HP Operations Agent y HP Operations Smart Plug-ins for Infrastructure

Para Sistemas operativos Windows ®, Linux, HP-UX, Solaris y AIX

Versión de software: 11.10

Guía de instalación y configuración

Fecha de publicación del documento: Septiembre de 2012

Fecha de publicación del software: Septiembre de 2012

Avisos legales

Garantía

Las únicas garantías de los productos y servicios HP se exponen en el certificado de garantía que acompaña a dichos productos y servicios. El presente documento no debe interpretarse como una garantía adicional. HP no es responsable de omisiones, errores técnicos o de edición contenidos en el presente documento.

La información contenida en esta página está sujeta a cambios sin previo aviso.

Leyenda de derechos limitados

Software informático confidencial. Es necesario disponer de una licencia válida de HP para su posesión, uso o copia. De conformidad con FAR 12.211 y 12.212, el Gobierno estadounidense dispone de licencia de software informático de uso comercial, documentación del software informático e información técnica para elementos de uso comercial con arreglo a la licencia estándar para uso comercial del proveedor.

Aviso de copyright

© Copyright 2010 - 2012 Hewlett-Packard Development Company, L.P.

Avisos de marcas comerciales

Intel® e Itanium® son marcas comerciales de Intel Corporation en EE.UU. y otros países.

Microsoft®, Windows® y Windows Vista® son marcas comerciales registradas en EE.UU. de Microsoft Corporation.

UNIX® es una marca comercial registrada de The Open Group.

Reconocimientos

Este producto incluye software criptográfico escrito por Eric Young (eay@cryptsoft.com).

Este producto incluye software desarrollado por OpenSSL Project para su uso en OpenSSL Toolkit (http://www.openssl.org/).

Este producto incluye software escrito por Tim Hudson (tjh@cryptsoft.com).

Este producto incluye software desarrollado por Apache Software Foundation (http://www.apache.org/).

Este producto incluye una interfaz de la biblioteca de compresión de uso general 'zlib' con Copyright © 1995-2002 Jean-loup Gailly y Mark Adler.

Actualizaciones de la documentación

La página de título de este documento contiene la siguiente información de identificación:

- Número de versión del software, que indica la versión del software.
- Fecha de publicación del documento, que cambia cada vez que se actualiza el documento.
- Fecha de lanzamiento del software, que indica la fecha desde la que está disponible esta versión del software.

Para buscar actualizaciones recientes o verificar que está utilizando la edición más reciente de un documento, visite:

http://h20230.www2.hp.com/selfsolve/manuals

Este sitio requiere que esté registrado como usuario de HP Passport. Para registrarse y obtener un ID de HP Passport, visite:

http://h20229.www2.hp.com/passport-registration.html

O haga clic en el enlace **New user registration** (Registro de nuevos usuarios) de la página de registro de HP Passport.

Asimismo, recibirá ediciones actualizadas o nuevas si se suscribe al servicio de soporte del producto correspondiente. Póngase en contacto con su representante de ventas de HP para obtener más información.

Soporte

Visite el sitio web HP Software Support Online en:

http://www.hp.com/go/hpsoftwaresupport

Este sitio web proporciona información de contacto y detalles sobre los productos, servicios y soporte que ofrece HP Software.

HP Software Support Online brinda a los clientes la posibilidad de auto-resolución de problemas. Ofrece una forma rápida y eficaz de acceder a las herramientas de soporte técnico interactivo necesarias para gestionar su negocio. Como cliente preferente de soporte, puede beneficiarse de utilizar el sitio web de soporte para:

- Buscar los documentos de la Base de conocimiento que le interesen
- Enviar y realizar un seguimiento de los casos de soporte y las solicitudes de mejora
- Descargar revisiones de software
- Gestionar contratos de soporte
- Buscar contactos de soporte de HP
- Consultar la información sobre los servicios disponibles
- Participar en debates con otros clientes de software
- Investigar sobre formación de software y registrarse para recibirla

Para acceder a la mayor parte de las áreas de soporte es necesario que se registre como usuario de HP Passport. En muchos casos también será necesario disponer de un contrato de soporte. Para registrarse y obtener un ID de HP Passport, visite:

http://h20229.www2.hp.com/passport-registration.html

Para obtener más información sobre los niveles de acceso, visite:

http://h20230.www2.hp.com/new_access_levels.jsp

Contenido

Guía de instalación y configuración 1

Contenido 5

Introducción 8

Planificación de la instalación 8

Registro de HP Operations Agent en el servidor de administración de HPOM (e instalación de SPI de infraestructura) 11

Registro en HPOM para el servidor de administración de Windows 11

Registro en HPOM en un servidor de administración de UNIX/Linux 14

Eliminación del paquete de implementación de HP Operations Agent 17

Requisitos para instalar HP Operations Agent 19

Requisitos para Windows 19

Requisitos para Linux 21

Requisitos para HP-UX: 23

Requisitos para Solaris 24

Requisitos para AIX 26

Notas de actualización 27

Tarea previa a la instalación: para instalar HP Operations Agent en HPOM en clúster 30

Instalación desde la consola de HPOM 31

Instalación manual de HP Operations Agent en el nodo 32

Tarea posterior a la instalación en un entorno NAT 37

Instalación de Agent en el modo inactivo 39

Configuración de certificados para el cliente de Operations Agent 43

Solicitud de certificados con una clave de instalación 43

Solicitud automática de los certificados 44

Implementación manual de certificados 45

Restauración de certificados 46

HP Operations Agent en clústeres High Availability 48

Implementación de HP Operations Agent en un entorno seguro 54
Configuración de servidores proxy 55
Organización del archivo de configuración del proxy 58
Configuración del puerto de Communication Broker 61
Configuración de los puertos de comunicación local 63
Configuración de nodos con varias direcciones IP 64
Configuración de la comunicación HTTPS a través de proxys 65
Comunicación en un entorno de alta seguridad 66
Introducción a Reverse Channel Proxy 67
Configuración de una comunicación segura en un entorno sólo de salida 69
Especificación de los detalles de RCP con un archivo de configuración 72
Configuración de un RCP para varios sistemas 72
Comprobación de la comunicación a través de RCP 73
Comunicación a través de dos cortafuegos 74
Configuración del Componente Performance Collection de manera remota 76
Antes de comenzar 76
Implementación de la política OA-PerfCollComp-opcmsg 77
Configuración del Componente Performance Collection 77
Configuración del archivo parm 77
En HPOM para Windows 78
En HPOM en UNIX/Linux 9.10 78
Configuración del archivo alarmdef 79
En HPOM para Windows 79
En HPOM en UNIX/Linux 9.10 80
Trabajar de manera remota con HP Operations Agent 81
Monitorización de HP Operations Agent 83
Antes de comenzar 83
Políticas Self Monitoring 84
Implementación de las directivas Self Monitoring 85
Visualización del estado de los componentes 86
Instalación sólo de los SPI de infraestructura 87
Componentes de los Infrastructure SPI en HPOM para Windows 92

Componentes de Infrastructure SPI en HPOM para UNIX 94

Desinstalación de HP Operations Agent 96

Desinstalación de SPI de infraestructura 97

Capítulo 1

Introducción

HP Operations Agent permite monitorizar un sistema recopilando métricas que indican el estado, rendimiento y disponibilidad de los elementos fundamentales del sistema. Mientras que HP Operations Manager ((HPOM) proporciona el marco de trabajo para monitorizar y administrar múltiples sistemas mediante una única consola interactiva, HP Operations Agent, implementado en nodos independientes, permite compilar información crucial para llevar a cabo el proceso de monitorización.

El soporte en DVD de *HP Operations Agent y SPI de infraestructura SPIs 11.10* proporciona HP Operations Smart Plug-ins for Infrastructure (SPI de infraestructura). Si desea instalar los SPI de infraestructura con el soporte electrónico, asegúrese de descargar el soporte para *todas* las plataformas del nodo (no un archivo ISO específico de la plataforma). Los archivos ISO específicos de una plataforma no contienen los SPI de infraestructura.

Planificación de la instalación

Instalación remota de HP Operations Agent desde el servidor de administración de HPOM

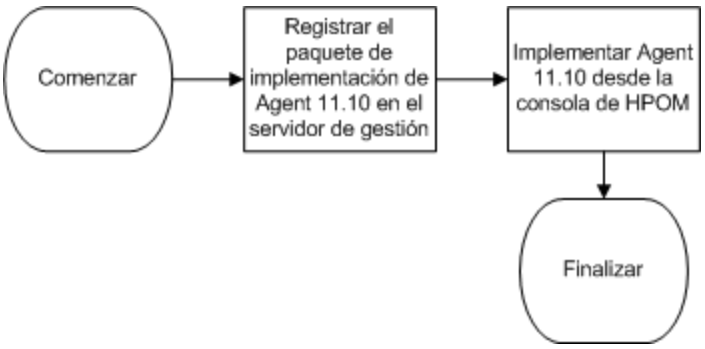
En un entorno de monitorización centralizada con HPOM, puede instalar los paquetes de implementación de HP Operations Agent 11.10 en el servidor de gestión y, a continuación, implementar centralmente los paquetes de Agent en los diferentes nodos desde la consola de HPOM.

Este proceso implica:

1. **Registro** de los paquetes de implementación de HP Operations Agent 11.10 en el servidor de administración de HPOM.

   El proceso de registrar automáticamente los paquetes de implementación de HP Operations Agent instala SPI de infraestructura en el servidor de administración de HPOM. Puede configurar el instalador para que omita la instalación de SPI de infraestructura.

2. Instalación centralizada de HP Operations Agent desde la consola de HPOM



Instalación manual de HP Operations Agent en el nodo

HP Operations Agent se puede instalar desde el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10*, para lo que es preciso iniciar sesión en el nodo gestionado.

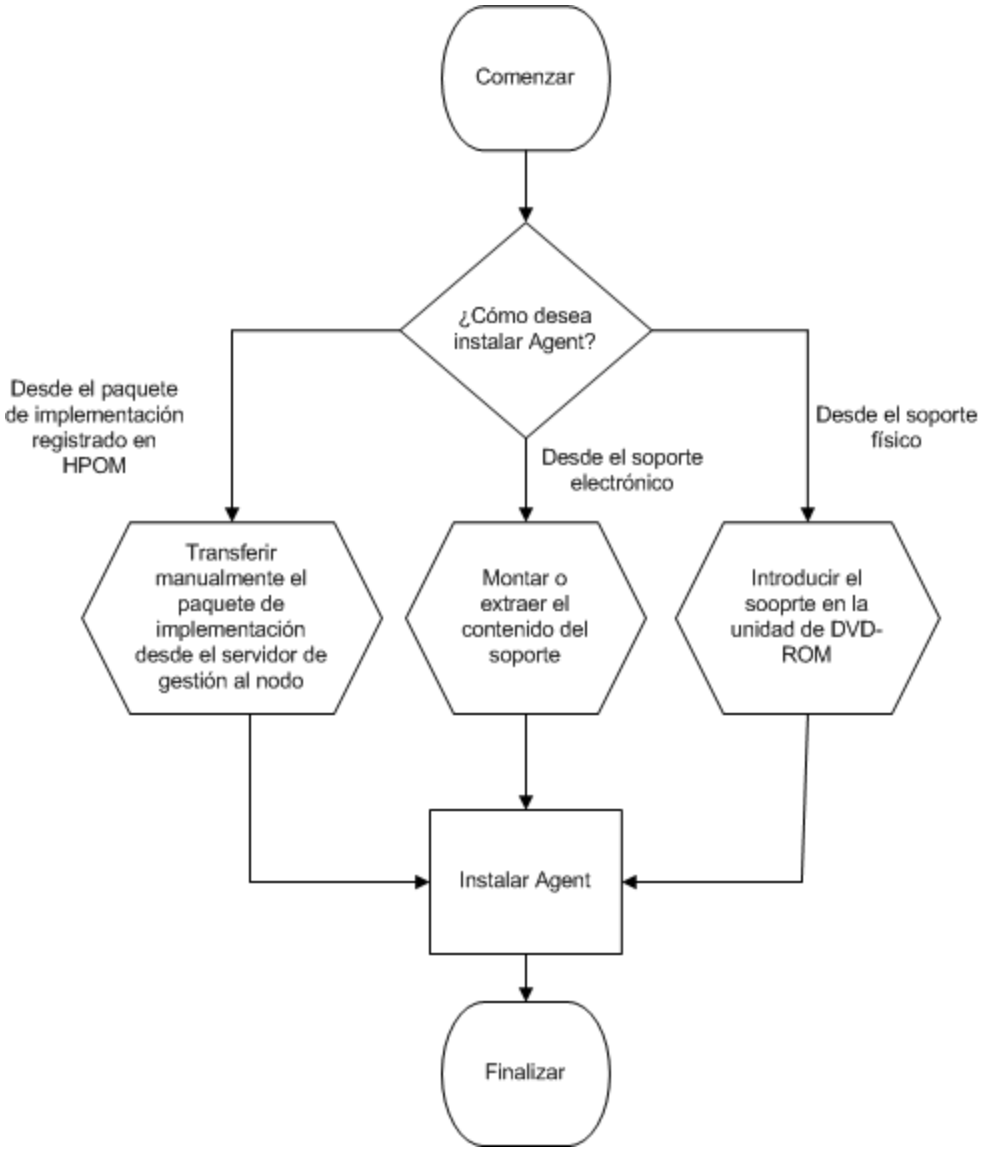
Este proceso implica:

1. Preparación del nodo

   Para preparar un nodo gestionado para la instalación de Agent, puede realizar una de las siguientes acciones:

   - Introduzca el soporte físico de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en la unidad de DVD.
   - Extraiga el contenido del soporte electrónico de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en un directorio local.
   - Monte el soporte físico de *HP Operations Agent y SPI de infraestructura SPIs 11.10*.
   - Transfiera manualmente los paquetes de implementación desde el servidor de administración de HPOM

2. Instale Agent con el programa de instalación (`oainstall` o `oasetup`) disponible en el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10* o el paquete de implementación.



Instalación sólo de los SPI de infraestructura

SPI de infraestructura sólo se puede instalar en el servidor de administración de HPOM usando *HP Operations Agent y SPI de infraestructura SPIs 11.10*.

Este proceso implica:

1. Preparación de un archivo de configuración en el servidor de administración de HPOM.
2. Instalación de SPI de infraestructura con el programa de instalación (`oainstall` o `oasetup`) disponible en el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10*.

Capítulo 2

Registro de HP Operations Agent en el servidor de administración de HPOM (e instalación de SPI de infraestructura)

Registro en HPOM para el servidor de administración de Windows

Requisitos previos

- No se deben ejecutar tareas de implementación en el momento de registrar el paquete de implementación.

  Para ver las tareas de implementación activas:

1. En el árbol de la consola, amplíe Gestión de políticas.
2. Haga clic en **Trabajos de despliegue**. En el panel de detalles se muestra la lista de las tareas de implementación activas. Es necesario asegurarse de que ninguna de las tareas de implementación está activa en el momento de instalar los paquetes de implementación del agente. No debe iniciar ninguna tarea de implementación hasta que el registro del paquete de implementación de Agent esté completa.

- Si la versión implementable de HP Performance Agent 4.70 para Windows o AIX está disponible en el servidor de gestión, debe instalar la versión implementable de HP Performance Agent 4.72 o quitar la versión implementable de HP Performance Agent 4.70 completamente antes de registrar los paquetes de implementación de HP Operations Agent 11.10.
- Espacio en disco: 1 GB

Registro del paquete de implementación

1. Inicie una sesión en el servidor de administración con privilegios administrativos.
2. Realice una de las siguientes tareas:
   - Si desea registrar el paquete de implementación con el soporte físico, inserte el DVD de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en la unidad de DVD-ROM.
   - Descargue el soporte de instalación de uno de los sitios web de HP. En los sitios web de HP hay diferentes archivos .iso específicos de cada plataforma para los paquetes de implementación de HP Operations Agent 11.10. Puede descargar un archivo .iso específico de una plataforma o el archivo .iso que incluya paquetes de implementación para todas las plataformas.

     Si desea instalar los SPI de infraestructura, use el DVD físico o el archivo .iso que incluye paquetes de implementación para todas las plataformas. Los archivos .iso específicos de una plataforma no contienen los SPI de infraestructura.

3. *Opcional.* Cree un archivo de configuración para omitir la instalación de los SPI de infraestructura.

   El programa `oainstall` instala los SPI de infraestructura en el servidor de gestión al registrar el paquete de implementación. Esta instalación incluye los paquetes de informes (para usarlos con HP Reporter) y gráficos (para usarlos con HP Performance Manager) para los SPI de infraestructura. Si desea desea omitir la instalación de los SPI de infraestructura, siga estos pasos:

   i. Cree un archivo con un editor de texto.

   ii. Añada el siguiente contenido:

   ```
   [agent.parameter]
   REGISTER_AGENT=YES
   [hpinfraspi.parameter]
   InfraSPI=NO
   InfraSPI_With_Graphs=NO
   InfraSPI_With_Reports=NO
   ```

   iii. Guarde el archivo.

4. En la raíz del soporte, ejecute el siguiente comando:

   cscript oainstall.vbs -i -m

   El comando registra los paquetes de implementación del agente para todas las plataformas en el servidor de gestión e instala los SPI de infraestructura.

   Si no desea instalar los SPI de infraestructura y ha realizado el paso 3, ejecute el siguiente comando:

   cscript oainstall.vbs -i -m -spiconfig <*archivo de configuración*>

   Sugerencia: Si lo desea, puede elegir registrar los paquetes de implementación sólo para determinadas plataformas. Sin embargo, el comando para registrar paquetes de implementación específicos de una plataforma no puede instalar los SPI de infraestructura.

   Ejecute el siguiente comando para instalar el paquete de implementación sólo para una plataforma:

   cscript oainstall.vbs -i -m -p <*plataforma*>

   En este caso, use uno de los siguientes valores para <*plataforma*>:

   Para Windows: WIN

   Para HP-UX: HP-UX

   Para Linux: LIN

   Para Solaris: SOL

   Para AIX: AIX

> Para registrar paquetes de implementación de varias plataformas de nodo con un solo comando, use varias opciones -p separadas por espacios.
>
> Por ejemplo:
>
> **cscript oainstall.vbs -i -m -p AIX -p SOL**

Si HPOM está en un clúster de alta disponibilidad (HA)

Siga los pasos anteriores en el nodo activo del clúster de alta disponibilidad (HA) de HPOM:

Después de realizar todos los pasos, y pasar al nodo pasivo, vaya al directorio `%OvShareDir%server\installation` en el nodo pasivo y ejecute el siguiente comando:

cscript oainstall_sync.vbs

Después de ejecutar el comando de instalación con las opciones y argumentos necesarios, se inicia el proceso de registro. Según el número de paquetes seleccionados, el proceso de registro puede tardar hasta 20 minutos en completarse.

Verificación

1. En el servidor de administración, vaya a la ubicación siguiente:

   `%ovinstalldir%bin\OpC\agtinstall`

2. Ejecute el comando siguiente:

   cscript oainstall.vbs -inv -listall

   El comando muestra la lista de los paquetes de implementación disponibles (activos) en el servidor de administración.

3. Localice una plataforma para la que ha instalado el paquete de implementación. Si la versión activa aparece como 11.10, la instalación es correcta.

Archivo de registro

El archivo de registro del registro (`oainstall.log`) está disponible en el directorio:

`%OvDataDir%shared\server\log`

Colocación de paquetes

Al registrar los paquetes de HP Operations Agent en el servidor de gestión, el programa `oainstall` coloca todos los paquetes de implementación necesarios en el siguiente directorio:

`%OvDataDir%shared\Packages\HTTPS`

Copia de seguridad de los paquetes de implementación

Al registrar los paquetes de implementación en el servidor de gestión, el script `oainstall` guarda una copia de los paquetes de implementación antiguos en el siguiente directorio local.

`%OvShareDir%server\installation\backup\HPOpsAgt\`*<OS>\<OA_Version>\<ARCH>*

Para ver los paquetes de implementación activos, ejecute el siguiente comando:

cscript oainstall.vbs -inv

Para todos los paquetes (activos y de copia de seguridad) del sistema, ejecute el siguiente comando:

cscript oainstall.vbs -inv -listall

```
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Active Versions
===============
AIX      :PowerPC(64)     :11.10.033
HP-UX    :IPF32           :11.10.033
HP-UX    :PA-RISC         :11.10.033
LIN      :PowerPC(2.6)    :11.10.033
LIN      :x64(2.6)        :11.10.033
LIN      :x86(2.6)        :11.10.033
SOL      :SPARC           :11.10.033
SOL      :x86             :11.10.033
WIN      :x64             :11.10.033
WIN      :x86             :11.10.033

Backed-up Versions
==================
AIX      :PowerPC(32)     :08.60.005
AIX      :PowerPC(64)     :08.60.005
AIX      :PowerPC(32)     :11.00.044
AIX      :PowerPC(64)     :11.00.044
HP-UX    :IPF32           :08.60.005
HP-UX    :PA-RISC         :08.60.005
HP-UX    :IPF32           :11.00.044
HP-UX    :PA-RISC         :11.00.044
LIN      :IPF64(2.6)      :08.60.005
LIN      :x64(2.6)        :08.60.005
LIN      :x86(2.6)        :08.60.005
LIN      :IPF64(2.6)      :11.00.044
LIN      :PowerPC(2.6)    :11.00.044
LIN      :x64(2.6)        :11.00.044
LIN      :x86(2.6)        :11.00.044
SOL      :SPARC           :08.60.005
SOL      :x86             :08.60.005
SOL      :SPARC           :11.00.044
SOL      :x86             :11.00.044
WIN      :x64             :11.00.044
WIN      :x86             :11.00.044
WIN      :x64             :11.10.017
WIN      :x86             :11.10.017
WIN      :x64             :11.10.030
WIN      :x86             :11.10.030
WIN      :x64             :11.10.031
```

Registro en HPOM en un servidor de administración de UNIX/Linux

Registre el paquete de implementación en el servidor de gestión de HPOM

Nota: En el servidor de gestión, debe estar disponible al menos 1 GB de espacio en disco.

1. Inicie sesión en el servidor de gestión como usuario raíz.
2. Realice una de las siguientes tareas:
   - Si desea registrar el paquete de implementación con el soporte físico, inserte el DVD de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en la unidad de DVD-ROM.

- Descargue el soporte de instalación de uno de los sitios web de HP. En los sitios web de HP hay diferentes archivos .iso específicos de cada plataforma para los paquetes de implementación de HP Operations Agent 11.10. Puede descargar un archivo .iso específico de una plataforma o el archivo .iso que incluya paquetes de implementación para todas las plataformas. Después del descargar el archivo .iso, extraiga el contenido del archivo en un directorio local en el servidor de gestión.

3. *Opcional.* Cree un archivo de configuración para omitir la instalación de los SPI de infraestructura.

   El programa `oainstall` instala los SPI de infraestructura en el servidor de gestión al registrar el paquete de implementación. Esta instalación incluye los paquetes de informes (para usarlos con HP Reporter) y gráficos (para usarlos con HP Performance Manager) para los SPI de infraestructura. Si desea desea omitir la instalación de los SPI de infraestructura, siga estos pasos:

   i. Cree un archivo con un editor de texto.

   ii. Añada el siguiente contenido:

   ```
   [agent.parameter]
   REGISTER_AGENT=YES
   [hpinfraspi.parameter]
   InfraSPI=NO
   InfraSPI_With_Graphs=NO
   InfraSPI_With_Reports=NO
   ```

   iii. Guarde el archivo.

4. En la raíz del soporte, ejecute el siguiente comando:

   ./oainstall.sh -i -m -p ALL

   El comando registra los paquetes de implementación del agente para todas las plataformas en el servidor de gestión e instala los SPI de infraestructura.

   Si no desea instalar los SPI de infraestructura y ha realizado el paso 3, ejecute el siguiente comando:

   ./oainstall.sh -i -m -p ALL -spiconfig <*archivo de configuración*>

   Sugerencia: Si lo desea, puede elegir instalar los paquetes de implementación sólo para determinadas plataformas.

   Ejecute el siguiente comando para instalar el paquete de implementación sólo para una plataforma:

   ./oainstall.sh -i -m -p <*plataforma*>

   En este caso, use uno de los siguientes valores para <*plataforma*>:

   Para Windows: WIN

   Para HP-UX: HP-UX

Para Linux: LIN

Para Solaris: SOL

Para AIX: AIX

Para instalar paquetes de implementación para varias plataformas de nodo con un solo comando, use varias opciones -p separadas por espacios.

Por ejemplo:

./oainstall.sh -i -m -p AIX -p SOL

Si HPOM está en un clúster de alta disponibilidad (HA)

Siga los pasos anteriores en el nodo activo del clúster de alta disponibilidad (HA) de HPOM:

Después de realizar todos los pasos, y pasar al nodo pasivo, vaya al directorio `/var/opt/OV/shared/server/installation` en el nodo pasivo y ejecute el siguiente comando:

./oainstall_sync.sh

Después de ejecutar el comando con las opciones y argumentos necesarios, se inicia el proceso de registro. Según el número de paquetes seleccionados, el proceso de registro puede tardar hasta 20 minutos en completarse.

Verificación

1. En el servidor de administración, vaya a la ubicación siguiente:

   `/opt/OV/bin/OpC/agtinstall`

2. Ejecute el comando siguiente:

   ./oainstall.sh -inv -listall

   El comando muestra la lista de los paquetes de implementación disponibles (activos) en el servidor de administración.

3. Localice una plataforma para la que ha instalado el paquete de implementación. Si la versión activa aparece como 11.10, la instalación es correcta.

Archivo de registro

El archivo de registro del registro (`oainstall.log`) está disponible en el directorio:

`/var/opt/OV/shared/server/log`

Colocación de paquetes

Al registrar los paquetes de HP Operations Agent en el servidor de gestión, el programa `oainstall` coloca todos los paquetes de implementación necesarios en el siguiente directorio:

`/var/opt/OV/share/databases/OpC/mgd_node/vendor`

Copia de seguridad de los paquetes de implementación

Al registrar los paquetes de implementación en el servidor de gestión, el script `oainstall` guarda una copia de los paquetes de implementación antiguos en el siguiente directorio local.

`/var/opt/OV/shared/server/installation/backup/HPOpsAgt/`<*SO*>`/`<*Versión_OA*>`/`<*ARCH*>

Para ver los paquetes de implementación activos, ejecute el siguiente comando:

./oainstall.sh -inv

Para todos los paquetes (activos y de copia de seguridad) del sistema, ejecute el siguiente comando:

./oainstall.sh -inv -listall

Eliminación del paquete de implementación de HP Operations Agent

1. En UNIX/Linux: Inicie sesión en el servidor de gestión como administrador y vaya al directorio `%ovinstalldir%bin\OpC\agtinstall`.

   En Windows: Inicie sesión en el servidor de gestión como usuario raíz y vaya al directorio `/opt/OV/bin/OpC/agtinstall`.

2. Ejecute el siguiente comando para anotar el el número de versión correcto del paquete de implementación que desea quitar.

   En Windows

   cscript oainstall.vbs -inv -listall

   En UNIX/Linux

   ./oainstall.sh -inv -listall

3. Ejecute el comando siguiente:

   En Windows

   cscript oainstall.vbs -r -m -v <*versión*> **-p** <*plataforma*>

   En UNIX/Linux

   ./oainstall.sh -r -m -v <*versión*> **-p** <*plataforma*>

   En este caso, <*versión*> la versión del paquete de implementación de Agent que desea eliminar.

   La opción **y**especifica el paquete específico de la plataforma de HP Operations Agent que desea eliminar del servidor de administración. Use la siguiente lista para especificar la información de la plataforma en forma de argumentos para esta opción:

   - Linux: LIN
   - Solaris: SOL
   - HP-UX: HP-UX
   - AIX: AIX
   - Windows: WIN
   - Todas las plataformas: ALL

Tanto en las opciones como en los argumentos se distinguen mayúsculas de minúsculas.

Al quitar los paquetes de implementación de HP Operations Agent 11.10, el programa de instalación vuelve a iniciar la versión de copia de seguridad más reciente de los paquetes de implementación (si está disponible) en el servidor de gestión:

Capítulo 3

Requisitos para instalar HP Operations Agent

Requisitos para Windows

Usuario

Para instalar HP Operations Agent en un nodo de Windows, debe utilizar un usuario con privilegios administrativos; el usuario debe tener acceso al recurso compartido del sistema predeterminado (el disco en el que está configurada la carpeta **Archivos de programa**) con los siguientes privilegios adicionales:

- Pertenencia al grupo de administradores locales
- Acceso de escritura en el recurso compartido admin$
- Acceso de lectura al Registro
- Permiso para iniciar una sesión como un servicio
- Permiso para iniciar y detener servicios

Software necesario

Windows Installer 4.5 o posterior: El software Windows Installer está incluido en el sistema operativo Microsoft Windows. El programa de instalación de HP Operations Agent requiere que la versión 4.5 de este componente de software esté en el sistema.

Windows Script Host: Windows Script Host debe estar habilitado en el sistema. El programa de instalación de HP Operations Agent requiere que Windows Script Host esté habilitado. Para comprobar si Windows Script Host está habilitado, siga estos pasos:

1. Inicie una sesión en el sistema Windows.
2. En el menú Inicio, abra la ventana Ejecutar.
3. En el mensaje Ejecutar, escriba **regedit** y pulse **Entrar**. Se abre la ventana Editor del Registro.
4. En la ventana Editor del Registro, amplíe **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft** y haga clic en **Windows Script Host**.
5. En el panel derecho, consulte la clave Habilitado.
6. Si la clave Habilitado está presente, haga doble clic en ella y asegúrese de que Información del valor está establecido en 1. Windows Script Host está desactivado si Información del valor para la clave Habilitado está establecido en 0.
7. Si falta la clave Habilitado, puede presuponer que Windows Script Host está habilitado.

Servicios necesarios

Antes de instalar el agente, asegúrese de que los siguientes servicios se están ejecutando:

- Registro de eventos
- Llamada a procedimiento remoto
- Plug and Play
- Administrador de cuentas de seguridad
- Inicio de sesión en red
- Registro remoto
- Servidor
- Estación de trabajo

Para verificar que los anteriores servicios se están ejecutando, siga estos pasos:

1. Inicie una sesión en el sistema con privilegios administrativos.
2. En el menú Inicio, abra la ventana Ejecutar.
3. En el mensaje Ejecutar, escriba **services.msc** y pulse **Entrar**. Se abre la ventana Servicios.
4. En la ventana Servicios, compruebe si el estado de cada uno de los servicios anteriores es Iniciado. Si el estado de uno de los servicios no es Iniciado, haga clic con el botón derecho en el servicio y, a continuación, haga clic en **Iniciar**.

Espacio en disco

Para una nueva instalación:

Para el directorio de instalación:

350 MB

Para el directorio de datos:

50 MB

Para actualizar desde una versión anterior del software Agent

Para el directorio de instalación:

100 MB

Para el directorio de datos:

50 MB

Software y servicios recomendados

Para las directivas del interceptor WMI: El servicio Instrumental de administración de Windows debe estar disponible en el sistema si desea implementar las directivas del interceptor WMI o las directivas del umbral de medición para monitorizar los eventos y clases de WMI, o bien si desea realizar una detección automática del servicio del nodo.

Para la monitorización de MIB de SNMP: Si desea monitorizar los objetos en una Base de información y administración (MIB) de SNMP en el sistema del agente, asegúrese de que el agente SNMP (compatible con MIB-I y MIB-II) está instalado en el sistema.

Para acciones y herramientas de HPOM: Para iniciar acciones y herramientas de HPOM en el nodo, es necesario que se esté ejecutando el servicio Proveedor de compatibilidad para seguridad NT LM.

Requisitos adicionales para Hyper-V en Windows Server 2008

Para poder monitorizar sistemas virtuales, aplique la siguiente revisión:

http://support.microsoft.com/kb/950050

Para poder registrar la clase de los datos de rendimiento BYLS, aplique la siguiente revisión:

http://support.microsoft.com/KB/960751

Requisitos para Linux

Usuario

Para instalar HP Operations Agent en un nodo de Linux, debe utilizar un usuario con privilegios raíz.

Nota: Puesto que HP Operations Agent no puede instalarse sin el usuario raíz en un nodo de Linux, no puede instalar el agente en un nodo de vSphere Management Assistant (vMA) (donde el usuario raíz está deshabilitado de forma predeterminada) remotamente desde la consola de HPOM.

Software necesario

Para instalar HP Operations Agent, son necesarios los siguientes paquetes y bibliotecas de tiempo de ejecución:

- glibc-2.3.4-2.36.i686.rpm
- Tiempo de ejecución de C++:
  - Para sistemas con la versión del núcleo 2.6:
    /usr/lib/libstdc++.so.5
  - Para sistemas con la versión del núcleo 2.6 sobre Itanium:
    /usr/lib/libstdc++.so.6
- Biblioteca de tiempo de ejecución de curses:
  /usr/lib/libncurses.so.5
- En sistemas x64:
  - libgcc-3.4.6-8.i386.rpm
  - libstdc++-3.4.6-8.i386.rpm

Si desea instalar el agente de forma remota desde la consola HPOM para Windows, asegúrese de que OpenSSH 5.2 o superior está instalado en el sistema.

Espacio en disco

Para una nueva instalación:

Para los directorios de instalación (**/opt/OV** y **/opt/perf**):

350 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

350 MB

Para una actualización:

Para los directorios de instalación (**/opt/OV** y **/opt/perf**):

100 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

350 MB

Nota: Si no dispone del suficiente espacio en el directorio de datos o de instalación, podrá vincular simbólicamente alguno de estos directorios con otra ubicación del sistema por medio del comando ln -s.
Por ejemplo, para vincular simbólicamente el directorio **/opt/OV** con el directorio **/new**, ejecute el comando siguiente:
ln -s /new /opt/OV

Software y servicios recomendados

Para la monitorización de MIB de SNMP: Si desea monitorizar los objetos en una Base de información y administración (MIB) de SNMP en el sistema del agente, asegúrese de que el agente SNMP (compatible con MIB-I y MIB-II) está instalado en el sistema.

Para xglance: Para usar la utilidad xglance, asegúrese de que los siguientes componentes están disponibles en el sistema:
Kit de herramientas Open motif 2.2.3 (En plataformas de Linux, excepto Red Hat Enterprise Linux 5.x y SUSE Linux Enterprise Server 10.x sobre x86_64 e Itanium, es necesario tener la versión de 32 bits del kit de herramientas Open motif y las bibliotecas asociadas.)

Requisitos adicionales para el modo vMA

- Asegúrese de que el servicio portmap se ha iniciado.
- Deshabilite en la unidad de disco en vMA.
- Aumente el tamaño de RAM para vMA a 1 GB
- Habilite la comunicación entre cortafuegos en el nodo de vMA

  El agente usa el puerto 383 para facilitar la comunicación con otros sistemas entre cortafuegos. Debe configurar el nodo de vMA para aceptar el tráfico de comunicaciones en el puerto 383. Para lograrlo, ejecute el siguiente comando:

  - **sudo iptables -I RH-Firewall-1-INPUT 3 -p tcp -m tcp --dport 383 --tcp-flags SYN,RST, ACK SYN -j ACCEPT**
  - **sudo service iptables save**

    Para verificar que los cambios surten efecto, ejecute el siguiente comando:

    sudo vi /etc/sysconfig/iptables

    El editor vi abre el archivo iptables del directorio `/etc/sysconfig`. En el archivo `iptables`, asegúrese de que existe la siguiente línea:

```
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 383 --tcp-flags SYN,
RST,ACK SYN -j ACCEPT
```

Nota: De forma predeterminada, el usuario raíz de un nodo de vMA (Linux) está deshabilitado. Como resultado, no puede implementar el agente de forma remota desde la consola de HPOM en un nodo vMA. El programa de instalación de HP Operations Agent (`el script oainstall`) también requiere que los privilegios raíz. Por tanto, debe usar el comando sudo para cambiar al usuario raíz antes de instalar Agent manualmente en el nodo vMA.

Requisitos para HP-UX:

Usuario

Para instalar HP Operations Agent en un nodo de HP-UX, debe utilizar un usuario con privilegios raíz.

Software necesario

En HP-UX, asegúrese de que las siguientes revisiones están instaladas:

- *Para HP-UX 11.23.* PHKL_36853, PHCO_38149 (o revisiones que las reemplacen)
- *Para HP-UX 11i v1.* PHNE_27063 (o una revisión que la reemplace)
- *Para HP-UX 11i v1.* Revisión acumulativa PHCO_24400 s700_800 11.11 libc (o una revisión que la reemplace)
- *Para HP-UX 11.11 PA-RISC.* PHCO_38226 (o una revisión que la reemplace)
- *Para HP-UX 11.31.* PHCO_36530 (o una revisión que la reemplace)
- *Para HP-UX 11i v1.* Las siguientes revisiones son necesarias para que las herramientas de rendimiento funcionen con VERITAS Volume Manager 3.2:
  - PHKL_26419 para HP-UX B.11.11 (11.11) (o una revisión que la reemplace)
  - PHCO_26420 for HP-UX B.11.11 (11.11) (o una revisión que la reemplace)

En los sistemas HP-UX que se ejecuten en Itanium, la biblioteca libunwind debe estar disponible.

Si se han configurado varios conjuntos de procesadores en un sistema HP-UX 11i v1 y está usando el conmutador log application=prm en el archivo de parámetros para registrar los datos de rendimiento APP_ mediante PRM Group, es necesario instalar la siguiente revisión:

PHKL_28052 (o una revisión que la reemplace)

En HP-UX 11i v1 y posterior, las herramientas de rendimiento funcionan con Instant Capacity on Demand (iCOD). La siguiente revisión pstat del kernel se debe instalar para generar correctamente informes de los datos de iCOD (Si iCOD no está instalado en el sistema, no instale la revisión del kernel.):

PHKL_22987 for HP-UX B.11.11 (11.11) (o una revisión que la reemplace)

HP GlancePlus, incluido en esta versión de HP Operations Agent, funciona con Process Resource Manager (PRM) versión C.03.02.

HP-UX 11.11 y posterior ejecutándose en EMC PowerPath v2.1.2 o v3.0.0 debe tener las últimas revisiones de EMC instaladas.

- Para la versión EMC PowerPath v2.1.2, use la siguiente revisión: EMCpower_patch213 HP.2.1.3_b002 (o una revisión que la reemplace)
- Para la versión EMC PowerPath v3.0.0, use la siguiente revisión: EMCpower_patch301 HP.3.0.1_b002 (o una revisión que la reemplace)

Espacio en disco

Para una nueva instalación:

Para los directorios de instalación (**/opt/OV** y **/opt/perf**):

400 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

550 MB

Para una actualización:

Para los directorios de instalación (**/opt/OV** y **/opt/perf**):

400 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

550 MB

Nota: Si no dispone del suficiente espacio en el directorio de datos o de instalación, podrá vincular simbólicamente alguno de estos directorios con otra ubicación del sistema por medio del comando ln -s.
Por ejemplo, para vincular simbólicamente el directorio **/opt/OV** con el directorio **/new**, ejecute el comando siguiente:
ln -s /new /opt/OV

Software y servicios recomendados

Para la monitorización de MIB de SNMP: Si desea monitorizar los objetos en una Base de información y administración (MIB) de SNMP en el sistema del agente, asegúrese de que el agente SNMP (compatible con MIB-I y MIB-II) está instalado en el sistema.

Requisitos para Solaris

Usuario

Para instalar HP Operations Agent en un nodo de Solaris, debe utilizar un usuario con privilegios raíz.

Software necesario

Antes de instalar HP Operations Agent en un nodo de Solaris, asegúrese de instalar las siguientes revisiones o las que las reemplazan:

Versión del sistema operativo	Plataforma	Revisiones necesarias
10	32 bits (x86)	• 118345-03 SunOS 5.10_x86: ld & libc.so. • Revisión de biblioteca compartida 119964-03 SunOS 5.10_x86 para C++_x86 • 120754-01 SunOS 5.10_x86 libmtsk
	64 bits (SPARC/x64)	• Vinculador 117461-04 • 120753-01 libmtsk • SunOS 5.10 119963-19: Revisión de biblioteca compartida para C++

Además, asegúrese de que están disponibles los siguientes paquetes:

SUNWlibC

SUNWlibms

SUNWmfrun

SUNWxwplt

Espacio en disco

Para una nueva instalación:

Para los directorios de instalación (**/opt/OV** y **/opt/perf**):

350 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

350 MB

Para una actualización:

Para los directorios de instalación (**/opt/OV** y **/opt/perf**):

100 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

350 MB

Nota: Si no dispone del suficiente espacio en el directorio de datos o de instalación, podrá vincular simbólicamente alguno de estos directorios con otra ubicación del sistema por medio del comando ln -s.
Por ejemplo, para vincular simbólicamente el directorio **/opt/OV** con el directorio **/new**, ejecute el comando siguiente:
ln -s /new /opt/OV

Software y servicios recomendados

Para la monitorización de MIB de SNMP: Si desea monitorizar los objetos en una Base de información y administración (MIB) de SNMP en el sistema del agente, asegúrese de que el agente SNMP (compatible con MIB-I y MIB-II) está instalado en el sistema.

Requisitos para AIX

Usuario

Para instalar HP Operations Agent en un nodo de AIX, debe utilizar un usuario con privilegios raíz.

Software necesario

- La biblioteca **libC.a** es necesaria para que HP GlancePlus funcione correctamente. La biblioteca está incluida en el paquete **xlC.rte**, que está disponible en el soporte óptico del sistema operativo AIX.
- El paquete bos.perf.libperfstat es necesario para el demonio de comunicaciones.
- Si desea instalar el agente de forma remota desde la consola HPOM para Windows, asegúrese de que OpenSSH 5.2 o superior está instalado en el sistema.

Espacio en disco

Para una nueva instalación:

Para los directorios de instalación (**/usr/lpp/OV** y **/usr/lpp/perf**):

350 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

350 MB

Para una actualización:

Para los directorios de instalación (**/usr/lpp/OV** y **/usr/lpp/perf**):

350 MB

Para los directorios de datos (**/var/opt/OV** y **/var/opt/perf**):

350 MB

Nota: Si no dispone del suficiente espacio en el directorio de datos o de instalación, podrá vincular simbólicamente alguno de estos directorios con otra ubicación del sistema por medio del comando ln -s.
Por ejemplo, para vincular simbólicamente el directorio **/usr/lpp/OV** con el directorio **/new**, ejecute el comando siguiente:
ln -s /new /usr/lpp/OV

Software y servicios recomendados

Para la monitorización de MIB de SNMP: Si desea monitorizar los objetos en una Base de información y administración (MIB) de SNMP en el sistema del agente, asegúrese de que el agente SNMP (compatible con MIB-I y MIB-II) está instalado en el sistema.

Para xglance: Para usar la utilidad xglance, asegúrese de que los siguientes componentes están disponibles en el sistema:

- Abra Motif 2.1 o posterior:
- X11 Revisión 6 (X11R6)

Para recopilar y registrar los datos de rendimiento de particiones cruzadas, el demonio xmservd o xmtopas debe estar disponible. xmtopas forma parte del conjunto de archivos perfagent.tools y xmservd está incluido en el cuadro de herramientas del componente AIX (un programa de software bajo licencia).

Notas de actualización

Actualización de un agente cuya versión es anterior a la 11.00

Puede actualizar una versión anterior (anterior a la 11.00) de HP Operations Agent, HP Performance Agent o HP GlancePlus a HP Operations Agent 11.10. Las siguientes versiones pueden actualizarse directamente a HP Operations Agent 11.10:

- HP Operations Agent: 8.53, 8.60
- HP Performance Agent: 4.70, 5.00
- HP GlancePlus: 4.70, 5.00

La instalación de HP Operations Agent 11.10 genera un error si se instala cualquier software del agente más antiguo que las versiones especificadas. Antes de instalar HP Operations Agent 11.10 en nodos con una versión de HP Operations Agent anterior a la 8.53, una versión de HP Performance Agent anterior a la 4.70 y una versión de HP GlancePlus anterior a la 4.70, realice una de estas acciones:

- Actualice el software Agent a la versión que pueda actualizarse a HP Operations Agent 11.10.

  Este es el método preferido de actualización. Este método garantiza que se mantienen en el nodo los paquetes y directivas necesarios.

- Elimine el software Agent completamente

  Esto puede eliminar las directivas y los archivos de instrumentación del nodo. Después de actualizar a HP Operations Agent 11.10, asegúrese de que se implementan de nuevo las políticas y los archivos de instrumentación necesarios en el nodo.

Comprobación de la versión del agente existente

En Windows

1. Inicie una sesión en el nodo con privilegios administrativos.
2. Compruebe la versión de HP Operations Agent:
3. Abra el símbolo del sistema.
4. Ejecute el comando siguiente:

   ```
   opcagt -version
   ```

Si la salida del comando muestra que la versión es anterior a la A.8.53, debe actualizar a la versión 8.53 o 8.60 antes (o eliminar totalmente la versión instalada) antes de instalar HP Operations Agent 11.10.

5. Compruebe la versión de HP Performance Agent:
   a. Abra el símbolo del sistema.
   b. Ejecute el comando siguiente:

      ```
      perfstat -v
      ```

      La salida del comando muestra las versiones de los distintos componentes de HP Performance Agent. Si la versión del componente **ovpa.exe** aparece como anterior a la C.04.70, debe actualizarla a la versión 4.70 o 5.00 antes (o eliminar totalmente la versión instalada de HP Performance Agent) antes de instalar HP Operations Agent 11.10.

En UNIX/Linux

1. Inicie sesión en el nodo con los privilegios raíz.
2. Compruebe la versión de HP Operations Agent:
3. Abra el símbolo del sistema.
4. Ejecute el comando siguiente:

   ```
   opcagt -version
   ```

   Si la salida del comando muestra que la versión es anterior a la A.8.53, debe actualizar a la versión 8.53 o 8.60 antes (o eliminar totalmente la versión instalada) antes de instalar HP Operations Agent 11.10.

5. Compruebe la versión de HP Performance Agent:
   a. Abra el símbolo del sistema.
   b. Ejecute el comando siguiente:

      ```
      perfstat -v
      ```

      La salida del comando muestra las versiones de los distintos componentes de HP Performance Agent. Si la versión del componente **ovpa** aparece como anterior a la C.04.70, debe actualizarla a la versión 4.70 o 5.00 antes (o eliminar totalmente la versión instalada de HP Performance Agent) antes de instalar HP Operations Agent 11.10.

6. Compruebe la versión de HP GlancePlus:
   a. Abra el símbolo del sistema.
   b. Ejecute el comando siguiente:

      ```
      perfstat -v
      ```

      La salida del comando muestra las versiones de los distintos componentes de HP Performance Agent y HP GlancePlus. Si la versión del componente **glance** aparece como anterior a la C.04.70, debe actualizarla a la versión 4.70 o 5.00 antes (o eliminar totalmente la versión de HP GlancePlus) antes de instalar HP Operations Agent 11.10.

Recopilación y almacenamiento de datos con HP Operations Agent 11.10

Las versiones anteriores de HP Operations Agent (anteriores a la 11.00) almacenan los datos de rendimiento del sistema en forma de aproximadamente 50 métricas en el componente de rendimiento incrustado (**EPC**), también conocido como **coda**. HP Performance Agent recopila más

de 500 métricas de rendimiento del sistema (con ayuda del recolector **scope**) y usa el mecanismo de almacenamiento basado en archivos del registro para almacenar los datos. La versión 11.10 de HP Operations Agent usa el mecanismo de recopilación y almacenamiento de datos de HP Performance Agent y, por tanto, recopila un mayor conjunto de métricas y almacena los datos de las métricas en el almacén de datos basado en el archivo de registro. Sin embargo, cualquier referencia al EPC en programas externos o directivas HPOM está dirigida al recolector scope y el almacén de datos basado en el archivo de registro. Esto garantiza que todas las políticas e integraciones implementadas previamente funcionan sin interrupciones después de actualizar a HP Operations Agent 11.10 desde una versión anterior de HP Operations Agent (anterior a la 11.00).

Comprobación de la versión de coda

Si la versión disponible de coda en el sistema está entre la 10.50.215 y la 10.50.245, se recomienda realizar una copia de seguridad de los datos de coda mediante las herramientas de análisis de datos (como HP Reporter o HP Performance Insight). Para conocer la versión de coda, abra el archivo **coda.txt** en el directorio de registro (*%ovdatadir%***log** en Windows; **/var/opt/OV/log** en UNIX/Linux) y compruebe la versión de coda (al lado de la instrucción `Starting CODA` (Inicio de CODA)).

Actualización de un servidor de gestión Solaris SPARC con nodos gestionados Solaris SPARC

Si usa un servidor de gestión de HPOM Solaris SPARC HPOM y si HP Operations Agent 8.60 (con la versión 06.20.050 del componente (HPOvSecCo) de HP Software Security Core) está instalado en el servidor de gestión, debe actualizar el agente en todos los nodos gestionados Solaris SPARC del entorno a la versión 11.10 y, a continuación, actualizar el agente del servidor de gestión a la versión 11.10. Si no lo hace, la comunicación entre el agente del nodo Solaris SPARC (con la versión 8.60) y el del servidor de gestión (con la versión 11.10) no funcionará hasta que actualice el agente del servidor de gestión a la versión 11.10.

Además, debe aplicar la revisión QCCR1A97520 al servidor de gestión antes de actualizar el agente en todos los nodos gestionados SPARC del entorno a la versión 11.10.

Si usa el servidor de gestión de HPOM SPARC con nodos SPARC, siga estos pasos:

1. Inicie sesión en el servidor de gestión con privilegios raíz.
2. Ejecute el siguiente comando para comprobar la versión del componente HP Software Security Core (OvSecCo) en el servidor de gestión:

   strings /opt/OV/lib/libOvSecCore.so | grep FileV

Si la salida del comando muestra que la versión de HPOvSecCo es la 06.20.050, aplique la revisión QCCR1A97520 al servidor de gestión (para obtener dicha revisión, póngase en contacto con el soporte técnico de HP). De lo contrario, continúe con la actualización.

Esta revisión garantiza que los nodos SPARC con HP Operations Agent 11.10 pueden comunicarse con el servidor de gestión de SPARC que incluye el componente HPOvSecCo, versión 06.20.050. Si no instala esta revisión en el servidor de gestión de SPARC, los nodos SPARC con HP Operations Agent 11.10 no podrán comunicarse con el servidor de gestión de SPARC hasta que actualice el agente del servidor de gestión a la versión 11.10.

Para comprobar que la versión del componente HPOvSecCo del servidor gestionado se ha actualizado a la 06.20.077, ejecute el siguiente comando:

```
strings /opt/OV/lib/libOvSecCore.so | grep FileV
```

La salida del comando muestra que la versión del componente HPOvSecCo es la 06.20.077.

Tarea previa a la instalación: para instalar HP Operations Agent en HPOM en clúster

Si está instalado en un entorno de clústeres de alta disponibilidad (HA), HP Operations Agent no conmuta en caso de error cuando el sistema activo en el cluster conmuta a otro sistema. Sin embargo, HP Operations Agent puede ayudarle a monitorizar aplicaciones preparadas para clúster que se ejecutan en un clúster.

Hay que instalar HP Operations Agent en todos los nodos que pertenecen al clúster. La instalación del agente en un clúster no implica ningún paso adicional ni ninguna configuración especial. Sin embargo, para instalar el agente en un servidor de administración de HPOM que se ejecuta en un clúster requiere pasos de configuración adicionales.

En HPOM para Windows

1. Asegúrese de que la base de datos de HPOM está activa y funcionando.
2. Inicie una sesión en el servidor de administración activo con privilegios administrativos.
3. Establezca el nodo activo para el modo de interrupción de actividad por mantenimiento ejecutando el siguiente comando:

   ovownodeutil -outage_node -unplanned -node_name <*FQDN_del_nodo*>
4. Instale Agent en el servidor activo siguiendo las instrucciones de "Installing from the HPOM Console" o "Installing the HP Operations Agent Manually on the Node".
5. Realice los pasos 4 y 5 en todos los nodos del clúster.

En este ejemplo:

<*FQDN del nodo*> es el nombre de dominio completo del nodo activo.

En HPOM en UNIX/Linux

1. Inicie una sesión en el servidor de administración activo con privilegios raíz.
2. Deshabilite la monitorización del grupo de recursos HA en el nodo activo estableciendo el modo de mantenimiento para el nodo:

   Ejecute el comando siguiente en el nodo activo:

   /opt/OV/lbin/ovharg -monitor <*nombre de grupo de recursos de HA*> **disable**

   En este ejemplo:

   <*nombre de grupo de recursos de HA*> es el grupo de recursos HA para HPOM en el servidor de gestión.
3. Instale Agent en el servidor activo siguiendo las instrucciones de "Installing from the HPOM Console" o "Installing the HP Operations Agent Manually on the Node".

   Asegúrese de que el disco compartido no está montado en el momento de la instalación.
4. Realice los pasos 2 y 3 en todos los nodos del clúster.

Capítulo 4

Instalación desde la consola de HPOM

Nota: No use este método de instalación para los nodos vSphere Management Assistant (vMA) (donde el usuario `raíz` está deshabilitado de manera predeterminada). En estos nodos, Agent se debe instalar manualmente.

Si el nodo aloja otro producto de software de HP, asegúrese de detener todos los procesos del producto antes de la instalación de Agent. Los procesos se pueden iniciar después de que finalice la instalación de Agent.

En HPOM para Windows

Para instalar HP Operations Agent en nodos gestionados desde la consola de HPOM, consulte el tema *Remote agent installation* en la *Ayuda en línea de HPOM para Windows*.

Desde HPOM en UNIX/Linux

Para instalar HP Operations Agent en nodos gestionados desde la consola de HPOM en UNIX/Linux, consulte el tema *HPOM for UNIX: New Agent Installation* en la *Ayuda en línea de HPOM en UNIX/Linux*.

Capítulo 5

Instalación manual de HP Operations Agent en el nodo

Tarea 1: Preparación de la instalación

Antes de instalar HP Operations Agent es preciso extraer o montar el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en el nodo.

Como alternativa, puede transferir manualmente el paquete de implementación de Agent del servidor de gestión de HPOM.

Para transferir el paquete de implementación desde un servidor de gestión de Windows:

1. Asegúrese de que se agrega el nodo como un nodo administrado en la consola de HPOM.
2. Cree un directorio en el servidor de administración y vaya al directorio.
3. Ejecute el comando siguiente:

   ovpmutil dnl pkg Operations-agent /pnn <*FQDN_nodo*>

   En este ejemplo, <*FQDN_nodo*> es el nombre de dominio completo del nodo.

   El paquete de implementación para el nodo se descarga en el directorio actual.
4. Transfiera el directorio del servidor de administración a un directorio temporal en el nodo.

Para transferir el paquete de implementación desde un servidor de gestión de UNIX/Linux:

1. Inicie una sesión en el servidor de administración y vaya al directorio siguiente:

   `/var/opt/OV/share/databases/OpC/mgd_node/vendor/`*<proveedor>/<arquit.>/<tipo de s.o.>*`/A.11.10.000`

   En este ejemplo:

   <*proveedor*>: nombre del proveedor del sistema operativo.

   <*arq*>: arquitectura del nodo.

   <*tipo_so*>: sistema operativo del nodo.

   En la siguiente tabla se proporciona una lista de las combinaciones de <*proveedor*>/<*arquit.*>/<*tipo de s.o.*> que puede usar:

Sistema operativo	Arquitectura	Seleccione esta combinación
Windows	Itanium	ms/ipf64/win2k3
Windows	x86_64	ms/x64/win2k3

Sistema operativo	Arquitectura	Seleccione esta combinación
Windows	x86	ms/x86/winnt
Linux	Itanium	linux/ipf64/linux26
Linux	x86_64	linux/x64/linux26
Linux	x86	linux/x86/linux26
Linux	PowerPC (64 bits)	linux/powerpc/linux26
HP-UX	Itanium	hp/ipf32/hpux1122
HP-UX	PA-RISC	hp/pa-risc/hpux1100
Solaris	SPARC	sun/sparc/solaris7
Solaris	x86	sun/x86/solaris10
AIX	PowerPC (32 bits)	ibm/rs6000/aix5
AIX	PowerPC (64 bits)	ibm/rs6k64/aix5

2. Transfiera el contenido del directorio `RPC_BBC` (disponible en el directorio `A.11.00.000`) a un directorio temporal del nodo.

Opcional. **Preparación del archivo de perfil**

Acerca del archivo de perfil

Puede usar un archivo de *perfil* en la instalación (instalación manual) para programar Agent para que se ejecute con ajustes de configuración que no sean los predeterminados (como el puerto de comunicaciones, el puerto del interceptor de eventos o el tipo de licencia). Los archivos de perfil se deben crear manualmente siguiendo las instrucciones que se especifican en este documento.

1. En el sistema en que desee instalar Agent, cree un archivo y ábralo con un editor de texto.
2. Escriba la siguiente sintaxis para configurar las variables de Agent para que usen un valor que no sea el predeterminado:

   set <*espacio de nombres*>**:**<*variable*>**=**<*valor*>

   En este ejemplo:

   <*espacio de nombres*> es el espacio de nombres de la variable de configuración

   <*variable*> es la variable que desea configurar

   <*valor*> es el valor que se desea asignar a la variable
3. Guarde el archivo en un directorio local.

Características clave que se pueden configurar en la instalación

- **Usuario de Agent:** en el momento de la instalación puede configurar el usuario bajo el que se ejecuta Agent. La variable `MODE` permite elegir un usuario, que no sea el predeterminado, que pueda utilizar Agent durante la ejecución en el sistema.

  Para configurar Agent para que se ejecute bajo un usuario que no sea raíz/sin privilegios, añada el siguiente contenido:

  set eaagt:MODE=NPU

  Para configurar Agent para ejecutar sólo el componente de monitorización de operaciones bajo un usuario que no sea raíz/sin privilegios, agregue el siguiente contenido (el resto de Agent se ejecuta con raíz/sistema local):

  set eaagt:MODE=MIXED

  Además, debe configurar un conjunto de variables de forma similar para habilitar que Agent se ejecute bajo un usuario que no sea el predeterminado. Para más información, consulte la sección *Configuración del usuario de Agent en la instalación* de la guía *HP Operations Agent Use Guide*.

- **Licencias:** si instala Agent manualmente en un nodo (es decir, sin usar la consola de HPOM), no se habilitan licencias de evaluación automáticamente después de la instalación. Puede configurar la variable específica de la licencia en el archivo de perfil para aplicar la licencia de uso (LTU) que prefiera en el momento de instalación.

  Por ejemplo, si desea aplicar la LTU de HP Operations OS Inst Adv SW de forma permanente, agregue el siguiente contenido:

  set eaagt.license:HP_Operations_OS_Inst_Adv_SW_LTU=PERMANENT

  Para más información sobre la aplicación de licencias en el momento de la instalación con un archivo de perfil, consulte la guía *HP Operations Agent License Guide*.

Tarea 2: instalación de HP Operations Agent

Nota: Si el nodo aloja otro producto de software de HP, asegúrese de detener todos los procesos del producto antes de la instalación de Agent. Los procesos se pueden iniciar después de que finalice la instalación de Agent.

1. Inicie sesión en el nodo como administrador o usuario raíz.
2. Si desea realizar la instalación desde el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10*, siga estos pasos:
   a. Vaya a la raíz del soporte.
   b. Ejecute el comando siguiente para realizar la instalación sin archivo de perfil:

      En Windows:

      cscript oainstall.vbs -i -a -s <*servidor de gestión*> **[-cs** <*servidor de certificados*>**][-install_dir** <*directorio de instalación*> **-data_dir** <*directorio de datos*>**]**

      En UNIX/Linux:

      ./oainstall.sh -i -a-s <*servidor de gestión*> **[-cs** <*servidor de certificados*>**]**

c. Ejecute el comando siguiente para realizar la instalación con un archivo de perfil:

En Windows:

cscript oainstall.vbs -i -a -agent_profile <*ruta de acceso*>****<*archivo de perfil*>**-s** <*servidor de gestión*> **[-cs** <*servidor de certificados***>] [-install_dir** <*directorio de instalación*> **-data_dir** <*directorio de datos*>**]**

En UNIX/Linux:

./oainstall.sh -i -a -agent_profile <*ruta de acceso*>**/**<*archivo de perfil*> **-s** <*servidor de gestión*> **[-cs** <*servidor de certificados***>]**

Sugerencia: En Windows, si no desea ejecutar el script `.vbs`, siga estos pasos:

- Vaya al directorio `packages\WIN` de la raíz del soporte.

- Vaya al directorio pertinente en función de la arquitectura del nodo (Windows_X64 para plataformas x64 y Windows_X86 para plataformas x86).

- Si Microsoft Visual C++ Redistributable Package no está instalado en el sistema, ejecute el archivo ejecutable de Microsoft Visual C++ Redistributable Package, que está disponible en este directorio.

- Ejecute el comando siguiente:

oasetup -install -management_server <*servidor de gestión*> [-certificate_server <*servidor de certificados*>] [-install_dir <*directorio de instalación*> **-data_dir** <*directorio de datos*>**]**

o bien
oasetup -install -management_server <*servidor de gestión*> [-certificate_server <*servidor de certificados*>] -agent_profile <*ruta de acceso*><*archivo de perfil*> **[-install_dir** <*directorio de instalación*> **-data_dir** <*directorio de datos*>**]**

3. Si ha transferido manualmente el paquete de Agent del servidor de gestión de HPOM, siga estos pasos:
   a. Vaya al directorio del nodo en el que haya almacenado el paquete de implementación.
   b. Ejecute el comando siguiente:

En Windows:

oasetup -install -management_server <*servidor de gestión*> **[-certificate_server** <*servidor de certificados*>**][-install_dir** <*directorio de instalación*> **-data_dir** <*directorio de datos*>**]**

En UNIX/Linux:

i. **chmod u+x oasetup.sh**

ii. **./oasetup.sh -install -management_server** <*servidor de gestión*> **[-certificate_server** <*servidor de certificados*>**]**

Para realizar la instalación con un archivo de perfil, agregue **-agent_profile** <*ruta de acceso*>****<*archivo de perfil*> después de **-install**.

En este ejemplo:

<*servidor_administración*>: FQDN del servidor de administración

<*servidor_certificados*>: FQDN del servidor de certificados

<*directorio_instalación*>: ruta para colocar todos los paquetes y los archivos binarios en el nodo.

<*directorio_datos*>: ruta para colocar todos los archivos de datos y configuración en el nodo.

<*ruta de acceso*> es la ruta de acceso al archivo de perfil.

<*archivo de perfil*> es el nombre del archivo de perfil.

Sugerencia: Los programas `oainstall` y `oasetup` proporcionan la posibilidad de rastrear el proceso de instalación. Si la instalación del agente falla y no puede detectar la causa, puede ejecutar el programa de instalación con la opción de rastreo, lo que genera archivos de rastreo. A continuación, puede enviar los archivos de rastreo generados al soporte técnico de HP para su análisis.

Para seguir paso a paso el proceso de instalación, ejecute el comando anterior con la siguiente opción adicional:

-enabletrace ALL

Por ejemplo:

```
./oainstall.sh -i -a -agent_profile /root/profile/profile_file -s
test_system1.domain.com -enabletrace ALL
```

El archivo de seguimiento (con la extensión .trc) está disponible en la siguiente ubicación:

En Windows

```
%ovdatadir%Temp
```

En UNIX/Linux

```
/var/opt/OV/tmp
```

Si instala Agent en en un servidor de gestión de HPOM, debe reiniciar todos los procesos de HPOM después de la instalación.

Colocación de paquetes

Al instalar HP Operations Agent en el servidor independiente, el programa de instalación coloca todos los paquetes y archivos necesarios en las siguientes ubicaciones:

- En Windows:
  - %ovinstalldir%
  - %ovdatadir%
- En HP-UX, Linux y Solaris:
  - /opt/OV
  - /opt/perf
  - /var/opt/OV
  - /var/opt/perf

- En AIX
  - /usr/lpp/OV
  - /usr/lpp/perf
  - /var/opt/OV
  - /var/opt/perf

Instalación de archivos de registro

El instalador coloca el archivo de registro de instalación (`oainstall.log`) en el siguiente directorio:

- En Windows: `%ovdatadir%\log`
- En UNIX/Linux: `/var/opt/OV/log`

Verificación de la instalación

Después de instalar HP Operations Agent, revise el contenido del archivo de registro de instalación (`oainstall.log`). Si la instalación es correcta, el archivo no debe tener errores y debe aparecer el siguiente mensaje casi al final del archivo:

```
Instalación de HP Operations Agent realizada correctamente
```

Tarea posterior a la instalación en un entorno NAT

Si instala el agente en nodos del entorno Network Address Translation (NAT), deberá configurar el agente en el nodo para que use la dirección IP utilizada con HPOM mientras se agrega el nodo.

Para configurar el agente para que utilice la dirección IP establecida con HPOM, siga estos pasos:

1. Inicie sesión en el nodo con privilegios raíz o administrativos.
2. Vaya al directorio siguiente:

   En Windows

   `%ovinstalldir%bin`

   En HP-UX, Linux o Solaris

   `/opt/OV/bin`

   En AIX

   `/usr/lpp/OV/bin`
3. Ejecute el comando siguiente:

   ovconfchg -ns eaagt -set OPC_IP_ADDRESS <*dirección IP*>

   En este ejemplo, <*dirección_IP*> es la dirección IP del nodo que se configuró con HPOM mientras se agregaba el nodo a la lista de nodos administrados.
4. Reinicie el agente ejecutando los siguientes comandos:

a. ovc -kill

b. ovc -start

Capítulo 6

Instalación de Agent en el modo inactivo

Acerca del modo inactivo

Si va a realizar una instalación local en el nodo gestionado, puede elegir programar el instalador de Agent para que coloque solamente los archivos y paquetes necesario en el nodo, pero que no configure los componentes. Como consecuencia, Agent no empieza a ejecutarse de forma automática y permanece *inactivo*. Posteriormente, tendrá que volver a usar el programa de instalación para configurar e iniciar Agent.

La ventana de este mecanismo es la posibilidad de clonar la imagen del sistema en el que HP Operations Agent se instala en el modo inactivo. La clonación de un sistema con HP Operations Agent preinstalado elimina el requisito de instalar Agent en el sistema después de agregar el sistema a la lista de nodos gestionados.

Instalación de HP Operations Agent en el modo inactivo

El modo inactivo de instalación garantiza que Agente no empieza a funcionar después de la instalación.

Para instalar HP Operations Agent:

1. Inicie sesión en el nodo como administrador o usuario raíz.
2. Si desea realizar la instalación desde el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10*, siga estos pasos:
   a. Vaya a la raíz del soporte.
   b. Ejecute el comando siguiente:

      En Windows:

      cscript oainstall.vbs -i -a -defer_configure [-install_dir <*directorio de instalación*> **-data_dir** <*directorio de datos*>**]**

      En UNIX/Linux:

      ./oainstall.sh -i -a -defer_configre

   En este ejemplo:

   <*directorio_instalación*>: ruta para colocar todos los paquetes y los archivos binarios en el nodo.

   <*directorio_datos*>: ruta para colocar todos los archivos de datos y configuración en el nodo.

Configuración posterior de Agent

Debe configurar HP Operations Agent con detalles de configuración (incluyendo la información sobre el servidor de gestión de HPOM y el servidor de certificados) para definir el agente en el modo activo. La opción `-configuration` del programa `oainstall` le permite realizar esta tarea.

Cuando desee iniciar el funcionamiento del agente, siga estos pasos:

1. Vaya al directorio siguiente:

   En los nodos de Windows 64 bits:

   `%ovinstalldir%bin\win64\OpC\install`

   En otros nodos de Windows:

   `%ovinstalldir%bin\OpC\install`

   En nodos de HP-UX, Linux o Solaris:

   `/opt/OV/bin/OpC/install`

   En nodos AIX:

   `/usr/lpp/OV/bin/OpC/install`

2. Ejecute el comando siguiente:

   En Windows

   cscript oainstall.vbs -a -configure -s <*servidor de gestión*> **[-cs** <*servidor de certificados*>**]**

   o bien

   oasetup -configure -management_server <*servidor de gestión*> **[-certificate_server** <*servidor de certificados*>**]**

   En UNIX/Linux

   ./oainstall.sh -a -configure -s <*servidor de gestión*> **[-cs** <*servidor de certificados*>**]**

Configuración remota de Agent desde un servidor de gestión de HPOM para Windows

Si HP Operations Agent se instala con la opción -defer_configure, debe configurar Agent para trabajar con un servidor de administración de HPOM más adelante. Puede configurar el agente de forma local en el nodo o de forma remota desde el servidor de administración de HPOM para Windows.

Para configurar Agent de forma remota:

1. Configure un cliente SSH.

   Nota: HPOM para Windows proporciona el software de cliente SSH de terceros PuTTY. Este procedimiento le indica el modo de configurar el cliente SSH PuTTY. PuTTY no es un software de HP. Se proporciona tal cual para su comodidad. El usuario asume todo el riesgo en relación a la utilización o el rendimiento de PuTTY.

2. En el directorio %ovinstalldir%contrib\OVOW\PuTTY del servidor de gestión, copie los archivos PLINK.EXE, PSCP.EXE y runplink.cmd a cualquier directorio que esté incluido en la variable de entorno PATH. Por ejemplo, si ha instalado el servidor de gestión en C:\Archivos de programa\HP\HP BTO Software, copie los archivos en el siguiente directorio: C:\Archivos de programa\HP\HP BTO Software\bin

3. Cree un usuario. Para instalar agentes remotamente, HPOM requiere las credenciales de un usuario que tenga acceso administrativo al nodo. En la siguiente lista se muestran los permisos específicos necesarios, en función del sistema operativo del nodo:

- Windows
  - Acceso de escritura al recurso compartido admin$ (el usuario debe ser parte del grupo de administradores local)
  - Acceso de lectura al Registro
  - Permiso para iniciar una sesión como un servicio (esto sólo es necesario si selecciona User/Password en la lista Set Credentials)
- UNIX/Linux
  - Permiso para iniciar una sesión en SSH en el nodo para la transferencia de archivos y para ejecutar comandos de instalación.

4. Configure el agente.

   Para los nodos de Windows 64 bits

   ovdeploy -cmd "%ovinstalldir%bin\win64\OpC\install\oasetup -configure -management_server <servidor de gestión> -certificate_server <servidor de certificados>" -node <nombre de nodo> -fem winservice -ostype Windows -user <usuario de nodo> -pw <contraseña de nodo>

   Para otros nodos de Windows

   ovdeploy -cmd "%ovinstalldir%bin\OpC\install\oasetup -configure -management_ server <servidor de gestión> -certificate_server <servidor de certificados>" -node <nombre de nodo> -fem winservice -ostype Windows -user <usuario de nodo> -pw <contraseña de nodo>

   Para un nodo HP-UX, Linux o Solaris

   ovdeploy -cmd "/opt/OV/bin/OpC/install/oainstall.sh -a -configure -srv <servidor de gestión> -cs <servidor de certificados>" -node <nombre de nodo> -fem ssh -ostype UNIX -user <usuario de nodo> -pw <contraseña de nodo>

   Para un nodo de AIX

   ovdeploy -cmd "/usr/lpp/OV/bin/OpC/install/oainstall.sh -a -srv <servidor de gestión> -cs <servidor de certificados>" -node <nombre de nodo> -fem ssh -ostype UNIX -user <usuario de nodo> -pw <contraseña de nodo>

   En este ejemplo:

   <servidor_administración>: Nombre de dominio completo del servidor de gestión.

   <servidor_certificados>: nombre de dominio completo del servidor de certificados. Este parámetro es opcional. Si no especifica la opción -cs, el servidor de gestión se convierte en el servidor de certificados para el nodo.

   <nombre_nodo>: Nombre de dominio completo del nodo.

   <usuario_nodo>: El usuario con el que puede configurar el agente en el nodo; el usuario que se creó.

   <contraseña de nodo>: contraseña de este usuario.

Capítulo 7

Configuración de certificados para el cliente de Operations Agent

Los certificados deben instalarse en todos los nodos administrados para facilitar la comunicación de red usando el protocolo Secure Socket Layer (SSL, Capa de sockets seguros) con cifrado. Los certificados permiten que los nodos se comuniquen con seguridad con el servidor de administración y con otros nodos.

El servidor de administración envía certificados a los nodos y actúa como la autoridad de certificados. Cada nodo administrado necesita los certificados siguientes del servidor de administración:

Un certificado de nodo único. El propio nodo se puede identificar a su servidor de gestión y a otros nodos enviándoles su certificado de nodo.

Una copia del certificado de confianza del servidor de gestión. El nodo sólo permite la comunicación de un servidor de administración si tiene el certificado de confianza para dicho servidor de administración.

En un entorno con varios servidores de administración, debe estar presente en el nodo una copia de los certificados de confianza para todos los demás nodos de administración.

Para que los nodos se comuniquen con seguridad en un entorno administrado por HPOM usando certificados, hay que instarlar los certificados después de instalar el agente en los nodos.

Solicitud de certificados con una clave de instalación

Para cifrar las solicitudes de certificados, se utilizan las claves de instalación. La clave de instalación se genera en el servidor de administración y después se transfiere al nodo.

Antes de solicitar certificados con una clave de instalación, hay que asegurarse de que HP Operations Agent se está ejecutando en el nodo. El agente envía una solicitud de certificado en el momento del inicio. Si después se solicita un certificado con una clave de instalación, la solicitud del nuevo certificado sobrescribe la solicitud de certificado original en el servidor de administración. La solicitud del primer certificado se suprime estableciendo el parámetro CERTIFICATE_ DEPLOYMENT_TYPE en manual en el espacio de nombres sec.cm.client usando los valores predeterminados de la instalación del agente o la utilidad ovconfchg.

Para solicitar de certificados con una clave de instalación:

1. Inicie sesión en el servidor de administración con una cuenta que pertenezca al grupo de administradores de HPOM.
2. Abra el símbolo del sistema (shell).

3. Ejecute el comando siguiente:

   En HPOM para Windows

   ovowcsacm -genInstKey [-file <*nombre de archivo*>**] [-pass** <*contraseña*>**]**

   En HPOM para UNIX o HPOM en UNIX/Linux

   opccsacm -genInstKey [-file <*nombre de archivo*>**] [-pass** <*contraseña*>**]**

   En este ejemplo:

   <*nombre_archivo*>*:* el nombre del archivo de clave de instalación.

   <*contraseña*>*:* necesita esta contraseña cuando vaya a solicitar posteriormente los certificados del nodo. Se puede omitir esta opción.

   El comando genera una clave de instalación.

   > **Nota:** Especifique la ruta completa con <*nombre_archivo*>; en caso contrario, el certificado se almacena en el directorio de trabajo actual. Si no se especifica la opción -file, el certificado se almacenará en <*dir_datos*>**\shared\server\certificates**.

4. Transfiera con seguridad el archivo generado al nodo. La clave de instalación es válida para cualquier nodo.
5. Inicie sesión en el nodo con la cuenta usada para instalar el nodo.
6. Abra el símbolo del sistema (shell).
7. En los nodos de UNIX/Linux, asegúrese de que la variable PATH contiene la ruta al directorio <*install_dir*>**/bin**.
8. Ejecute el comando siguiente:

   ovcert -certreq -instkey <*nombre_archivo*>

El servidor de administración debe conceder la solicitud. Se puede configurar para que tenga lugar automática o manualmente. Después de esto, el servidor de administración envía los certificados al nodo.

En los nodos de agente que se encuentren en clústeres de alta disponibilidad, ejecute el siguiente comando:

```
ovc -restart ovconfd
```

Solicitud automática de los certificados

Al implementarse el agente en un nodo desde la consola de HPOM, el nodo solicita certificados automáticamente desde el servidor de administración. El nodo cifra la solicitud de certificado con una clave.

El servidor de administración concede entonces la solicitud de certificado. Puede configurarlo para que tenga lugar automáticamente. Después de conceder la solicitud, el servidor de administración envía los certificados al nodo. Si el servidor de administración deniega la solicitud de certificado, se puede enviar otra solicitud ejecutando el siguiente comando en el nodo administrado:

```
ovcert -certreq
```

Una vez que el servidor de gestión otorgue la solicitud del certificado, ejecute el siguiente comando en los nodos de agente que se encuentren en los clústeres de alta disponibilidad:

```
ovc -restart ovconfd
```

En un entorno de alta seguridad, se pueden deshabilitar las solicitudes de certificados automáticas estableciendo el tipo de implementación del certificado en manual. A continuación, hay que solicitar los certificados con la clave de instalación o implementar manualmente los certificados.

Implementación manual de certificados

El nodo puede enviar automáticamente solicitudes de certificados al servidor de administración. Si se desean instalar los certificados manualmente en el nodo, se establece la variable CERTIFICATE_DEPLOYMENT_TYPE (en el espacio de nombres sec.cm.client) del nodo en MANUAL.

Para implementar los certificados manualmente:

1. Inicie sesión en el servidor de administración con una cuenta que pertenezca al grupo de administradores de HPOM.
2. Abra el símbolo del sistema (shell).
3. Asegúrese de que se agrega el nodo a la lista de nodos administrados en la consola de HPOM.
4. Ejecute el comando siguiente:

   En HPOM para Windows

   ovowcsacm -issue -name <*nombre de nodo*> **[-file** <*nombre de archivo*>**] [-coreid** <*OvCoreId*>**] [-pass** <*contraseña*>**]**

   En HPOM para UNIX

   opccsacm -issue -file <*nombre de archivo*> **[-pass** <*contraseña*>**] -name** <*nombre de nodo*> [**-coreid** <*OvCoreId*>**]**

   > **Nota:** Especifique la ruta completa con <*nombre_archivo*>; en caso contrario, el certificado se almacena en el directorio de trabajo actual. Si no se especifica la opción -file, el certificado se almacenará en <*dir_datos*>**\shared\server\certificates**.

   En este ejemplo:

   <*nombre_nodo*>*:* nombre de dominio completo o dirección IP del nodo.

   <*OvCoreId*>*:* el ID de núcleo del nodo. Para recuperar el ID de núcleo del nodo donde ya está instalado el agente, ejecute el paso siguiente en el servidor de administración:
   En HPOM para UNIX o HPOM en UNIX/Linux

   Ejecute el comando siguiente:

   opcnode -list_id node_list=<*nombre_nodo*>

   En HPOM para Windows

   En el árbol de consola, haga clic con el botón derecho en el nodo y, a continuación, haga clic en **Propiedades**. Se abrirá el cuadro de diálogo Node properties. En el cuadro de diálogo Node

properties, vaya a la pestaña General, haga clic en **Advanced Configuration**. Se abrirá el cuadro de diálogo Advanced Configuration, que muestra el ID de núcleo del nodo.

<*nombre_archivo*>*:* el nombre del archivo de certificado generado por el comando. Si no se especifica esta opción, el comando crea un archivo en el directorio siguiente con el nombre predeterminado <*nombre_nodo*>**-**<*OvCoreId*>**.p12**:

En HPOM para UNIX o HPOM en UNIX/Linux

```
/var/opt/OV/temp/OpC/certificates
```

En HPOM para Windows

```
%OvShareDir%server\certificates
```

5. Transfiera con seguridad el archivo generado al nodo. La clave de instalación es válida para cualquier nodo.
6. Instale el agente en el nodo si no está instalado. Utilice una instalación basada en archivo del perfil y establezca la variable CERTIFICATE_DEPLOYMENT_TYPE en manual. Además, utilice el mismo OvCoreID que se generó en el servidor de administración (establezca CERTIFICATE_SERVER_ID del espacio de nombres sec.cm.client en el ID generado en el servidor de administración).
7. Abra el símbolo del sistema (shell) en el nodo.
8. Si el agente se está ejecutando en el nodo, ejecute el comando siguiente:

   ```
   ovc -stop
   ```

9. Para importar los certificados del archivo generado, ejecute el comando siguiente:

   ovcert -importcert -file <*nombre_archivo*>

10. Ejecute el comando siguiente en el nodo:

    ```
    ovc -start
    ```

Después de importar los certificados, ejecute el siguiente comando en los nodos de agente que se encuentren en clústeres de alta disponibilidad:

```
ovc -restart ovconfd
```

Restauración de certificados

Si se pierden los certificados en un nodo, hay que volver a crearlos. Si se realiza una copia de seguridad de los certificados existentes en un archivo, se pueden restaurar en caso de que se produzca un error en el certificado. Para realizar una copia de seguridad de los certificados, siga estos pasos:

1. Inicie sesión en el nodo con privilegios raíz o administrativos.
2. Abra el símbolo del sistema (shell).
3. Ejecute el comando siguiente:

   ovcm -exportcacert -file <*nombre de archivo*> **[-pass** <*contraseña*>**]**

4. El comando realiza una copia de seguridad del certificado del servidor de administración en el archivo especificado con la opción -file.
5. Ejecute el comando siguiente:

   ovcert -exporttrusted [-ovrg *<servidor>***] -file** <*nombre de archivo*>
6. En este caso, *<servidor>* es el nombre del grupo de recursos de alta disponibilidad si el servidor de administración está instalado en un clúster de alta disponibilidad.

   El comando realiza una copia de seguridad del certificado de confianza del servidor de administración en el archivo especificado con la opción -file.
7. Determine el alias del certificado del nodo ejecutando el comando siguiente:

   ovcert -list [-ovrg *<servidor>***]**

   El alias del certificado del nodo es la secuencia larga de caracteres que aparece bajo la sección Certificates de la salida. Por ejemplo:

   ```
   +-----------------------------------------------+
   | Keystore Content | +-----------------------------------------------
   ---------+
   | Certificates: | cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*) | +--------
   ---------------------------------------------+
   | Trusted Certificates: |
   | CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55 | +------------------------
   -------------------------------+
   ```
8. Ejecute el comando siguiente:

   ovcert -exportcert -file *<nombre de archivo>* **-alias** *<alias>* **[-pass** *<contraseña>***]**

   El comando realiza una copia de seguridad del certificado del nodo en el archivo especificado con la opción -file.

Para restaurar el certificado del servidor de administración, ejecute el siguiente comando:

ovcm -importcacert -file *<file_name>* **[-pass** <*contraseña*>**]**

Para restaurar el certificado de confianza, ejecute el siguiente comando:

ovcert -importtrusted -file <*nombre de archivo*>

Para restaurar el certificado del nodo, ejecute el siguiente comando:

ovcert -importcert -file <*nombre_de_archivo*> **[-pass** <*contraseña*>**]**

Capítulo 8

HP Operations Agent en clústeres High Availability

HP Operations Agent se puede usar para monitorizar nodos en un clúster de High Availability. Para monitorizar aplicaciones preparadas para clúster en un clúster de alta disponibilidad, hay que implementar el agente con las directrices siguientes:

Deben estar presentes todos los nodos de un clúster en la lista de nodos administrados de la consola de HPOM.

Hay que instalar HP Operations Agent en todos los nodos del clúster de alta disponibilidad.

Es necesario que defina la variable MAX_RETRIES_FOR_CLUSTERUP (bajo el espacio de nombres conf.cluster) del nodo como un valor entero. La instalación basada en archivo de perfil garantiza que en la variable se selecciona un valor apropiado en todos los nodos en el momento de la instalación.

Nodos virtuales. Si se utiliza el nodo con HPOM para UNIX 8.3x, HPOM en UNIX/Linux 9.1x o HPOM para Windows 9.00, se puede sacar partido del concepto de nodos virtuales. Un nodo virtual es un grupo de nodos físicos vinculados por un grupo de recursos común. En función de los cambios del grupo de recursos, el agente puede habilitar o deshabilitar automáticamente las directivas en los nodos físicos.

La función de nodo virtual no está disponible en HPOM para Windows 8.1x.

Para monitorizar los nodos en un clúster de alta disponibilidad, hay que implementar las directivas de monitorización únicamente en el nodo virtual y no en los nodos físicos. Por consiguiente, es importante crear un nodo virtual para un clúster de alta disponibilidad en la consola de HPOM antes de comenzar a monitorizar las aplicaciones preparadas para clúster.

A continuación se indican las directrices para crear nodos virtuales en la consola de HPOM:

- Un nodo virtual no debe ser un nodo físico.
- Los nodos virtuales no admiten DHCP, autoimplementación ni certificados.
- No debe instalar un agente en un nodo virtual.

Monitorización de nodos en clústeres de alta disponibilidad

Se puede configurar HP Operations Agent para que monitorice aplicaciones preparadas para clúster que se ejecutan en los nodos de un clúster de alta disponibilidad.

Para monitorizar aplicaciones preparadas para clúster en los nodos de un clúster de alta disponibilidad, siga estos pasos:

1. *Sólo clústeres de Microsoft Cluster Server.* Asegúrese de que el grupo de recursos, que contiene el recurso que se está monitorizando, contiene tanto un nombre de red como un recurso de dirección IP.
2. Identifique las directivas requeridas para monitorizar la aplicación preparada para clúster.

3. Cree un archivo XML que describa la aplicación preparada para clúster y llámelo **apminfo.xml**.
4. Este archivo se utiliza para definir los grupos de recursos que se van a monitorizar y para asignar los grupos de recursos a las instancias de la aplicación.
5. El archivo **apminfo.xml** tiene el formato siguiente:

   Nota: No se permiten nuevas líneas entre las etiquetas de paquete del archivo **apminfo.xml**.

   T

```
<?xml version="1.0"?>

 <APMClusterConfiguration>

 <Application>

 <Name>Name of the cluster-aware application.</Name>

 <Instance>

 <Name>Application's name for the first instance. The instance name is
used for start and stop commands and corresponds to the name used to
designate this instance in messages.<Name>

 <Package>Resource group in which the application's first instance
runs.</Package>

 </Instance>

 <Instance>

 <Name>Application's name for the second instance.</Name>

 <Package>Resource group in which the application's second instance
runs.</Package>

 </Instance>

 </Application>

 </APMClusterConfiguration>
```

   DTD for apminfo.xml

```
<!ELEMENT APMClusterConfiguration (Application+)>

<!ELEMENT Application (Name, Instance+)>

<!ELEMENT Name (#PCDATA)>

<!ELEMENT Instance (Name, Package)>

<!ELEMENT Package (#PCDATA)>
```

   EJEMPLO

   En el ejemplo siguiente, el nombre del grupo de recursos es SQL-Server y el nombre de la red (o instancia) es CLUSTER04:

```
<?xml version="1.0"?>
```

```
<APMClusterConfiguration>
 <Application>
 <Name>dbspi_mssqlserver</Name>
 <Instance>
 <Name>CLUSTER04</Name>
 <Package>SQL-Server</Package>
 </Instance>
 </Application>
</APMClusterConfiguration>
```

6. Guarde el archivo **apminfo.xml** completado en cada nodo del clúster en el directorio siguiente:

   En Windows: *%OvDataDir%***conf\conf**

   En UNIX/Linux: **/var/opt/OV/conf/conf/**

7. Cree un archivo XML que describa las directivas que van a estar preparadas para clúster. El nombre de archivo debe tener el formato <*appl_name*>**.apm.xml**. <*nombre_aplicación*> debe ser idéntico al contenido de la etiqueta <Application><Name> del archivo **apminfo.xml**. El archivo <*nombre_aplicación*>**.apm.xml** incluye los nombres de las directivas identificadas en "HP Operations Agent en clústeres High Availability" en la página 48.
8. Utilice el siguiente formato al crear el archivo <*nombre_aplicación*>**.apm.xml**:

```
<?xml version="1.0"?>
 <APMApplicationConfiguration>
 <Application>
 <Name>Nombre de la aplicación preparada para clúster (debe coincidir con el contenido de <Application><Name> del archivo apminfo.xml).</Name>
 <Template>Primera directiva que debería estar preparada para clúster.</Template>
 <Template>Segunda directiva que debería estar preparada para clúster.</Template>
 <startCommand>Un comando opcional que ejecuta el agente siempre que se inicia una instancia de la aplicación.</startCommand>
 <stopCommand>Un comando opcional que ejecuta el agente siempre que se detiene una instancia de la aplicación.</stopCommand>
 </Application>
 </APMApplicationConfiguration>
```

Nota: En las etiquetas startCommand y stopCommand, si desea invocar a un programa que no proporcionó el sistema operativo, debe especifcar la extensión de archivo del programa.

Por ejemplo:

```
<startCommand>test_command.sh</startCommand>
<startCommand>dbspicol.exe ON $instanceName</startCommand>
```

Los comandos stop y start pueden usar las variables siguientes:

Variable	Descripción
$instanceName	Nombre (tal y como se muestra en <Instance><Name>) de la instancia que se está iniciando o deteniendo.
$instancePackage	Nombre (tal como se muestra en <Instance><Package>) del grupo de recursos que se está iniciando o deteniendo.
$remainingInstances	Número de instancias restantes de esta aplicación.
$openViewDirectory	El directorio de comandos en los agentes.

Ejemplo

El archivo de ejemplo siguiente llamado **dbspi_mssqlserver.apm.xml** muestra cómo el complemento inteligente para bases de datos configura las directivas para Microsoft SQL Server.

```
<?xml version="1.0"?>
<APMApplicationConfiguration>
 <Application>
 <Name>dbspi_mssqlserver</Name>
 <Template>DBSPI-MSS-05min-Reporter</Template>
 <Template>DBSPI-MSS-1d-Reporter</Template>
 <Template>DBSPI-MSS-05min</Template>
 <Template>DBSPI-MSS-15min</Template>
 <Template>DBSPI-MSS-1h</Template>
 <Template>DBSPI-MSS6-05min</Template>
 <Template>DBSPI-MSS6-15min</Template>
 <Template>DBSPI-MSS6-1h</Template>
 <Template>DBSPI Microsoft SQL Server</Template>
 <StartCommand>dbspicol.exe ON $instanceName</StartCommand>
 <StopCommand>dbspicol.exe OFF $instanceName</StopCommand>
 </Application>
</APMApplicationConfiguration>
```

9. Guarde el archivo <*nombre de aplic.*>**.apm.xml** completo en cada nodo del clúster en el directorio siguiente:

   En Windows: *%OvDataDir%***bin\instrumentation\conf**

   En UNIX/Linux: **/var/opt/OV/bin/instrumentation/conf**

10. Asegúrese de que todos los nodos físicos donde residen los grupos de recursos son nodos administrados.
11. Compruebe la sintaxis de los archivos XML en todos los nodos físicos ejecutando el comando siguiente:
12. En Windows: *%OvInstallDir%***\bin\ovappinstance -vc**

    En HP-UX, Linux o Solaris: **/opt/OV/bin/ovappinstance -vc**

    En AIX: **/usr/lpp/OV/bin/ovappinstance -vc**

13. *Opcional.* En algunos nodos físicos, por ejemplo, en nodos de host múltiples, el nombre de host estándar puede ser diferente del nombre del nodo en la configuración del clúster. Si éste es el caso, el agente no puede determinar correctamente el estado actual del grupo de recursos. Configure el agente para que use el nombre de host que aparece en la configuración del clúster:
14. Obtenga el nombre del nodo físico que aparece en la configuración del clúster:

    ovclusterinfo -a

15. Configure el agente para que use el nombre del nodo que aparece en la configuración del clúster:

    ovconfchg -ns conf.cluster -set CLUSTER_LOCAL_NODENAME <*nombre*>

    En esta instancia, <*nombre*> es el nombre del nodo, tal como se indicó en la salida de **ovclusterinfo -a**.

16. Reinicie el agente en todos los nodos físicos ejecutando los comandos siguientes:

```
ovc -stop
```

```
ovc -start
```

Si está usando HPOM para Windows 8.1x, implemente las directivas identificadas para monitorizar la aplicación preparada para clúster (en "HP Operations Agent en clústeres High Availability" en la página 48) en todos los nodos físicos del clúster de alta disponibilidad.

Para el resto de tipos de servidores de administración, implemente las directivas identificadas para monitorizar la aplicación preparada para clúster (en "HP Operations Agent en clústeres High Availability" en la página 48) en el nodo virtual creado para el clúster.

Usuario del agente

De manera predeterminada, HP Operations Agent comprueba regularmente el estado del grupo de recursos. En los nodos de UNIX y Linux, los agentes utilizan comandos de clúster específicos de la aplicación que, por lo general, sólo pueden ser ejecutados por usuarios con privilegios raíz. En los nodos de Windows, los agentes usan las API en lugar de ejecutar comandos.

Si se cambia el usuario de un agente, es posible que éste ya no disponga de los permisos requeridos para ejecutar correctamente los comandos de clúster. En este caso, hay que configurar

el agente para que utilice un programa de seguridad (por ejemplo, sudo o .do) al ejecutar comandos de clúster.

Para configurar el agente que se ejecuta con una cuenta sin privilegios raíz para ejecutar comandos de clúster, siga estos pasos:

1. Ejecute el comando siguiente para detener el agente:

   ovc -kill

2. Para configurar el agente para que use un programa de seguridad, escriba el comando siguiente:

   ovconfchg -ns ctrl.sudo -set OV_SUDO <*programa_seguridad*>

   En este ejemplo, <*programa_seguridad*> es el nombre del programa que desea que use el agente, por ejemplo /usr/local/bin/.do.

3. Ejecute el comando siguiente para iniciar el agente:

```
ovc -start
```

Capítulo 9

Implementación de HP Operations Agent en un entorno seguro

HP Operations Agent y el servidor de administración de HPOM se comunican entre sí en la red mediante el protocolo HTTPS. El servidor de administración abre las conexiones al nodo del agente para realizar tareas como implementar directivas o iniciar acciones, entre otras.
El nodo HP Operations Agent abre conexiones al servidor de gestión para enviar mensajes y respuestas.

De manera predeterminada, los sistemas operativos del nodo del agente y del servidor de administración asignan puertos de comunicación local. Sin embargo, tanto el agente como el servidor de administración utilizan el componente **Communication Broker** para la comunicación entrante. De manera predeterminada, el componente Communication Broker utiliza el puerto 383 para recibir datos. Por consiguiente, el nodo y el servidor de administración utilizan dos conjuntos de puertos:

Puerto asignado por el sistema operativo para la comunicación saliente

Puerto usado por el agente de comunicación para la comunicación entrante

En una red de alta seguridad basada en cortafuegos, la comunicación entre el servidor de administración y el nodo del agente puede fracasar debido a las restricciones en la configuración del cortafuegos. En estas situaciones, se pueden realizar tareas de configuración adicionales para configurar una comunicación bidireccional entre el servidor de administración y el nodo administrado.

Planificación de la configuración

- Si la red permite conexiones HTTPS a través del cortafuegos en ambas direcciones, pero con ciertas restricciones, son posibles las siguientes opciones de configuración en HPOM para adaptar dichas restricciones:
- Si la red sólo permite las conexiones de salida de ciertos puertos locales, se puede configurar HPOM de manera que use puertos locales específicos.
- Si la red sólo permite conexiones de entrada a ciertos puertos de destino distintos al puerto 383, se pueden configurar puertos de agentes de comunicación alternativos.
- Si la red sólo permite la conexión de ciertos sistemas proxy para abrir conexiones a través del cortafuegos, se podrá redireccionar la comunicación de HPOM a través de estos servidores proxy.
- Si la red sólo permite conexiones HTTPS salientes del servidor de gestión por el cortafuegos y bloquea las conexiones entrantes de los nodos, se puede configurar un proxy de canal inverso (RCP) ().

Antes de comenzar

Omita esta sección si se está utilizando HP Operations Agent sólo en nodos de Windows.

La mayoría de las tareas de configuración se realizan con la utilidad ovconfchg, que reside en el directorio siguiente:

En HP-UX, Linux y Solaris

```
/opt/OV/bin
```

En AIX

```
/usr/lpp/OV/bin
```

Para ejecutar el comando ovconfchg (y cualquier otro comando específico del agente) desde cualquier lugar del sistema, hay que agregar el directorio **bin** a la variable PATH del sistema. En los sistemas Windows, el directorio **bin** se agrega automáticamente a la variable PATH. Para agregar el directorio **bin** a la variable PATH en sistemas UNIX/Linux, siga estos pasos:

Realice una de las siguientes opciones:

En los nodos de HP-UX o Linux, ejecute el comando siguiente:

```
export PATH=/opt/OV/bin:$PATH
```

En los nodos AIX, ejecute el comando siguiente:

```
export PATH=/usr/lpp/OV/bin:$PATH
```

La variable PATH del sistema se configura ahora en la ubicación especificada. Puede ejecutar ahora comandos específicos del agente desde cualquier ubicación del sistema.

Configuración de servidores proxy

Se pueden redireccionar conexiones desde servidores de administración y nodos que se encuentran en redes diferentes a través de un proxy.

El servidor de administración abre las conexiones al servidor proxy, por ejemplo para implementar directivas e instrumentación, para sondeos de latidos o para iniciar acciones. El servidor proxy abre conexiones al nodo en nombre del servidor de administración y redirige la comunicación entre ellas.

El nodo abre conexiones al servidor proxy, por ejemplo, para enviar mensajes y respuestas de acción. El servidor proxy abre conexiones al servidor de administración en nombre del nodo.

También puede redirigir la comunicación a través de servidores proxy en entornos más complejos, de la manera siguiente:

Todos los servidores de administración y nodos pueden usar un servidor proxy diferente para comunicarse entre sí.

Se pueden configurar servidores de administración y nodos para seleccionar el proxy correcto, de acuerdo con el host al que tienen que conectarse.

En la figura siguiente se muestran las conexiones entre un servidor de administración y los nodos a través de varios servidores proxy:

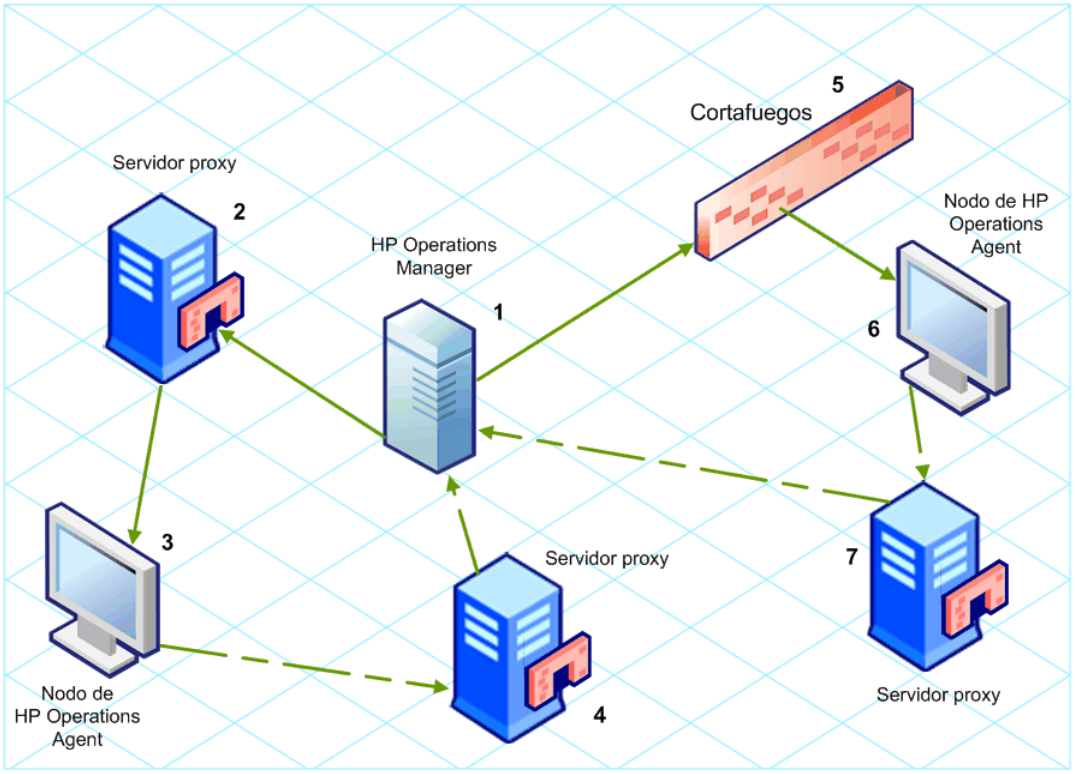
El servidor de administración (1) abre conexiones a un proxy (2). El proxy abre conexiones al nodo (3) en nombre del servidor de administración.

El nodo (3) abre conexiones a otro proxy (4). El proxy abre conexiones al servidor de administración (1) en nombre del nodo.

La red permite al servidor de administración (1) realizar conexiones HTTP salientes directamente del cortafuegos (5) a otro nodo (6). (Los nodos (3, 6) se encuentran en distintas redes.)

El cortafuegos (5) no permite conexiones HTTP entrantes. Por consiguiente, el nodo (6) abre conexiones al servidor de administración a través de un proxy (7).

Comunicación con servidores proxy



Sintaxis del parámetro PROXY

Los proxys redirigen la comunicación HTTPS saliente mediante la configuración del parámetro PROXY en el espacio de nombres bbc.http en los servidores de comunicación y nodos. Este parámetro se puede configurar de las siguientes formas:

- Configure los valores del ajuste predeterminado de la instalación de HP Operations Agent. Esto se recomienda si es preciso configurar proxys para un gran número de nodos. Hay que planificar y configurar los valores predeterminados de la instalación antes de crear o migrar los nodos.
- Utilice ovconfchg en el símbolo del sistema.

El valor del parámetro PROXY puede contener una o más definiciones de proxys. Especifique cada proxy en el formato siguiente:

*<nombrehost_proxy>***:***<puerto_proxy>***+(***<hosts incluidos>***)-(***<hosts excluidos>***)**

Sustituya *<host_incluidos>* por una lista separada por comas de nombres de host o direcciones IP en los que el proxy permite la comunicación. Sustituya *<host_excluidos>* por una lista separada por comas de nombres de host o direcciones IP a los que el proxy no se puede conectar. Los

asteriscos (*) son caracteres comodín en los hombres de host y direcciones IP. Tanto <*hosts_incluidos*> como <*host_excluidos*> son opcionales.

Para especificar varios proxys, separe cada uno de ellos por un punto y coma (;). El primer proxy adecuado de la lista tiene prioridad.

Ejemplo de valores del parámetro PROXY

Para configurar un nodo para que utilice el puerto 8080 del proxy1.example.com en todas las conexiones salientes, se usa el valor siguiente:

```
proxy1.example.com:8080
```

Para configurar un servidor de administración con el fin de que utilice proxy2.example.com:8080 para conectarse a cualquier host con un nombre de host que coincida con *.example.com o *example.org con una dirección IP en el rango 192.168.0.0 a 192.168.255.255, se utiliza el siguiente valor:

```
proxy2.example.com:8080+(*.example.com,*.example.org)-(192.168.*.*)
```

Para ampliar el ejemplo anterior con el fin de usar proxy3.example.com para conectarse únicamente a backup.example.com, se utiliza el siguiente valor:

```
proxy3.example.com:8080+(backup.example.com); proxy2.example.com:8080+
(*.example.com,*.example.org)-(192.168.*.*)
```

En el ejemplo anterior, proxy3.example.com:8080+(backup.example.com) debe ir primero, porque la lista de inclusión para proxy2.example.com contiene *.example.com.

Para redirigir la comunicación HTTPS a través de servidores proxy:

1. Inicie sesión en el servidor de gestión o nodo como administrador o usuario raíz, y abra el símbolo del sistema o shell.
2. Especifique los proxys que debería usar el nodo. Puede especificar otros proxys en función del host al que desea conectarse el agente. Ejecute el comando siguiente:

   ovconfchg -ns bbc.http -set PROXY <*proxy*>

   > **Nota:** Cuando use el comando ovconfchg en un servidor de administración que se ejecuta en un clúster, agregue el parámetro -ovrg <*servidor*>.

Sintaxis del parámetro PROXY_CFG_FILE

En lugar de especificar los detalles del servidor proxy con la variable de configuración PROXY, se puede usar un archivo de configuración externo para especificar la lista de servidores proxy y configurar HP Operations Agent para que lea los datos del servidor proxy del archivo de configuración.

Antes de configurar la variable PROXY_CFG_FILE es preciso crear el archivo de configuración externo. El archivo de configuración del proxy es un archivo XML que permite especificar los datos del servidor proxy en elementos XML Use un editor de texto para crear el archivo y guárdelo en el siguiente directorio:

En Windows

*%ovdatadir%***conf\bbc**

En UNIX/Linux

/var/opt/OV/conf/bbc

Organización del archivo de configuración del proxy

El archivo XML de configuración del proxy incluye distintos elementos XML para especificar detalles del servidor proxy, nodo del agente y servidor de gestión. En dicho archivo se pueden proporcionan los datos de configuración de varios servidores proxy.

Estructura del archivo XML de configuración del proxy

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<proxies>
  <proxy>
    <server>proxy_server.domain.example.com:8080</server>
    <for>
      <target> *.domain.example.com    </target>
      <target> *.domain2.example.com </target>
      <target> *.domain3.example.com   </target>
    </for>
  </proxy>
<proxies>
```

- proxies: el elemento proxies le permite agregar detalles de los servidores proxy que desea usar en su entorno gestionado por HPOM. Todo el contenido de este archivo XML se encuentra dentro del elemento proxies.
- proxy: este elemento captura los datos del servidor proxy y de los sistemas que se comunican con el nodo local a través del servidor proxy. En este archivo XML se pueden configurar varios elementos proxy.
- server: este elementos se usa para especificar el nombre de dominio completo (o la dirección IP) del servidor proxy que desea usar en su entorno de monitorización.
- for: en el elemento for incluya el nombre de dominio completo o las direcciones IP de los restantes nodos de agente o servidores de gestión que deben comunicarse con el nodo local sólo a través del servidor proxy que se ha especificado en el elemento server. Debe agregar cada uno de los nombres de dominio completos o direcciones IP del elemento target.

Por ejemplo:

```
<for>
      <target> system3.domain.example.com </target>
      <target> system3.domain.example.com </target>
</for>
```

Puede usar el carácter comodín para configurar varios sistemas dentro de un solo elemento target. También puede especificar un intervalo de direcciones IP.

Por ejemplo:

```
<for>
       <target> *.domain2.example.com </target>
       <target> 172.16.5.* </target>
       <target> 192.168.3.50-85 </target>
</for>
```

- except: este elemento se usa para crear una lista de exclusión de sistemas que *no* deben comunicarse con el nodo local a través del servidor proxy configurado (especificado en el elemento server). Incluya los nombres de dominio completos o las direcciones IP de todos esos sistemas en el elemento target.

Por ejemplo:

```
<except>
       <target> *.domain3.example.com   </target>
       <target> 172.16.10.* </target>
       <target> 192.168.9.5-25 </target>
</except>
```

Ejemplos del archivo de configuración del proxy

Sintaxis	Descripción
<proxies> <proxy> <server> server1.domain.example.com:8080 </server> <for> <target> *.domain2.example.com </target> </for> </proxy> <proxies>	El servidor server1.domain.example.com está configurado como servidor proxy y todos los sistemas que pertenecen al dominio domain2.example.com deben comunicarse con el nodo exclusivamente a través de server1.domain.example.com .
<proxies> <proxy> <server>	El servidor server2.domain.example.com está configurado como servidor proxy y todos los sistemas que pertenecen al dominio domain2.example.com o cuya dirección IP comience

Sintaxis	Descripción
server2.domain.example.com:8080 </server> <for> <target> *.domain2.example.com</target> <target>192.168.2.*/target> </for> </proxy> <proxy> <server> server3.domain.example.com:8080 </server> <for> <target>192.168.3.*</target> </for> <except> <target>192.168.3.10-20</target> </except> </proxy> <proxies>	por 192.168.2 deben comunicarse con el nodo exclusivamente a través de server2.domain.example.com . El servidor server3.domain.example.com está configurado como segundo servidor proxy y todos los sistemas cuya dirección IP comience por 192.168.2 deben comunicarse con el nodo exclusivamente a través de server3.domain.example.com . Además, los sistemas cuya dirección IP se encuentre dentro del intervalo 192.168.3.10-20 no podrán usar el servidor proxy server3.domain.example.

Configuración de la variable PROXY_CFG_FILE

1. Inicie sesión en el nodo como administrador o usuario raíz.
2. Cree un archivo XML con un editor de texto.
3. Agregue la siguiente línea al principio del archivo:

   ```
   <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
   ```

4. Incorpore el contenido al archivo.
5. Guarde el archivo en el siguiente directorio:

   En Windows

   *%ovdatadir%***conf\bbc**

En UNIX/Linux

`/var/opt/OV/conf/bbc`

6. Ejecute el comando siguiente:

   En Windows

   *%ovinstalldir%***bin\ovconfchg -ns bbc.http -set PROXY_CFG_FILE** *<nombre de archivo>***.xml**

   En HP-UX, Linux o Solaris

   /opt/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE *<nombre de archivo>***.xml**

   En AIX

   /usr/lpp/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE *<nombre de archivo>***.xml**

Configuración del puerto de Communication Broker

De manera predeterminada, los nodos de HP Operations Agent utilizan el puerto 383 para la comunicación entrante. El componente Communication Broker facilita la comunicación entrante en cada servidor o nodo de HP Operations Agent a través del puerto 383.

Puede configurar cualquier agente de comunicación para que escuche en un puerto distinto de 383. Si lo hace, también debe configurar los demás servidores de administración y nodos en el entorno, de tal forma que sus conexiones salientes estén dirigidas al puerto correcto. Por ejemplo, si se configura un agente de comunicación de un nodo para que escuche en el puerto 5000, también hay que configurar el servidor de administración para que se conecte al puerto 5000 cuando se comunica con ese nodo.

Sintaxis del parámetro PORTS

Los puertos del agente de comunicación se configuran estableciendo el parámetro PORTS del espacio de nombres bbc.cb.ports en todos los servidores de administración y nodos que se comunican entre sí.

Este parámetro se puede configurar de las siguientes formas:

- Configure los valores en los ajustes predeterminados de la instalación HP Operations Agent en un archivo de perfil durante la instalación. Esto se recomienda si se precisa configurar los puertos del agente de comunicación para un gran número de nodos. Hay que planificar y configurar los valores predeterminados de la instalación antes de crear o migrar los nodos.
- Utilice **ovconfchg** en el símbolo del sistema.

Los valores deben contener uno o más nombres de host o direcciones IP y tener el formato siguiente:

*<host>***:***<puerto>***[,***<host>***:***<puerto>***] ...**

El <*host*> puede ser un nombre de dominio o una dirección IP. Por ejemplo, para configurar el puerto del agente de comunicación a 5000 en un servidor de administración con el nombre de host manager1.emea.example.com, utilice el comando siguiente en el mismo servidor de administración y también en cualquier otro servidor de administración y nodos que abran conexiones a él.

```
ovconfchg -ns bbc.cb.ports -set PORTS manager1.domain.example.com:5000
```

Si hay que configurar puertos del agente de comunicación en varios sistemas, se pueden usar caracteres comodines y rangos, de la manera siguiente:

Se puede usar un carácter comodín al comienzo de un nombre de dominio agregando un asterisco (*). Por ejemplo:

*.test.example.com:5000

*.test.com:5001

*:5002

Para usar los caracteres comodín al final de una dirección IP, se agregan hasta tres asteriscos (*). Por ejemplo:

192.168.1.*:5003

192.168.*.*:5004

10.*.*.*:5005

Se puede reemplazar un octeto en una dirección IP con un rango. El rango debe preceder a cualquier carácter comodín. Por ejemplo:

192.168.1.0-127:5006

172.16-31.*.*:5007

Si se especifican varios valores para el parámetro PORTS, cada uno de ellos debe ir separado por una coma (,). Por ejemplo:

```
ovconfchg -ns bbc.cb.ports -set PORTS *.test.example.com:5000,
10.*.*.*:5005
```

Cuando se especifican varios valores con caracteres comodín y rangos que se solapan, el servidor de administración o el nodo selecciona el puerto que se va a usar en el orden siguiente:

Nombres de dominio completos.

Nombres de dominio con caracteres comodín.

Direcciones IP completas.

Direcciones IP con rangos.

Direcciones IP con caracteres comodín.

Ejemplo

Debe configurar el entorno de administración de HPOM para la especificación siguiente:

Configure todos los sistemas dentro del dominio *.test2.example.com para que utilicen el puerto 6000 para el agente de comunicación.

Configure todos los sistemas con 10 como primer octeto de la dirección IP (10.*.*.*) para que usen el puerto 6001 para el agente de comunicación, con la excepción siguiente:

Configure todos los sistemas en los que el segundo octeto de la dirección IP se encuentre entre 0 y 127 (10.0-127.*.*) para usar el puerto 6003 para el agente de comunicación.

Configure el sistema manager1.test2.example.com para que utilice el puerto 6002 para el agente de comunicación.

Para configurar el entorno de monitorización de HPOM con la especificación anterior, se ejecuta el comando siguiente:

```
ovconfchg -ns bbc.cb.ports -set PORTS *.test2.example.com:6000,
10.*.*.*:6001,manager1.test2.example.com:6002,10.0-127.*.*:6003
```

Los cambios surtirán efecto sólo si se ejecuta este comando en *todos* los nodos de agente y en *todos* los servidores de administración de HPOM del entorno de monitorización.

Para averiguar qué puerto está configurado actualmente, se ejecuta el comando siguiente:

bbcutil -getcbport *<host>*

Para configurar el componente Communication Broker para que utilice un puerto que no sea el predeterminado:

Nota: Hay que asegurarse de configurar el componente Communication Broker en todos los servidores y nodos de HPOM de HP Operations Agent en el entorno del usuario para usar el mismo puerto.

1. Inicie sesión en el nodo de HP Operations Agent.
2. Abra el símbolo del sistema o shell.
3. Ejecute el siguiente comando para establecer el puerto de Communication Broker a un valor no predeterminado:

   ovconfchg -ns bbc.cb.ports -set PORTS <host>:<puerto>[,<host>:<puerto>] ...

   Si se utiliza el comando **ovconfchg** en un nodo de HP Operations Agent que se ejecuta en un clúster, es preciso agregar el parámetro **-ovrg** <*servidor*>, donde <*servidor*> es el grupo de recursos.
4. Ejecute el comando anterior en todos los nodos de agente y en todos los servidores de administración.

Configuración de los puertos de comunicación local

De manera predeterminada, los servidores de administración y nodos utilizan el puerto local 0 para las conexiones salientes, lo que significa que el sistema operativo asigna el puerto local a cada

conexión. De manera habitual, el sistema operativo asignará los puertos locales secuencialmente. Por ejemplo, si el sistema operativo ha asignado el puerto local 5055 a un explorador Internet y el agente HTTPS abre después una conexión, éste recibirá el puerto local 5056.

Sin embargo, si un cortafuegos restringe los puertos que se pueden usar, se pueden configurar los servidores de administración y nodos para que utilicen en su lugar un rango específico de puertos locales.

Sintaxis del parámetro CLIENT_PORT

Los puertos de comunicación local se configuran estableciendo el parámetro CLIENT_PORT del espacio de nombres bbc.http en el servidor de administración o nodo. Este parámetro se puede configurar de las siguientes formas:

- Configure los valores del ajuste predeterminado de la instalación de HP Operations Agent. Esto se recomienda si se precisa configurar los puertos de comunicación local para un gran número de nodos. Hay que planificar y configurar los valores predeterminados de la instalación antes de crear o migrar los nodos.
- Utilice ovconfchg en el símbolo del sistema.

El valor deben ser un rango de puertos con el formato siguiente:

<número de puerto inferior>-<número de puerto superior>

Por ejemplo, si el cortafuegos sólo permite conexiones salientes que se originan en los puertos 5000 a 6000, se debería usar el valor siguiente:

```
5000-6000
```

Para configurar los puertos de comunicación locales:

1. Inicie sesión en el nodo de HP Operations Agent.
2. Abra el símbolo del sistema o shell.
3. Especifique el rango de puertos locales que puede usar el servidor de administración o uso para las conexiones siguientes escribiendo el comando siguiente:

   ovconfchg -ns bbc.http -set CLIENT_PORT *<número de puerto inferior>-<número de puerto superior>*

   Cuando se usa el comando ovconfchg en un servidor de administración que se ejecuta en un clúster, hay que agregar el parámetro -ovrg <*servidor*>.

Configuración de nodos con varias direcciones IP

Si el nodo tiene varias direcciones IP, el agente usa las direcciones siguientes para establecer la comunicación:

El agente de comunicación acepta las conexiones entrantes en todas las direcciones IP.

El agente abre conexiones al servidor de administración con la primera interfaz de red que encuentre.

Para comunicarse con HP Reporter o HP Performance Manager, el demonio de comunicación (CODA) acepta conexiones entrantes en todas las direcciones IP.

Para configurar HP Operations Agent con objeto de que utilice una dirección IP específica:

1. Inicie sesión en el nodo de HP Operations Agent.
2. Abra el símbolo del sistema o shell.
3. Ejecute el comando siguiente para establecer la dirección IP para el Communication Broker:

   ovconfchg -ns bbc.cb SERVER_BIND_ADDR <*dirección ip*>
4. Ejecute el comando siguiente para establecer la dirección IP que va a utilizar el agente al abrir las conexiones salientes al servidor de administración:

   ovconfchg -ns bbc.http CLIENT_BIND_ADDR <*dirección ip*>
5. Ejecute el comando siguiente para establecer la dirección IP que va a utilizar para las conexiones entrantes desde HP Performance Manager o HP Reporter:

   ovconfchg -ns coda.comm SERVER_BIND_ADDR <*dirección ip*>

Configuración de la comunicación HTTPS a través de proxys

Si la red sólo permite la conexión de ciertos sistemas proxy para abrir conexiones a través del cortafuegos, se podrá redireccionar la comunicación de HPOM a través de estos servidores proxy. En la lista siguiente se muestra el flujo de trabajo del servidor de administración y la comunicación del agente con esta configuración:

1. El servidor de administración abre las conexiones al proxy.
2. El servidor proxy abre las conexiones al nodo en nombre del servidor de administración y redirige la comunicación entre ellas.
3. El nodo abre las conexiones al proxy.
4. El proxy abre las conexiones al servidor de administración en nombre del nodo.

Para redirigir la comunicación a través de servidores proxy:

1. Inicie sesión en el servidor de gestión o en el nodo con los privilegios de usuario raíz/administrativo.
2. Ejecute el comando siguiente en el símbolo del sistema:

   ovconfchg -ns bbc.http -set PROXY <*proxy*>**:** <*puerto*>

En este ejemplo, <*proxy*> es la dirección IP o nombre de dominio completo (FQDN) del servidor proxy; <*puerto*> es el puerto de comunicación del servidor proxy.

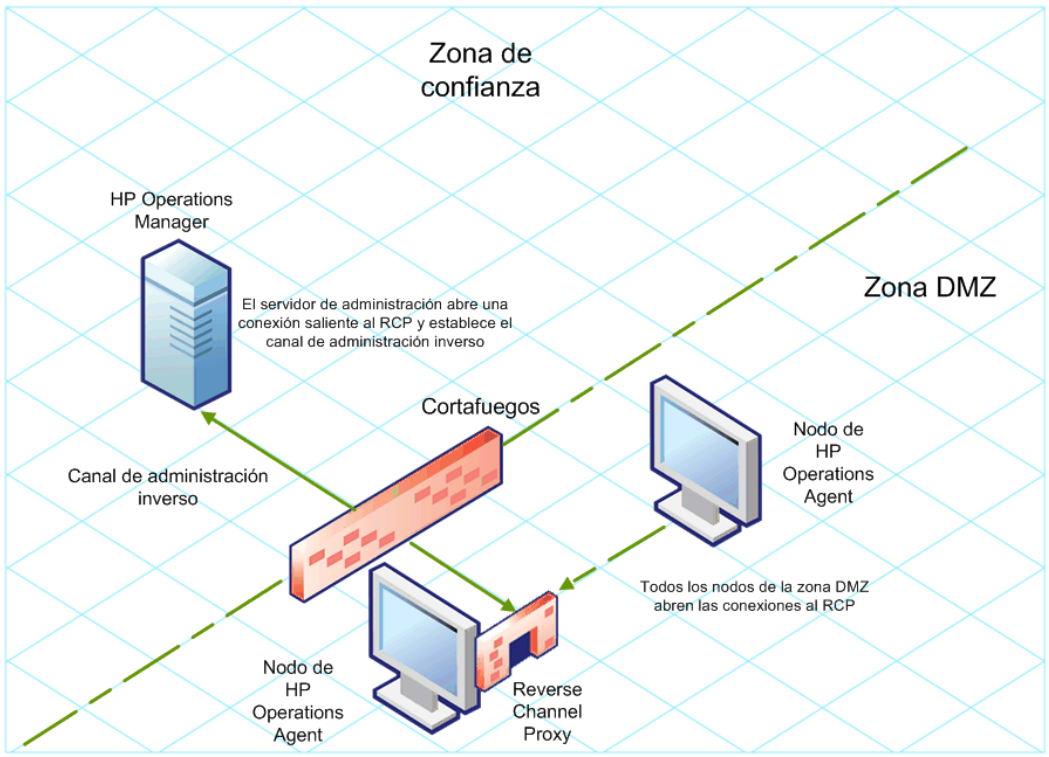
Comunicación en un entorno de alta seguridad

En un entorno seguro, controlado por cortafuegos, los sistemas que están presentes en la zona de confianza pueden comunicarse libremente e intercambiar información entre sí. Sin embargo, una configuración específica del cortafuegos puede restringir la comunicación con los sistemas que no pertenecen a la zona de confianza. Es posible que la red que no sea de confianza, también conocida como zona desmilitarizada (**DMZ**) no envíe datos a la zona de confianza debido a las restricciones de la configuración del cortafuegos.

En muchas situaciones de implementación, el servidor de administración de HPOM puede residir en la zona de confianza y los nodos administrados pueden residir en la zona DMZ. Si el cortafuegos está configurado para evitar que los sistemas de la zona DMZ se comuniquen con los sistemas de la zona de confianza, la comunicación entre servidor y agente será imposible.

En la siguiente situación, los nodos administrados están ubicados en la zona DMZ, mientras que el servidor de administración pertenece a la zona de confianza. En este ejemplo, la configuración del cortafuegos permite únicamente la comunicación saliente. Por consiguiente, la comunicación entrante al servidor de administración está bloqueada por el cortafuegos.

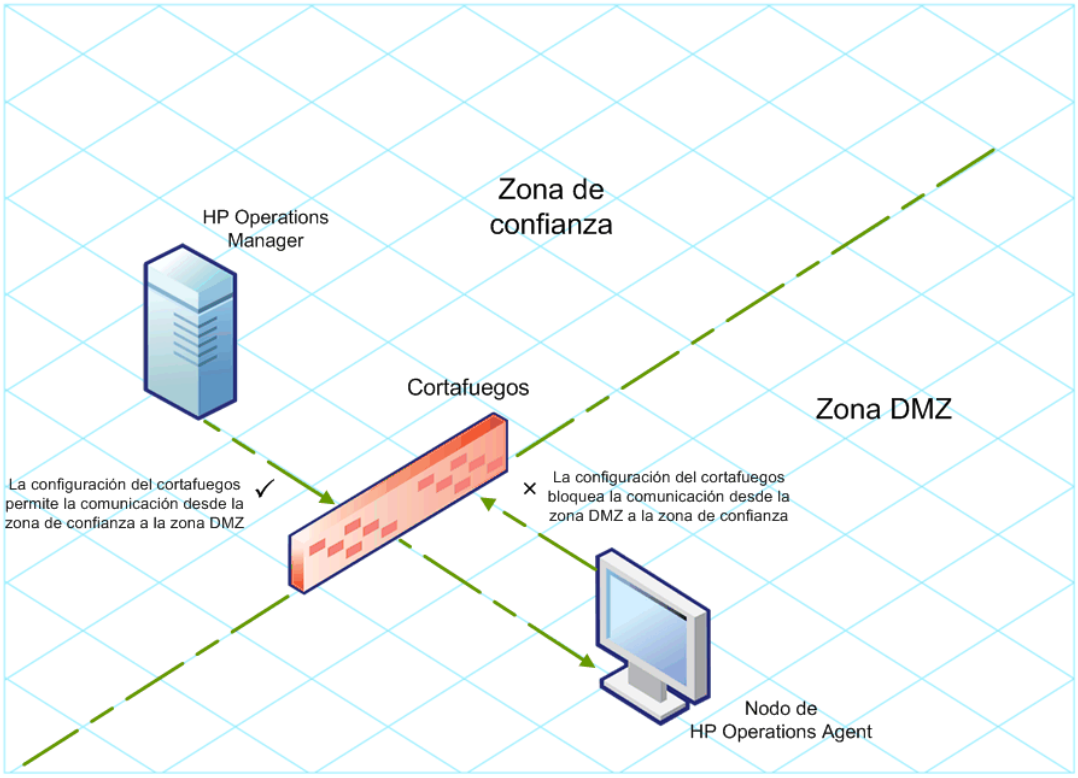
Nodos gestionados en la zona DMZ



En la siguiente situación, los nodos administrados están ubicados en la zona de confianza, mientras que el servidor de administración pertenece a la zona DMZ. En este ejemplo, la

configuración del cortafuegos permite únicamente la comunicación saliente desde el nodo al servidor de administración de HPOM, pero bloquea la comunicación entrante al nodo.

Servidor de gestión de HPOM en la zona DMZ



Introducción a Reverse Channel Proxy

Una solución sencilla para habilitar la comunicación bidireccional es configurar el cortafuegos para que permita el tráfico entrante al puerto 383 (el puerto de Communication Broker). Sin embargo, este procedimiento podría hacer vulnerable al sistema a los ataques externos. Para habilitar la comunicación segura sin permitir el tráfico entrante al puerto de Communication Broker, hay que configurar un Reverse Channel Proxy (**RCP**).

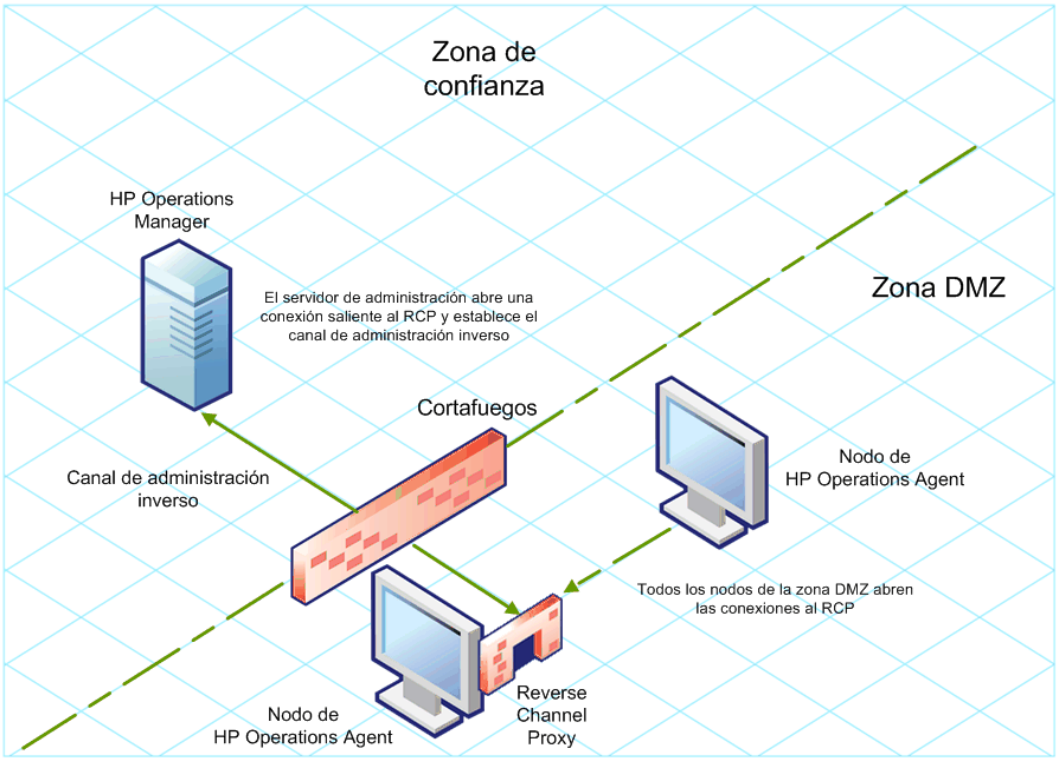
Los sistemas que pertenecen a la zona DMZ abren la conexión al RCP en lugar de al sistema dentro de la zona de confianza. Puede configurar el sistema en la zona de confianza para abrir un canal de comunicación saliente (el canal de administración inverso) al RCP. El sistema de la zona de confianza mantiene el canal saliente; los sistemas de la zona DMZ usa el canal de administración inverso para enviar detalles a la zona de confianza mediante el RCP.

Cuando los nodos se encuentran en la zona DMZ y el servidor de administración en la zona de confianza, la configuración de HPOM utiliza el siguiente flujo de trabajo:

1. El RCP está configurado en un nodo de la zona DMZ.
2. Todos los nodos de la zona DMZ abren las conexiones al RCP.

3. El servidor de administración abre una conexión saliente al RCP y establece un canal de administración inverso. Éste permite al servidor de administración aceptar los datos entrantes que se originan en el RCP sin que se impliquen puertos adicionales.
4. Todos los nodos de la zona DMZ se comunican con el servidor de administración de HPOM mediante el canal de administración inverso.

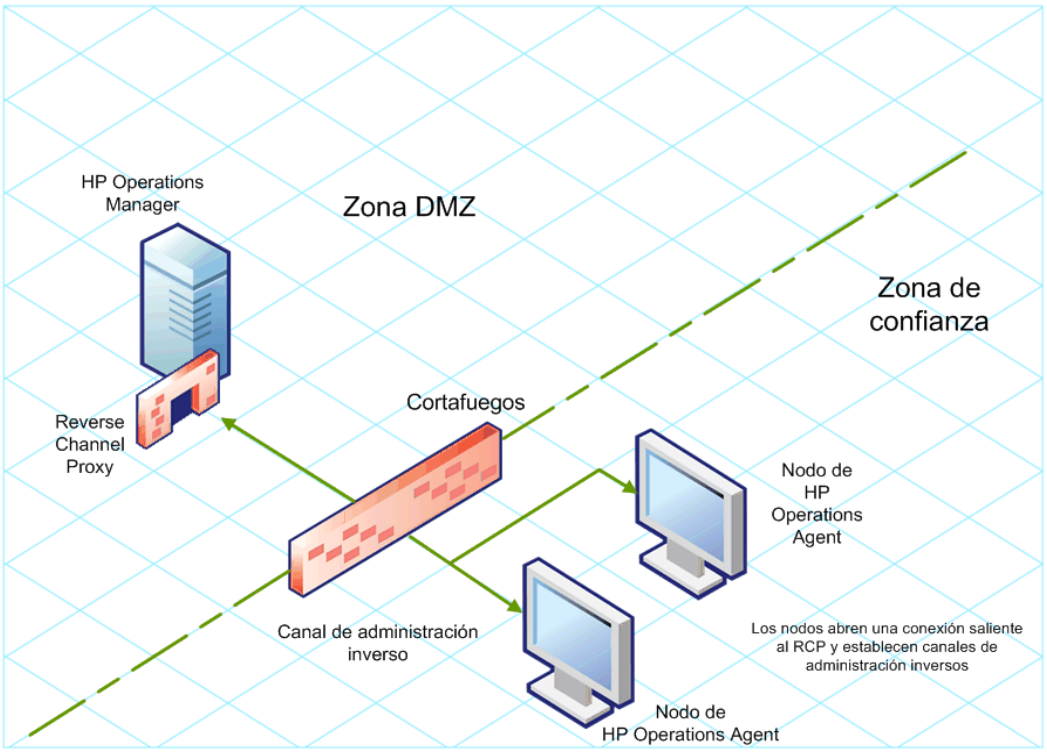
Comunicación segura a través del RCP con nodos de la zona DMZ



Cuando los nodos se encuentran en la zona de confianza y el servidor de administración en la zona DMZ, la configuración de HPOM utiliza el siguiente flujo de trabajo:

1. El RCP está configurado en el servidor de administración de la zona DMZ.
2. Los nodos abren una conexión saliente al RCP y establecen canales de administración inversos. Éstos permiten a los nodos que acepten los datos entrantes que se originan en el RCP sin que se impliquen puertos adicionales.
3. El servidor de administración de la zona DMZ se comunica con los nodos mediante el canal de administración inverso.

Comunicación segura a través del RCP con el servidor de gestión de la zona DMZ



Configuración de una comunicación segura en un entorno sólo de salida

Para configurar la comunicación segura con la ayuda del RCP y el canal de administración inverso en un entorno sólo de salida, realice las tareas siguientes:

Configurar un RCP

Antes de configurar el RCP, hay que configurar el certificado del nodo.

Para configurar un RCP:

1. Inicie sesión en el nodo o en el servidor de administración (dependiendo de su ubicación en la red) como usuario con privilegios administrativos o raíz.
2. Abra el símbolo del sistema o shell.
3. Ejecute el comando siguiente:

   ovconfchg -ns bbc.rcp -set SERVER_PORT *<número_puerto>*.

   En este ejemplo, *<número_puerto>* es el puerto que utilizará el RCP. Asegúrese de que el puerto especificado no lo está utilizando ninguna otra aplicación.
4. *Sólo en UNIX/Linux.* Communication Broker (ovbbccb) se ejecuta con /var/opt/OV como directorio raíz. Los archivos de configuración que son necesarios para abrir las conexiones del Protocolo de control de transmisión (TCP) se encuentran en el directorio /etc. Esto impide a ovbbccb crear conexiones con RCP. Debe hacer lo siguiente para resolver este problema:

a. Cree el directorio llamado etc en /var/opt/OV

b. Copie los archivos de configuración relevantes del servicio de nombres (por ejemplo, archivos como resolv.conf, hosts, nsswitch.conf) de /etc a /var/opt/OV/etc

c. Además, también puede deshabilitar la función ovbbccb chroot ejecutando el comando siguiente. Este método resuelve el problema de impedir a ovbbccb crear conexiones con RCP.

ovconfchg -ns bbc.cb -set CHROOT_PATH /

5. Registre el componente de RCP para que ovc lo inicie, detenga y monitorice. Escriba los comandos siguientes:

ovcreg -add <*dir. de instalación*>**/newconfig/DataDir/conf/bbc/ovbbcrcp.xml**

```
ovc -kill
```

```
ovc -start
```

Configurar un canal de administración inverso

Con la ayuda de los RCP creados, hay que configurar un canal de administración inverso para facilitar la comunicación entrante en un entorno de cortafuegos sólo de salida. Para configurar un canal de administración inverso, siga estos pasos:

1. Inicie sesión en el nodo o en el servidor de administración (dependiendo de su ubicación en la red) como usuario con privilegios administrativos o raíz.
2. Abra el símbolo del sistema o shell.
3. Ejecute el comando siguiente para crear el canal de administración inverso:

ovconfchg [-ovrg <*servidor*>**] -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true**

4. Ejecute los comandos siguientes para especificar los detalles de RCP:

ovconfchg [-ovrg <*servidor*>**] -ns bbc.cb -set RC_CHANNELS <rcp>:<puerto>[, <OvCoreId>][;<rcp2>...]**

ovconfchg [-ovrg <*servidor*>**] -ns bbc.cb -set PROXY <rcp>:<puerto>[,<OvCoreId>] [;<rcp2>...]**

En este ejemplo:

<*rcp*>: nombre de dominio completo o dirección IP del sistema donde está configurado el RCP.

<*puerto*>: El número de puerto configurado para el RCP (el puerto especificado para la variable SERVER_PORT)

<*OvCoreId*>: el ID de núcleo del sistema donde ha configurado el RCP.

Además, puede proporcionar los detalles de RCP mediante un archivo de configuración.

5. *Opcional.* Configure el servidor para restaurar automáticamente las conexiones erróneas del canal de administración inverso. De manera predeterminada, el servidor no restaura las conexiones con error. Para cambiar el valor predeterminado, ejecute el comando siguiente:

ovconfchg [-ovrg <*servidor*>**] -ns bbc.cb -set RETRY_RC_FAILED_CONNECTION TRUE**

6. *Opcional.* Establezca el número máximo de intentos que debe realizar el servidor para conectarse a un RCP. De manera predeterminada, está establecido en -1 (infinito). Para cambiar el valor predeterminado, ejecute el comando siguiente:

   ovconfchg [-ovrg <*servidor*>**] -ns bbc.cb -set MAX_RECONNECT_TRIES** <*número de intentos*>

7. *Opcional.* El servidor de administración se puede configurar para que genere un mensaje de advertencia al producirse un error en la conexión del canal de administración inverso. De manera predeterminada, el servidor de administración no genera el mensaje de error. Para cambiar el valor predeterminado, ejecute el comando siguiente:

   ovconfchg [-ovrg <*servidor*>**] -ns bbc.cb -set RC_ENABLE_FAILED_OVEVENT TRUE**

   Si se establece RETRY_RC_FAILED_CONNECTION en TRUE, el servidor de administración no genera el mensaje.

8. *Opcional.* Para comprobar que el canal de administración inverso está abierto, ejecute el comando siguiente:

   ovbbccb -status

   La salida muestra todos los canales de administración inversos abiertos.

9. *Opcional.* Para restaurar un canal de administración inverso con errores, ejecute el comando siguiente:

   ovbbccb -retryfailedrcp [-ovrg <*servidor*>**]**

Consideraciones sobre el rendimiento del canal de administración inverso

El rendimiento de un canal de administración inverso puede depender del número de nodos conectados al canal. La variable RC_MAX_WORKER_THREADS permite ajustar el rendimiento de un canal de administración inverso.

Para usar la variable RC_MAX_WORKER_THREADS:

1. Inicie sesión en el nodo que establece el canal de administración inverso.
2. Anote el tiempo que tarda el agente en establecer el canal. Se puede determinar ejecutando el comando **ovbbccb -status**. La salida del comando **ovbbccb -status** muestra el estado de los canales de administración inversos que se originan en el sistema. Al ejecutar de manera repetida el comando **ovbbccb -status**, se puede determinar el tiempo aproximado que tarda el agente en establecer el canal.
3. Calcule la relación entre el tiempo deseado para establecer el canal y el tiempo real aproximado que tarda el agente en establecer el canal.
4. Establezca la variable RC_MAX_WORKER_THREADS al siguiente entero superior de la relación. Utilice el comando siguiente para establecer esta variable:

ovconfchg -ns bbc.cb -set RC_MAX_WORKER_THREADS <*número máximo de subprocesos*>

Especificación de los detalles de RCP con un archivo de configuración

Con la ayuda de un archivo de configuración, se pueden especificar los detalles de los RCP. Para usar el archivo de configuración, siga estos pasos:

1. Cree un archivo de texto.
2. Especifique los detalles de cada RCP en una nueva línea con el formato siguiente:

   <rcp>:<puerto>[,<OvCoreId>]

   En este ejemplo:

   <*rcp*>: nombre de dominio completo o dirección IP del sistema donde está configurado el RCP.

   <*puerto*>: El número de puerto configurado para el RCP (el puerto especificado para la variable SERVER_PORT).

   <*OvCoreId*>: el ID de núcleo del sistema donde ha configurado el RCP.
3. Guarde el archivo en la ubicación siguiente:

   <*data_dir*>**/conf/bbc**

   Si va a realizar este paso en un servidor de gestión en un clúster de alta disponibilidad o en una configuración de agrupamiento de servidores, guarde el archivo en la siguiente ubicación:

   <*data_dir*>**/shared/** <*servidor*>**/conf/bbc**
4. Ejecute el comando siguiente:

   ovconfchg [-ovrg <*servidor*>**] -ns bbc.cb -set RC_CHANNELS_CFG_FILES** <*nombre de archivo*>

En este ejemplo:

<*nombre_archivo*>: Nombre del archivo creado.

<*server*>: Nombre del grupo de recursos del clúster o configuración de agrupamiento de servidores.

Configuración de un RCP para varios sistemas

Se puede configurar sólo un RCP en la zona DMZ y después configurar otros sistemas en la zona DMZ para que utilicen el RCP. Para ello, debe establecerse la variable PROXY de todos los sistemas de la zona DMZ en la dirección IP (o nombre de dominio completo) y puerto del sistema que hospeda el RCP. Para configurar varios sistemas con objeto de que utilicen un único RCP, siga estos pasos:

1. Inicie sesión en el nodo con privilegios raíz o administrativos.
2. Abra el símbolo del sistema (shell).

3. Ejecute el comando siguiente:

   ovconfchg -ns bbc.http -set PROXY "*<rcp>***:***<puerto>***+***<host_incluidos>***-***<host_excluidos>***"**

   En este ejemplo:

   <*rcp*>: nombre de dominio completo o dirección IP del sistema donde está configurado el RCP.

   <*puerto*>: El número de puerto configurado para el RCP (el puerto especificado para la variable SERVER_PORT).

   <*host_incluidos*>: especifique el nombre de dominio completo o dirección IP del sistema que abre un canal de administración inverso al RCP. En esta situación, hay que especificar el nombre de dominio completo o dirección IP del servidor de administración que pertenece a la zona de confianza. Si se desean utilizar varios servidores de administración, hay que especificar varios nombres de dominio completos separados por comas.

   <*host_excluidos*>: especifique el nombre de dominio completo o dirección IP de los sistemas cuyo contacto no debe establecerse mediante el RCP. Se pueden especificar varios nombres de dominio completos separados por comas. Sin embargo, debe especificar el nombre de dominio completo y nombre de host (separados por comas) del sistema local. Por ejemplo, **ovconfchg -ns bbc.http -set PROXY "<rcp>:<puerto>-<localhost>, <localhost>.domain.com"**

4. Si el sistema es un nodo de HP Operations Agent, ejecute el comando siguiente para reiniciar el agente de mensajes:

   ```
   ovc -restart opcmsga
   ```

Repita los pasos 3 y 4 en todos los sistemas de la zona DMZ.

Consideraciones sobre el rendimiento del RCP

Si se configura un RCP para un único sistema, es suficiente con cumplir los requisitos mínimos para el sistema de agente.

Si se configura un RCP que utilizarán varios modos de agente, hay que asegurarse de que el sistema de RCP podrá prestar servicio a todas las peticiones entrantes sin una importante demora de tiempo.

Comprobación de la comunicación a través de RCP

Después de configurar los RCP y de establecer un canal de administración inverso, se pueden realizar las tareas siguientes para comprobar si las comunicaciones entre el servidor y el nodo se han establecido correctamente.

Comprobar la comunicación al RCP

Para comprobar que el sistema de la zona DMZ puede comunicarse con el RCP, siga estos pasos:

1. Inicie sesión en el sistema de la zona DMZ con los privilegios raíz o administrativos.
2. Abra el símbolo del sistema (shell).

3. Ejecute el comando siguiente:

   bbcutil -gettarget *<FQDN>*

En este ejemplo, *<FQDN>* es el nombre de dominio completo que establece el canal de administración inverso en el RCP. Si el servidor de administración está ubicado en la zona de confianza, especifique el nombre de dominio completo del servidor de administración.

Si el RCP se creó correctamente, la salida debería mostrar el mensaje siguiente:

HTTP Proxy: *<rcp>*:*<puerto>*

En este ejemplo:

<rcp>: nombre de dominio completo o dirección IP del sistema donde está configurado el RCP.

<puerto>: El número de puerto configurado para el RCP (el puerto especificado para la variable SERVER_PORT).

Comprobar el canal de administración inverso

Para comprobar que el canal de administración inverso está establecido de manera correcta, siga estos pasos:

1. Inicie sesión en el sistema de la zona de confianza con los privilegios raíz o administrativos.
2. Abra el símbolo del sistema (shell).
3. Ejecute el comando siguiente:

   ovbbccb –status

Si los canales se crearon correctamente, la salida debería mostrar el mensaje siguiente:

```
HTTP Communication Reverse Channel Connections

Opened:

system1.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000

system2.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000

system3.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000

system4.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000
```

En este ejemplo, el sistema ha establecido canales de administración inversos en los siguientes sistemas RCP: system1, system2, system3 y system4.

Si se produce un error en el canal de administración inverso a un RCP, el comando **ovbbccb –status** muestra el estado con el formato siguiente:

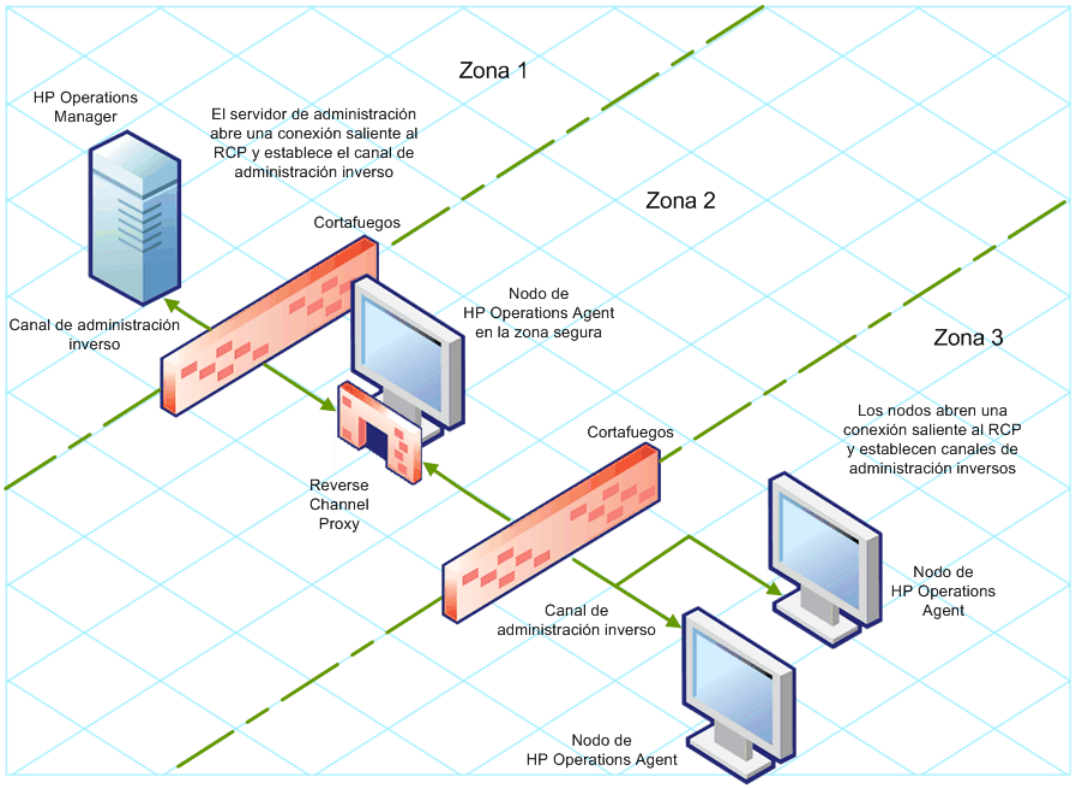
```
Pending:

system5.mydomain.com:1025 Connection To Host Failed
```

Comunicación a través de dos cortafuegos

En algunos casos, el entorno de administración está configurado con dos cortafuegos distintos; el servidor de administración reside detrás de un cortafuegos y el grupo de nodo reside detrás de otro

cortafuegos.

Comunicación segura con dos cortafuegos



En esta situación, hay que instalar el agente en un sistema de la zona intermedia (zona 2) y configurar el RCP en el sistema. Después de configurar los nodos en la zona 3 y el servidor de administración en la zona 1 para establecer los canales de administración inversos en el RCP, la comunicación bidireccional entre el servidor y el nodo tiene lugar a través del RCP.

Para configurar la comunicación bidireccional segura en esta situación, siga estos pasos:

1. Instale el agente en un nodo de la zona 2.
2. Configure un RCP en el nodo de la zona 2.
3. Configure el canal de administración inverso del servidor de administración al RCP.
4. Configure los canales de administración inversos de los nodos de la zona 3 al RCP.

Capítulo 10

Configuración del Componente Performance Collection de manera remota

Se pueden realizar determinadas tareas de configuración de manera remota en el nodo administrado desde el servidor de administración. En lugar de realizar las tareas de configuración de manera remota para el Componente Performance Collection en cada nodo, se puede utilizar un conjunto especial de directivas y herramientas desde la consola de HPOM para configurar y trabajar con los nodos de Componente Performance Collection.

Esta función sólo está disponible si instala el paquete de implementación de HP Operations Agent en los servidores de administración de HPOM para Windows o HPOM para UNIX/Linux. Esta función no está disponible en el servidor de administración de HPOM para UNIX 8.x.

Antes de comenzar

Antes de comenzar a configurar y controlar de manera remota el Componente Performance Collection desde la consola de HPOM, hay que implementar los archivos de instrumentación del grupo de instrumentación de HP Operations Agent en aquellos nodos en donde se ejecuta el agente.

Para implementar la instrumentación desde la consola de HPOM para Windows, siga estos pasos:

1. Si se monitorizan nodos de clúster, hay que asegurarse de implementar la instrumentación en todos los nodos que constituyen el clúster y no en el nodo virtual.
2. En el árbol de la consola, haga clic con el botón derecho en el nodo o en el grupo de nodos (donde se está ejecutando el agente) y, a continuación, haga clic en **Todas las tareas > Desplegar instrumental**. Se abrirá el cuadro de diálogo Desplegar instrumental.
3. En el cuadro de diálogo Desplegar instrumental, haga clic en **HP Operations Agent** y, a continuación, haga clic en **Aceptar**. La implementación de los archivos de instrumentación necesarios comienza en los nodos.

Para implementar la instrumentación de HPOM en la consola UNIX/Linux, siga estos pasos:

Nota: Si se monitorizan nodos de clúster, hay que asegurarse de implementar la instrumentación en todos los nodos que constituyen el clúster y no en el nodo virtual.

1. Inicie sesión en la interfaz de usuario de administración.
2. Haga clic en **Deployment > Deploy Configuration**.
3. En la sección Distribution Parameters, seleccione Instrumentation y, a continuación, haga clic en **Please Select**. Se abrirá el cuadro emergente Selector.

4. En el cuadro emergente Selector, seleccione los nodos en donde se está ejecutando el programa de agente.
5. Seleccione la opción Force Update para sobrescribir los archivos de instrumentación anteriores.

   Seleccione esta opción en un nodo que se actualizó desde una versión anterior del agente.
6. Haga clic en **Distribute**.

Implementación de la política OA-PerfCollComp-opcmsg

La directiva OA-PerfCollComp-opcmsg envía los mensajes de alerta al explorador de mensajes de HPOM cuando el Componente Performance Collection genera las alarmas. La directiva está ubicada en el grupo de directivas **HP Operations Agent > Componente Performance Collection > Message Interceptor**. Antes de implementar otras directivas para el Componente Performance Collection, hay que implementar esta directiva en los nodos.

Nota: Si se monitorizan nodos de clúster, hay que asegurarse de implementar la directiva en todos los nodos que constituyen el clúster y no en el nodo virtual.

Configuración del Componente Performance Collection

El comportamiento del Componente Performance Collection de HP Operations Agent depende de los ajustes de la configuración especificada en los archivos siguientes:

- Archivos de parámetros de la recopilación (**parm**)
- Archivo de definición de alarmas (**alarmdef**)

Consulte la sección *Componente Performance Collection* de la *Guía de conceptos de HP Operations* para obtener más información sobre los parámetros de recopilación y los archivos de definición de alarmas.

Configuración del archivo parm

El archivo **parm** define el mecanismo de recopilación de datos del recopilador de ámbito. HP Operations Agent coloca un archivo **parm** en cada nodo, disponible en la ruta siguiente:

En HP-UX, Solaris, AIX y Linux: **/var/opt/perf/**

En Windows: *%ovdatadir%*

La configuración especificada en el archivo **parm** se puede modificar para personalizar el mecanismo de recopilación de datos. Sin embargo, si se administra un gran número de nodos con HP Operations Agent, puede resultar difícil modificar cada copia del archivo **parm** en cada nodo.

Con la consola de HPOM, se puede implementar el archivo **parm** modificado de manera central en varios nodos desde el servidor de administración.

En HPOM para Windows

La consola de HPOM para Windows ofrece directivas ConfigFile que ayudarán al usuario a implementar los cambios realizados en el archivo **parm** por varios nodos desde el servidor de administración central. Hay varias directivas ConfigFile disponibles para los distintos sistemas operativos de los nodos.

Para modificar el mecanismo de recopilación editando el archivo **parm**, siga estos pasos:

1. Identifique los nodos en donde desea que surta efecto el mecanismo de recopilación modificado.
2. En el árbol de la consola, haga clic en **Gestión de políticas** > **Grupos de políticas** > **HP Operations Agent** > **Componente de recopilación de rendimiento** > **Configuración de recopilación**. Las directivas ConfigFile para configurar el archivo **parm** aparecerán en el panel de detalles.
3. Haga doble clic en la directiva ConfigFile para la plataforma en la que desea que surta efecto el mecanismo de recopilación modificado (por ejemplo: archivo **parm** para HP-UX). Se abrirá el cuadro de diálogo **parm** file for <*plataforma*>.
4. En la pestaña Datos, modifique la configuración. Consulte la sección *Parámetros del archivo parm* en la *Guía de usuario de HP Operations Agent* para obtener más información sobre los parámetros de configuración del archivo **parm**.
5. Haga clic en **Guardar y cerrar**. En el panel de detalles, la versión de la directiva aumenta en .1.
6. Implemente la directiva actualizada en los nodos que prefiera. Si se monitorizan nodos de clúster, hay que asegurarse de implementar la directiva en todos los nodos que constituyen el clúster y no en el nodo virtual.

En HPOM en UNIX/Linux 9.10

En la consola de HPOM en UNIX/Linux 9.10 se encontrarán directivas ConfigFile que ayudarán al usuario a implementar los cambios realizados en el archivo **parm** por varios nodos desde el servidor de administración central. Hay varias directivas ConfigFile disponibles para los distintos sistemas operativos de los nodos.

Para modificar el mecanismo de recopilación editando el archivo **parm** desde la consola de HPOM para UNIX 9.10, siga estos pasos:

1. Identifique los nodos en donde desea que surta efecto el mecanismo de recopilación modificado.
2. En la consola, haga clic en **Examinar** > **Todos los grupos de políticas**. En la página se mostrará la lista de todos los grupos de directivas disponibles.
3. Haga clic en **H**. Se mostrará el grupo de directivas de HP Operations Agent.

4. Haga clic sucesivamente en **HP Operations Agent**, **Componente de recopilación de rendimiento** y, a continuación, en **Configuración de recopilación**. Se mostrará una lista de las directivas ConfigFile disponibles para el archivo **parm**.
5. Haga clic en la directiva ConfigFile para la plataforma en la que desea que surta efecto el mecanismo de recopilación modificado. Se mostrará la página Policy "OA_ <*plataforma*>ParmPolicy".
6. Haga clic en  y, a continuación, haga clic en **Edit (Raw Mode)**. Se mostrará la página Edit Config File policy…
7. En la pestaña Contenido, modifique la configuración.

   Consulte la sección *Parámetros del archivo parm* en la *Guía de usuario de HP Operations Agent* para obtener más información sobre los parámetros de configuración del archivo **parm**.
8. Haga clic en **Guardar**.
9. Implemente la directiva actualizada en los nodos que prefiera.

Si se monitorizan nodos de clúster, hay que asegurarse de implementar la directiva en todos los nodos que constituyen el clúster y no en el nodo virtual.

Configuración del archivo alarmdef

El archivo de definición de alarmas (**alarmdef**) proporciona al subagente de rendimiento la especificación predeterminada para el proceso de generación de alarmas. HP Operations Agent coloca un archivo **alarmdef** en cada nodo, disponible en la ruta siguiente:

En HP-UX, Solaris, AIX y Linux: **/var/opt/perf/**

En Windows: *%ovdatadir%*

Se puede modificar la configuración predeterminada del archivo **alarmdef** para personalizar el mecanismo de generación de alarmas. En la consola de HPOM se puede distribuir centralmente el archivo **alarmdef** modificado en varios nodos.

En HPOM para Windows

La consola de HPOM para Windows ofrece directivas ConfigFile que ayudarán al usuario a implementar los cambios realizados en el archivo **alarmdef** por varios nodos desde el servidor de administración central. Hay varias directivas ConfigFile disponibles para los distintos sistemas operativos de los nodos.

Para modificar el mecanismo de recopilación mediante la edición del archivo **alarmdef**, siga estos pasos:

Identifique los nodos en donde desea que surta efecto el mecanismo de recopilación modificado.

1. En el árbol de la consola, haga clic en **Gestión de políticas** > **Grupos de políticas** > **HP Operations Agent** > **Componente de recopilación de rendimiento** >**Definición de alarma**. Las directivas ConfigFile para configurar el archivo **alarmdef** aparecerán en el panel de detalles.

2. Haga doble clic en la directiva ConfigFile para la plataforma en la que desea que surta efecto el mecanismo de recopilación modificado (por ejemplo: archivo Alarmdef para HP-UX). Se abrirá el cuadro de diálogo Alarmdef file for <*plataforma*>.
3. En la pestaña Datos, modifique la configuración. Consulte la sección *Parámetros del archivo alarmdef* en la *Guía de usuario de HP Operations Agent* para obtener más información sobre los parámetros de configuración del archivo **alarmdef**.
4. Haga clic en **Guardar y cerrar**. En el panel de detalles, la versión de la directiva aumenta en .1.
5. Implemente la directiva actualizada en los nodos que prefiera.

Si se monitorizan nodos de clúster, hay que asegurarse de implementar la directiva en todos los nodos que constituyen el clúster y no en el nodo virtual.

En HPOM en UNIX/Linux 9.10

En la consola de HPOM en UNIX/Linux 9.10 se encontrarán directivas ConfigFile que permitirán implementar los cambios realizados en el archivo **alarmdef** por varios nodos desde el servidor de administración central. Hay varias directivas ConfigFile disponibles para los distintos sistemas operativos de los nodos.

Para modificar el mecanismo de recopilación editando el archivo **alarmdef** desde la consola de HPOM para UNIX 9.10, siga estos pasos:

1. Identifique los nodos en que desea que surta efecto el mecanismo de alerta modificado.
2. En la consola, haga clic en **Examinar** > **Todos los grupos de políticas**. En la página se mostrará la lista de todos los grupos de directivas disponibles.
3. Haga clic en **H**. Se mostrará el grupo de directivas de HP Operations Agent.
4. Haga clic sucesivamente en **HP Operations Agent**, **Componente de recopilación de rendimiento** y, a continuación, en **Definición de alarma**. Se mostrará una lista de las directivas ConfigFile disponibles para el archivo **alarmdef**.
5. Haga clic en la directiva ConfigFile para la plataforma en la que desea que surta efecto el mecanismo de recopilación modificado. Se mostrará la página Policy “"OA_ <*plataforma*>AlarmdefPolicy".
6. Haga clic en  y, a continuación, haga clic en **Edit (Raw Mode)**. Se mostrará la página Edit Config File policy…
7. En la pestaña Contenido, modifique la configuración. Consulte la sección *Parámetros del archivo alarmdef* en la *Guía de usuario de HP Operations Agent* para obtener más información sobre los parámetros de configuración del archivo **alarmdef**.
8. Haga clic en **Guardar**.
9. Implemente la directiva actualizada en los nodos que prefiera.

   Si se monitorizan nodos de clúster, hay que asegurarse de implementar la directiva en todos los nodos que constituyen el clúster y no en el nodo virtual.

Trabajar de manera remota con HP Operations Agent

La consola de HPOM se puede utilizar para iniciar, detener, monitorizar y visualizar los detalles de HP Operations Agent. La consola de HPOM ofrece distintas herramientas para administrar el funcionamiento de HP Operations Agent. Estas herramientas se deben iniciar en los nodos en donde se implementa el agente. En la sección siguiente, se muestra el resultado de la ejecución de una herramienta:

HPOM para Windows

Sección Salida de la herramienta de la ventana Estado de las herramientas

HPOM en UNIX/Linux

En la ventana Salida de aplicación de la GUI de Java (UI operativa de HPOM para UNIX)

Puede usar las herramientas siguientes en la consola de HPOM:

Start Agent	Permite iniciar HP Operations Agent en el nodo administrado.
Stop Agent	Permite detener HP Operations Agent en el nodo administrado.
Restart Agent	Permite reiniciar HP Operations Agent en el nodo administrado.
View Status	Permite ver el estado del proceso, servicios y demonios de HP Operations Agent en el nodo administrado.
View Version Information	Permite ver la versión de HP Operations Agent en el nodo administrado.
Refresh Alarm Service	Actualiza el servicio de alarma del Componente Performance Collection.
Scan Performance Component's Log Files	Examina los archivos de registros usados por el recopilador de ámbito en el nodo.
Check Performance Component's Parameter File Syntax	Permite comprobar la sintaxis del archivo de parámetros en el nodo administrado.
Check Performance Component's Alarmdef File Syntax	Permite comprobar la sintaxis del archivo alarmdef en el nodo administrado.
View status of	Permite comprobar el estado de implementación de las directivas parm o

post policy deploy action	alarmdef en los nodos. Al iniciar esta herramienta, hay que asegurarse de especificar parm o alarmdef (según corresponda) como parámetro de la herramienta. Al usar HPOM para Windows, se puede establecer el parámetro de la herramienta en el cuadro Parámetro de la ventana Editar parámetros. Al usar HPOM en UNIX/Linux, hay que abrir la página Edit Tool Status en la herramienta, ir a la pestaña OVO Tool y, a continuación, especificar el parámetro de la herramienta en el cuadro Parameters.
Set Realtime Permanent License	Establece la licencia permanente del HP Ops OS Inst en Realtime Inst LTU.
Set Glance Permanent License	Establece la licencia permanente de Glance Software LTU.
Get License Status	Muestra el estado de LTU en el nodo.

Capítulo 11

Monitorización de HP Operations Agent

El paquete de implementación de HP Operations Agent proporciona un conjunto de directivas para monitorizar el estado de HP Operations Agent. Con la ayuda de estas directivas, se garantiza que los procesos necesarios del agente no se detienen.

Al instalar el paquete de implementación de HP Operations Agent en el servidor de administración de HPOM, se crea el grupo de directivas Self Monitoring. El grupo de directivas Self Monitoring incluye las directivas necesarias para garantizar el buen funcionamiento de HP Operations Agent.

Nota: El grupo de directivas Self Monitoring y las directivas para monitorizar el estado de los procesos de HP Operations Agent sólo están disponibles si se instala el paquete de implementación de HP Operations Agent en los servidores de administración de HPOM para Windows o de HPOM de UNIX/Linux. Estas directivas no están disponibles en el servidor de administración de HPOM para UNIX 8.x.

Antes de comenzar

Antes de comenzar la monitorización de HP Operations Agent con las directivas Self Monitoring, hay que implementar los archivos de instrumentación del grupo de instrumentación de HP Operations Agent en aquellos nodos donde se ejecuta el agente.

Para implementar la instrumentación desde la consola de HPOM para Windows, siga estos pasos:

Nota: Si se monitorizan nodos de clúster, hay que asegurarse de implementar la instrumentación en todos los nodos que constituyen el clúster y no en el nodo virtual.

1. En el árbol de la consola, haga clic con el botón derecho en el nodo o en el grupo de nodos (donde se está ejecutando el agente) y, a continuación, haga clic en **Todas las tareas > Desplegar instrumental**. Se abrirá el cuadro de diálogo Desplegar instrumental.
2. En el cuadro de diálogo Desplegar instrumental, haga clic en **HP Operations Agent** y, a continuación, haga clic en **Aceptar**. La implementación de los archivos de instrumentación necesarios comienza en los nodos.

Para implementar la instrumentación en HPOM en UNIX/Linux:

Nota: Si se monitorizan nodos de clúster, hay que asegurarse de implementar la instrumentación en todos los nodos que constituyen el clúster y no en el nodo virtual.

1. Inicie sesión en la interfaz de usuario de administración.
2. Haga clic en **Deployment > Deploy Configuration**.

3. En la sección Distribution Parameters, seleccione Instrumentation y, a continuación, haga clic en **Please Select**. Se abrirá el cuadro emergente Selector.
4. En el cuadro emergente Selector, seleccione los nodos en donde se está ejecutando el programa de agente.
5. Seleccione la opción Forzar actualización para sobrescribir los archivos de instrumentación antiguos (esta opción se selecciona en los nodos en los que se ha actualizado la versión de Agent).
6. Haga clic en **Distribute**.

Políticas Self Monitoring

Se puede monitorizar el estado de los componentes siguientes de HP Operations Agent mediante las directivas Self Monitoring:

- **opcmona** (agente de monitorización)
- **opcmsga (**agente de mensajes)
- **opcmsgi (**interceptor de mensajes)
- **opcacta** (agente de acciones)
- **scope** (recopilador de datos)
- **opcle (**encapsulador de archivos de registro)
- **opctrapi** (interceptor de capturas)
- **coda** (demonio de comunicaciones)
- **perfd**

El grupo de directivas Self Monitoring incluye las directivas siguientes:

- **OA-SelfMonTstMonaExt:** prueba el agente de monitorización.
- **OA-SelfMonVerifyMon:** comprueba los archivos del indicador por el agente de monitorización.
- **OA-SelfMonTstLe:** prueba el encapsulador de archivos de registro.
- **OA-SelfMonVerifyLe:** comprueba los archivos del indicador por el encapsulador de archivos de registro.
- **OA-SelfMonTstTrapi:** prueba el interceptor de capturas SNMP.
- **OA-SelfMonTstMsgi:** prueba el interceptor de mensajes.
- **OA-SelfMonTstActa:** prueba el agente de acciones.
- **OA-SelfMonTstAll:** prueba todos los procesos que no sean opcle, opcmona, opcmsgi y opctrapi.

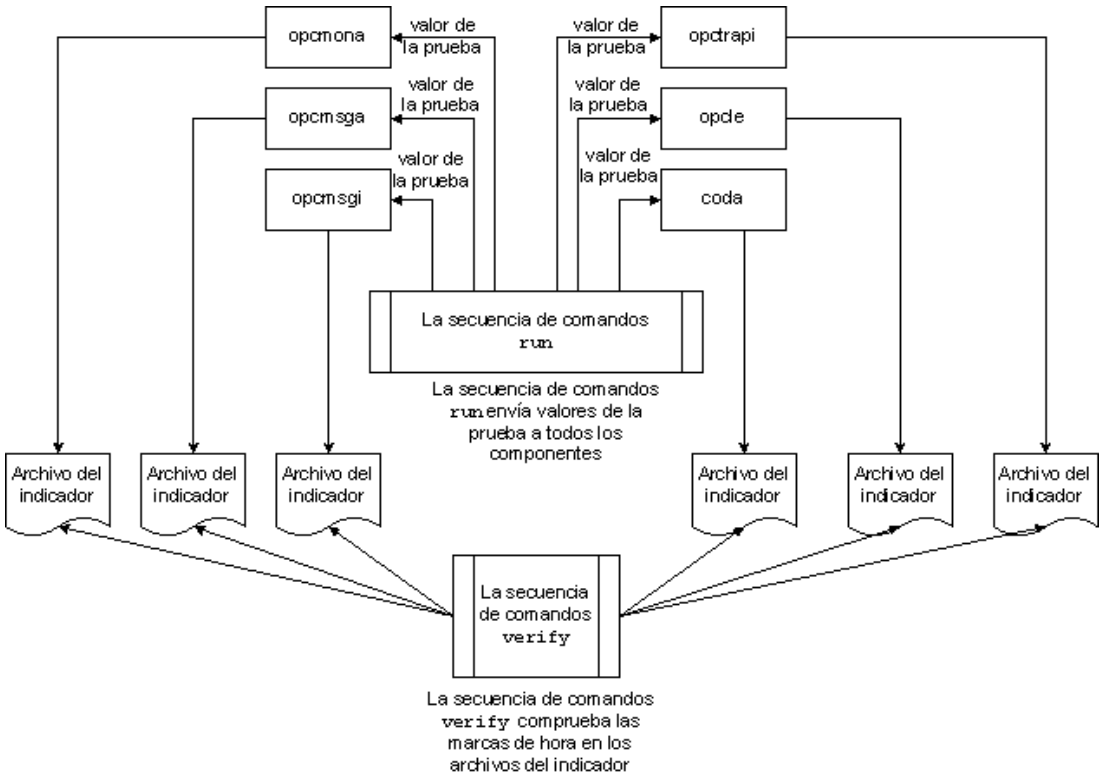
Para monitorizar el estado y la disponibilidad del componente opctrapi, el servicio/demonio de capturas SNMP debe estar ejecutándose en el nodo.

Las secuencias de comandos y programas implementados con el grupo de instrumentación de HP Operations Agent envía valores de prueba (una vez cada minuto) a diferentes componentes de HP

Operations Agent. Además, se crean los **archivos del indicador** para cada componente monitorizado. Cuando un componente monitorizado recibe correctamente el valor de la prueba que se origina en las secuencias de comandos de instrumentación de HP Operations Agent, se actualiza el archivo del indicador correspondiente con la marca de hora.

La secuencia de comandos verify de la instrumentación de HP Operations Agent monitoriza constantemente (una vez cada **tres minutos**) los estados de los archivos del indicador. Cuando la secuencia de comandos encuentra que la marca de hora del archivo del indicador es anterior a la hora actual, lo que significa que el componente monitorizado no pudo recibir el valor de la prueba, se envía un mensaje de alerta al explorador de mensajes de HPOM.

Flujo de trabajo de los scripts de automonitorización



Implementación de las directivas Self Monitoring

No se pueden implementar selectivamente las directivas disponibles en el grupo de directivas Self Monitoring. Estas directivas son interdependientes y por tanto deben implementarse al mismo tiempo en el nodo.

Para implementar las directivas Self Monitoring desde la consola de HPOM para Windows, siga estos pasos:

1. En el árbol de consola de la consola de HPOM, expanda **Gestión de políticas > Grupos de políticas > HP Operations Agent**.

2. Haga clic con el botón derecho en Automonitorización y, a continuación, haga clic en **Todas las tareas > Desplegar en**. Se abrirá el cuadro de diálogo Desplegar políticas.
3. En el cuadro de diálogo Desplegar políticas, seleccione los nodos y, a continuación, haga clic en **Aceptar**. HPOM se inicia implementando las directivas Self Monitoring en los nodos seleccionados.

   Nota: Si se monitorizan nodos de clúster, hay que asegurarse de implementar las directivas en todos los nodos que constituyen el clúster y no en el nodo virtual.

Para implementar las directivas Self Monitoring desde la consola de HPOM en UNIX/Linux, siga estos pasos:

1. Inicie sesión en la interfaz de usuario de administración.
2. Haga clic en **OMU** y, a continuación, haga clic en **Browse > All Policy Groups**. Se abrirá la página All Policy Groups.
3. En la página All Policy Groups, seleccione el grupo de directivas de **HP Operations Agent**, seleccione **Assign to Node / Group** en la lista desplegable Choose an Action y, a continuación, haga clic en  . Se abrirá el cuadro emergente Selector.
4. En el cuadro emergente Selector, seleccione los nodos en donde se está ejecutando el programa Agent y, a continuación, haga clic en **Aceptar**.

   Si se monitorizan nodos de clúster, hay que asegurarse de implementar las directivas en todos los nodos que constituyen el clúster y no en el nodo virtual.

Visualización del estado de los componentes

Las directivas Self Monitoring activan el agente para que envíe los mensajes de alerta apropiados al explorador de mensajes de HPOM cuando detectan un fallo en uno de los componentes. Los mensajes que se originan de las directivas Self Monitoring siempre llevan el prefijo Self Monitor. Se pueden abrir los mensajes con el prefijo Self Monitor para ver los detalles de los errores.

Además, para ver si los componentes del agente están operativos, se pueden comprobar los archivos del indicador en el nodo. Los archivos del indicador están disponibles en las ubicaciones siguientes:

*En Windows: %ovdatadir%***tmp\OpC\selfmon**

En UNIX/Linux: **/var/opt/OV/tmp/selfmon**

Los archivos del indicador se pueden abrir con un editor de textos y comprobar la última marca de hora. Si la última marca de hora es superior a tres minutos, significa que el componente monitorizado no está funcionando.

Capítulo 12

Instalación sólo de los SPI de infraestructura

Requisitos de hardware y software

Para ver una lista del hardware compatible, los sistemas operativos, la versión de HPOM y la versión de Agent, consulte la *matriz de compatibilidades*.

Requisitos de espacio en disco

Sistema operativo del servidor de gestión de HPOM	Directorio temporal[a]	Espacio en disco total
Windows	%tmp% - 15 MB	90 MB
Linux	/tmp - 35 MB	90 MB
HP-UX	/tmp - 17 MB	240 MB
Solaris	/tmp - 35 MB	80 MB

[a]El espacio en disco para el directorio/unidad temporales sólo se requiere durante la instalación. Éstos son valores aproximados.

Instalación de los SPI de infraestructura

1. Inicie una sesión en el servidor de gestión
2. Realice una de las siguientes tareas:
   - Si desea realizar la instalación de los SPI de infraestructura desde el soporte físico, inserte el DVD de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en la unidad de DVD-ROM.
   - Descargue el soporte de instalación (archivo .iso) de uno de los sitios web de HP.

     Use el DVD físico o el archivo .iso que incluye paquetes de implementación para todas las plataformas. Los archivos .iso específicos de una plataforma no contienen los SPI de infraestructura.
3. Cree un archivo de configuración para especificar los detalles de la instalación.

   El programa `oainstall` instala los SPI de infraestructura en el servidor de gestión al registrar el paquete de implementación. Esta instalación incluye los paquetes de informes (para usarlos con HP Reporter) y gráficos (para usarlos con HP Performance Manager) para los SPI de infraestructura. Como desea omitir el registro de los paquetes de HP Operations Agent, siga estos pasos:

a. Cree un archivo con un editor de texto.

b. Añada el siguiente contenido:

```
[agent.parameter]
REGISTER_AGENT=NO
[hpinfraspi.parameter]
InfraSPI=
InfraSPI_With_Graphs=
```

c. *Sólo en Windows. Añada la siguiente línea:*

```
InfraSPI_With_Reports=
```

Dado que HP Reporter sólo es compatible con Windows, la adición de la línea anterior al archivo de configuración en un sistema UNIX/Linux no tendrá efecto alguno.

d. En la sección `[hpinfraspi.parameter]`:
   - No realice cambios en el archivo (es decir, no defina valores para las propiedades en la sección `[hpinfraspi.parameter]`) si desea instalar los SPI de infraestructura con informes (sólo para Windows) y gráficos.
   - En `InfraSPI` seleccione YES y en el resto de las propiedades NO si desea instalar sólo los SPI de infraestructura sin informes (sólo para Windows) y gráficos.
   - En `InfraSPI_With_Graphs`seleccione YES y en el resto de las propiedades NO si desea instalar sólo los SPI de infraestructura y gráficos.
   - En `InfraSPI_With_Graphs`seleccione YES y en el resto de las propiedades NO si desea instalar sólo los SPI de infraestructura y gráficos (y no los informes).
   - En `InfraSPI_With_Reports`seleccione YES y en el resto de las propiedades NO si desea instalar sólo los SPI de infraestructura e informes (y no los gráficos).

   Nota: No instale los paquetes de gráficos si HP Performance Manager no está instalado en el servidor de gestión. Si HP Performance Manager está instalado en un servidor remoto, debe instalar los paquetes de gráficos por separado en dicho servidor. Al no ser no es compatible con UNIX/Linux, HP Reporter debe estar disponible en un servidor remoto. Para instalar paquetes de informes para los SPI de infraestructura en el servidor remoto de HP Reporter, siga este procedimiento.

   Si usa HPOM en UNIX/Linux y desea ver los gráficos con HP Performance Manager, debe integrar HP Performance Manager con HPOM en UNIX/Linux (consulte Integración de HP Performance Manager con HPOM en UNIX/Linux).

e. Guarde el archivo en un directorio local.

4. Ejecute el comando siguiente:

   En Windows

   cscript oainstall.vbs -i -m -spiconfig <*archivo de configuración*>

En UNIX/Linux

./oainstall.sh -i -m -spiconfig <*archivo de configuración*>

En este caso, <*archivo de configuración*> es el nombre del archivo de configuración (con la ruta de acceso completa al archivo).

Si HPOM está en un clúster HA, siga los pasos anteriores en el nodo activo del clúster y, a continuación, realice los pasos 1 a 4 en todos los nodos del clúster HA.

Ejemplo

i. Cree un archivo de configuración con el siguiente contenido:

```
[agent.parameter]
REGISTER_AGENT=NO
[hpinfraspi.parameter]
InfraSPI=YES
InfraSPI_With_Graphs=NO
InfraSPI_With_Reports=NO
```

ii. Guarde el archivo como `config_file` en el siguiente directorio:

C:\temp

iii. Ejecute el comando siguiente para instalar los SPI de infraestructura.

cscript oainstall.vbs -i -m -spiconfig C:\temp\config_file

El comando instala los SPI de infraestructura sin instalar Agent, el paquete de informes y el paquete de gráficos.

Instalación de paquetes de informes y de gráficos en un servidor remoto

Cuando HP Reporter y HP Performance Manager estén instalados en cualquier servidor, salvo en el servidor de gestión de HPOM, debe seguir este procedimiento para instalar los paquetes de informes y de gráficos para los SPI de infraestructura.

Para instalar paquetes de informes:

1. Inicie sesión en el servidor de HP Reporter como administrador.
2. Coloque o monte el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en el sistema.
3. Vaya al directorio siguiente:

   En sistemas con Windows x64

   <raíz soporte>`\integration\infraspi\WIN\Windows_X64`

   En sistemas con Windows x86

   <raíz soporte>`\integration\infraspi\WIN\Windows_X86`
4. Instale el siguiente archivo:

   `HPSpiInfR.msi`

Para instalar paquetes de gráficos:

1. Inicie sesión en el servidor de HP Performance Manager como administrador o usuario raíz.
2. Coloque o monte el soporte de *HP Operations Agent y SPI de infraestructura SPIs 11.10* en el sistema.
3. Vaya al directorio siguiente:

   En un sistema Linux

   <raíz soporte>`\integration\infraspi\LIN\Linux2.6_X64`

   En un sistema HP-UX

   <raíz soporte>`\integration\infraspi\HP-UX\HP-UX_IA32`

   En un sistema Solaris

   <raíz soporte>`\integration\infraspi\SOL\Solaris_SPARC32`

   En sistemas con Windows x64

   <raíz soporte>`\integration\infraspi\WIN\Windows_X64`

   En sistemas con Windows x86

   <raíz soporte>`\integration\infraspi\WIN\Windows_X86`
4. *En Linux*

   Extraiga el contenido del archivo `HPSpiInfG.rpm.gz` y, seguidamente, instale el archivo `HPSpiInfG.rpm`.

   En HP-UX

   Extraiga el contenido del archivo `HPSpiInfG.depot.gz` y, seguidamente, instale el archivo `HPSpiInfG.depot`.

   En Solaris

   Extraiga el contenido del archivo `HPSpiInfG.sparc.gz` y, seguidamente, instale el archivo `HPSpiInfG.sparc`.

   En Windows

   Instale el archivo `HPSpiInfG.msi`.
5. Integre HP Performance Manager con HPOM en UNIX/Linux (consulte Integración de HP Performance Manager con HPOM en UNIX/Linux)

Archivo de registro

El archivo de registro del registro (`oainstall.log`) está disponible en el directorio:

`/var/opt/OV/shared/server/log`

`%OvDataDir%shared\server\log`

Verificación de la instalación

Después de instalar los SPI de infraestructura, revise el contenido del archivo de registro de instalación (`oainstall.log`). Si la instalación es correcta, el archivo no debe tener errores y debe aparecer el siguiente mensaje casi al final del archivo:

```
HPSpiSysI installation completed successfully

HPSpiVmI installation completed successfully

HPSpiClI installation completed successfully
```

Integración de HP Performance Manager con HPOM en UNIX/Linux

1. En el servidor de gestión de HPOM, vaya al directorio /opt/OV/contrib/OpC/OVPM.
2. Ejecute el siguiente comando:

   ./install_OVPM.sh <*nombre de host*>**:**<*puerto*>

   En este caso, <*nombre de host*>es el nombre de dominio completo del servidor de HP Performance Manager y <*puerto*>es el puerto que usa HP Performance Manager. Use el mismo comando con las mismas opciones aunque HP Performance Manager esté instalado en el servidor de gestión de HPOM.

SPI de infraestructura Licencias

No se requiere una licencia independiente para los SPI de infraestructura del sistema ni el SPI de infraestructura de virtualización. Estos SPI se incluyen al comprar LUT (licencias de uso) de HP Software Operations Instance Advanced. Cada LTU de HP Software Operations Instance Advanced incluye una LTU para el SI SPI y otra LTU para el SPI de infraestructura del clúster.

Los requisitos de licencia del SPI de infraestructura de virtualización se definen en función del número de instancias virtuales del entorno virtualizado que gestiona el servidor de HPOM con el SPI de infraestructura de virtualización.

- **Microsoft Hyper-V:** Las licencias dependen del número de hosts de Hyper-V en los que se implementa el SPI de infraestructura de virtualización. Cada uno de los sistemas de los hosts de Hyper-V que monitoriza el SPI de infraestructura de virtualización requiere una LTU de VI SPI independiente.
- **VMware:** los hosts de ESX y ESXi que se agregan a vMA para realizar la monitorización con SPI de infraestructura de virtualización requieren una LTU de VI SPI independiente. Cada vCenter que se agrega a para realizar la monitorización con SPI de infraestructura de virtualización también requiere una LTU de VI SPI independiente.
- **HPVM:** Las licencias dependen del número de servidores de HPVM en los que se implementa el SPI de infraestructura de virtualización. Cada uno de los servidores de HPVM que supervisa el SPI de infraestructura de virtualización requiere una LTU de VI SPI independiente.
- **AIX LPAR:** las licencias dependen del número de LPAR en los que se implementa el SPI de infraestructura de virtualización. Cada instalación de SPI de infraestructura de virtualización requiere una LTU de VI SPI independiente.
- **Zonas de Oracle Solaris:** las licencias dependen del número de zonas globales en las que se implementa el SPI de infraestructura de virtualización. Cada una de las zonas globales que supervisa el SPI de infraestructura de virtualización requiere una LTU de VI SPI independiente.

El SPI de infraestructura de virtualización incluye una licencia de prueba que permite usar el producto durante 60 días después de su instalación.

Para más información sobre cómo obtener una licencia, cómo aplicar la contraseña de la clave de licencia permanente o cómo ver un informe de licencias en HPOM, consulte *HP Operations Manager for Windows Installation Guide* o *HP Operations Manager for UNIX Installation Guide*.

Componentes de los Infrastructure SPI en HPOM para Windows

Los siguientes componentes de los Infrastructure SPI están disponibles en la consola HPOM para Windows.

Servicios

Cuando se añade un nodo al grupo de nodos de HPOM para Windows, la política de detección del servicio SI SPI se implementa automáticamente.

La política de detección de servicios detecta la infraestructura de sistemas y los servicios del nodo, e incorpora esta información al área de servicios de HPOM.

Para ver el mapa de servicios de SI SPI, seleccione **Servicios** → **Infraestructura de sistemas**. El mapa de servicios de SI SPI representa gráficamente los sistemas e instancias detectados.

Nota: La política de detección de SI SPI y las políticas de QuickStart se implementan automáticamente en los nodos nuevos (si está habilitada la opción de habilitación automática) agregados al servidor de HPOM para Windows. En los nodos existentes, la política de detección de SI SPI se debe implementar manualmente.

Detección de Virtual Infrastructure

Una vez que la política de detección de sistemas identifica SI SPI como un nodo es un nodo de virtualización la detección de VI SPI se implementa automáticamente. Los equipos virtuales que se ejecutan en dichos nodos se agregan bajo el grupo de nodos de infraestructura de virtualización y las políticas de QuickStart específicas del proveedor se implementan automáticamente en dichos nodos.

La política de detección de VI SPI añade los elementos detectados al mapa de servicios de HPOM. Para ver el mapa de servicios de VI SPI, seleccione **Servicios** → **Virtualization Infrastructure**. El mapa de servicios de VI SPI representa gráficamente los sistemas virtuales detectados.

Detección de Cluster Infrastructure

En HPOM para Windows, si la política de detección de SI SPI identifica el nodo como un nodo de clúster, inicia la política de detección de CI SPI en el nodo. La detección de CI SPI detecta los clústeres, nodos de clústeres y grupos de recursos. Para ver el mapa de servicios de Cluster Infrastructure SPI, seleccione **Servicios** → **Cluster Infrastructure**.

Modelos de tipo de servicio

Los modelos de tipo de servicio muestran las categorías del tipo de servicio a las que se asignan lógicamente los nodos del banco de nodos. El modelo del tipo de servicio se puede ver en HPOM para Windows.

Grupos de nodos

Después de instalar Systems Infrastructure SPI 2.01, los grupos de nodos se agregan a la carpeta **Nodes** del árbol de la consola.

Nota: Los nombres de los grupos de nodos aparecen en inglés, incluso cuando las configuraciones regionales no estén en dicho idioma.

Gestión de políticas

En el grupo Infrastructure Management, las políticas se agrupan por idioma. Por ejemplo, las políticas en inglés se agrupan bajo **en**, las políticas en japonés se agrupan bajo **ja** y las políticas en chino simplificado se agrupan bajo **zh**. Los grupos de idiomas aparecen en función del idioma que se seleccione en el momento de la instalación.

Nota: Las políticas de ConfigFile SI-ConfigureDiscovery y VI-VMwareEventTypes no tienen nombres traducidos. Los nombres de las políticas están en inglés aunque las configuraciones regionales no estén en dicho idioma

Los posteriores grupos se basan en SI SPI, CI SPI y VI SPI, según lo que se haya seleccionado en el momento de la instalación. En cada SPI, las políticas se agrupan en función del rendimiento, disponibilidad, capacidad, registros y eventos.

También hay un grupo de políticas basado en proveedor. En este grupo, las políticas se reagrupan según los distintos sistemas operativos o proveedores. Las políticas agrupadas por proveedor incluyen las políticas de QuickStart y las políticas avanzadas. Las políticas de QuickStart se implementan automáticamente a los nodos gestionados compatibles una vez que se agregan a los grupos de nodos respectivos. Puede elegir desactivar la implementación automática de políticas cuando se detectan servicios. Además, puede modificar y guardar las políticas preconfiguradas con nombres nuevos para crear políticas personalizadas para fines especiales propios.

Para ver y acceder a las políticas de Systems Infrastructure SPI, seleccione **Gestión de políticas → Grupos de políticas → Infrastructure Management → <*idioma*> → Infraestructura de sistemas**.

Para ver y acceder a las políticas de VI SPI, seleccione **Gestión de políticas → Grupos de políticas → Infrastructure Management → <*idioma*> → Virtualization Infrastructure**.

Para ver y acceder a las políticas de Cluster Infrastructure SPI, seleccione **Gestión de políticas → Grupos de políticas → Infrastructure Management → <*idioma*> → Cluster Infrastructure**.

Herramientas

Se proporcionan herramientas para SI SPI y VI SPI Para acceder al grupo de herramientas de Systems Infrastructure SPI, seleccione **Herramientas → Infraestructura de sistemas** y para acceder al grupo de herramientas de VI SPI, seleccione **Herramientas → Virtualization Infrastructure**.

Informes

Si HP Reporter está instalado en el servidor de gestión de HPOM para Windows, puede ver el grupo Informes desde la consola de HPOM para Windows.

Gráficos

Con el SI SPI y el VI SPI se proporciona un conjunto de gráficos preconfigurados. Para acceder a dichos gráficos desde la consola de HPOM, es preciso instalar HP Performance Manager en el servidor de gestión de HPOM antes que el paquete de gráficos de Infrastructure SPI.

Para acceder a los gráficos de SI SPI, seleccione **Gráficos** → **Infrastructure Performance**, mientras que para acceder a los de VI SPI, debe seleccionar **Gráficos** → **Infrastructure Performance** → **Virtualización**.

Como alternativa, si HP Performance Manager está instalado en un sistema separado (independiente) conectado al servidor de gestión de HPOM, puede ver los gráficos en el sistema independiente de HP Performance Manager.

Componentes de Infrastructure SPI en HPOM para UNIX

Los siguientes componentes de Infrastructure SPI están disponibles en la interfaz de usuario del administrador de HPOM para UNIX (HP-UX, Linux y Solaris).

Servicios

La política de detección de servicios de SI detecta la infraestructura de sistemas y los servicios del nodo, e incorpora esta información al área de servicios de HPOM. Para ver el mapa de servicios y la consola del operador, utilice Java GUI. Java GUI se debe instalar en un sistema independiente.

Detección de Virtual Infrastructure

Una vez que la detección de sistemas haya identificado que un nodo es un nodo de virtualización la detección de VI SPI se implementa automáticamente. Los equipos virtuales que se ejecutan en dichos nodos se agregan bajo el grupo de nodos de Virtualization Infrastructure y las políticas de QuickStart específicas del proveedor se asignan automáticamente a dichos nodos.

La política de detección de servicios de VI SPI detecta los equipos virtuales (equipos invitados) alojados en los nodos gestionados (equipos host) e incorpora esta información al área de servicios de HPOM. Para ver el mapa de servicios de VI SPI, seleccione **Servicios**> **Virtualization Infrastructure** > **Mostrar gráfico**. El mapa de servicios representa gráficamente los sistemas virtuales detectados.

Detección de Cluster Infrastructure

En los nodos de clústeres que se agregan al banco de nodos de HPOM para HP-UX, Linux, o Solaris, implemente manualmente la detección del servicio CI SPI. La detección de CI SPI detecta los clústeres, nodos de clústeres y grupos de recursos. Para ver el mapa de servicios de CI SPI, seleccione **Servicios**→ **Cluster Infrastructure** → **Mostrar gráfico**.

Gestión de políticas

En el grupo Infrastructure Management, las políticas se agrupan por idioma. Por ejemplo, las políticas en inglés se agrupan bajo **en**, las políticas en japonés se agrupan bajo **ja** y las políticas en chino simplificado se agrupan bajo **zh**. Los grupos de idiomas aparecen en función del idioma que se seleccione en el momento de la instalación.

También hay un grupo de políticas basado en proveedor. En este grupo, las políticas se reagrupan según los distintos sistemas operativos o proveedores. Las políticas agrupadas por proveedor

incluyen las políticas de QuickStart y las políticas avanzadas. Las políticas de QuickStart se asignan automáticamente a los nodos gestionados después de que se agregan a los grupos de nodos respectivos. Estas políticas se pueden implementar manualmente en los nodos.

También es posible modificar y guardar las políticas preconfiguradas con nombres nuevos para crear políticas personalizadas para fines especiales propios.

Para ver y acceder a las políticas SI SPI, seleccione **Banco de políticas** → **Infrastructure Management**→ **<*idioma*>**→ **Infraestructura de sistemas**.

Para ver y acceder a las políticas VI SPI, seleccione **Banco de políticas** → **Infrastructure Management**→ **<*idioma*>**→ **Infraestructura de virtualización**.

Para ver y acceder a las políticas CI SPI, seleccione **Banco de políticas** → **Infrastructure Management**→ **<*idioma*>**→ **Infraestructura de clúster**.

Herramientas

Los Infrastructure SPI proporcionan herramientas para el SI SPI y el VI SPI. Para acceder al grupo de herramientas de SI SPI, seleccione **Banco de herramientas**→ **Systems Infrastructure** y para acceder al grupo de herramientas de VI SPI, seleccione **Banco de herramientas**→ **Virtualization Infrastructure**.

Informes

Si usa HPOM para los sistemas operativos HP-UX, Linux y Solaris, HP Reporter se instala en un sistema separado (independiente) conectado al servidor de gestión. Los informes se puede ver en el sistema independiente de HP Reporter.

Para más información sobre la integración de HP Reporter con HPOM, consulte el manual *HP Reporter Installation and Special Configuration Guide (Guía de instalación y configuración especial de HP Reporter)*.

Gráficos

Los Infrastructure SPI proporcionan gráficos para el SI SPI y el VI SPI. Para generar y ver gráficos de los datos recopilados, es preciso usar HP Performance Manager en conjunción con HPOM.

Para acceder a los gráficos, seleccione el mensaje activo, abra la ventana Propiedades del mensaje y haga clic en **Acciones.** En la sección El operador inició la acción, haga clic en **Realizar**. Como alternativa, puede hacer clic con el botón secundario en el mensaje, seleccionar **Realiza/detener acción** y haga clic en **Realizar acción iniciada por el operador**.

Si HP Performance Manager está instalado en el servidor de gestión, es posible lanzar y ver gráficos en el servidor de gestión. Si HP Performance Manager está instalado en un sistema separado (independiente) conectado al servidor de gestión de HPOM, puede ver los gráficos en el sistema independiente de HP Performance Manager.

Capítulo 13

Desinstalación de HP Operations Agent

1. Inicie sesión en el nodo como administrador o usuario raíz.
2. Detenga todos los procesos de Agent ejecutando los siguientes comandos:

   opcagt -stop

   ttd -k
3. Vaya al directorio siguiente:

   Windows 64 bits

   %OvInstallDir%bin\win64\OpC\install\%OvInstallDir%bin\win64\OpC\install

   Otros Windows

   %OvInstallDir%bin\OpC\install\cscript oainstall.vbs -r -a

   Linux, HP-UX, Solaris

   /opt/OV/bin/OpC/install/oainstall.sh -r -a

   AIX

   /usr/lpp/OV/bin/OpC/install/oainstall.sh -r -a
4. Elimine manualmente los siguientes directorios:

   En Windows:

   ```
   %OvInstallDir%
   %OvDataDir%
   ```

   En HP-UX, Solaris y Linux:

   ```
   /opt/OV
   /var/opt/OV
   /opt/perf
   /var/opt/perf
   ```

   En AIX:

   ```
   /usr/lpp/OV
   /var/opt/OV
   /usr/lpp/perf
   /var/opt/perf
   ```

También puede, en un nodo de Windows, eliminar HP Operations Agent 11.10 con la ventana Agregar o quitar programas.

Capítulo 14

Desinstalación de SPI de infraestructura

Eliminación de políticas de Infrastructure SPI de nodos gestionados

En HPOM para Windows

1. En el árbol de consola de HPOM, expanda las carpetas **Operations Manager > Gestión de políticas > Grupos de políticas > Infrastructure Management**.
2. Haga clic con el botón secundario en Infrastructure Management y, a continuación, seleccione **Todas las tareas > Implementar en**.
3. En el cuadro de diálogo Desinstalar políticas, seleccione **Todos los nodos** y, a continuación, haga clic en **Aceptar**.

Desde HPOM en UNIX/Linux

1. Inicie sesión en la consola de HPOM como administrador.
2. Seleccione **Todas las asignaciones de política** en el menú Examinar. Se abrirá la ventana Todas las asignaciones de política.
3. En la ventana Todas las asignaciones de política, seleccione la política o el grupo de políticas que desea eliminar de un nodo o grupo de nodos haciendo clic en la casilla Modo de asignación de las políticas.
4. Seleccione **Suprimir asignación…** en el cuadro Elegir una acción y haga clic en **Enviar**. Aparecerá una ventana de mensaje en la que se especifica que la operación no se puede deshacer.
5. Haga clic en **OK**. La asignación de política seleccionada se elimina de los nodos.
6. En la interfaz de usuario de administración de HPOM, haga clic en Banco de nodos en la categoría Bancos de objetos. Se abre la ventana Banco de nodos.
7. En la ventana Banco de nodos, seleccione los nodos o grupos de nodos de los que desea quitar las políticas.
8. Seleccione **Desasignar de este grupo…** en el cuadro Elegir una acción y haga clic en **Enviar**.

Las políticas se eliminan de los nodos seleccionados.

Debe esperar hasta que todas las políticas se desinstalen de todos los nodos. El estado de la desinstalación de las políticas se puede ver en la ventana Tareas de implementación.

Desinstalación de los SPI de infraestructura

Nota: Para quitar los SPI de infraestructura, asegúrese de que tiene aproximadamente 240 MB de espacio total en el disco y 35 MB de espacio en las carpetas temporales disponibles en el servidor de gestión.

1. Inicie sesión en el servidor de gestión.
2. Vaya al directorio siguiente:

   En Windows

   `%ovinstalldir%bin\OpC\agtinstall`

   En UNIX/Linux

   `/opt/OV/bin/OpC/agtinstall`
3. Ejecute el comando siguiente:

   En Windows

   cscript oainstall.vbs -r -m -spiconfig

   En UNIX/Linux

   ./oainstall.sh -r -m -spiconfig

En un clúster HA, realice los pasos anteriores primero en el nodo activo y, seguidamente, en todos los nodos del clúster.