HP Operations Agent

para los sistemas operativos Windows®, HP-UX, Solaris, Linux y AIX

Versión de software: 11.00

Guía de implementación

Fecha de publicación del documento: Octubre de 2010
Fecha de publicación del software: Octubre de 2010

Avisos legales

Garantía

Las únicas garantías para los productos y servicios de HP se establecen en los términos de garantía expresos que acompañan a dichos productos y servicios. Nada de lo que contiene este documento podrá interpretarse como garantía adicional. HP no asume responsabilidad alguna por los errores editoriales, técnicos u omisiones contenidos en el presente documento.

La información aquí contenida está sujeta a cambios sin previo aviso.

Leyenda de derechos restringidos

Software informático confidencial. Se requiere una licencia válida de HP para su posesión, uso o copia. De conformidad con FAR 12.211 y 12.212, se autoriza el uso del software informático comercial, de documentación del software informático y de datos técnicos para componentes comerciales al gobierno de EE.UU. bajo licencia comercial estándar del fabricante.

Avisos de copyright

Avisos de marcas registradas

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

Microsoft®, Windows®, Windows® XP 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 identificativa:

- 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 publicación del software, que indica la fecha de publicación de esta versión del software.

Para buscar actualizaciones recientes o para asegurarse de estar usando la edición más reciente de un documento, vaya a:

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

Este sitio requiere que el usuario se registre para obtener un HP Passport y que inicie sesión.
Para registrarse y obtener un ID de HP Passport, vaya a:

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

O haga clic en el vínculo **Nuevo registro de usuario** en la página de inicio de sesión de HP Passport.

Soporte técnico

Visite el sitio web de HP Software Support Online en:

www.hp.com/go/hpsoftwaresupport

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

El soporte técnico en línea de HP Software permite al cliente solucionar los problemas por sí mismo. Ofrece una forma rápida y eficaz de acceder a las herramientas de soporte técnico interactivas necesarias para gestionar su negocio. Como valorado cliente de soporte técnico, se puede beneficiar del sitio web de soporte técnico para:

- Buscar documentos en la base de conocimiento que le puedan interesar.
- Enviar y rastrear casos de soporte técnico y solicitudes de mejora.
- Descargar revisiones de software.
- Gestionar contratos de soporte técnico.
- Buscar contactos de soporte técnico de HP.
- Revisar la información sobre servicios disponibles.
- Participar en conversaciones con otros clientes de software.
- Investigar y registrarse en cursos de formación de software.

La mayoría de las áreas de soporte técnico requieren que se registre como usuario de HP Passport y que inicie sesión. Algunas pueden requerir también un contrato de soporte técnico. Para registrarse y obtener un ID de usuario de HP Passport, vaya a:

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

Para obtener más información sobre los niveles de acceso, vaya a:

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

Tabla de contenido

1 Introducción general

Con la combinación de HP Operations Manager (HPOM) y HP Operations Agent, se puede crear una solución de monitorización distribuida con objeto de monitorizar varios sistemas en el propio entorno. El agente de cada nodo monitoriza el rendimiento del sistema y envía mensajes de alerta a la consola central de HPOM. Además de proporcionar una consola central para monitorizar las respuestas del agente, la consola de HPOM ayuda al usuario a realizar determinadas tareas de configuración en el agente.

Las redes grandes de los sistemas administrados por HPOM suelen crear desafíos adicionales a la hora de implementar y mantener el agente. Esta guía contiene información, directrices y mejores prácticas para implementar el producto HP Operations Agent en un entorno administrado por HPOM.

Después de instalar HP Operations Agent en los nodos, esta guía se puede utilizar para obtener información sobre las tareas siguientes:

- Implementar certificados en los nodos
- Configurar el agente para comunicarse con el servidor de administración de HPOM en un entorno seguro controlado por cortafuegos
- Configurar el agente con varios servidores de administración
- Configurar el mecanismo de recopilación de datos del agente de forma remota desde la consola de HPOM
- Implementar el agente en un clúster de High Availability

Mapa de documentación

El mapa de documentación presenta una lista que incluye los principales documentos de HP Operations Agent. Este mapa ayuda a identificar un documento en particular.

Figura 1 Mapa de documentación de HP Operations Agent

Documentación relacionada

La documentación del usuario relativa a HP Operations Agent se encuentra en el directorio `paperdocs` del soporte multimedia del producto. Para buscar actualizaciones recientes o para asegurarse de estar usando la edición más reciente de un documento, vaya a:

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

Este sitio requiere que el usuario se registre para obtener un HP Passport y que inicie sesión. Para registrarse y obtener un ID de HP Passport, vaya a:

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

O haga clic en el vínculo **Nuevo registro de usuario** en la página de inicio de sesión de HP Passport.

Tabla 1 Documentación del usuario acerca de HP Operations Agent

Documento	Uso	Temas principales
Notas de la versión	Consulte este documento para obtener más información sobre la versión del producto, nuevas funciones y problemas conocidos.	• Nuevas funciones • Mejoras • Correcciones • Problemas conocidos y limitaciones
Guía de conceptos	La Guía de conceptos ayudará al usuario a comprender el mecanismo de funcionamiento de HP Operations Agent en distintos entornos.	• Introducción a HP Operations Agent • Principales componentes de HP Operations Agent
Guía de instalación	Con la ayuda de la Guía de instalación, el usuario podrá instalar HP Operations Agent en los entornos siguientes: • En un servidor de administración de HPOM (para su uso en el entorno de administración distribuido administrado por HPOM) • En un servidor independiente (para recopilar métricas de rendimiento del sistema del servidor local para su uso con herramientas de análisis de datos externos, como HP Performance Manager)	• Instalación de HP Operations Agent desde la consola de HPOM • Instalación manual de HP Operations Agent • Licencias

Tabla 1 Documentación del usuario acerca de HP Operations Agent

Documento	Uso	Temas principales
Guía de usuario	Consulte esta guía si necesita ayuda para realizar las tareas diarias en HP Operations Agent.	• Administración de la recopilación de datos • Generación de alarmas
Guía de referencia	La Guía de referencia incluye una lista con todos los comandos, procesos y servicios disponibles en el nodo del HP Operations Agent.	• Utilidades de línea de comando • Variables de configuración

2 Configuración de certificados

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 mismo nodo se puede identificar a su servidor de administración y a otros nodos enviándoles su certificado de nodo.
- **Una copia del certificado de confianza del servidor de administración.** 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 instalar los certificados después de instalar el agente en los nodos.

Instalación de certificados

El certificado se podrá instalar mediante una de las formas siguientes:

- Solicitud automática de los certificados
- Solicitud de certificados con una clave de instalación
- Implementación manual de los certificados

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
```

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.

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 certificados con una clave de instalación, siga estos pasos:

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_de_archivo*>*:* el nombre del archivo de clave de instalación.

   > Especifique la ruta completa con <*nombre_de_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_de_datos*>`\shared\server\certificates`.

   <*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.
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 <*dir_de_instalación*>`/bin`.
8. Ejecute el comando siguiente:

   ovcert -certreq -instkey <*nombre_de_archivo*>

9 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.

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 de forma manual, siga estos pasos:

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 o HPOM en UNIX/Linux

opccsacm -issue -file <*nombre_de_archivo*> **[-pass** <*contraseña*>**] -name** <*nombre_de_nodo*> [**-coreid** <*OvCoreId*>**]**

Especifique la ruta completa con <*nombre_de_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_de_datos*>`\shared\server\certificates`.

En este ejemplo:

<*nombre_de_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_de_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 **Properties**. 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_de_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_de_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_de_archivo*>

El comando puede solicitar que se especifique la contraseña proporcionada en paso 4 en la página 13.

10 Ejecute el comando siguiente en el nodo:

```
ovc -start
```

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*>**]**

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

4 Ejecute el comando siguiente:

ovcert -exporttrusted [-ovrg <*servidor*>**] -file** <*nombre_de_archivo*>

En este caso, <*servidor*> es el nombre del grupo de recursos de High Availability si el servidor de administración está instalado en un clúster de High Availability.

El comando realiza una copia de seguridad del certificado de confianza del servidor de administración en el archivo especificado con la opción `-file`.

5 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            |
+-------------------------------------------------------+
```

6 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 los certificados en el nodo, siga estos pasos:

1 Inicie sesión en el nodo con privilegios raíz o administrativos.

2 Abra el símbolo del sistema (shell).

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

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

En este ejemplo, <*nombre_de_archivo*> es el nombre de archivo especificado en paso 3 en la página 14.

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

ovcert -importtrusted -file <*nombre_de_archivo*>

En este ejemplo, <*nombre_de_archivo*> es el nombre de archivo especificado en paso 4 en la página 14.

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

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

En este ejemplo, <*nombre_de_archivo*> es el nombre de archivo especificado en paso 6 en la página 15.

Solución de problemas con los certificados

Para comprobar que todos los certificados necesarios están correctamente instalados en el nodo, ejecute el siguiente comando en el nodo:

ovcert -list

El comando muestra la salida en el formato siguiente:

```
+-------------------------------------------------------+

| Keystore Content                          |
+-------------------------------------------------------+

| Certificates:                                         |     | |
cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)                |
+-------------------------------------------------------+

| Trusted Certificates:                                 |

|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55            |
+-------------------------------------------------------+
```

La sección `Certificates` de la salida muestra el nombre del certificado del nodo. La sección `Trusted Certificates` de la salida muestra el nombre del certificado de confianza del servidor de administración.

El nombre del certificado del nodo es idéntico al parámetro `OvCoreID` del nodo.

El nombre del certificado de confianza se crea con el prefijo `CA_` y el parámetro `OvCoreID` de la autoridad de certificados de confianza (el servidor de administración).

Certificado del nodo ausente

Para comprobar si falta el certificado del nodo, ejecute el comando siguiente en el nodo:

ovcert -list

Si falta el certificado del nodo, el comando muestra la salida en el formato siguiente:

```
+-------------------------------------------------------+

| Keystore Content                          |
+-------------------------------------------------------+

| Certificates:                                         |
+-------------------------------------------------------+

| Trusted Certificates:                                 |

|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55            |
+-------------------------------------------------------+
```

La sección `Certificates` vacía indica que el certificado del nodo no está presente.

Para resolver esto, siga estos pasos:

1. Quite el certificado de confianza del servidor de administración del nodo ejecutando el comando siguiente:

   ovcert -remove <*nombre_de_certificado*>

   En este ejemplo, <*nombre_de_certificado*> es el nombre del certificado de confianza (en el ejemplo, `CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55`).

2 Detenga todos los procesos en el Componente de monitorización de operaciones ejecutando el comando siguiente:

ovc -kill

3 Inicie los procesos centrales ejecutando el siguiente comando:

ovc -start CORE

4 Si el nodo y el servidor de administración están configurados para implementar automáticamente el certificado, el nodo envía una solicitud al servidor de administración y, después, el servidor de administración concede la solicitud.

Para comprobar si la solicitud de certificado ha llegado al servidor de administración, ejecute el comando siguiente (en el servidor de administración):

ovcm -listpending -l

La salida del comando debería mostrar el ID de núcleo del nodo en el campo `CN`.

Si no se puede ver el ID de núcleo del nodo en el campo `CN`, ejecute el comando siguiente en el nodo para activar manualmente una solicitud de certificado:

ovcert -certreq

Si el servidor de administración y el nodo están configurados para la implementación manual del certificado, siga las instrucciones indicadas en Implementación manual de certificados en la página 13.

Para comprobar si los certificados están correctamente instalados en el nodo, ejecute el siguiente comando (en el nodo):

ovcert -list

La salida debería mostrar un nombre de certificado válido en la sección `Certificates` (que es idéntico al ID de núcleo del nodo).

Certificado de confianza ausente

Para comprobar si falta el certificado de confianza, ejecute el comando siguiente en el nodo:

ovcert -list

Si falta el certificado de confianza, el comando muestra la salida en el formato siguiente:

```
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                                                 |
| cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)
+-------------------------------------------------------+
| Trusted Certificates:                                 |
+-------------------------------------------------------+
```

La sección `Trusted Certificates` vacía indica que el certificado de confianza no está presente.

Puede resolver este problema importando el certificado de confianza desde el servidor de administración u otro nodo administrado por el mismo servidor de administración.

Para importar el certificado de confianza desde otro origen, siga estos pasos:

1. Inicie sesión en el servidor de administración o en otro nodo (administrado por el mismo servidor de administración) con privilegios raíz o administrativos.
2. Ejecute el comando siguiente:

   ovcert -exporttrusted [-ovrg <*servidor*>**] -file** <*nombre_de_archivo*>

   En este caso, <*servidor*> es el nombre del grupo de recursos de High Availability si el servidor de administración está instalado en un clúster de High Availability.

   El comando exporta el certificado de confianza del servidor de administración al archivo especificado con la opción `-file`.
3. Transfiera el archivo en el nodo (donde falta el certificado de confianza).
4. Para importar el certificado de confianza, ejecute el siguiente comando:

   ovcert -importtrusted -file <*nombre_de_archivo*>
5. Para comprobar si los certificados están correctamente instalados en el nodo, ejecute el siguiente comando (en el nodo):

   ovcert -list

   La salida debería mostrar un nombre de certificado válido en la sección `Trusted Certificates`.

Clave privada del nodo ausente

Para comprobar si falta la clave privada del certificado del nodo, ejecute el comando siguiente en el nodo:

ovcert -list

Si falta la clave privada del nodo, el comando muestra la salida en el formato siguiente:

```
+-------------------------------------------------------+
| Keystore Content                          |
+-------------------------------------------------------+
| Certificates:                                                                 |
| cdc7b5a2-9dd6-751a-1450-eb556a844b55
+-------------------------------------------------------+
| Trusted Certificates:                                 |
|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55           |
+-------------------------------------------------------+
```

La ausencia del signo `*` junto al nombre de certificado del nodo indica que falta la clave privada del nodo. Para resolver esto, hay que quitar el certificado del nodo y, a continuación, instalar un nuevo certificado. Siga estos pasos:

1. Quite el certificado del nodo ejecutando el comando siguiente:

   ovcert -remove <*nombre_de_certificado*>

   En este ejemplo, <*nombre_de_certificado*> es el nombre del certificado del nodo (en el ejemplo, `cdc7b5a2-9dd6-751a-1450-eb556a844b55`).
2. Consulte de paso 2 en la página 17 a paso 4 en la página 17.

3 Para comprobar si la clave privada del nodo está correctamente instalada en el nodo, ejecute el siguiente comando (en el nodo):

`ovcert -list`

La salida debería mostrar el signo `*` junto al nombre del certificado del nodo en la sección `Certificates`.

3 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 de HP Operations Agent abre conexiones al servidor de administración 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 entrantes a ciertos puertos de destino distintos al puerto 383, se pueden configurar puertos de agentes de comunicación alternativos (Configuración del puerto de Communication Broker en la página 25).
- Si la red sólo permite la conexión de ciertos sistemas proxy para abrir conexiones por el cortafuegos, el usuario podrá redireccionar la comunicación a través de estos servidores proxy (consulte Configuración de la comunicación HTTPS a través de proxys en la página 29).

- Si la red sólo permite conexiones HTTPS salientes del servidor de administración por el cortafuegos y bloquea las conexiones entrantes de los nodos, se puede configurar un Reverse Channel Proxy (RCP) (Comunicación en un entorno de alta seguridad en la página 29).

En un entorno con varios servidores de administración, también se pueden configurar los servidores de administración para comunicarse entre sí mediante cortafuegos. La configuración es la misma que para la comunicación entre servidores de administración y nodos.

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:

1. En el nodo, abra el símbolo del sistema (shell).
2. 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 proxys

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.

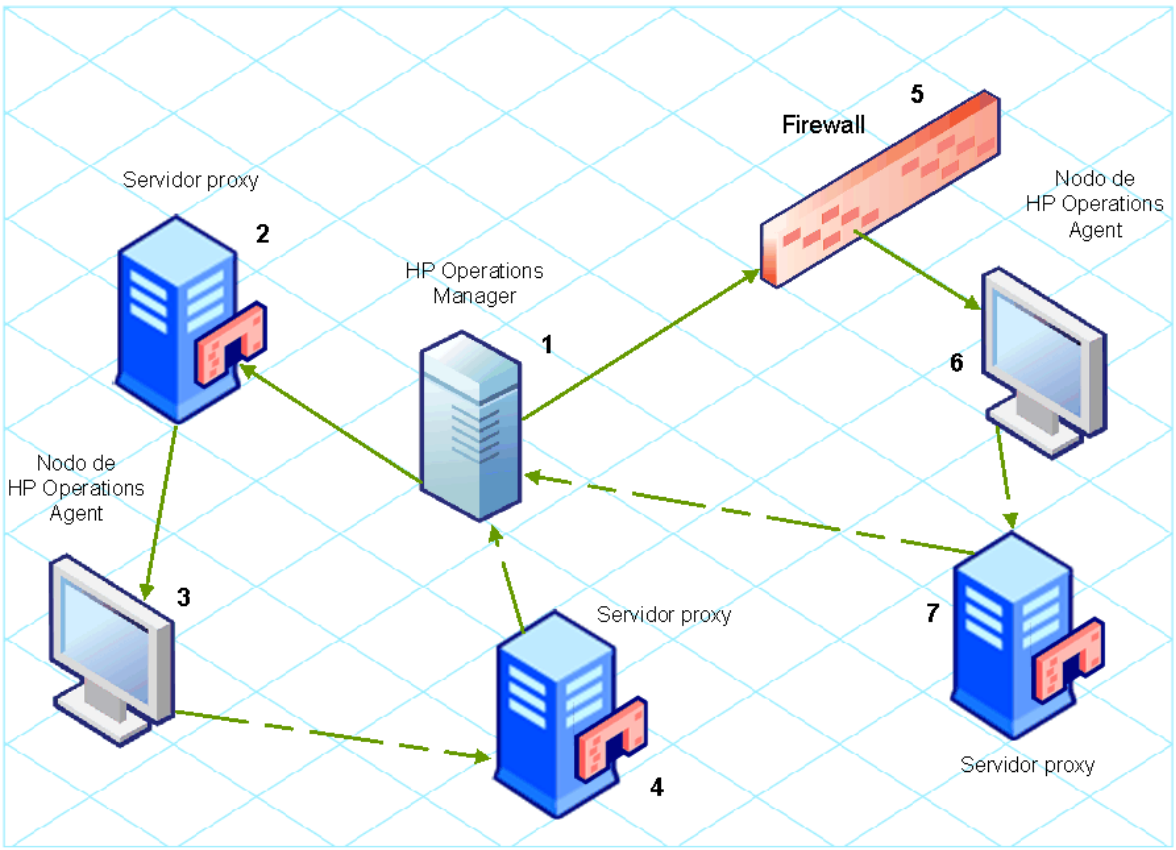
También puede redirigir la comunicación a través de servidores proxy en entornos más complejos, de la manera siguiente:

- 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).

Figura 2 Comunicación con proxys



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:

<*nombre_de_host_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 proxys, siga estos pasos:

1. Inicie sesión en el servidor de administración o nodo como usuario con derechos administrativos o 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*>

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

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, siga estos pasos:

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, hay que 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 local, siga estos pasos:

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 use 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, siga estos pasos:

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 proxys, siga estos pasos:

1. Inicie sesión en el servidor de administración o en el nodo con los privilegios raíz o administrativos.
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.

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

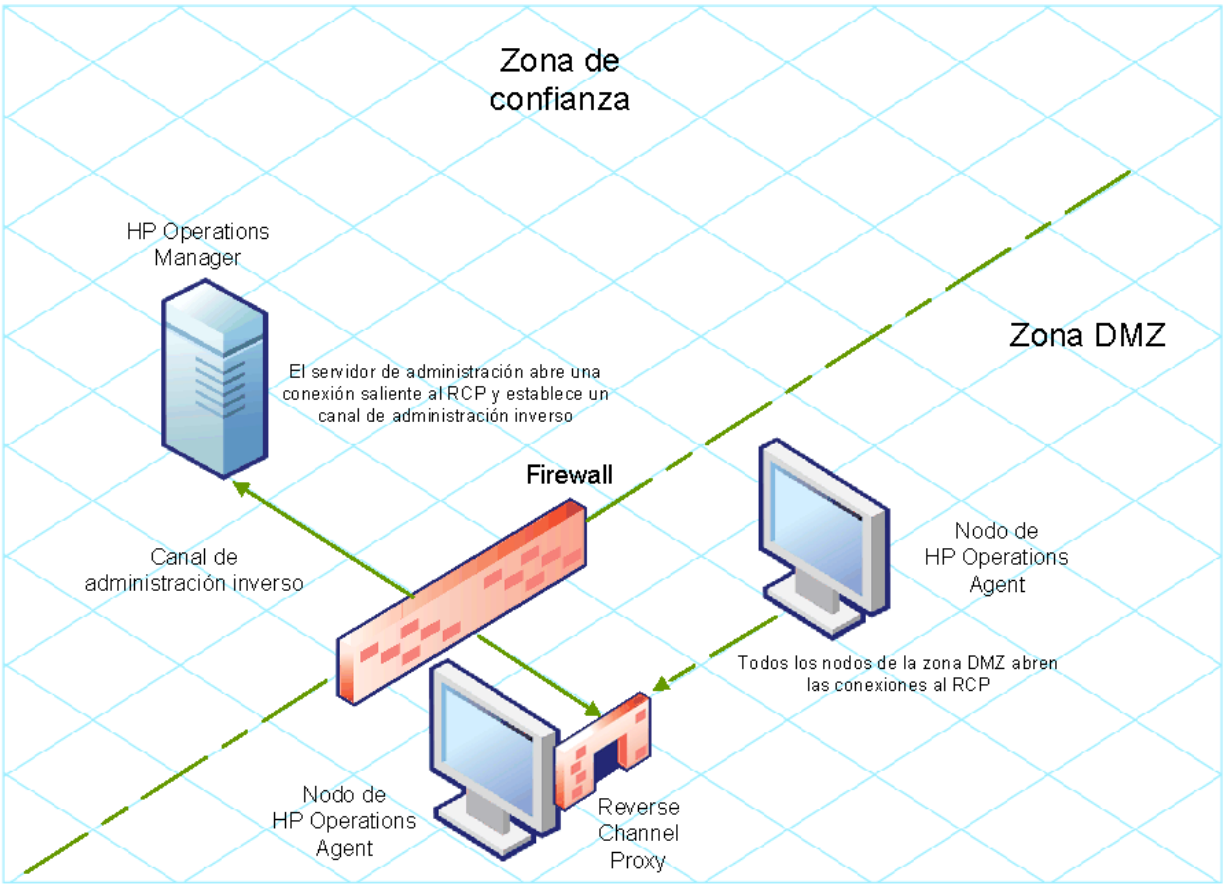
Comunicación en un entorno de alta seguridad

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.

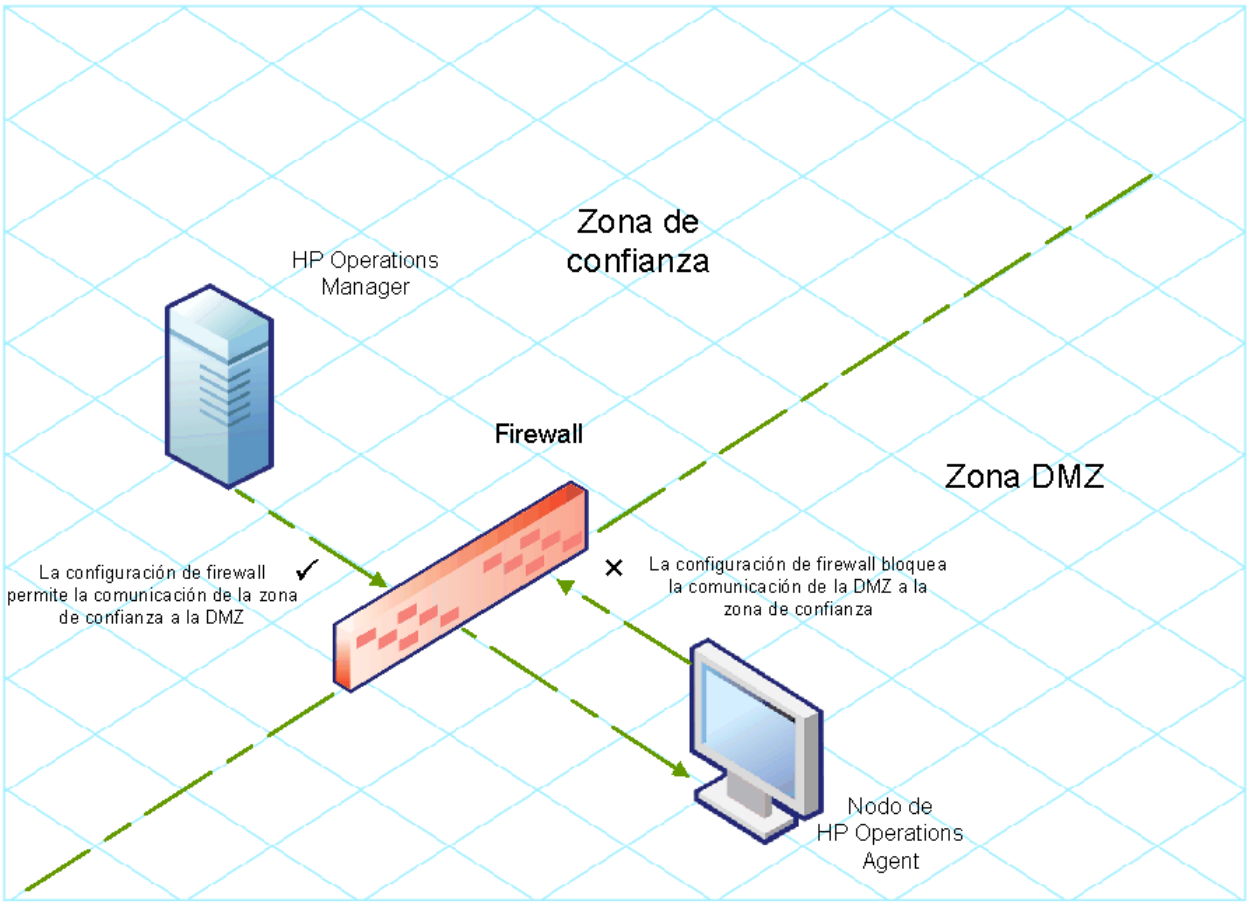
En la siguiente situación, los nodos administrados están ubicados en la zona DMZ, mientras que el servidor de administración pertenece a la zona de confianza. En este ejemplo, la configuración del cortafuegos permite únicamente la comunicación saliente. Por consiguiente, la comunicación entrante al servidor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

Figura 3 Nodos administrados 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.

Figura 4 Servidor de administración de HPOM en la zona DMZ



Introducción a Reverse Channel Proxy

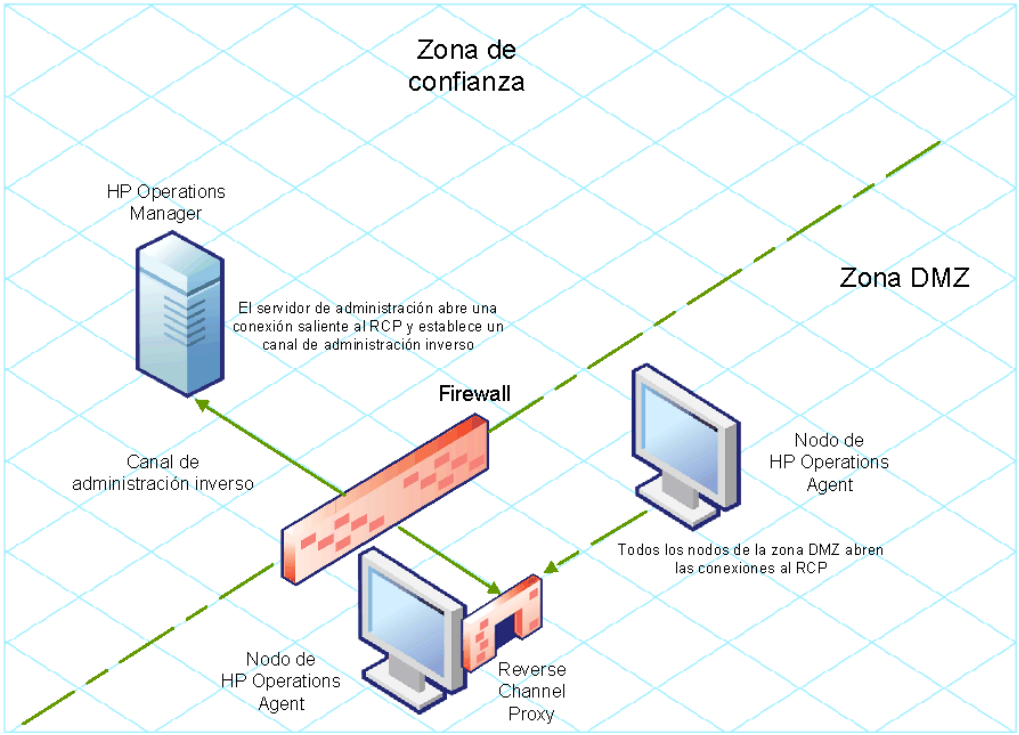
Una solución sencilla para habilitar la comunicación bidireccional es configurar el cortafuegos para que permita el tráfico entrante al puerto 383 (el puerto de Communication Broker). Sin embargo, este procedimiento podría hacer vulnerable al sistema a los ataques externos. Para habilitar la comunicación 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:

- El RCP está configurado en un nodo de la zona DMZ.
- Todos los nodos de la zona DMZ abren las conexiones al RCP.
- 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.
- Todos los nodos de la zona DMZ se comunican con el servidor de administración de HPOM mediante el canal de administración inverso.

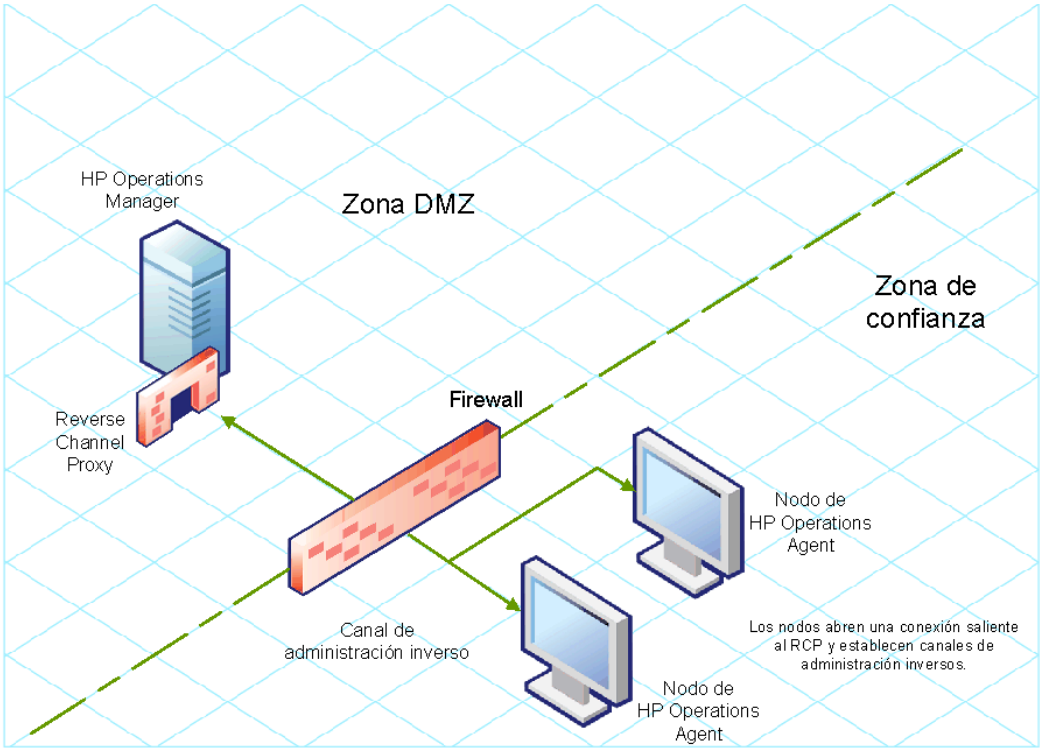
Figura 5 Comunicación segura a través del RCP con nodos de la zona DMZ



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:

- El RCP está configurado en el servidor de administración de la zona DMZ.
- 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.
- El servidor de administración de la zona DMZ se comunica con los nodos mediante el canal de administración inverso.

Figura 6 Comunicación segura a través del RCP con el servidor de administración 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:

Tarea 1: Configurar un RCP

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

Para configurar un RCP, 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:

   `ovconfchg -ns bbc.rcp -set SERVER_PORT` <*número_de_puerto*>.

   > Si se utiliza el comando **`ovconfchg`** en el servidor de administración de HPOM que se ejecuta en un clúster, hay que agregar el parámetro **`-ovrg`** <*servidor*>, donde <*servidor*> es el grupo de recursos.

   En este ejemplo, <*número_de_puerto*> es el puerto que utilizará el RCP. Asegúrese de que el puerto especificado no lo está utilizando ninguna otra aplicación.

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

   a **ovcreg -add** <*dir_de_instalación*>**/newconfig/DataDir/conf/bbc/ovbbcrcp.xml**

   b **ovc -kill**

   c **ovc -start**

Tarea 2: 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
```

> Si se utiliza el comando **ovconfchg** en el servidor de administración de HPOM que se ejecuta en un clúster, hay que agregar el parámetro **-ovrg** <*servidor*>, donde <*servidor*> es el grupo de recursos.

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

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

   b **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 en paso 3 en la página 33)

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

   Además, puede proporcionar los detalles de RCP mediante un archivo de configuración. Consulte Especificación de los detalles de RCP con un archivo de configuración en la página 35 para obtener más información.

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, siga estos pasos:

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 <*máximo_de_subprocesos*>

Especificación de los detalles de RCP con un archivo de configuración

Con 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 en paso 3 en la página 33)

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

3 Guarde el archivo en la ubicación siguiente:

<*dir_de_datos*>\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_de_archivo*>: nombre del archivo creado en el paso 1 en la página 35.

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 en el paso 3 en la página 33)

<*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`

5 Repita el paso 3 y el paso 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.

Tarea 1: 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` en paso 3 en la página 33)

Tarea 2: 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`.

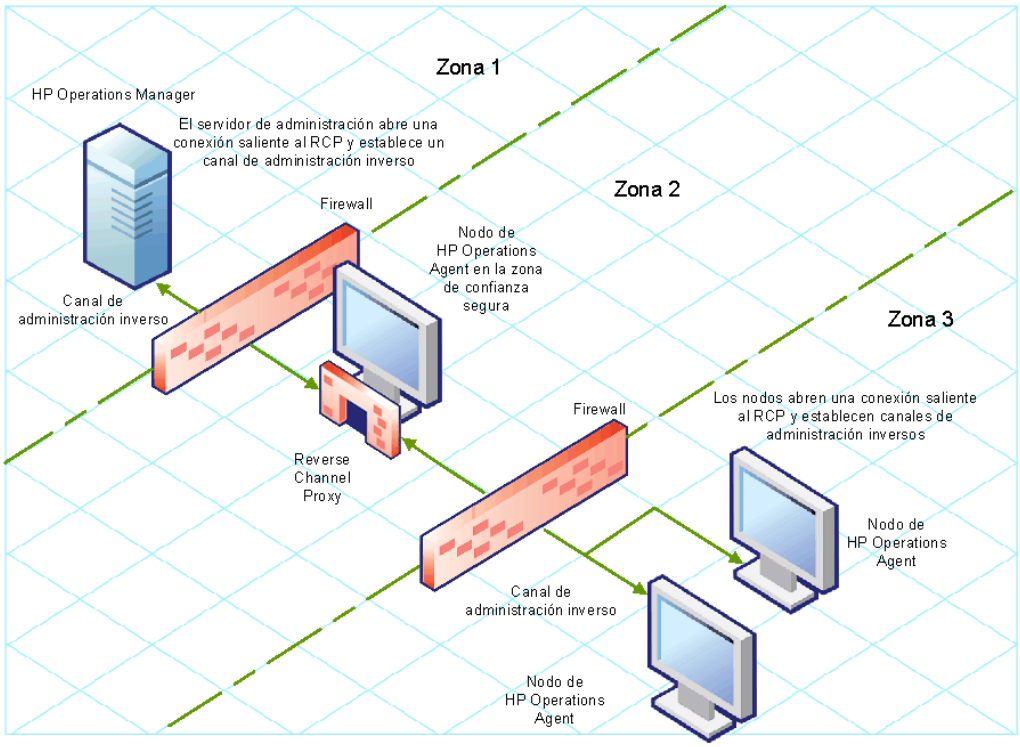
Si se produce un error en el canal de administración inverso a un RCP, el comando **ovbbccb -status** muestra el estado con el formato siguiente:

```
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.

Figura 7 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.

4 HP Operations Agent en clústeres de 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 High Availability, 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 High Availability.
- **Nodos virtuales.** Si se está utilizando el nodo con HPOM para UNIX 8.35, 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 High Availability, 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 High Availability 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 High Availability

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

Para monitorizar aplicaciones preparadas para clúster en los nodos de un clúster de High Availability, 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`.

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.

El archivo `apminfo.xml` tiene el formato siguiente:

> No se permiten nuevas líneas entre las etiquetas de paquete del archivo `apminfo.xml`.

```
<?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>
```

4 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/`

5 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_de_aplicación*> debe ser idéntico al contenido de la etiqueta `<Application><Name>` del archivo `apminfo.xml`. El archivo <*nombre_de_aplicación*>`.apm.xml` incluye los nombres de las directivas identificadas en paso 2.

Utilice el siguiente formato al crear el archivo <*nombre_de_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>
```

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 ON $instanceName</StartCommand>

<StopCommand>dbspicol OFF $instanceName</StopCommand>

</Application>

</APMApplicationConfiguration>
```

6 Guarde el archivo <*nombre_de_aplicación*>`.apm.xml` completado en cada nodo del clúster en el directorio siguiente:

- En Windows: *%OvDataDir%*`bin\instrumentation\conf`
- En UNIX/Linux: `/var/opt/OV/bin/instrumentation/conf`

7 Asegúrese de que todos los nodos físicos donde residen los grupos de recursos son nodos administrados.

8 Compruebe la sintaxis de los archivos XML en todos los nodos físicos ejecutando el comando siguiente:

- 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`**

9 *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:

a Obtenga el nombre del nodo físico que aparece en la configuración del clúster:

`ovclusterinfo -a`

b 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**.

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

a **ovc -stop**

b **ovc -start**

11 Si está usando HPOM para Windows 8.1x, implemente las directivas identificadas para monitorizar la aplicación preparada para clúster (en paso 2) en todos los nodos físicos del clúster de High Availability.

Para el resto de tipos de servidores de administración, implemente las directivas identificadas para monitorizar la aplicación preparada para clúster (en paso 2) 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 Inicie sesión en el nodo con los privilegios raíz.

2 Vaya al directorio siguiente:

En HP-UX, Linux o Solaris:

`/opt/OV/bin`

En AIX:

`/usr/lpp/OV/bin`

3 Ejecute el comando siguiente para detener el agente:

ovc -kill

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

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

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

5 Ejecute el comando siguiente para iniciar el agente:

ovc -start

5 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:

➤ 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 **All Tasks > Deploy Instrumentation**. Se abrirá el cuadro de diálogo Deploy Instrumentation.
2. En el cuadro de diálogo Deploy Instrumentation, haga clic en **HP Operations Agent** y, a continuación, haga clic en **OK**. 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:

➤ 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 directiva 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.

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 scope. 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 **Policy management** → **Policy groups** → **HP Operations Agent** → **Performance Collection Component** → **Collection configuration**. 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 archivo `parm` para el cuadro de diálogo <*plataforma*>.
4. En la pestaña Data, 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 **Save and Close**. En el panel de detalles, la versión de la directiva aumenta en `.1`.
6. Implemente la directiva actualizada en los nodos deseados.

   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 **Browse** → **All Policy Groups**. 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**, **Performance Collection Component** y, a continuación, en **Collection Configuration**. 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 Content, 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 **Save**.

9 Implemente la directiva actualizada en los nodos deseados.

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

En la consola de HPOM para Windows 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 mediante la edición del archivo `alarmdef`, siga estos pasos:

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

2 En el árbol de consola, haga clic en **Policy management** → **Policy groups** → **HP Operations Agent** → **Performance Collection Component** → **Alarm definition**. Las directivas ConfigFile para configurar el archivo `alarmdef` 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 Alarmdef para HP-UX). Se abrirá el cuadro de diálogo Alarmdef file for <*plataforma*>.

4 En la pestaña Data, 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`.

5 Haga clic en **Save and Close**. En el panel de detalles, la versión de la directiva aumenta en `.1`.

6 Implemente la directiva actualizada en los nodos deseados.

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 donde desea que surta efecto el mecanismo de alerta modificado.
2. En la consola, haga clic en **Browse** → **All Policy Groups**. 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**, **Performance Collection Component** y, a continuación, en **Alarm Definition**. 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 Content, 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 **Save**.
9. Implemente la directiva actualizada en los nodos deseados.

   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 Tool Output de la ventana Tool Status
- *HPOM en UNIX/Linux*

  En la ventana Application Output 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 scope 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 post policy deploy action	Permite comprobar el estado de implementación de las directivas parm o 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 Parameter de la ventana Edit Parameters. 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.

6 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 ni dejan de responder.

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.

➤ 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:

➤ 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 **All Tasks > Deploy Instrumentation**. Se abrirá el cuadro de diálogo Deploy Instrumentation.
2. En el cuadro de diálogo Deploy Instrumentation, haga clic en **HP Operations Agent** y, a continuación, haga clic en **OK**. La implementación de los archivos de instrumentación necesarios comienza en los nodos.

Para implementar la instrumentación, siga estos pasos:

➤ 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**.

Directivas 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:

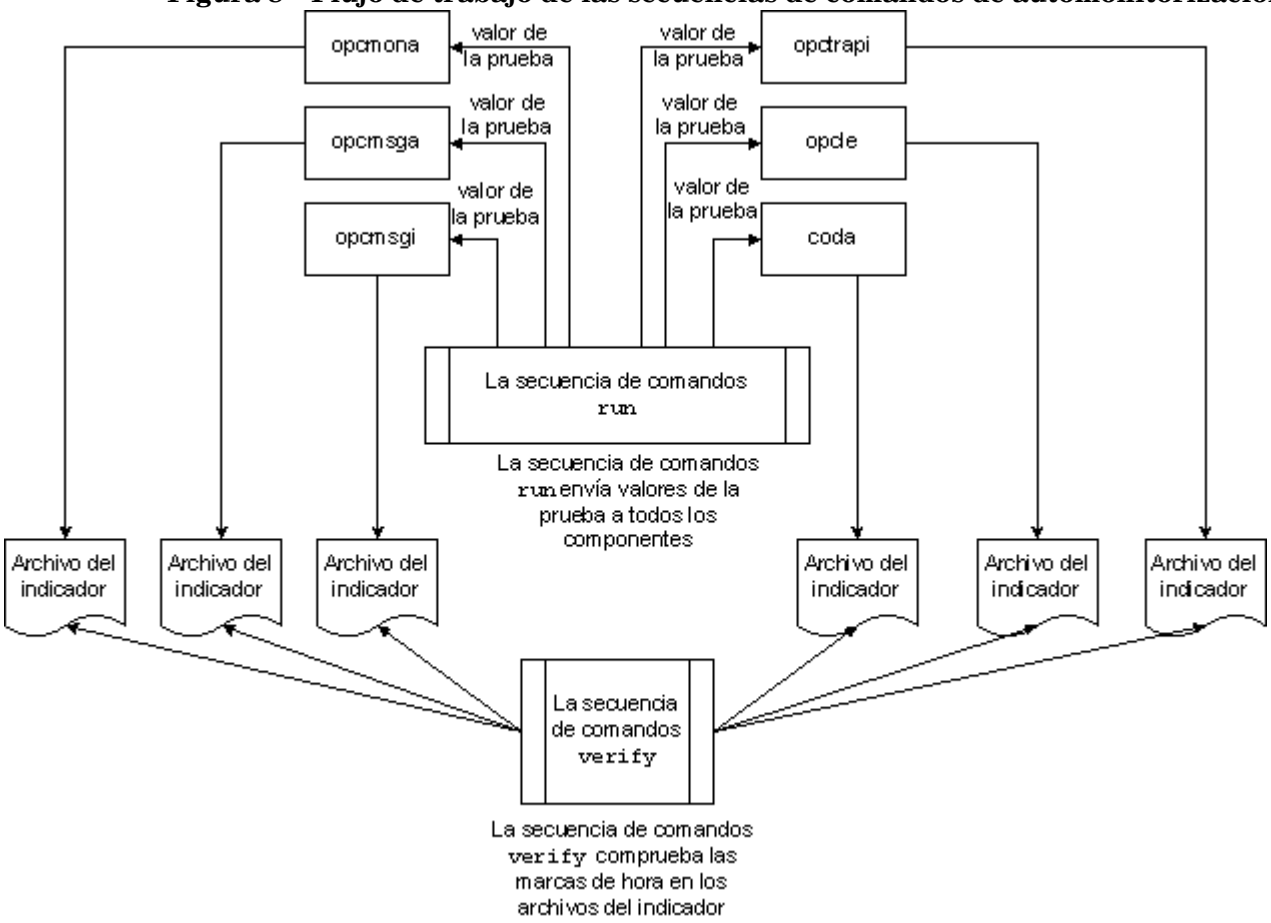
- **OA-SelfMonTstMonaExt:** prueba el agente de monitorización.
- **OA-SelfMonVerifyMon:** comprueba los archivos del indicador por el agente de monitorización.
- **OA-SelfMonTstLe:** prueba el encapsulador de archivos de registro.
- **OA-SelfMonVerifyLe:** comprueba los archivos del indicador por el 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.

Figura 8 Flujo de trabajo de las secuencias de comandos 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, amplíe **Policy management > Policy groups > HP Operations Agent**.
2. Haga clic con el botón derecho en Self Monitoring y, a continuación, haga clic en **All Tasks > Deploy on**. Se abrirá el cuadro de diálogo Deploy Policies.
3. En el cuadro de diálogo Deploy Policies, seleccione los nodos y, a continuación, haga clic en **OK**. HPOM se inicia implementando las directivas `Self Monitoring` en los nodos seleccionados.

   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/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 de agente y, a continuación, haga clic en **OK**.

   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 error 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.

Índice