mediante el servidor de gestión de IT Operations Analyzer.
3. Cierre el explorador Web.

Para SNMPv3

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `configure`.
   b. Escriba `snmp engineid local default`, y configure el ID de motor.
   c. Escriba `snmp view allView 1 included` (donde `allView` es un nombre de vista y se puede cambiar).
   d. Cree una vista.
   e. Escriba `snmp group authGroup v3 auth read allView notify allView` (donde `authGroup` es un nombre de grupo y se puede cambiar y `allView` es el nombre de la vista que especificó en el paso c).
   f. Cree un grupo.

g. Escriba `snmp user Md5NoneUser authGroup auth-md5 password1` (donde: `Md5NoneUser` es un nombre de usuario y se puede cambiar. `authGroup` es el nombre de grupo que especificó en el paso e. `auth-md5` es un método de autenticación y se puede cambiar. `password1` es una contraseña de autenticación y se puede cambiar). Establezca el método o contraseña de autenticación según el nivel de seguridad.

h. Cree un usuario.

2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador Allied-Telesis (AT-9424T)

Para SNMPv3

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `enable snmp` y active el SNMP.
   b. Escriba `create snmpv3 view allView Subtree=1 Type=Included` (donde `allView` es un nombre de vista y se puede cambiar).
   c. Cree una vista.
   d. Escriba `create snmpv3 access authGroup SecurityModel=V3 SecurityLevel=Authentication ReadView=allView NotifyView=allView` (donde `authGroup` es un nombre de grupo y se puede cambiar y `allView` es el nombre de vista que especificó en el paso b).
   e. Cree un grupo.
   f. Escriba `add snmpv3 user Md5NoneUser Authentication=Md5 AuthPassword=password1` (donde: `Md5NoneUser` es un nombre de usuario y se puede cambiar. `Md5` es un método de autenticación y se puede cambiar. `password1` es una contraseña de autenticación y se puede cambiar). Establezca el método o contraseña de autenticación según el nivel de seguridad.
   g. Cree un usuario.
   h. Escriba `create snmpv3 group UserName=Md5NoneUser SecurityModel=V3 GroupName=authGroup` (donde `Md5NoneUser` es el nombre de usuario que especificó en el paso f y `authGroup` es el nombre de grupo que especificó en el paso d).
2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador ALAXALA (AX3600)

Para SNMPv3

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `configure terminal`.
   b. Escriba `snmp-server view allView 1 included` (donde `allView` es un nombre de la vista y se puede cambiar).
   c. Cree una vista.

d. Escriba `snmp-server group authGroup v3 auth read allView notify allView` (donde `authGroup` es un nombre de grupo y se puede cambiar y `allView` es el nombre de vista que especificó en el paso b).

e. Cree un grupo.

f. Escriba `snmp-server user Md5NoneUser authGroup v3 auth md5 password1` (donde:
`Md5NoneUser` es un nombre de usuario y se puede cambiar.
`authGroup` es el nombre de Grupo que especificó en el paso d.
`md5` es un método de autenticación y se puede cambiar.
`password1` es una contraseña de autenticación y se puede cambiar).
Establezca el método o contraseña de autenticación según el nivel de seguridad.

g. Cree un usuario.

h. Escriba `write`.

2. Desconéctese de telnet.

Activación de capturas SNMP

IT Operations Analyzer puede recibir una captura SNMP cuando el enlace de comunicación del conmutador IP está activo o inactivo. Para configurar opcionalmente estas recepciones de capturas, aplique la siguiente configuración:

- Active la opción **Enviar captura** (la versión debe ser SNMP v1).
- Configure la **dirección de destino de envío de capturas** como la dirección IP del servidor de gestión de IT Operations Analyzer y establezca el **puerto de destino de envío de capturas** como el **puerto de capturas** del servidor de gestión de IT Operations Analyzer (el número de puerto es 162).

NOTA: Para obtener información acerca de los números de puerto predeterminados que utiliza IT Operations Analyzer, consulte el Capítulo 2 de la *Guía de introducción de Hitachi IT Operations Analyzer*.

Ejemplo de procedimiento de configuración para un conmutador IP de Cisco (IOS)

1. Utilice telnet para conectarse al conmutador IP. Introduzca lo siguiente:

   a. `enable`. Si se le solicita, introduzca la contraseña.

   b. `configure terminal`.

   c. `snmp-server enable traps`.

   d. `snmp-server host 192.168.1.1 version 1 public` (donde `192.168.1.1` es el destino de envío de las capturas y `public` es el nombre de comunidad. Ambos se pueden cambiar según sea necesario.).

   e. `end`.

   f. `show running-config` y, a continuación, confirme la configuración.

2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador IP de HP

1. Utilice telnet para conectarse al conmutador IP.
   a. Escriba `configure`.
   b. Escriba `snmp-server host 192.168.1.1 public all`. (Donde `192.168.1.1` es el destino para las capturas de envío y `public` es el nombre de comunidad. Ambos se pueden cambiar en caso necesario).
   c. Escriba `show snmp-server` y después confirme la configuración.
2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador IP de Juniper (serie EX)

1. Utilice el explorador Web para acceder a Juniper Web Device Manager:
   a. Inicie sesión.
   b. Haga clic en **Configure** (Configurar).
   c. Haga clic en **Service** (Servicio) y seleccione **SNMP**.
   d. Haga clic en **Add** (Añadir) dentro de **Trap Groups** (Grupos de capturas).
   e. Especifique un **nombre de grupo de captura**.
   f. En el área **Categories** (Categorías), seleccione **Link** (Enlace) o **none** (ninguno).
   g. Añada la dirección IP del servidor de gestión a **Targets** (Objetivos).
   h. Haga clic en **Aceptar**.
2. Cierre el explorador Web.

Ejemplo del procedimiento de configuración para un conmutador IP Enterasys

1. Utilice telnet para conectarse al conmutador IP. Inicie sesión con un modo de administrador y ejecute los siguientes comandos:
   a. `set snmp targetparams testParams user public security-model v1 message-processing v1`.

      Tenga en cuenta que **testParams** es un nombre que se puede cambiar según sea necesario.
   b. `set snmp notify testNotify tag testTag trap`.

      Tenga en cuenta que **testNotify** y **testTag** son nombres que se pueden cambiar según sea necesario.
   c. `set snmp targetaddr testTargetAddr 192.168.55.11 param testParams udpport 162 mask 255.255.255.0 taglist testTag`.

      Tenga en cuenta que **testTargetAddr** es un nombre por voluntad propia, **192.168.55.11** es la dirección IP del destino de capturas, **162** es el número de puerto del destino de capturas y **255.255.255.0** es una máscara de subred del destino de capturas. Puede cambiar esta información, si es necesario.
   d. `show running-config` y, a continuación, confirme la configuración.
2. Desconéctese de telnet.

Ejemplo del procedimiento de configuración para un conmutador IP Extreme

1. Utilice telnet para conectarse al conmutador IP. Inicie sesión con un modo de administrador y ejecute los siguientes comandos:
   a. `configure snmpv3 add target-params testTargetParam user v1v2c_ro mp-model snmpv1 sec-model snmpv1 sec-level noauth`.

      Tenga en cuenta que **testTargetParam** es un nombre arbitrario y **v1v2c_ro** es un nombre de seguridad. Estos nombres se pueden cambiar según sea necesario. Puede confirmar el nombre de seguridad mediante `show snmpv3 community`.

   b. `configure snmpv3 add target-addr 192.168.55.11 param testTargetParam ipaddress 192.168.55.11/FFFFFF00 transport-port 162 from 192.168.55.7`.

      Tenga en cuenta que **191.168.55.11** es la dirección IP del destino de capturas, **FFFFFF00** es una máscara de subred del destino de capturas, **162** es el número de puerto del destino de capturas y **192.168.55.7** es la dirección IP del origen de capturas. Puede cambiar esta información, si es necesario.

   c. `show running-config` y, a continuación, confirme la configuración.

2. Desconéctese de telnet.

Ejemplo de procedimiento de configuración para un conmutador IP de NETGEAR

1. Utilice el explorador Web para acceder al conmutador NETGEAR:
   a. Inicie sesión.
   b. Desde el panel de navegación, seleccione **System** (Sistema), **Management** (Gestión), **SNMP** y **Trap Config** (Config. de captura).
   c. En el panel **Trap Config** (Config. de captura) añada o actualice una configuración de captura para enviar una captura SNMP al servidor de gestión de IT Operations Analyzer. Para la **versión de SNMP**, indique **SNMP V1**.
   d. En el panel de navegación, seleccione **Trap Flags** (Indicadores de captura).
   e. En el panel **Trap Flags**, configure **Link Up/Down** (Enlazar hacia arriba/hacia abajo) en **Enable** (Activado).

2. Cierre el explorador Web.

Ejemplo de procedimiento de configuración para un conmutador IP de DELL

1. Utilice el explorador Web para acceder al **OpenManage Switch Administrator** de DELL:
   a. Inicie sesión.
   b. Desde el panel de navegación, seleccione **System** (Sistema), **SNMP** y **Global Parameters** (Parámetros globales).
   c. En el panel **Global Parameters**, configure **SNMP Notifications** (Notificaciones SNMP) en **Enable** (Activar).
   d. En el panel de navegación, seleccione **Notification Recipients** (Destinatarios de la notificación).
   e. En el panel **Notification Recipients**, añada o actualice una configuración de captura para enviar una captura SNMP al servidor de gestión de IT Operations Analyzer. Para la configuración, seleccione **SNMPv1.2**.
2. Cierre el explorador Web.

6

Preparación del almacenamiento de Hitachi

IT Operations Analyzer puede supervisar Hitachi AMS/WMS/SMS series y Hitachi Unified Storage series. También puede supervisar Hitachi 9500V e Hitachi USP VM mediante el agente SMI-S de Device Manager. Sin embargo, no supervisara el rendimiento de Hitachi 9500V.

Este capítulo describe la información que se debe recopilar para la conexión con los nodos de almacenamiento de Hitachi AMS/WMS/SMS, Hitachi Unified Storage, Hitachi 9500V y Hitachi USP VM. También describe las tareas de preparación para adquirir información de rendimiento de Hitachi AMS/WMS/SMS series, Hitachi Unified Storage series e Hitachi USP VM.

- Preparación para la conexión a la serie Hitachi AMS/WMS/SMS y a la serie Hitachi Unified Storage
- Preparaciones para adquirir información del rendimiento para la serie Hitachi AMS/WMS/SMS y la serie Hitachi Unified Storage
- Preparación para la conexión a Hitachi 9500V y a Hitachi USP VM
- Preparación para obtener información de rendimiento para Hitachi USP VM

Preparación para la conexión a la serie Hitachi AMS/WMS/SMS y a la serie Hitachi Unified Storage

IT Operations Analyzer puede supervisar Hitachi AMS/WMS/SMS series y Hitachi Unified Storage series. Cuando se conecta a la serie Hitachi AMS/WMS/SMS y la serie Hitachi Unified Storage, la información que aparece en la Tabla 6-1 es necesaria.

Tabla 6-1: Información para la conexión a la serie Hitachi AMS/WMS/SMS y a la serie Hitachi Unified Storage

Elemento	Detalles
Dirección IP	Dirección IP utilizada para conectarse al almacenamiento.
Identificador de usuario	Si está activada la opción **Autenticación de cuenta** o **Protección con contraseña**, especifique el identificador del usuario que puede iniciar sesión en el almacenamiento.
Contraseña	Contraseña asociada al identificador de usuario. Es necesaria si la opción **Autenticación de cuenta** o **Protección con contraseña** está activada.

NOTA: si se utiliza **Protección con contraseña**, se pueden producir errores. Por ejemplo, cuando varios servidores de gestión están intentando acceder simultáneamente al almacenamiento de Hitachi y la **Protección con contraseña** está activada. Para evitar errores, se recomienda desactivar la **Protección con contraseña**.

Acerca de la modificación del número de puerto

Cuando el número de puerto de gestión del almacenamiento de Hitachi se cambia, registre el número de puerto que se ha cambiado en el archivo de servicios. El archivo de servicios se encuentra en el siguiente directorio de Windows:

<Directorio de Windows>\system32\drivers\etc\services

- Nombre de servicio del número del **puerto normal**: df-damp-snm
- Nombre de servicio del número del **puerto seguro**: df-damp-snm-ssl

En el ejemplo siguiente, el **puerto normal** se define en 2300 y el **puerto seguro,** en 25000:

df-damp-snm 2300/tcp nº puerto normal

df-damp-snm-ssl 25000/tcp nº del puerto seguro- SSL

NOTA: El número de puerto del almacenamiento Hitachi que supervisa IT Operations Analyzer debería coincidir. Cuando el archivo de servicios cambia, el cambio afecta a los productos que utilizan HSNM2-API, como Hitachi Storage Navigator Modular 2, HiCommand series, etc.

Preparaciones para adquirir información del rendimiento para la serie Hitachi AMS/WMS/SMS y la serie Hitachi Unified Storage

Realice los siguientes pasos para obtener la información de rendimiento.

1. Abra el panel **Estadísticas de rendimiento** del dispositivo de almacenamiento cuyo rendimiento se va a supervisar desde Hitachi Storage Navigator Modular 2.
2. Complete las tareas dependiendo de si el cuadro de diálogo de gestión se muestra en una ventana nueva:
   - **Cuando el cuadro de diálogo de gestión se muestra en una ventana nueva**

   a. Inicie sesión en Hitachi Storage Navigator Modular 2.

   b. Haga clic en el nombre de la matriz de destino y abra el cuadro de diálogo de gestión.

   c. En el menú, haga clic en **Herramienta**, **Rendimiento** y, a continuación, en **Configuración**.

   - **Cuando el diálogo de gestión se muestra en la misma ventana**

   a. Inicie sesión en Hitachi Storage Navigator Modular 2.

   b. Haga clic en el nombre de la matriz de destino y abra la pantalla de gestión.

   c. Desde la vista de árbol, abra **Rendimiento** y, a continuación, haga clic en **Supervisión**.

   d. Haga clic en **Cambio de elemento de adquisición**.
3. Confirme que está seleccionado lo siguiente: **Grupo RAID / Información de unidad lógica**, **Información de caché**, **Información de procesador** e **Información de activación de la unidad** y, a continuación, haga clic en **Aceptar**.

Preparación para la conexión a Hitachi 9500V y a Hitachi USP VM

IT Operations Analyzer puede supervisar:

- Hitachi 9500V mediante el agente SMI-S de Hitachi Device Manager. Instale Device Manager 5.9 o posterior y active el uso del proveedor de SMI-S.
- Hitachi USP VM mediante el agente SMI-S de Device Manager. Instale Device Manager 6.2 o posterior y active el uso del proveedor de SMI-S.

A continuación, se incluye un resumen del procedimiento general para obtener información de conexión de Hitachi 9500V e Hitachi USP VM. Para obtener información específica, consulte los manuales correspondientes:

- Hitachi Device Manager (Administrador de dispositivos Hitachi), Provisioning Manager (Administrador de aprovisionamiento) y Tiered Storage Manager Software Installation Guide (Guía de instalación del software de gestor de almacenamiento de varios niveles)
- Hitachi Device Manager (Administrador de dispositivos Hitachi) y Provisioning Manager Software System Configuration Guide (Guía de configuración del sistema de software del administrador de aprovisionamiento)
- Hitachi Device Manager Software Web Client User Guide (Guía del usuario del cliente Web de software del administrador de dispositivos Hitachi)

1. Instale **Device Manager** en cualquier servidor. Debido a que puede seleccionar la existencia de un agente SMI-S durante la instalación, actívelo.
2. Inicie sesión en **Device Manager** y haga clic en **Subsystems** (Subsistemas) y, a continuación, en **Add Subsystem** (Añadir subsistema) y registre los dispositivos de almacenamiento.

   Al registrar los dispositivos, utilice las direcciones IP, identificadores de usuario y contraseñas de los controladores de almacenamiento. La Tabla 6-2 muestra la información necesaria al conectarse al almacenamiento de Hitachi.
3. Cuando utilice agente SMI-S, como se describe en este manual, tiene que aumentar el tamaño del montón de memoria del servidor Device Manager. A continuación, se muestra un ejemplo del procedimiento al trabajar con Microsoft Windows:
   a. Calcular el tamaño del montón de memoria.
   b. Abrir el archivo **Server.ini** mediante un editor de textos:

      <*Ubicación de instalación del servidor Device Manager*>\HiCommandServer\Server.ini
   c. Según los cálculos del paso a, cambie el valor de **JVM_XOPT_HEAP_MAX**. Por ejemplo:

      JVM_XOPT_HEAP_MAX=Xmx<*Valor de configuración*>m
   d. Reinicie el servidor Device Manager.

Tabla 6-2: Información para la conexión a Hitachi 9500V e Hitachi USP VM

Elemento	Detalles
Dirección IP	Utilice la dirección IP del servidor en el que está instalado Device Manager.
Espacio de nombres	Para Device Manager 5.9 o posterior, especifique: root/smis/smis12 Para Device Manager 6.2 o posterior, especifique: root/smis/smis13 Para Device Manager 7.0 o posterior, especifique: root/smis/smis14
Existencia de SSL	Utilice la configuración aplicada durante la instalación de Device Manager.
Número de puerto	Utilice la configuración aplicada durante la instalación de Device Manager. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario de Device Manager.
Contraseña	Utilice la contraseña asociada al identificador de usuario.

NOTA: Cuando el sitio supervisa el almacenamiento de Hitachi mediante el administrador de dispositivos Hitachi, siempre se informará de que los siguientes componentes funcionan correctamente, dentro del módulo **Supervisión**:
-Controlador de almacenamiento
-Puerto FC de almacenamiento
-Unidad de disco de almacenamiento
-Volumen de almacenamiento
-LUN
Por lo tanto, no se detectará ninguna condición de error.

Preparación para obtener información de rendimiento para Hitachi USP VM

A continuación se muestra un resumen general de cómo obtener la información de rendimiento de Hitachi USP VM. Para obtener más información, consulte los manuales de Hitachi Device Manager.

1. Prepare el subsistema de almacenamiento.

   Prepare el dispositivo de comando en todos los subsistemas de almacenamiento de los que desea obtener los datos de rendimiento. (El dispositivo de comando es un dispositivo de control que emite el comando de control a la unidad de disco de gran escala.) A continuación, asigna una ruta al anfitrión que recopila datos de rendimiento y configura el anfitrión para reconocer el dispositivo de comando.

2. Prepare el anfitrión que recopila los datos de rendimiento.

   Instale el agente Device Manager y configure el dispositivo de comando.

3. Prepare el servidor Device Manager.

   Establezca el nombre del anfitrión que recopila los datos de rendimiento, en el archivo de propiedades del servidor Device Manager.

7

Preparación de SMI-S para conmutadores FC y almacenamiento

IT Operations Analyzer utiliza SMI-S para detectar y supervisar otros almacenamientos y conmutadores FC. Este capítulo describe SMI-S y las tareas necesarias para configurar el almacenamiento y los conmutadores FC.

Revisión de la preparación de SMI-S

SMI-S es el estándar de SNIA (Storage Networking Industry Association) que proporciona una interfaz de programación de aplicaciones (API) de gestión abierta. Admite la gestión interoperable de redes y dispositivos de almacenamiento, que incluyen anfitriones, conmutadores y almacenamiento virtual.

Si el entorno utiliza el almacenamiento de terceros (es decir, un almacenamiento distinto al del almacenamiento de Hitachi o conmutadores FC), IT Operations Analyzer puede detectarlo y supervisarlo mediante el uso del agente SMI-S.

En un entorno que utiliza almacenamiento de terceros con un agente SMI-S, puede haber uno de dos modelos en uso: un modelo integrado o un modelo proxy.

- En el **modelo integrado**, el agente SMI-S se ejecuta en un dispositivo. Es lo que denominamos agente SMI-S (integrado).
- En el **modelo proxy**, el agente SMI-S se instala en un servidor. Es lo que denominamos agente SMI-S (proxy).

La Figura 7-1 proporciona un ejemplo de un entorno de SMI-S, formado por un servidor (también conocido como servidor SMI-S) y un cliente. IT Operations Analyzer funciona como el cliente y, en este ejemplo, recopila información sobre los conmutadores de canal de fibra (FC). Tenga en cuenta que el área sombreada en azul, formada por modelos integrados y proxy, se debe preparar antes de iniciar la detección inicial.

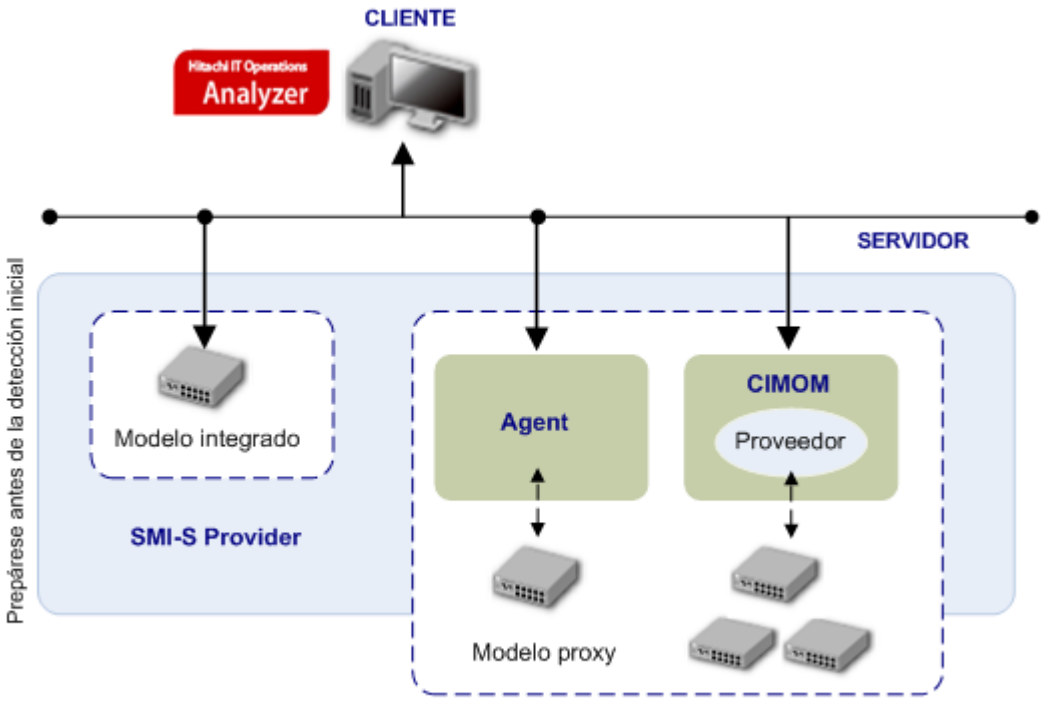

Figura 7-1: Ejemplo de un entorno SMI-S

Las siguientes secciones describen las preparaciones necesarias para los conmutadores FC y almacenamiento en su entorno.

Preparación de SMI-S para conmutadores de canal de fibra (FC)

Para especificar dispositivos como objetivos de supervisión, deben admitir SMI-S versión 1.0 - 1.3 y el servicio que gestiona dichos dispositivos debe estar en ejecución. Esta sección describe la configuración del agente SMI-S para:

- Conmutadores FC de Brocade®
- Conmutadores FC de la serie Brocade Sphereon
- Conmutadores FC de QLogic®
- Conmutadores FC de Cisco®

Configuración de conmutadores FC de Brocade (excepto serie Sphereon)

Establezca la configuración del agente SMI-S según las siguientes directrices. Para obtener más información, consulte la documentación del agente SMI de Brocade que se encuentra en el siguiente sitio Web: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

Puede confirmar los requisitos y procedimientos de instalación, la configuración posterior a la instalación y las actualizaciones que se encuentran en la notas de la versión como se indica a continuación:

- Requisitos para la instalación

  Guía de instalación del agente SMI de Brocade v120.6.0a, capítulo 1 "Requisitos para la instalación"
- Procedimientos de instalación

  Guía de instalación del agen"
- Configuración posterior a la instalación

  Guía del usuario del agente SMI de Brocade v120.6.0a
- Notas de la versión

  Notas de la versión v1.1 del agente SMI de Brocade v120.6.0a

Requisitos previos a la instalación

- Agente SMI-S de Brocade versión: Agente SMI de Brocade v120.6.0a
- Sistema operativo: Microsoft Windows Server 2003 (32 bits)

Complete la siguiente tarea de instalación al instalar una versión previa del agente SMI-S de Brocade.

Para instalar el agente SMI de Brocade:

1. Descargue el agente SMI-S de Brocade v120.6.0a del siguiente sitio Web y, a continuación, ejecute **install.exe**: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. Complete cada solicitud del asistente de instalación. Para determinadas solicitudes, compruebe las siguientes directrices:
   a. **Configuración del puerto HTTP**. El número de puerto predeterminado es 5988. Tenga en cuenta que el número de puerto que especifique se utilizará para conectarse a IT Operations Analyzer.
   b. **Configuración del puerto HTTPS**. El número de puerto predeterminado es 5988. Tenga en cuenta que el número de puerto que especifique se utilizará para conectarse a IT Operations Analyzer.
   c. **Configuración de las conexiones proxy**. Especifique lo siguiente:

      IP Proxy: Dirección IP del conmutador FC

      Nombre de usuario: Nombre de usuario del conmutador FC

      Contraseña: Contraseña del conmutador FC

      Especifique otra configuración según su entorno.
3. Para guardar los cambios al final de la instalación del agente de Brocade, haga clic en **Done** (Hecho).

   Ahora está listo para registrar el conmutador FC.

Para registrar el conmutador FC:

1. Inicie la **herramienta de configuración del agente SMI de Brocade**:
   a. En el menú **Inicio**, seleccione **Todos los programas**.

NOTA: En Windows Server 2012, los pasos para navegar al menú **Inicio** son diferentes.

   b. Seleccione **SMIAgent120.6.0a** y, a continuación, **Brocade SMI Agent Configuration Tool** (Herramienta de configuración del agente SMI de Brocade).
2. Haga clic en **Add** (Agregar) para iniciar el diálogo **Proxy Configuration** (Configuración de proxy).
3. Introduzca la información solicitada y, a continuación, haga clic en **OK** (Aceptar) para guardar la configuración y cerrar el diálogo **Proxy Configuration** (Configuración de proxy).
4. En la **Herramienta de configuración del agente SMI de Brocade**, cambie el estado del proxy de **Not Connected** (No conectado) a **Connected** (Conectado) haciendo clic en **Apply** (Aplicar).

La Tabla 7-1 muestra la información necesaria al conectarse a un conmutador FC de Brocade.

Tabla 7-1: Información para la conexión a un conmutador FC de Brocade

Elemento	Detalles
Dirección IP	Especifique la dirección IP del servidor en el que está instalado Brocade SMI Agent.
Espacio de nombres	Especifique `root/brocade1`.
Existencia de SSL	Aplique la configuración de Brocade SMI Agent establecida durante la instalación.
Número de puerto	Aplique la configuración de Brocade SMI Agent establecida durante la instalación. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario de Brocade SMI Agent.
Contraseña	Introduzca una contraseña para el identificador de usuario.

NOTA: Cuando un estado del puerto FC-Enrutamiento FC es "inactivo", el estado del conmutador Phantom cambia a "inaccesible". El estado inalcanzable del conmutador no cambiará, ni siquiera si el estado del puerto vuelve a ser normal otra vez.

Para cambiar el estado del conmutador de inalcanzable a normal, IT Operations Analyzer necesita redescubrir el conmutador. Es obligatorio porque el proveedor SMI-S del conmutador Phantom no responderá, cuando el estado del puerto sea desactivado. Incluso si el estado del puerto vuelve de nuevo a ser normal, el proveedor SMI-S informará del estado del conmutador como inalcanzable.

Consulte la Ayuda en línea para obtener información sobre el descubrimiento de conmutadores, nodos y otros dispositivos.

Configuración de conmutadores FC de Brocade Sphereon

Establezca la configuración del agente SMI-S según las siguientes directrices. Para obtener más información, consulte la documentación del agente SMI de Brocade para EOS que se encuentra en el siguiente sitio Web. http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

Puede confirmar los requisitos y procedimientos de instalación, la configuración posterior a la instalación y las actualizaciones que se encuentran en la notas de la versión como se indica a continuación:

- Requisitos para la instalación

  Guía del usuario del agente SMI de Brocade para productos EOS 2.0, capítulo 1 "Requisitos del sistema"

- Procedimientos de instalación

  Guía del usuario del agente SMI de Brocade para productos EOS 2.0, capítulo 2 "Instalación del agente SMI de Brocade para productos de EOS"

- Configuración posterior a la instalación

  Guía del usuario del agente SMI de Brocade para productos EOS 2.0, capítulo 3 "Uso del programa de configuración del servidor del agente SMI para productos EOS 2.0" y capítulo 4 "Configuración del servidor para operaciones de cliente"

- Notas de la versión

  Notas de la versión del agente SMI de Brocade para productos EOS 2.0

Requisitos previos a la instalación

- Agente SMI-S de Brocade versión: Agente SMI de Brocade para productos EOS 2.0 para Windows
- Sistema operativo: Microsoft Windows Server 2003 (32 bits)

Para instalar el agente SMI de Brocade:

1. Descargue el agente SMI de Brocade para EOS para Windows desde el siguiente sitio Web y, a continuación, ejecute **install.exe**: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. Complete cada solicitud del asistente de instalación.
3. Para guardar los cambios al final de la instalación del agente de Brocade, haga clic en **Done** (Hecho).

   Ahora está listo para registrar el conmutador FC.

Para registrar el conmutador FC:

1. Abra el archivo **Switch.properties** que está ubicado en la ruta siguiente: <*Directorio de instalación*>\agent\server\jserver\bin
2. Especifique los siguientes parámetros:
   - **cimserver**

     La URL del servidor, por ejemplo: https://localhost/root/mcdata
   - **cimserverusername**

     El nombre de usuario para iniciar sesión en el servidor CIM, por ejemplo: Administrador
   - **cimserverpassword**

     La contraseña para iniciar sesión en el servidor CIM, por ejemplo: Contraseña
   - **switchip**

     La dirección IP del conmutador, por ejemplo: 172.26.24.180
   - **switchtype**

     El código de tipo de producto de conmutador. Consulte la nota de más abajo.
   - **switchusername**

     El nombre de usuario para iniciar la sesión en el conmutador.
   - **switchpassword**

     La contraseña para iniciar la sesión en el conmutador.

NOTA: A continuación, se indican los códigos de tipos de producto de conmutador FC:

Sphereon 3016: Código 2

Sphereon 3032: Código 3

Sphereon 3216: Código 4

Sphereon 3232: Código 5

Sphereon 4300: Código 6

Sphereon 4400: Código 12

Sphereon 4500: Código 7

Sphereon 4700: Código 13

3. Mover información a la ruta de acceso siguiente, desde el símbolo del sistema: <*Directorio de instalación*>\agent\server\jserver\bin
4. Ejecute el siguiente comando: ManageSwitch Add

La Tabla 7-2 muestra la información necesaria para conectarse a un conmutador FC de la serie Brocade Sphereon.

Tabla 7-2: Información para la conexión a un conmutador FC de Brocade

Elemento	Detalles
Dirección IP	Especifique la dirección IP del servidor en el que está instalado Brocade SMI Agent for EOS.
Espacio de nombres	Especifique `root/mcdata`.
Existencia de SSL	Aplique la configuración de Brocade SMI Agent establecida durante la instalación.
Número de puerto	Aplique la configuración de Brocade SMI Agent for EOS establecida durante la instalación.
Identificador de usuario	Utilice el identificador de usuario de Brocade SMI Agent for EOS.
Contraseña	Introduzca una contraseña para el identificador de usuario.

Configuración de conmutadores FC de QLogic

El proveedor de SMI-S está integrado en el conmutador FC de QLogic. El procedimiento en esta sección describe cómo conectar al puerto de gestión del conmutador FC de QLogic usando un explorador Web.

Para obtener más información sobre la configuración del proveedor de SMI-S usando la interfaz de línea de comandos (CLI), consulte la documentación del conmutador FC de QLogic. La documentación está disponible en el siguiente sitio Web:

http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/NewDefault.aspx

Para configurar los conmutadores FC de QLogic:

1. En el explorador Web, conéctese al puerto de gestión del conmutador FC de QLogic (por ejemplo, http://10.208.113.46). Aparecerá la ventana **Switch Manager** (Gestor de conmutadores).
2. En la barra de menús de **Switch Manage**r (Gestor de conmutadores), seleccione **Switch** (Conmutador) y, a continuación, **Services** (Servicios). Se muestra el cuadro de diálogo **System Services** (Servicios del sistema).
3. Verifique si el servicio del proveedor de SMI-S está activado:
   - Si **CIM service** (Servicio CIM) está seleccionado, el servicio del proveedor de SMI-S está activado. Haga clic en **Close** (Cerrar).
   - Si **CIM service** no está seleccionado, selecciónelo y haga clic en **OK** (Aceptar).
4. Si existe una opción para especificar el **servicio SSL** en el cuadro de diálogo **System Services** (Servicios del sistema), esto significa que puede utilizar el puerto SSL **5989**.

La Tabla 7-3 muestra la información necesaria al conectarse a un conmutador FC de QLogic.

Tabla 7-3: Información para la conexión a un conmutador FC de QLogic

Elemento	Detalles
Dirección IP	Dirección IP del conmutador FC de QLogic.
Espacio de nombres	Especifique `root/switch`.
Existencia de SSL	Aplique la configuración del conmutador FC de QLogic.
Número de puerto	Aplique la configuración del conmutador FC de QLogic establecida durante la instalación. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario del conmutador FC de QLogic.
Contraseña	Introduzca una contraseña para el identificador de usuario.

Configuración de conmutadores FC de la familia Cisco MDS 9000

El proveedor de SMI-S está integrado en el conmutador FC de Cisco. El procedimiento de esta sección describe cómo activar el servidor y conectarse a él usando el protocolo HTTP (puerto 5988). Si el sitio utiliza el protocolo HTTPS (puerto 5989), aplique la autenticación de Nivel de socket seguro (SSL) para cifrar la información de inicio de sesión y, a continuación, active HTTPS y SMI-S Agent (proxy). Encontrará detalles del procedimiento en el enlace de la Tabla 7-4.

Para obtener información adicional, consulte la referencia de programación de SMI-S de la familia Cisco MDS 9000. El documento está disponible en el siguiente sitio Web:

http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html

Para configurar los conmutadores FC de la familia Cisco MDS 9000:

Después del paso 8 se incluye un ejemplo de la ejecución de comandos que se describe en el siguiente procedimiento.

1. Acceda al conmutador FC a través de telnet e inicie sesión.
2. Introduzca `show cimserver` y verifique que cimserver Http está activado.
3. Introduzca `config terminal` e inicie el modo de configuración.
4. De forma predeterminada, HTTP está activado. En caso contrario, actívelo introduciendo `cimserver enableHttp`.
5. Introduzca `cimserver enable` para activar el servidor CIM.
6. Introduzca `end` para finalizar el modo de configuración.
7. Introduzca `show cimserver` y verifique la configuración:
   - cimserver está activado
   - cimserver Http is enabled
8. Introduzca `exit` para desconectar telnet.

Ejemplo de comando

```
Inicio de sesión FCGS03: ********
Contraseña:
FCGS03# show cimserver
 cimserver is not enabled
 cimserver Http is enabled
 cimserver Https is not enabled
 cimserver certificate file is not installed
FCGS03# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
FCGS03(config)# cimserver enable
```

```
FCGS03(config)# end

FCGS03# show cimserver

 cimserver está activado

 cimserver Http is enabled

 cimserver Https is not enabled

 cimserver certificate file is not installed

 Current value for the property logLevel in CIMServer is
'WARNING'.

FCGS03# exit
```

Tabla 7-4: Información para la conexión a un conmutador FC de Cisco

Elemento	Detalles
Dirección IP	Dirección IP del conmutador FC de Cisco.
Espacio de nombres	Especifique `root/cimv2`.
Existencia de SSL	Aplique la configuración del conmutador FC de Cisco. Para obtener más información, consulte el material de referencia de programación de SMI-S de la familia Cisco MDS 9000: http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html
Número de puerto	Aplique la configuración del conmutador FC de Cisco establecida durante la instalación. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario del conmutador FC de Cisco.
Contraseña	Introduzca una contraseña para el identificador de usuario.

Preparación de SMI-S para el almacenamiento

Para especificar el almacenamiento como objetivo de supervisión, debe admitir SMI-S versión 1.0 - 1.3 y el servicio que gestiona dicho almacenamiento debe estar en ejecución. Esta sección describe la configuración de SMI-S para:

- Almacenamiento de EMC
- Almacenamiento de la serie HP EVA
- Almacenamiento de la serie HP MSA
- Almacenamiento de IBM y de Engenio OEM Sun
- Almacenamiento de NetApp

NOTA: Para obtener información sobre la configuración del almacenamiento de Hitachi y la obtención del rendimiento de almacenamiento de Hitachi (USP VM), consulte el capítulo 6, Preparación del almacenamiento de Hitachi.

Notas sobre el volumen máximo de supervisión para un dispositivo de almacenamiento

El número máximo de volúmenes (dispositivos lógicos) que se pueden supervisar para un dispositivo de almacenamiento es de 2000. Cuando los volúmenes de almacenamiento exceden de 2000, el volumen de almacenamiento (Tipo de componente), que se muestra en la ficha **Componentes** del módulo **Supervisión**, refleja la siguiente información y el volumen no se puede supervisar:

- Nombre de componente: Volúmenes (número de volúmenes).
- Estado de componente: No se puede supervisar el volumen porque el número de volúmenes supera 2000.

Además, no se ha obtenido la siguiente información relacionada con el volumen. La información que aparece en el módulo **Supervisión** es la siguiente:

- Ficha **Componentes**. Para los siguientes tipos de componente, no se muestra nada: "LUN", "Sistema de archivos compartidos exportado de almacenamiento", "Puerto de sistema de archivos compartidos de almacenamiento", "Volumen de almacenamiento".
- Ficha **Rendimiento**. Para el ratio de coincidencias de caché de escritura, el estado es Desconocido, y no se obtiene el rendimiento.

Configuración del almacenamiento de EMC

Establezca la configuración del agente SMI-S según las siguientes directrices. Para obtener más información, consulte la documentación del agente SMI-S de EMC.

- Notas de la versión del proveedor de SMI-S de ECM

  Descripción general: método de instalación y método de configuración tras la instalación

  http://Powerlink.EMC.com

Asistencia > **Documentación técnica y avisos** > **Documentación ~ S ~ de software** > **proveedor de SMI-S** > **Notas de la versión**

- Matriz de asistencia de EMC

  Descripción general: objetivo de la asistencia del proveedor de SMI-S de EMC

  http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

Requisitos previos a la instalación

- Versión de proveedor de SMI-S de EMC: V3.2.3, V3.3.1
- Sistema operativo: Microsoft Windows 2003 [x86] R2, SP1
- Matriz de almacenamiento: CLARiiON

Consulte el siguiente enlace para obtener información sobre la matriz de asistencia de EMC para los requisitos de entorno operativo de almacenamiento:

http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

NOTA: El valor de la métrica de rendimiento, **WriteHitIOs**, no se adquiere en EMC CLARiiON.

Para instalar el proveedor de SMI-S de EMC:

Tenga en cuenta que, si está instalado el proveedor de SMI-S de EMC de la versión anterior o Solutions Enabler, se desinstalarán.

1. Descargue el proveedor de SMI-S de EMC del siguiente sitio Web:

   http://Powerlink.EMC.com

2. Navegue a la siguiente ubicación: **Asistencia** > **Descargas de software y licencias** > **Descargas S** > **Proveedor de SMI-S**.
3. Cierre todas las aplicaciones antes de iniciar la instalación.
4. Descargue **se6430-WINDOWS-x86-SMI.msi** o **se65132-WINDOWS-x86-SMI.msi**.
5. Ejecute el archivo ejecutable de la instalación para iniciar el asistente **EMC Solutions Enabler with SMI**.
6. Complete todas las solicitudes en el asistente. Cuando termine, haga clic en **Finish** (Salir).

   Ahora puede registrar la información de almacenamiento.

Para registrar información de almacenamiento:

El siguiente procedimiento garantizará que pueda gestionar el almacenamiento usando el proveedor de SMI-S de EMC.

1. Cuando no se aplica el volumen de almacenamiento de EMC a un servidor en el que está instalado el proveedor de SMI-S de EMC, complete los siguientes pasos fuera de banda. Después del paso j se incluye un ejemplo de la ejecución de comandos que se describe en el siguiente procedimiento:
   a. Ejecute el archivo **TestSmiProvider.exe** que se encuentra en la siguiente ruta: <*Carpeta de instalación*>\SYMCLI\storbin\ TestSmiProvider.exe
   b. Para todos los anfitriones, tipo de conexión, ruta de archivo de registro, puerto, nombre de usuario y contraseña, haga clic en Intro para mantener la información predeterminada.
   c. Escriba **addsys** y, a continuación, haga clic en **Intro**.
   d. Escriba **y** y, a continuación, haga clic en **Intro**.
   e. Seleccione el tipo de matriz de almacenamiento. Para CLARiiON, escriba **1** y, a continuación, haga clic en **Intro**.
   f. Especifique la dirección IP del **Processor A** (Procesador A) y, a continuación, haga clic en **Intro**. También especifique la dirección IP del **Procesador B** (Procesador B) y, a continuación, haga clic en **Intro**, dos veces.
   g. Elija el tipo de dirección especificada en el paso f. Tipo **2** y, a continuación, haga clic en **Intro**.
   h. Especifique el ID de usuario y la contraseña asociada a la autoridad administrativa para el almacenamiento que está registrando.
   i. Cuando el registro se realice correctamente, se mostrará **OUTPUT: 0**. Anote el número de serie indicado en el área aplicable del comando, por ejemplo, CK200080001000.
   j. Escriba **dv** y, a continuación, haga clic en **Intro**. Compruebe si el número de serie que ha anotado en el paso **i** se indica en la **información de versión de firmware**.

Ejemplo de comando

```
Host [localhost]:
Connection Type (ssl,no_ssl) [no_ssl]:
Logfile path [Testsmiprovider.log]:
Port [5988]:
Username []:
Password []:
Connecting to localhost: 5988
(localhost:5988) ? addsys
Add System {y|n} [n]: y
ArrayType (1=Clar, 2=Symm) [1]: 1
```

```
One or more IP address or Hostname or Array ID

Elements for Addresses

IP address or hostname or array id 0 (blank to quit):
192.168.10.31

IP address or hostname or array id 1 (blank to quit):
192.168.10.32

IP address or hostname or array id 2 (blank to quit):

Address types corresponding to addresses specified above.

(1=URL, 2=IP/Nodename, 3=Array ID)

Address Type (0) [default=2]: 2

Address Type (1) [default=2]: 2

User [null]: analyzer

Password [null]: analyzerpass

++++ EMCAddSystem ++++

OUTPUT : 0

Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout,
4=Failed

       5=Invalid Parameter

       4096=Job Queued, 4097=Size Not Supported

System: //kaede/root/
emc:Clar_StorageSystem.CreationClassName="Clar_StorageSys
tem",Name="CLARiiON+CK200080001000"

(localhost:5988) ? dv

++++ Display version information ++++

CIM ObjectManager Name: PG:5B48A8C4-682F-4FCB-AE98-
F0687C31225F

CIMOM Version: Pegasus CIM Server Version 2.6.1

SMI-S spec version: 1.3.0

SMI-S Provider version: V3.3.1.0

Solutions Enabler version: V6.5-883 1.32

Firmware version information:

CLARiiON Array CK200080001000 (Rack Mounted CX3_10_C) :
3.26.10.5.019
```

2. Cuando se aplica el volumen de almacenamiento de EMC a un servidor en el que está instalado el proveedor de SMI-S de EMC, complete los siguientes pasos fuera de banda. Después del paso f se incluye un ejemplo de la ejecución de comandos que se describe en el siguiente procedimiento:
   a. Confirme que, al menos, se ha registrado un CLARiiON LUN. Ejecute el siguiente comando desde el servidor en el que se ha instalado el proveedor de SMI-S de EMC:

      <*Carpeta de instalación*>\SYMCLI\bin> syminq -cids

b. Confirme que ese valor está establecido en **true** para la siguiente configuración:
OslProv/com.emc.se.osls.osl.StorApi.database.discover
Este ajuste se ubica en el archivo de configuración de **emcprovider.conf**: <*Carpeta de instalación*>\SYMCLI\storbin

Si el valor es **false**, cámbielo a **true**.

c. Ejecute el siguiente comando para suspender el servicio del proveedor de SMI-S de EMC:

<*Carpeta de instalación*>\SYMCLI\strobin> cimserver -stop EMC_SMI_Provider

d. Ejecute el siguiente comando para registrar la información de autenticación:

<*Carpeta de instalación*>\SYMCLI\bin>symcfg authorization add -host <*Dirección IP de almacenamiento*> -Username <Identificador de usuario de almacenamiento> -Password <*Contraseña de almacenamiento*>

Los siguientes comandos se ejecutarán a modo de ejemplo cuando la contraseña de IT Operations Analyzer sea **analyzerpass**, la dirección IP del **Procesador A** sea **192.168.10.31**, y la dirección IP del **Procesador B** para CLARiiON sea **192.168.10.32**.
El Procesador A se registra primero:

<*Carpeta de instalación*>\SYMCLI\bin>symcfg authorization add -host

192.168.10.31 -username analyzer -password analyzerpass

<*Carpeta de instalación*>\SYMCLI\bin>symcfg authorization add -host

192.168.10.32 -username analyzer -password analyzerpass

e. Ejecute el siguiente comando para iniciar el servicio de proveedor de SMI-S de EMC. Después, llevará cierto tiempo hasta que pueda buscar desde IT Operations Analyzer:

<*Carpeta de instalación*>\SYMCLI\strobin> cimserver -start EMC_SMI_Provider

f. Ejecute el siguiente comando para confirmar la información de registro:

<*Carpeta de instalación*>\SYMCLI\bin> symcfg list auth

Ejemplo de comando

```
C:\Program Files\EMC\SYMCLI\bin>syminq -cids
Device                 Clariion               Device
------------------------ --------------------- ---------
Name               Type   ID Rev  Ser Num     Cap (KB)
------------------------ --------------------- ---------
\\.\PHYSICALDRIVE2      CK200080001000  0326 070000B5
1048576
```

```
C:\Program Files\EMC\SYMCLI\storbin>cimserver -stop
EMC_SMI_Provider

Pegasus stopped as a Windows service

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.31 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.32 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\storbin>cimserver -start
EMC_SMI_Provider

Pegasus started as a Windows service

C:\Program Files\EMC\SYMCLI\bin>symcfg list auth

Hostname            Username          Namespace     Port

192.168.10.31         analyzer

192.168.10.32         analyzer
```

Obtención del rendimiento de almacenamiento de EMC

Utilice el siguiente procedimiento para obtener los datos de rendimiento del almacenamiento de EMC.

1. Utilice el software de gestión de almacenamiento de EMC para obtener los datos de rendimiento. Por ejemplo, a continuación se muestran las instrucciones de **EMC Navisphere Management Suite**:
   a. Abra la ventana **Data Logging** (Inicio de sesión de datos) desde la barra de menús de **EMC Navisphere Management Suite**: En el menú **Herramientas**, seleccione **Analyzer** y, a continuación, **Data Logging (Inicio de sesión de datos)...**
   b. En el área **Target** (Destino), seleccione el almacenamiento del que desea obtener el rendimiento y confirme el campo **Status** (Estado) para el inicio de sesión**:**

      Si **Status** (Estado) es **Stopped** (Detenido), haga clic en **Start** (Iniciar).

      Si **Status** (Estado) es **Running. Started on date time** (En ejecución. Iniciado a las), haga clic en **Cancel** (Cancelar).
      No es necesario reiniciar el agente SMI-S.
2. Reinicie el proveedor de SMI-S. Si utiliza la CLI, ejecute el comando `cimserver` y, a continuación, detenga e inicie el proveedor de SMI-S:

```
<Installation folder>\SYMCLI\strobin> cimserver -stop
EMC_SMI_Provider

Pegasus stopped as a Windows service

<Installation folder>\SYMCLI\strobin> cimserver -start
EMC_SMI_Provider

Pegasus started as a Windows service
```

Tabla 7-5: Información para la conexión a almacenamiento de EMC

Elemento	Detalles
Dirección IP	Utilice la dirección IP del servidor en el que está instalado el proveedor de SMI-S de ECM.
Espacio de nombres	Especifique `root/emc`.
Existencia de SSL	Utilice la configuración del proveedor de EMC.
Número de puerto	Utilice la configuración del proveedor de SMI-S de ECM. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario del proveedor de EMC. Predeterminado, vacío.
Contraseña	Utilice la contraseña asociada al identificador de usuario. Predeterminado, vacío.

Configuración del almacenamiento de la serie HP EVA

Establezca la configuración del proveedor de SMI-S según las siguientes directrices. Para obtener más información, consulte los manuales de Command View EVA.

NOTA: SMI-S Agent de la serie HP EVA no admite la función de recopilación de información de rendimiento.

Requisitos previos a la instalación

- Versión admitida: HP StorageWorks Command View EVA 8.0
- Sistema operativo: Microsoft Windows Server 2003
- Almacenamiento: HP StorageWorks 4400 Enterprise Virtual Array

Para instalar HP StorageWorks Command View EVA 8.0:

1. Ejecute el archivo ejecutable HP StorageWorks Command View EVA Software Suite.exe.
2. Haga clic en **Aceptar** para iniciar el asistente de instalación.
3. En el panel de instalación, **Choose Install Set** (Seleccionar conjunto de instalación), compruebe que **SMI-S CIMOM** está seleccionado.

   HP SMI-S EVA utiliza el número de puerto predeterminado 5988 o 5989.

   Si no es posible utilizar los puertos predeterminados, aparecerá un mensaje indicando los puertos que no están disponibles. Si obtiene un mensaje de este tipo, indique el número de puerto disponible (de 60000 a 65536). A continuación, continúe con la instalación.
4. El último panel del asistente de instalación muestra **Install Complete** (Instalación completa). Para terminar, haga clic en **Done** (Hecho).

   Ahora, puede aplicar la configuración de HP Command View EVA.

Para aplicar la configuración de HP Command View EVA:

1. Configure el servidor CIMOM:
   a. Modifique el siguiente archivo para cambiar el número de puerto y HTTP/HTTPS que se utiliza para el servidor CIMOM:

      <*Directorio de instalación*>\SMI-S\CXWSCimom\config\cxws.properties

   b. A continuación, se indican los valores predeterminados:

      enableHttp: true

      enableHttps: true

      cxws.http.port: 5988

      cxws.https.port: 5989

      Especifique **False** (Falso) cuando invalide enableHttp (Https) y especifique el número de puerto que se va a usar.

c. Después de cambiar la configuración, reinicie StorageWorks CIM Object Manager Service (servicio Administrador de objetos CIM de HP StorageWorks):

   En el menú **Inicio**, seleccione: **Ajuste**, **Panel de control**, **Herramienta de gestión**, a continuación, **Servicio**.

NOTA: En Windows Server 2012, los pasos para navegar al menú Inicio son diferentes.

2. Registre el almacenamiento:
   a. Abra el explorador y especifique la siguiente URL:

      https://host_name:2372

      Especifique el **Nombre de servidor** o la **Dirección IP** para **host_name**.

   b. Inicie sesión en la **solicitud del HP Command View EVA**.

      Cuando inicie la sesión, use la información de cuenta de usuario para el servidor en el que ha instalado HP Command View EVA. Asegúrese de que la cuenta de usuario pertenece al **Grupo de administración de almacenamiento HP**.

   c. Cuando haya iniciado una sesión, confirme que el almacenamiento se muestra en el panel **Sistema de almacenamiento**. Si no se muestra, haga clic en **Detectar** para registrar el almacenamiento.

NOTA: Para que el almacenamiento se registre, el servidor en el que se ha instalado HP Command View EVA debe estar conectado directamente con el conmutador FS.

Tabla 7-6: Información para la conexión al almacenamiento HP EVA

Elemento	Detalles
Dirección IP	Utilice la dirección IP del servidor en el que está instalado Command View EVA.
Espacio de nombres	Especifique `root/eva`.
Existencia de SSL	Utilice la configuración de Command View EVA.
Número de puerto	Utilice la configuración de Command View EVA. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario de Command View EVA.
Contraseña	Utilice la contraseña asociada al identificador de usuario.

Configuración del almacenamiento de la serie HP MSA

Establezca la configuración del agente SMI-S según el siguiente procedimiento. Para obtener más información, consulte los documentos del agente SMI-S de MSA.

NOTA: El agente SMI-S de la serie HP MSA no admite la función de recopilación de información de rendimiento.

1. Descargue el **proveedor de SMI-S de MSA** de la siguiente Web:
   http://h18006.www1.hp.com/storage/smis.html
2. Instale el **proveedor de SMI-S de MSA** en cualquier servidor.

Tabla 7-7: Información para la conexión al almacenamiento HP MSA

Elemento	Detalles
Dirección IP	Utilice la dirección IP del servidor en el que está instalado el proveedor de SMI-S de MSA.
Espacio de nombres	Especifique `root/hpmsa`.
Existencia de SSL	Utilice la configuración del proveedor de SMI-S de MSA.
Número de puerto	Utilice la configuración del proveedor de SMI-S de MSA.
Identificador de usuario	Utilice el identificador de usuario del proveedor de SMI-S de MSA.
Contraseña	Utilice la contraseña asociada al identificador de usuario.

Configuración de almacenamiento de IBM y de Engenio OEM Sun

Establezca la configuración del proveedor de SMI-S según el siguiente procedimiento. Para obtener más información, consulte los documentos del proveedor de SMI-S de Engenio. Para descargar los documentos se necesita una cuenta de inicio de sesión en el sitio web de NetApp:

http://support.netapp.com/NOW/apbu/oemcp/protcd/

Requisitos previos a la instalación

- Versión admitida: proveedor de SMI de Engenio 09.19.G0.07
- Sistema operativo: Microsoft Windows Server 2003 (32 bits)

Para instalar el proveedor de SMI-S de Engenio:

1. Ejecute el archivo ejecutable para instalar el proveedor de SMI de Engenio 09.19.G0.07.
2. Complete todas las solicitudes del asistente de instalación.
3. Cuando haya completado la instalación, haga clic en **Done** (Hecho).

Para registrar el dispositivo de almacenamiento:

El siguiente procedimiento registra el dispositivo de almacenamiento que desea gestionar, utilizando el proveedor de SMI de Engenio.

1. Inicie la solicitud de comando.
2. Pase al siguiente directorio:
   <Directorio de instalación>\SMI_SProvider\bin

3. Ejecute el comando `ProviderUtil` e introduzca la siguiente información:
   - **Input CIMOM Username**

     Opcionalmente, especifique el nombre de usuario de CIMOM, por ejemplo: cualquiera
   - **Input CIMOM Password**

     Opcionalmente, especifique la contraseña de CIMOM, por ejemplo: cualquiera
   - **Input Port [5988]**

     Opcionalmente especifique un número de puerto. El valor predeterminado es 5988.
   - **Input Operation**

     1) add Device

     2) remove Device

     3) Add credentials for an array

     Please Input 1, 2, or 3

     Especifique **1** para registrar un dispositivo de almacenamiento.
   - **Input device DNS-resolvable hostname or IP address**

     Especifique la dirección IP o el nombre de anfitrión para el dispositivo de almacenamiento.
   - **Input Array Password** (en blanco de forma predeterminada)

     Especifique la contraseña del dispositivo de almacenamiento.

   El dispositivo de almacenamiento se habrá registrado correctamente cuando se muestre el mensaje **The extrinsic call succeeded** (Llamada extrínseca realizada correctamente).

La Tabla 7-8 muestra la información necesaria para conectarse al nodo de almacenamiento que desea supervisar.

Tabla 7-8: Información para la conexión al almacenamiento de IBM y de Engenio OEM Sun

Elemento	Detalles
Dirección IP	Utilice la dirección IP del servidor en el que está instalado el proveedor de SMI-S de Engenio.
Espacio de nombres	Especifique `root/lsissi11`.
Existencia de SSL	Utilice la configuración del proveedor de SMI-S de Engenio.
Número de puerto	Utilice la configuración del proveedor de SMI-S de Engenio. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario del proveedor de SMI-S de Engenio.
Contraseña	Utilice la contraseña asociada al identificador de usuario.

Configuración del almacenamiento de NetApp

Establezca la configuración del proveedor de SMI-S para el almacenamiento de NetApp según el siguiente procedimiento. Para obtener más información, consulte la documentación del proveedor de SMI-S de NetApp. Para descargar los documentos se necesita una cuenta de inicio de sesión en el sitio web de NetApp:

http://support.netapp.com/NOW/apbu/oemcp/protcd/

Requisitos previos a la instalación

- Versión admitida del agente SMI-S de NetApp Data ONTAP: Data ONTAP SMI-S Agent 3.0.
- Sistema operativo: Microsoft Windows Server 2003 (32 bits)

Son necesarios JDK 1.5.0 o posterior y JRE 1.5.0 para utilizar el agente SMI-S de NetApp Data ONTAP. Confirme si la información está instalada en el servidor de Windows en el que instalará el agente SMI-S.

Para instalar el agente SMI-S de Data ONTAP SMI-S 3.0:

1. Descargue el archivo de instalación del agente SMI-S de Data ONTAP.
2. Seleccione **Windows** en **Select Platform** (Seleccionar plataforma) del **Data ONTAP SMI-S Agent** (Agente SMI-S de Data ONTP) y, a continuación, haga clic en **Go** (Ir).
3. Haga clic en **View & Download** (Ver y descargar).
4. Haga clic en **CONTINUE** (CONTINUAR) en la página **Software download Instructions** (Instrucciones para la descarga de software).
5. Haga clic en **Accept** (Aceptar) para continuar. Descargue el agente SMI-S y los manuales correspondientes.
6. Ejecute el archivo ejecutable para instalar el agente SMI-S de Data ONTAP 3.0.
7. Según su preferencia, indique el tipo de instalación, **Typical** (Típica) o **Custom** (Personalizada), que preferiría seguir.
8. Complete todas las solicitudes del asistente de instalación.
9. Cuando haya completado la instalación, haga clic en **Finish** (Salir).

Para configurar el proveedor de SMI-S:

1. En el diálogo **Edit System Variable** (Editar variable del sistema), especifique **JAVA_HOME** como la variable de entorno de sistema o la variable de entorno de usuario. Si especifica una ruta que contiene un espacio en blanco, incluya la ruta con comilla (").
2. Para conectarse al proveedor de SMI-S, utilice el número de puerto **5989** y el protocolo **https**. Para cambiar el número de puerto o activar la conexión con el protocolo http, edite el archivo **WEBSconfig.ini** que se encuentra en el siguiente directorio: **C:\Program Files\ws\server\cserver\bin**. A continuación, se incluye la configuración predeterminada que se enumera en el archivo **WEBSconfig.ini**. Si la cambia, establezca **enableOverride** en **True**.

   enableOverride=False (debe establecerse en **True** si modifica alguno de los parámetros posteriores)

HTTPPort=5988

HTTPSPort=5989

enableSSL=True

enableHTTP=False

Para registrar el dispositivo de almacenamiento:

1. Desde el símbolo del sistema, pase a la siguiente ruta:

   C:\Program Files\ws\server\cserver\bin

2. Especifique **C:\Program Files\ws\bin**

3. Para registrar el dispositivo de almacenamiento, ejecute el siguiente comando:

   ```
   smis.bat <Identificador de usuario> <Contraseña> add <Dirección IP de
   almacenamiento> <Identificador de usuario de almacenamiento>
   <Contraseña de almacenamiento> [-p http]*
   ```

   *Especificar sólo si utiliza el protocolo http.

   < Identificador de usuario > y < Contraseña > utilizan la cuenta de autoridad de administración de Windows si el servidor está instalado en SMI-S. La dirección IP del dispositivo, el < Identificación de usuario de almacenamiento > y < Contraseña de almacenamiento > especifican la información autenticación del almacenamiento para < IP de almacenamiento >.

4. Para comprobar que esta información se ha registrado, ejecute el archivo **smis.bat**:

   ```
   smis.bat <Identificador de usuario> <Contraseña> list
   ```

5. Ejecute el script natest que se encuentra en el directorio **ws\bin** para comprobar si el proveedor de SMI-S podría obtener la información de almacenamiento. El ejemplo siguiente da como resultado información de disco del almacenamiento:

   ```
   Discos natest.bat <Identificador de usuario> <Contraseña>
   ```

Tabla 7-9 enumera la información necesaria cuando se conecta al almacenamiento NetApp.

Tabla 7-9: Información para la conexión a almacenamiento de NetApp

Elemento	Detalles
Dirección IP	Especifique la dirección IP del servidor en el que está instalado el agente SMI-S de Data ONTAP.
Espacio de nombres	Especifique `root/ontap`.
Existencia de SSL	Utilice la configuración del el agente SMI-S Data ONTAP.
Número de puerto	Utilice la configuración del el agente SMI-S Data ONTAP. De forma predeterminada: • Comunicación no SSL: 5988 • Comunicación SSL: 5989
Identificador de usuario	Utilice el identificador de usuario del servidor en el que está instalado el agente SMI-S Data ONTAP.
Contraseña	Utilice la contraseña asociada al identificador de usuario.

NOTA: En el módulo **Supervisión**, al seleccionar un nodo de almacenamiento NetApp, aparece un icono cuando IT Operations Analyzer procesa la información de estado o cuando recopila información del componente. Además, el siguiente mensaje de error podría aparecer a los 15 minutos:

KAZZ20087-E La actualización de la configuración no se ha realizado correctamente. Nombre del nodo en el que se ha producido el fallo: <Nombre de dispositivo>

Este mensaje de error aparece cuando se cumplen todas las condiciones siguientes:

1. El almacenamiento NetApp se está supervisando.
2. El almacenamiento NetApp se gestiona en un servidor Linux utilizando una versión del agente SMI-S para Linux.
3. Existe una conexión HTTPS entre el servidor de gestión de IT Operations Analyzer y el agente SMI-S de la versión Linux que se está supervisando.

Lleve a cabo una de las siguientes tareas:

- Registre la dirección IP y el nombre de anfitrión del agente SMI-S de la versión Linux en el archivo de anfitrión del servidor en el que está instalado IT Operations Analyzer: el servidor de gestión.
- Cambie el método de conexión HTTPS utilizado entre el servidor de gestión de IT Operations Analyzer y el agente SMI-S de la versión Linux, a HTTP.
- Cambie el agente SMI-S de la versión Linux al agente SMI-S de la versión Windows.

8

Preparación de los servidores Dell

Este capítulo describe las tareas necesarias para configurar los servidores Dell.

Descripción general

Deben configurarse dos de cada una de las siguientes opciones:

- WMI/SNMP para servidor Dell basado en Windows (información de credencial).
- SSH/SNMP para servidor Dell basado en Linux (información de credencial).

La Tabla 8-1 muestra la información necesaria para conectarse a un servidor Dell.

Tabla 8-1: Información para la conexión a un servidor Dell

Elemento	Detalles
Dirección IP	Especifique la dirección IP del servidor Dell.
Número de puerto	El puerto SNMP en el que el servidor Dell espera la comunicación (puerto 161).
Nombre de comunidad	Nombre de comunidad utilizado por el servidor Dell SNMP.

Activación del servicio SNMP y comunicación mediante capturas

El agente SNMP de cada servidor Dell supervisado debe configurarse para enviar capturas SNMP al servidor de gestión de Hitachi IT Operations Analyzer.

Cuando se recibe una captura OMSA de Dell de un servidor, IT Operations Analyzer actualiza el estado del Componente de captura OMSA de Dell basándose en la gravedad de la captura recibida.

Configuración de un agente SNMP en un entorno de Microsoft Windows

Para configurar el Agente SNMP del servidor Dell en un entorno de Microsoft Windows:

1. Desde el menú **Inicio de su Escritorio**, seleccione **Panel de control**.

NOTA: En Windows Server 2012, los pasos para navegar al menú Inicio son diferentes.

2. Abra **Herramientas administrativas**.
3. Abra **Servicios**.
4. Haga clic con el botón derecho en **Servicio SNMP** y seleccione **Propiedades**.
5. Haga clic en la ficha **Seguridad** para abrir el cuadro de diálogo **Seguridad**.
6. Seleccione **Aceptar paquetes SNMP de cualquier host** o seleccione **Aceptar paquetes SNMP de estos hosts** y, a continuación, haga clic en **Agregar**.

   Aparece la casilla **Configuración del servicio SNMP**.

7. Introduzca el nombre de anfitrión o la dirección IP del servidor de gestión de IT Operations Analyzer y haga clic en **Agregar**.
8. Haga clic en la ficha **Capturas** para abrir el cuadro de diálogo **Capturas**.
9. Seleccione el nombre de comunidad SNMP adecuado de la lista desplegable **Nombre de comunidad** y, a continuación, haga clic en **Agregar** bajo la lista **Destinos de capturas**.

   Aparece la casilla **Configuración del servicio SNMP**.
10. Introduzca el nombre de anfitrión o la dirección IP del servidor de gestión de IT Operations Analyzer y haga clic en **Agregar**.
11. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Configuración del agente SNMP en un entorno de Linux

Para configurar el Agente SNMP del servidor Dell en un entorno de Red Hat Enterprise Linux:

1. Añada la línea siguiente al archivo de configuración **/etc/snmp/snmpd.conf**:

   trapsink IP_address community_name

   El valor de la variable **IP_address** es la dirección IP del servidor de gestión de IT Operations Analyzer. El valor de la variable **community_name** es el nombre de la comunidad SNMP.

2. Reinicie el agente SNMP mediante el comando siguiente:

   /sbin/service snmpd restart

Índice

T

Hitachi Data Systems

Sede corporativa
2845 Lafayette Street
Santa Clara, California 95050-2639
EE. UU.
www.hds.com

Información de contacto regional

América
+1 408 970 1000
info@hds.com

Europa, Oriente Medio y África
+44 (0)1753 618000
info.emea@hds.com

Pacífico asiático
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-90IOS006ES-12