Hewlett Packard Enterprise

Guía de usuario de HPE OneView 3.0

Resumen

En esta guía se describen las funciones, las interfaces, el diseño del modelo de recursos y el entorno de trabajo seguro de HPE OneView. En ella se describen las consideraciones previas de planificación y la forma de utilizar la interfaz de usuario o las API de REST del dispositivo HPE OneView para configurar, gestionar, supervisar y solucionar problemas de la infraestructura del centro de datos. También incluye información sobre el SCMB (State-Change Message Bus). Se ha concebido para administradores de infraestructuras, administradores de redes y administradores de servidores que planifiquen, configuren y gestionen software y hardware de centros de datos a lo largo de todo su ciclo de vida, así como para administradores de copias de seguridad y personal de operaciones que supervisen y solucionen problemas de software o hardware de centros de datos.

Nº de referencia: 5200-1736
Publicado: Octubre de 2016
Edición: 1

Reconocimientos

Garantía

Hewlett Packard Enterprise sustituirá los soportes de distribución defectuosos durante un período de 90 días a partir de la fecha de la compra.

Contenido

Parte I Información acerca de HPE OneView

En esta parte se describe HPE OneView y su modelo de recursos del centro de datos, y es una introducción a los términos y conceptos utilizados en el presente documento y en la ayuda en línea del dispositivo.

1 Información acerca de HPE OneView

Diseñada para entornos de infraestructura convergente, HPE OneView es una plataforma única integrada, presentada como dispositivo, que implementa un enfoque definido por software para la gestión de la infraestructura física a lo largo de su ciclo de vida completo. Para obtener más información sobre HPE OneView, puede comenzar por la introducción o seleccionar un tema en la lista siguiente.

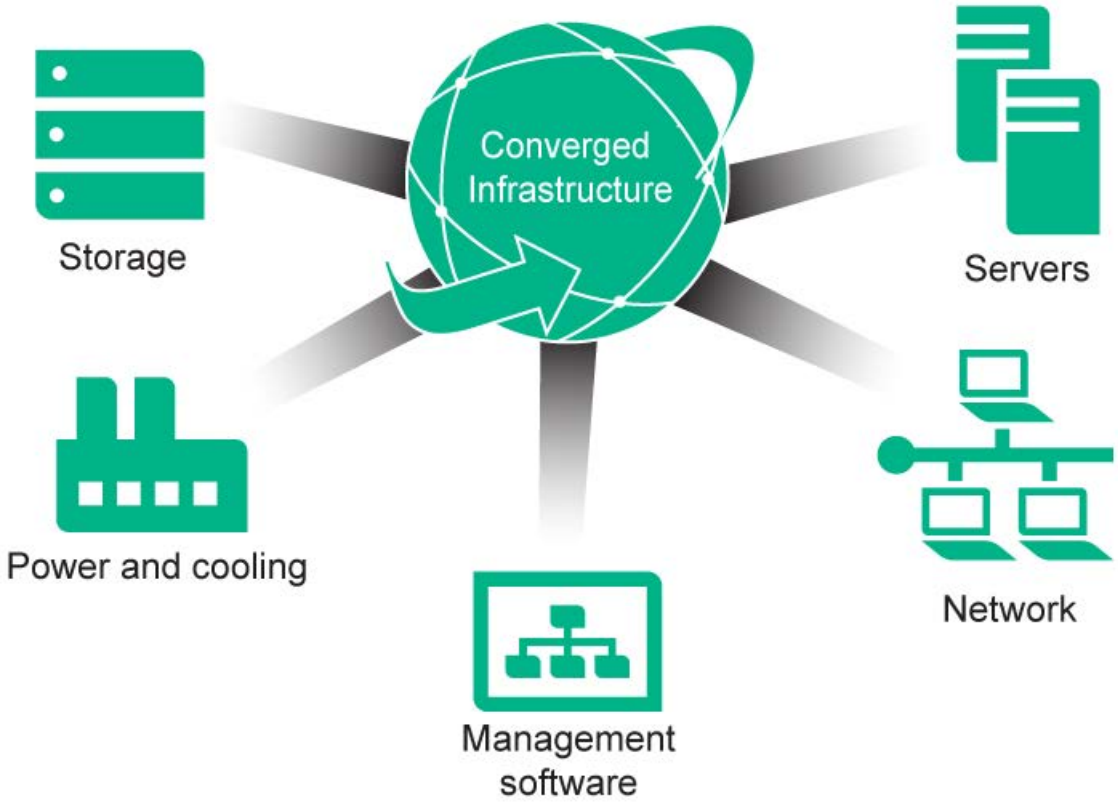
- «Licencias de HPE OneView»
- «Gestión, supervisión o migración de hardware de servidor en receptáculos c7000»
- «Funciones de aprovisionamiento»
- «Funciones de gestión de firmware y de cambios de configuración»
- «Supervisión del entorno y respuestas a los problemas»
- «Funciones de copia de seguridad y restauración»
- «Funciones de seguridad»
- «Funciones de alta disponibilidad»
- «Interfaces gráfica y de programación»
- «Integración con otro software de gestión»
- «Integración abierta»
- «Funciones de red»
- «Funciones de HPE Smart Update Tools»

1.1 HPE OneView para la gestión de infraestructura convergente

HPE OneView, que se ha optimizado para la colaboración, productividad y fiabilidad, se ha diseñado con el fin de ofrecer una gestión de ciclo de vida de hoja de vidrio única y simple para aspectos complejos de TI empresarial—servidores, red, software, encendido y refrigeración, y almacenamiento.

HPE OneView permite supervisar, configurar y gestionar servidores físicos y lógicos, y almacenar recursos con facilidad a través de una interfaz gráfica de usuario o mediante API REST (REpresentational State Transfer).

HPE OneView está diseñado para gestionar su infraestructura convergente y dar soporte a escenarios clave como la implementación de servidores sin configurar, la implementación de clústeres de hipervisores partiendo de equipos sin configurar, el mantenimiento periódico de hardware, y la respuesta a las alertas y a las averías en los suministros. Está diseñado para la infraestructura física necesaria para admitir la virtualización, la informática en la nube, grandes volúmenes de datos y entornos informáticos mixtos.



HPE OneView se distribuye como un dispositivo virtual, una máquina virtual preconfigurada lista para implementarla en un host del hipervisor.

HPE OneView es una solución escalable orientada a recursos centrada en el ciclo de vida completo,— desde la configuración inicial hasta el mantenimiento y la supervisión continuas, —de los recursos tanto físicos como lógicos:

- Los recursos físicos son objetos que se pueden tocar, como el hardware de servidor, las interconexiones, los conmutadores de la parte superior del bastidor, los receptáculos, los sistemas de almacenamiento y los bastidores.
- Los recursos lógicos son objetos virtuales, por ejemplo, las plantillas o los grupos que, cuando se aplican a los recursos físicos, proporcionan una estructura común en todo el centro de datos. Por ejemplo, las plantillas de perfiles de servidor, los grupos de interconexiones lógicas, los grupos de receptáculos, los perfiles de servidor y las plantillas de volumen son recursos lógicos.

Flexibilidad definida por software—sus expertos diseñan configuraciones para implementaciones eficaces y coherentes

HPE OneView ofrece varios recursos definidos por software, como perfiles de servidor y grupos, que le permiten capturar las prácticas recomendadas de los expertos en una gran variedad de disciplinas, que incluyen la red, el almacenamiento, la configuración de hardware y la configuración y compilación de sistemas operativos. El hecho de que sus expertos definan los perfiles de servidor y los grupos y recursos de redes, le permitirá eliminar la falta de comunicación entre las distintas disciplinas. El RBAC (role-based access control, control de acceso basado en roles) y los grupos, conjuntos y perfiles de servidor que establecen los expertos, hace que pueda ofrecerle a los administradores del sistema el aprovisionamiento y gestión de cientos de servidores sin que sea necesario que los expertos se impliquen en cada implementación de servidor.

HPE OneView combina la gestión y el aprovisionamiento de centro de datos interdependiente y complejo en una interfaz unificada y simplificada. Es posible:

- Aprovisionar el centro de datos (página 27)
- Gestionar y mantener cambios de firmware y configuración (página 32)
- Supervisar el centro de datos y dar respuesta a los problemas (página 33)

La solución también proporciona capacidades clave de gestión empresarial, como son:

- Funciones de alta disponibilidad (página 38)
- Funciones de seguridad (página 37)
- Interfaces gráfica y de programación (página 38)
- Soporte remoto (página 36)

HPE OneView gestiona servidores y recursos de red de los chasis, admite conexiones entre los chasis y el almacenamiento, y proporciona información para ayudar a gestionar la energía y la refrigeración del centro de datos:

- Los servidores se representan y gestionan a través de sus perfiles de servidor y de las plantillas de perfiles de servidor.
- Las redes son un componente esencial para el aprovisionamiento y la gestión de los servidores de los centros de datos.
- El Software de administración se integra con HPE OneView para un funcionamiento sin problemas.
- La gestión del entorno—, como la alimentación, la refrigeración y la planificación del espacio—requiere que tenga en cuenta todos los equipos del centro de datos, incluidos los que no gestiona HPE OneView. HPE OneView muestra toda la información relacionada con la alimentación y la refrigeración del centro de datos en una vista de la interfaz.
- El aprovisionamiento de almacenamiento con distribución automática en zonas está disponible. Los dispositivos de almacenamiento se conectan con los receptáculos mediante conexiones Fibre Channel Fabric attach (con un conmutador SAN), conexiones Fibre Channel sobre Ethernet (FCoE) fabric attach (con un conmutador SAN) o conexiones Fibre Channel Direct attach (de conexión directa o Flat SAN).

1.2 Licencias de HPE OneView

HPE OneView admite los siguientes tipos de licencias:

- Licencia HPE OneView Advanced para gestionar hardware de servidor
- Licencia HPE OneView Standard para supervisar hardware de servidor

La licencia HPE OneView Standard permite realizar la supervisión, gestión de inventario y generación de informes de servidores HPE BladeSystem y HPE ProLiant BL y DL. La licencia HPE OneView Advanced permite realizar todas las operaciones admitidas por HPE OneView. En la tabla siguiente se muestra información general sobre las funciones disponibles para cada tipo de licencia.

Funciones	HPE OneView Standard	HPE OneView Advanced
Integraciones con socios		√
Infraestructura definida por software (perfiles, grupos, conjuntos y otros tipos)		√
Aprovisionamiento de almacenamiento y distribución en zonas SAN		√

Funciones	HPE OneView Standard	HPE OneView Advanced
Gestión avanzada de Virtual Connect		√
Gestión de firmware		√
Gestión de energía (visualización en 3D)		√
Aprovisionamiento del sistema operativo		√
Gestión remota (HPE iLO Advanced)		√
Vista Map (Mapa)	√	√
Búsqueda inteligente, vista Activity (Actividad) y panel de control	√	√
Supervisión del estado	√	√
Inventario	√	√
Generación de informes	√	√
Acceso a la API de REST	√	√
Soporte remoto	√	√
Soporte técnico y actualizaciones de software	Soporte 9x5 durante 1 año (opcional)	Soporte 24x7 durante 3 años (incluido)

Más información

«Gestión, supervisión o migración de hardware de servidor en receptáculos c7000»
«Acerca de las licencias»

1.3 Gestión, supervisión o migración de hardware de servidor en receptáculos c7000

Es posible añadir hardware de servidor, como receptáculos y servidores de montaje en bastidor, en HPE OneView de una de las siguientes maneras:

Gestionada Si se agrega un servidor gestionado a HPE OneView, ya sea en un receptáculo o en un servidor de montaje en bastidor, se pueden aplicar configuraciones, implementar perfiles de servidor, supervisar el estado de funcionamiento, recopilar estadísticas y alertar a los usuarios cuando se den determinadas situaciones. Para obtener más información, consulte «Acerca de los receptáculos c7000 gestionados» y «Gestión del hardware de servidor». Para gestionar hardware de servidor se necesita la licencia HPE OneView Advanced.

Supervisado Si se agrega un servidor supervisado a HPE OneView, ya sea en un receptáculo o en un servidor de montaje en bastidor, únicamente se puede supervisar su estado de hardware e inventario. Para obtener más información, consulte «Acerca de los receptáculos c7000 supervisados». La supervisión del hardware de servidor utiliza una licencia gratuita denominada HPE OneView Standard.

Migrado Los receptáculos de Virtual Connect Manager (VCM) y Virtual Connect Enterprise Manager (VCEM) se pueden migrar a HPE OneView con la información de configuración para que HPE OneView pueda gestionarlos. Para gestionar un receptáculo se requiere una licencia HPE OneView Advanced. Para obtener más información sobre la migración, consulte «Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión».

Más información

«Licencias de HPE OneView»

1.4 Funciones de aprovisionamiento

Después de instalar el dispositivo HPE OneView y llevar a cabo las tareas de configuración inicial, puede incluir rápidamente hardware existente en la gestión, así como preparar y realizar la implementación de hardware en el centro de datos.

Las funciones de aprovisionamiento de hardware e inclusión de recursos en la gestión son:

- Conjuntos, grupos y plantillas de recursos (página 27)
- Perfiles de servidor y plantillas de perfiles de servidor (página 29)
- Proceso optimizado para incluir el hardware en la gestión (página 30)
- Implementación de sistemas operativos (página 31)
- Gestión y aprovisionamiento de almacenamiento (página 31)

1.4.1 Conjuntos, grupos y plantillas de recursos

Con el enfoque basado en plantillas de HPE OneView, podrá:

- Utilizar a sus expertos para definir las configuraciones de red y servidores para entornos concretos.
- Aprovisionar cientos de servidores de forma rápida y coherente sin necesidad de que los expertos tengan que intervenir para cada servidor que se implemente.
- Simplificar la distribución de los cambios de configuración por el centro de datos.

Grupos y recursos de plantillas

Los siguientes recursos son plantillas que los expertos definen para cubrir diferentes cargas de trabajo. Estas plantillas se pueden aplicar una y otra vez a los recursos físicos, garantizando así unas configuraciones rápidas y coherentes.

Plantilla o grupo	Descripción
Grupo de receptáculos	Una plantilla que define una configuración coherente para un receptáculo. Un grupo de receptáculos especifica la ubicación de las diferentes interconexiones y los grupos de interconexiones lógicas que se aplican a las primeras. Cuando se aplica un grupo de receptáculos a un receptáculo físico, HPE OneView crea un receptáculo lógico que queda listo para su uso. Un mismo grupo de receptáculos se puede aplicar a muchos receptáculos físicos para crear muchos receptáculos lógicos con la misma configuración.
Grupo de interconexiones lógicas	Una plantilla que define la configuración de conexión a red deseada de una interconexión física o conjunto de interconexiones. Los grupos de interconexiones lógicas se utilizan cuando se definen grupos de receptáculos y representan la plantilla de conexión de red de dicho grupo de receptáculos. Cuando se aplica un grupo de receptáculos a un receptáculo físico, HPE OneView: • Crea un receptáculo lógico. • Utiliza los grupos de interconexiones lógicas de dicho grupo de receptáculos para configurar las interconexiones físicas del receptáculo en interconexiones lógicas.

Plantilla o grupo	Descripción
Grupo de conmutadores lógicos	Una plantilla que define cómo se combinan los conmutadores lógicos para formar conmutadores lógicos. Los conmutadores lógicos son una agregación de hasta dos conmutadores físicos de la parte superior del bastidor. Una vez que se crea a partir de un grupo de conmutadores lógicos, un conmutador lógico sigue estando asociado a su grupo de conmutadores lógicos. Cualquier cambio en la coherencia entre el grupo de conmutadores lógicos y sus conmutadores lógicos asociados se supervisa y se muestra en la pantalla del conmutador lógico asociado en HPE OneView.
Plantillas de perfiles de servidor	Una plantilla que define las características de un perfil de servidor. Una plantilla de perfil de servidor se puede aplicar a varios servidores para crear servidores con una configuración idéntica. Un perfil de servidor se puede actualizar para que coincida con cualquier plantilla de perfil de servidor.
Plantillas de volumen	Una plantilla que define una configuración estándar para los volúmenes de almacenamiento.

Recursos lógicos

Los siguientes recursos lógicos representan los recursos físicos definidos por el software configurados para funcionar según sea necesario en el entorno. Estos recursos controlan las cargas de trabajo.

Recurso	Descripción
Receptáculo lógico	Un receptáculo lógico representa una vista lógica de un único receptáculo con un grupo de receptáculos que actúa como plantilla. De forma predeterminada, al agregar un receptáculo c7000 se crean un grupo de receptáculos y un grupo de interconexiones lógicas. O bien, puede crear varios grupos de interconexiones lógicas y un grupo de receptáculos antes de agregar el receptáculo. Cuando se agrega un receptáculo c7000, se crea automáticamente un receptáculo lógico.
Interconexiones lógicas	Una interconexión lógica es una sola entidad administrativa que consta de la configuración de un conjunto de interconexiones físicas de un único receptáculo. Una interconexión lógica representa las redes, conjuntos de enlaces ascendentes, redes internas y enlaces de apilamiento disponibles para las interconexiones físicas.
Conmutador lógico	Un conmutador lógico puede estar formado por un máximo de dos conmutadores físicos de la parte superior del bastidor (externos al receptáculo c7000) configurados en un único dominio de apilamiento.
Perfil de servidor	Un perfil de servidor representa un servidor físico que se ha configurado completamente para realizar la función deseada. El perfil de servidor especifica todos los ajustes de almacenamiento, conexión de red, firmware y servidor exigidos por la carga de trabajo del servidor. El perfil de servidor se basa en todos los otros recursos lógicos de HPE OneView.
Volúmenes	Un volumen es un espacio de almacenamiento lógico aprovisionado desde un pool de almacenamiento de un sistema de almacenamiento.

Definición de configuraciones para entornos específicos

Los grupos y las plantillas permiten definir configuraciones específicas para el entorno que se desea crear, como hosts virtuales, entornos de Microsoft Exchange, servidores web externos o internos, o servidores de bases de datos corporativas.

Por ejemplo, para configurar varios servidores web externos:

1. Su experto en redes puede crear grupos de interconexiones lógicas, conjuntos de enlaces ascendentes, redes y conjuntos de redes para establecer todas las directivas de conexión entre las redes de los centros de datos y las interconexiones gestionadas por el dispositivo.

2. Su experto en servidores puede crear grupos de receptáculos, agregar receptáculos y crear plantillas de perfil de servidor para establecer la configuración completa necesaria para un servidor web externo.
3. Sus administradores de servidores pueden utilizar las plantillas de perfiles de servidor cada vez que necesiten implementar servidores de este tipo.

Flexibilidad en el diseño y la implementación

HPE OneView proporciona flexibilidad para la creación de grupos, plantillas y conjuntos. Por ejemplo, puede crear un grupo de interconexiones lógicas con estos métodos:

- Antes de agregar un receptáculo al dispositivo para gestionarlo, puede crear uno o varios grupos de interconexiones lógicas que especifiquen cómo desea configurar las interconexiones, y un grupo de receptáculos que especifique cómo desea que se configure el receptáculo. A continuación, cuando agregue el receptáculo, podrá especificar el grupo de receptáculos que ya habrá creado.
- Puede agregar un receptáculo al dispositivo para gestionarlo y, después de que el dispositivo detecte y agregue el hardware de interconexión del receptáculo, puede usar o modificar el grupo de interconexiones lógicas predeterminado que crea el dispositivo.
- Existe la posibilidad de migrar un dominio de Virtual Connect a HPE OneView, con lo que se crean grupos de interconexiones lógicas.
- Copie cualquier grupo de interconexiones lógicas para crear un nuevo grupo de interconexiones lógicas.

Los grupos, las plantillas y los conjuntos también simplifican la distribución de los cambios de configuración en el dispositivo.

Más información

Capítulo 1, «Información acerca de HPE OneView»
«Conceptos básicos sobre el modelo de recursos» (página 45)

1.4.2 Perfiles de servidor y plantillas de perfiles de servidor

Un perfil de servidor captura los aspectos clave de una configuración de servidor en un mismo sitio, incluyendo:

- Selección y programación de las actualizaciones del firmware.
- Configuración del BIOS
- Configuración del RAID local
- Conectividad con la red
- Configuración de la orden de arranque
- Almacenamiento local y almacenamiento SAN
- ID únicos

Puede aplicar un perfil directamente a un único servidor o guardar la configuración en una plantilla de perfil de servidor.

Guarde la configuración recomendada en una plantilla de perfil de servidor y, a continuación, utilícela para crear e implementar perfiles de servidor. Los perfiles de servidor permiten que sus expertos especifiquen una configuración de servidor antes de que este llegue. Cuando el hardware del servidor está instalado, los administradores pueden gestionar rápidamente el nuevo servidor.

Por ejemplo, puede implementar un perfil de servidor partiendo de una plantilla que no esté asignada a un servidor determinado, pero que especifique todos los aspectos de configuración, como la configuración del BIOS, las conexiones de red y el orden de arranque, que se deben

utilizar para un tipo de hardware de servidor. Antes de que el servidor esté instalado en un compartimento de un receptáculo, puede realizar una de las acciones siguientes:

- Asigne el perfil de servidor en el momento de crearlo a un compartimento vacío de un receptáculo en el que residirá el servidor.
- Cree un perfil sin asignar y asígnelo cuando llegue el hardware.

Puede mover un perfil de servidor que se ha asignado al hardware de un compartimento de un receptáculo. Puede copiar perfiles de servidor a múltiples servidores utilizando plantillas de perfil de servidor.

Puede controlar el comportamiento del perfil de servidor. Por ejemplo, puede asignar un perfil de servidor a un compartimento vacío de modo que, cuando se introduzca un servidor en el compartimento, el perfil de servidor se aplique automáticamente al hardware de servidor. El perfil de servidor también puede asociarse con un servidor concreto para asegurarse de que el perfil no se aplique si se introduce el servidor erróneo en el compartimento.

Más información

«Acerca de los perfiles de servidor»
«Acerca de las plantillas de perfiles de servidor»
Capítulo 1, «Información acerca de HPE OneView»

1.4.3 Proceso optimizado para incluir el hardware en la gestión

HPE OneView simplifica el proceso de inclusión de los receptáculos, las interconexiones y el hardware de servidores en la gestión.

Por ejemplo:

- Cuando se **agrega** un receptáculo, el dispositivo detecta automáticamente todo el hardware que contiene y lo incluye en la gestión. Por ejemplo, el dispositivo:
  - Actualiza el Onboard Administrator del receptáculo, los módulos de interconexión de Virtual Connect y el firmware de iLO de los servidores a la versión mínima requerida
  - Configura cada módulo de interconexión de Virtual Connect, eliminando la configuración de VC existente. Para conservar la configuración de VC existente, migre el receptáculo.
  - Configura el Onboard Administrator, lo que incluye configurar el protocolo NTP (Network Time Protocol) y un certificado de SSO (Single Sign-On, inicio de sesión único) para el acceso a la interfaz de usuario
  - Configura el iLO de cada servidor, lo que incluye la configuración de un certificado de SSO para el acceso a la interfaz de usuario
  - Configura el hardware para la supervisión, lo que incluye la configuración de las capturas SNMP (Simple Network Management Protocol)
- Cuando se **migra** un receptáculo gestionado por VCM, el dispositivo valida automáticamente la información de configuración (incluyendo hardware, dominio de Virtual Connect, redes y perfiles de servidor) antes de importar el receptáculo. Durante la migración, la información de configuración se traslada a HPE OneView.
- Cuando se agrega un dispositivo de energía HPE Intelligent Power Distribution Unit (iPDU), el dispositivo detecta y presenta automáticamente los dispositivos conectados para que pueda incluir los dispositivos en la gestión.

Más información

«Acerca de los receptáculos c7000 gestionados»
Capítulo 1, «Información acerca de HPE OneView»

1.4.4 Implementación de sistemas operativos

Los perfiles de servidor y los grupos de receptáculos facilitan la tarea de preparar un servidor sin configurar para la implementación del sistema operativo.

Por ejemplo, puede utilizar perfiles de servidor junto con herramientas de implementación, tales como:

- HPE Insight Control Server Provisioning para instalar un sistema operativo en el servidor
- HPE OneView for VMware vCenter Auto Deploy para implementar hipervisores partiendo de equipos sin configurar y añadirlos a los clústeres existentes de forma automática

Más información

Información acerca de HPE OneView (página 23)

1.4.5 Gestión y aprovisionamiento de almacenamiento

HPE OneView proporciona aprovisionamiento automatizado y basado en políticas de recursos de almacenamiento admitidas. Está completamente integrado con los perfiles de servidor para que pueda gestionar su infraestructura de almacenamiento nueva o existente. Con HPE OneView puede ver y gestionar el sistema de almacenamiento y los pools de almacenamiento. Añade volúmenes existentes, crea otros nuevos y puede crear plantillas de volumen nuevos para aprovisionar varios volúmenes con la misma configuración.

Se admiten topologías SAN de estructura conmutada, direct attach y vSAN.

Al dispositivo se le agregan sistemas de almacenamiento y pools de almacenamiento seguidos de volúmenes, que están asociados con redes. A continuación, los volúmenes se pueden conectar con perfiles de servidor.

También puede agregar administradores de SAN para que sus SAN gestionadas estén disponibles para el dispositivo. Las SAN gestionadas pueden asociarse con redes Fibre Channel o Fibre Channel sobre Ethernet en el dispositivo para habilitar la distribución automática en zonas y la detección automática de conectividad.

Funciones de automatización de almacenamiento compatibles

Aprovisionamiento de almacenamiento automatizado

Cuando se importan sistemas de almacenamiento compatibles y pools de almacenamiento existentes, HPE OneView puede crear volúmenes rápidamente.

Distribución automática en zonas SAN

HPE OneView gestiona automáticamente la distribución en zonas SAN a través de las conexiones de volúmenes de los perfiles de servidor.

Integración de almacenamiento a través de perfiles de servidor

Agregue conexiones de volumen al perfil de servidor para crear y permitir el acceso a nuevos volúmenes privados al hardware del servidor.

Agregue conexiones de volumen al perfil de servidor para permitir el acceso a volúmenes privados o compartidos al hardware del servidor.

HPE OneView realiza un seguimiento del estado de la conexión entre los perfiles de servidor y las SAN.

Gestión de volúmenes

Puede utilizar HPE OneView para gestionar el ciclo de vida completo de sus volúmenes. Puede agregar volúmenes existentes, crear volúmenes nuevos, aumentar el tamaño de los volúmenes y quitar o eliminar volúmenes mediante HPE OneView.

También puede crear instantáneas de volúmenes, crear un volumen a partir de una instantánea y revertir un volumen a una instantánea mediante HPE OneView.

Directivas de distribución en zonas

HPE OneView le permite definir una directiva de distribución en zonas para sus SAN gestionadas. Puede elegir `single initiator/all targets` (iniciador único/todos los destinos), `single initiator/single storage system` (iniciador único/sistema de almacenamiento único) o `single initiator/single target` (iniciador único/destino único).

Nomenclatura y alias de zonas

HPE OneView utiliza una nomenclatura de zonas basada en reglas que le permite tener un control total de los nombres de sus zonas. Puede utilizar la nomenclatura de zonas para incorporar su estructura de nomenclatura actual, con objeto de que HPE OneView la use durante el proceso de distribución automática en zonas.

HPE OneView le permite crear alias para iniciadores, destinos y grupos de destinos, con objeto de que HPE OneView los muestre en lugar de sus WWPN.

Más información

Matriz de compatibilidad de HPE OneView
«Acerca de los sistemas de almacenamiento»
«Acerca de los administradores de SAN»

1.5 Funciones de gestión de firmware y de cambios de configuración

1.5.1 Gestión de firmware simplificada

HPE OneView proporciona una gestión de firmware rápida, fiable y sencilla en todo el dispositivo.

Cuando se agrega un recurso al dispositivo para gestionarlo, con objeto de garantizar la compatibilidad y un funcionamiento sin problemas, el dispositivo actualiza automáticamente el firmware del recurso a la versión mínima necesaria para poder gestionarlo.

NOTA: HPE OneView no gestiona el firmware de los recursos supervisados.

Un lote de firmware, también conocido como SPP (Service Pack para ProLiant), es un paquete comprobado de actualización de firmware, controladores y utilidades. Los lotes de firmware le permiten actualizar el firmware de los blades de servidor gestionados y la infraestructura (receptáculos e interconexiones).

Un repositorio de firmware en el dispositivo permite cargar lotes de firmware del SPP e implementarlos en todo el entorno siguiendo las prácticas recomendadas. Por ejemplo, es posible:

- Ver las versiones y el contenido de los lotes de firmware almacenados en el repositorio de firmware.
- Consulte la versión del firmware instalada en el hardware admitido desde el hardware de servidor.
- Establecer una línea de base de firmware; un estado deseado para las versiones de firmware; para un recurso gestionado, como un perfil de servidor o para un grupo de recursos, como por ejemplo, todas las interconexiones de una interconexión lógica.
- Detectar si un recurso gestionado no cumple con la línea de base de firmware.
- Identificar problemas de compatibilidad de firmware.
- Actualizar el firmware de un receptáculo completo.
- Actualizar el firmware de recursos individuales o de grupos de recursos, como las interconexiones lógicas.[1]

1. Los grupos de receptáculos no incluyen una línea de base de firmware, por lo que las actualizaciones del firmware de los receptáculos se gestionan a través de una configuración de receptáculo lógica.

- Actualizar el firmware y los controladores del sistema operativo.
- Quitar un lote de firmware del repositorio

En ocasiones, Hewlett Packard Enterprise publica revisiones para los componentes entre las versiones principales del SPP. Hewlett Packard Enterprise le notificará que hay una revisión disponible para cargarla y le proporcionará información detallada sobre el SPP al que se aplica. Existen distintos mecanismos para aplicar una revisión en HPE OneView.

1.5.2 Gestión de cambios de configuración simplificada

Los grupos y las plantillas simplifican la distribución de los cambios de configuración en el dispositivo. Por ejemplo:

- Puede reducir los errores haciendo varios cambios complejos en un grupo. A continuación, para cada miembro del grupo, puede utilizar una sola acción para actualizar la configuración con objeto de que coincida con la del grupo.
- El dispositivo le avisa cuando detecta que un equipo no se ajusta a la plantilla o al grupo actual. Usted controla si se actualiza la configuración de un dispositivo y cuándo.
- La configuración de las interconexiones lógicas gestionar el firmware de las interconexiones físicas para garantizar que todas las interconexiones del receptáculo lógico utilicen un firmware compatible.

1.6 Supervisión del entorno y respuestas a los problemas

Una sola interfaz de usuario

Se utiliza la misma interfaz para la supervisión que para aprovisionar recursos. No es necesario aprender herramientas ni interfaces adicionales.

Aislamiento de la red de gestión

La arquitectura del dispositivo está diseñada para separar el tráfico de gestión de la red de producción, lo que aumenta la fiabilidad y la seguridad de la solución global. Por ejemplo, los recursos del centro de datos siguen funcionando incluso en el improbable caso de que se interrumpa la alimentación del dispositivo.

Configuración automática para la supervisión del estado y la utilización

Cuando se agregan recursos al dispositivo, se configuran automáticamente para la supervisión de estado, actividad, alertas y utilización. Esto permite supervisar recursos inmediatamente sin realizar ningún paso de configuración o de detección adicional.

Gestión sin agentes y fuera de banda

Todos los procesos de supervisión y gestión de estado y utilización de los servidores HPE ProLiant Gen8 (o posteriores) se realizan sin agentes y fuera de banda para una mayor seguridad y fiabilidad. Para estos servidores:

- No existen agentes que deban vigilarse o actualizarse.
- El dispositivo no requiere abrir puertos SNMP en el sistema operativo host.
- El dispositivo no interactúa con el sistema operativo en el host, lo que libera recursos de memoria y procesador en el host para que los usen las aplicaciones del servidor, y permite supervisar servidores que no tienen instalado ningún sistema operativo host.

Gestión desde otras plataformas mediante las API de REST y los buses de mensajes

Las API de REST y el bus SCMB (State-Change Message Bus) o el bus MSMB (Metric Streaming Message Bus) también permiten supervisar el entorno de HPE OneView desde otras plataformas de gestión. Para obtener más información sobre los buses de mensajes, consulte «Uso de un bus de mensajes para enviar datos a los suscriptores» (página 357).

Supervisión del entorno y respuestas a los problemas

Las funciones siguientes permiten supervisar el entorno y responder a los problemas:

- La pantalla Dashboard (Panel de control) (página 346), que muestra una vista de resumen de la capacidad del centro de datos y la información de estado
- La pantalla Activity (Actividad) (página 340), que muestra y permite filtrar todas las tareas y alertas del sistema
- Gestión del entorno del centro de datos (página 34)
- Supervisión de la utilización de recursos (página 35)
- Gestión de la actividad y el estado (página 35)
- Información de inventario de hardware y firmware (página 36)

Más información

HPE iLO 4 con capturas AMS compatibles para emitir alertas en HPE OneView en **http://www.hpe.com/info/oneview/docs**

1.6.1 Gestión del entorno del centro de datos

HPE OneView integra estas áreas críticas para la gestión del entorno del centro de datos:

- Visualización de los datos de temperaturas en 3D
- Representación de la infraestructura de suministro de energía

- Ubicación de elementos físicos en 3D

Función	Descripción
Visualización de los datos de temperaturas	La representación en 3D de las temperaturas del centro de datos proporciona una vista del estado térmico de todo el centro de datos. El dispositivo recopila datos de temperaturas de los recursos gestionados de cada bastidor del centro de datos y presenta los datos de forma gráfica, lo que permite identificar fácilmente de los puntos calientes de un bastidor.
Representación de la infraestructura de suministro de energía	HPE OneView recopila el historial de temperaturas y energía y de uso de los procesadores para el hardware del centro de datos y genera informes con dichos datos. El dispositivo supervisa la energía, detecta e informa automáticamente sobre los errores de suministro de energía y proporciona información precisa sobre los requisitos de energía para los servidores HPE ProLiant Gen8 (o posteriores) y los receptáculos HPE BladeSystem; dicha información se puede utilizar para planificar el uso de los bastidores y la energía. Power Discovery Services permite detectar y visualizar automáticamente la topología de suministro de energía del centro de datos. Las iPDU de HPE le permiten al dispositivo representar automáticamente la topología de energía de los bastidores. El dispositivo detecta errores de cableado, como la falta de redundancia, y actualiza automáticamente el inventario eléctrico cuando se instalan nuevos servidores. El dispositivo también admite el control de alimentación de cada toma para apagar y volver a encender cada toma de la iPDU. Puede definir manualmente los requisitos y la topología de energía para los dispositivos que no son compatibles con Power Discovery Services.
Ubicación de elementos físicos	Location Discovery Services le permite al dispositivo mostrar automáticamente la ubicación exacta en 3D de los servidores HPE ProLiant Gen8 (o posteriores) ubicados en bastidores HPE Intelligent Series, lo que reduce la mano de obra y los costes operativos, y elimina los errores humanos relacionados con la gestión de activos y del inventario. Puede definir manualmente las posiciones de los bastidores y los dispositivos que no son compatibles con Location Discovery Services.

1.6.2 Supervisión de la utilización de recursos

HPE OneView recopila y conserva periódicamente información de uso de CPU para todos los servidores que gestiona. HPE OneView también recopila estadísticas en el ámbito de los puertos de red, incluyendo contadores de transmisión, recepción y errores. HPE OneView muestra todos estos datos en la interfaz de usuario y permite el acceso a ellos a través de las API de REST.

1.6.3 Gestión de la actividad y el estado

HPE OneView proporciona métodos sencillos de supervisión y gestión de actividades. El dispositivo registra automáticamente las alertas y las notificaciones de todos los recursos gestionados, y los recursos que se añaden al dispositivo están disponibles inmediatamente para supervisarlos y gestionarlos. Cuando el dispositivo avisa de un problema, siempre que sea posible sugiere una forma de corregirlo.

La interfaz de usuario y las API de REST le permiten:

- Ver todas las actividades (alertas y tareas) por descripción u origen, y filtrar las actividades utilizando varios criterios de filtro.
- Asignar alertas a determinados usuarios.
- Anotar actividades con las notas de los administradores, lo que permite a los administradores del centro de datos colaborar a través del dispositivo en lugar de a través de herramientas externas, como el correo electrónico.
- Ver las alertas de un recurso específico desde la pantalla de la interfaz de usuario de ese recurso o mediante la API de REST de ese recurso.

- Reenviar automáticamente capturas SNMP desde los recursos gestionados a las consolas de supervisión empresarial o a recopiladores de capturas SNMP centralizados.

Más información

HPE iLO 4 con capturas AMS compatibles para emitir alertas en HPE OneView en **http://www.hpe.com/info/oneview/docs**

1.6.4 Información de inventario de hardware y firmware

HPE OneView proporciona información detallada sobre el inventario de hardware y firmware de los recursos que gestiona. Puede acceder a los siguientes datos a través de la interfaz de usuario y las API de REST:

- Vistas detalladas y resumidas del hardware gestionado, como servidores, receptáculos, e interconexiones.
- Resumen del hardware supervisado, como por ejemplo, servidores y receptáculos.
- Vistas detalladas y resumidas del contenido de los lotes de firmware.
- Inventario de firmware para los componentes de servidores y receptáculos.

Puede utilizar la función Smart Search (Búsqueda inteligente) de la interfaz de usuario para buscar elementos específicos en el inventario.

Existen informes que pueden ayudarle a supervisar el inventario y el entorno. Los informes de inventario proporcionan información sobre los servidores o receptáculos, como por ejemplo, modelo, número de serie, número de referencia, etc. Otros informes ofrecen una visión del estado general del entorno.

1.6.5 Soporte remoto

HPE OneView ofrece soporte remoto a los socios registrados para permitir la creación automática de casos para fallos de hardware en los servidores y los receptáculos y para activar **Proactive Care**. Cuando se activa, todos los dispositivos aptos que se agreguen en el futuro se habilitarán automáticamente para el soporte remoto.

Hewlett Packard Enterprise se pondrá en contacto con usted para enviarle una pieza de recambio o enviarle a un ingeniero para los dispositivos en garantía o dentro de un contrato de soporte.

Remote support habilita los servicios de Proactive Care, incluidos los informes de Proactive Scan y Firmware/Software Analysis con recomendaciones basadas en los datos de configuración recopilados.

Más información

«Sobre el soporte remoto»

1.7 Funciones de copia de seguridad y restauración

HPE OneView ofrece servicios para realizar una copia de seguridad de un dispositivo en un archivo y para restaurar un dispositivo desde un archivo de copia de seguridad. Las copias de seguridad pueden configurarse para llevarse a cabo de forma automática y almacenarse remotamente.

Un archivo de copia de seguridad de propiedad para el dispositivo y su base de datos

Los archivos de copia de seguridad de propiedad y contienen parámetros de configuración y datos de gestión, por lo que no hay necesidad de crear copias de seguridad separadas para el dispositivo y su base de datos.

Hewlett Packard Enterprise no recomienda el uso de capturas de VM para proteger el dispositivo. Se pueden producir errores de sincronización que pueden resultar en un comportamiento impredecible y no deseado.

Programación flexible y una interfaz abierta para las operaciones de copia de seguridad

Puede crear archivos de copia de seguridad mientras el dispositivo está en línea. Además, puede utilizar las API de REST para:

- Programar un proceso de copia de seguridad desde fuera del dispositivo.
- Recopilar archivos de copia de seguridad de acuerdo con las directivas de la organización.
- Realizar la integración con los productos de copia de seguridad y restauración de la empresa.
- Utilizar secuencias de comandos de copia de seguridad y restauración.

Un archivo de copia de seguridad es una instantánea de la configuración y los datos de gestión del dispositivo en el momento en que se crea la copia de seguridad. Hewlett Packard Enterprise recomienda crear copias de seguridad regulares, preferiblemente una vez al día, y después de realizar cambios de configuración de hardware o de software en el entorno gestionado.

Rol de usuario especializado para la creación de archivos de copia de seguridad

HPE OneView proporciona un rol de usuario (Administrador de copia de seguridad) específicamente para realizar copias de seguridad del dispositivo; este rol permite acceder a otras vistas de recursos, pero no realizar acciones con esos recursos, ni otras tareas.

Recuperación de fallos catastróficos

Puede realizar la recuperación cuando se produzca un fallo catastrófico restaurando el dispositivo desde el archivo de copia de seguridad.

Al restaurar un dispositivo desde un archivo de copia de seguridad, todos los datos de gestión y la mayoría de los parámetros de configuración del dispositivo se sustituyen por los datos y la configuración del archivo de copia de seguridad, incluyendo cosas como los nombres de usuario y contraseñas, registros de auditoría y redes disponibles.

Es probable que el estado del entorno gestionado sea diferente del que tenía en el momento en que se creó el archivo de copia de seguridad. Durante una operación de restauración, el dispositivo combina los datos del archivo de copia de seguridad con el estado actual del entorno gestionado. Después del operación de restauración, el dispositivo utiliza alertas para informar sobre cualquier discrepancia que no pueda resolver de forma automática.

Más información

«Copia de seguridad de un dispositivo» (página 307)

1.8 Funciones de seguridad

CATA (Comprehensive Applications Threat Analysis) es una potente herramienta de evaluación de calidad de la seguridad de Hewlett Packard Enterprise diseñada para reducir sustancialmente el número de defectos de seguridad latentes. El diseño del dispositivo HPE OneView se basó en los principios de CATA y se sometió a revisión siguiendo las directrices de CATA. Para garantizar una plataforma segura para la gestión de centros de datos, el dispositivo incluye funciones como las siguientes:

- Separación de los entornos de datos y de gestión, lo cual es fundamental para evitar la pérdida de control cuando se producen ataques de Denegación de servicio. Por ejemplo, el dispositivo está diseñado para funcionar completamente en una LAN de gestión aislada;

no se requiere acceso a la LAN de producción. Los dispositivos gestionados permanecen en línea en el improbable caso de que se interrumpa la alimentación del dispositivo.

- RBAC (control de acceso basado en roles), que permite a un administrador establecer rápidamente la autenticación y autorización de usuarios en función de sus responsabilidades con respecto a recursos específicos. El RBAC también simplifica lo que se muestra en la interfaz de usuario:
  - Los usuarios solo pueden ver los recursos para los que disponen de autorización. Por ejemplo, el dispositivo no muestra a los usuarios con el rol Administrador de redes las pantallas que no les corresponden, como **Server Profiles** (Perfiles de servidor) y **Server Hardware** (Hardware de servidor).
  - Los usuarios solo pueden iniciar acciones con los recursos para los que disponen de autorización. Por ejemplo, los usuarios con el rol de administrador de red solo pueden iniciar acciones con recursos de red, y los usuarios con el rol de administrador de servidores solo pueden iniciar acciones con recursos de servidor.
  - Los usuarios con el rol de administrador de infraestructuras tienen acceso completo a todas las pantallas y a todas las acciones.
- Onboard Administrator e iLO de inicio de sesión único sin guardar las credenciales creadas por el usuario de iLO y Onboard Administrator.
- Registro de auditoría para todas las acciones de los usuarios.
- Compatibilidad con la autenticación y autorización mediante un servicio de directorio opcional, como Microsoft Active Directory.
- Uso de certificados para la autenticación a través de Transport Layer Security (TLS).
- Cortafuegos que permite el tráfico en puertos específicos y bloquea todos los puertos no utilizados.
- Interfaz de usuario que restringe el acceso de los usuarios del sistema operativo host.
- Descargas de datos restringidas a los archivos de volcado de soporte (cifrados de forma predeterminada), archivos de copia de seguridad de propiedad, registros de auditoría y certificados.
- Una función de copia de seguridad automatizada que le permite configurar el día y la hora en la que se realizará una copia de seguridad y la capacidad de especificar un servidor SSH o SFTP remoto para almacenar automáticamente los archivos de la copia de seguridad.

Más información

«Información sobre las funciones de seguridad del dispositivo» (página 69)

1.9 Funciones de alta disponibilidad

HPE OneView se distribuye como un dispositivo virtual preconfigurado listo para implementarlo en un host del hipervisor. El software hipervisor proporciona una máquina virtual con capacidades de alta disponibilidad y recuperación que permiten reiniciar la máquina virtual en otro host del clúster y reanudar la gestión sin interrupciones en los recursos gestionados.

1.10 Interfaces gráfica y de programación

HPE OneView fue desarrollado para utilizar un modelo de recursos único y coherente integrado en una interfaz de usuario HTML5 rápida, moderna y escalable, así como las API de REST estándar del sector para permitir el acceso móvil seguro y la integración abierta con otro software de gestión.

Interfaz de usuario: eficiencia y simplicidad por diseño

La interfaz de usuario está diseñada para adaptarse a su forma de trabajar, y proporciona herramientas potentes y fáciles de usar, como las siguientes:

Función	Descripción
Pantalla Dashboard (Panel de control)	Proporciona una representación gráfica del estado general y la capacidad de los recursos del centro de datos. En **Dashboard** (Panel de control) puede ver inmediatamente las áreas que requieren su atención.
Vista Map (Mapa)	Disponible para cada recurso, la vista **Map** (Mapa) permite examinar la configuración y entender las relaciones entre los recursos lógicos y físicos del centro de datos.
Cuadro Smart Search (Búsqueda inteligente)	En la barra superior de cada pantalla se incluye la función Smart Search (Búsqueda inteligente), que le permite encontrar información sobre recursos específicos, como determinados nombres de recursos, números de serie, WWN y direcciones IP y MAC.
Vista Labels (Etiquetas)	La vista **Labels** (Etiquetas) permite organizar los recursos en grupos; por ejemplo, puede que desee identificar los servidores utilizados principalmente por el equipo financiero o los sistemas de almacenamiento asignados a la división de Asia Pacífico.
Vista Scopes (Ámbitos)	Una agrupación de recursos que se puede utilizar para limitar el alcance de una operación o acción. Los recursos se organizan por categorías. Todos los recursos de estas categorías se pueden agregar o eliminar de un ámbito, incluidos receptáculos, hardware de servidor, redes, conjuntos de redes, interconexiones, conmutadores, conmutadores lógicos, grupos de conmutadores lógicos, interconexiones lógicas y grupos de interconexiones lógicas.
Fuente Activity (Actividad)	La fuente **Activity** (Actividad) le ofrece una perspectiva única del estado del entorno, intercalando las tareas, alertas y notas del administrador en una sola vista. La fuente **Activity** (Actividad) simplifica la correlación entre la actividad del usuario y el estado del sistema, lo que permite dar una respuesta oportuna a los problemas.
Pantallas de gestión específicas del recurso	Estas pantallas le permiten concentrarse en los recursos que puede ver y gestionar con los permisos que tiene. La pantalla Resource Group (Grupos de recursos) mejora la capacidad de ampliación, ya que permite gestionar varios recursos como uno solo.

La interfaz de usuario proporciona sugerencias y consejos en pantalla para ayudarle a evitar y corregir errores, y proporciona enlaces para obtener más información acerca de las tareas. En la parte superior de cada pantalla, el icono de ayuda le da acceso a todo el sistema de ayuda.

API de REST: automatización e integración

HPE OneView tiene una arquitectura orientada a recursos que proporciona una interfaz REST uniforme.

Las API de REST:

- Proporcionan una interfaz estándar del sector para la integración abierta con otras plataformas de gestión.
- Están diseñadas para ser omnipresentes: cada recurso tiene un URI (Uniform Resource Identifier) y representa un dispositivo físico o una construcción lógica.
- Le permiten automatizar cualquier cosa que pueda hacer desde la interfaz de usuario mediante su lenguaje de programación o de secuencias de comandos favorito.
- Están diseñadas para admitir una gran capacidad de ampliación.

Más información

Capítulo 4, «Navegación por la interfaz gráfica de usuario»
«Acceso a la documentación y la ayuda» (página 115)
Ayuda sobre secuencias de comandos de la API de HPE OneView REST

1.11 Integración con otro software de gestión

Para utilizar el software de gestión integrado indicado en esta sección, deberá adquirir licencias HPE OneView Advanced. Para obtener más información, consulte «Acerca de las licencias».

Onboard Administrator para receptáculos HPE BladeSystem c7000

HPE OneView interactúa perfectamente con el Onboard Administrator para proporcionar una gestión completa de los receptáculos BladeSystem c7000. Los privilegios del Onboard Administrator vienen determinados por el rol asignado a su cuenta de usuario de HPE OneView.

HPE Integrated Lights-Out

HPE OneView interactúa perfectamente con el procesador de gestión de iLO para proporcionar una gestión completa del hardware de servidor. HPE OneView configura automáticamente iLO de acuerdo con la configuración especificada por el perfil de servidor de HPE OneView. HPE OneView configura un acceso transparente a la consola remota gráfica de iLO, lo que le permite iniciar la consola remota de iLO desde la interfaz de usuario de HPE OneView con un solo clic. Los privilegios de iLO están determinados por el rol asignado a su cuenta del dispositivo HPE OneView.

HPE Insight Control

Las licencias completas de HPE OneView Advanced incluyen el derecho de utilizar HPE Insight Control, que proporciona funciones esenciales de gestión de infraestructuras. Insight Control puede ahorrarle tiempo y dinero, ya que simplifica la implementación, migración, supervisión y optimización de su infraestructura de TI a través de una sola consola de gestión sencilla para los servidores ProLiant ML/DL/SL y BladeSystem. Puede optar por utilizar HPE OneView o la licencia correspondiente para HPE Insight Control para gestionar dispositivos. No es necesario adquirir dos licencias para el mismo servidor. Sin embargo, no se pueden utilizar las licencias de HPE OneView e Insight Control para gestionar el mismo servidor al mismo tiempo. Insight Control Server Provisioning constituye una excepción. Puede utilizarse simultáneamente con HPE OneView para gestionar el mismo servidor.

HPE Insight Control no se incluye en los soportes ni la descarga de HPE OneView, pero se puede descargar desde **http://www.hpe.com/servers/software/insightupdates** con la clave de licencia de HPE Insight Control suministrada durante el proceso de concesión o cumplimiento.

HPE Insight Control Server Provisioning.

HPE OneView Advanced incluye el derecho a utilizar Insight Control Server Provisioning, una función para el aprovisionamiento físico del sistema operativo en varios servidores y para la configuración de servidores. El software de Insight Control Server Provisioning no se incluye en los soportes de HPE OneView, pero se puede descargar desde **http://www.hpe.com/servers/software/insightupdates**.

HPE OneView para Microsoft System Center

HPE OneView Advanced incluye el derecho a utilizar HPE OneView para Microsoft System Center. HPE OneView para Microsoft System Center integra plenamente el ecosistema de gestión de HPE en Microsoft System Center, y proporciona capacidades como la supervisión proactiva y la gestión y aprovisionamiento remotos de almacenamiento, redes y servidores HPE. HPE OneView para Microsoft System Center puede descargarse desde **http://www.hpe.com/products/ovsc**.

HPE OneView para VMware vCenter

HPE OneView Advanced incluye el derecho de utilizar HPE OneView para VMware vCenter, HPE OneView para VMware vCenter/vRealize Operations y HPE OneView para VMware vCenter

Log Insight. HPE OneView para VMware integra plenamente el ecosistema de gestión de HPE para proporcionar capacidades como la supervisión proactiva, la solución de problemas importantes, la gestión y el aprovisionamiento remotos de almacenamiento, redes y servidores HPE. Las integraciones de HPE OneView con VMware pueden descargarse desde **http://www.hpe.com/products/ovvcenter**.

1.11.1 Otros mensajes de advertencia del software de gestión

No utilice gestores externos, como por ejemplo, HPE Systems Insight Manager (SIM) o software de gestión de otros fabricantes, para gestionar el hardware incluido en la gestión con HPE OneView. El uso de otro gestor externo puede provocar errores y un comportamiento inesperado. Por ejemplo: iLO tiene un máximo de tres destinos de captura, uno de los cuales es HPE OneView. Si los gestores externos definen destinos de captura adicionales, iLO eliminará uno de los destinos de captura existentes. Si OneView HPE es el destino de captura que elimina iLO, HPE OneView dejará de recibir capturas de SNMP y dejará de mostrar el estado del servidor y las alertas del ciclo de vida.

NOTA: Las herramientas de otros fabricantes no ofrecen advertencias, así que úselas con cuidado en caso de que estas realicen o tengan que realizar cambios en el servidor.

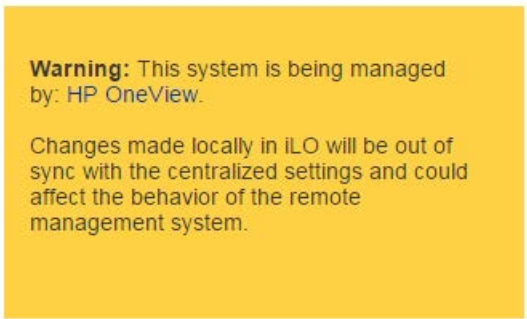
Si intenta modificar un recurso gestionado por HPE OneView con otras herramientas de gestión de HPE como ROM-Based Setup Utility (RBSU), aparecerá un mensaje de advertencia.

- Si intenta modificar el firmware del servidor utilizando SUM y la línea de base de firmware asociada con el perfil de servidor de dicho servidor no está configurada como `Managed manually (Gestionado manualmente)`, SUM mostrará una advertencia:

  `HPE OneView gestiona el servidor y está configurado para el Service Pack para ProLiant versión x. No se puede actualizar directamente a otra versión utilizando SUM.`

- Si HPE OneView gestiona el iLO, en la pantalla de inicio de sesión de iLO aparecerá una advertencia.

  Figura 1 Advertencia de iLO



- Si intenta realizar cambios en BIOS o iLO en Intelligent Provisioning, aparecerá una advertencia.

Más información

https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA5-6605ENW.pdf

1.12 Integración abierta

El modelo de recursos único y coherente, las API de REST, el SCMB (State-Change Message Bus) y el MSMB (Metric Streaming Message Bus) permiten utilizar secuencias de comandos

para integrar HPE OneView con otras aplicaciones empresariales para satisfacer las necesidades del usuario y realizar tareas tales como:

- Automatizar flujos de trabajo estándar y pasos de solución de problemas
- Automatizar la integración con otros programas, como una CMDB (base de datos de gestión de contenido)
- Conectar con departamentos de servicio técnico
- Supervisar recursos, recopilar datos y crear mapas y modelos de sistemas
- Exportar datos a formatos que se adapten a sus necesidades
- Conectar con bases de datos, almacenes de datos o herramientas de inteligencia empresarial de otros fabricantes personalizadas
- Realizar la integración de personalizaciones de usuario internas

El bus SCMB es una interfaz que utiliza la mensajería asíncrona para notificar a los suscriptores los cambios en los recursos gestionados, tanto lógicos como físicos. Por ejemplo, puede programar aplicaciones para recibir notificaciones cuando se añade nuevo hardware de servidor al entorno gestionado o cuando cambia el estado de los recursos físicos, sin tener que sondear continuamente el dispositivo para conocer el estado mediante las API de REST.

Más información

Ayuda sobre secuencias de comandos de la API de HPE OneView REST
«Uso de un bus de mensajes para enviar datos a los suscriptores» (página 357)

1.13 Funciones de red

- Redes compatibles
- Interconexiones lógicas
- Grupo de interconexiones lógicas
- Conjunto de redes
- Conmutadores
- Logical switches (Conmutadores lógicos)
- Logical switch groups (Grupos de conmutadores lógicos)

HPE OneView ofrece diversas funciones de red para optimizar el aprovisionamiento de recursos de red para blades de servidor y gestionar los cambios de configuración, incluidas las actualizaciones de firmware, en los módulos de interconexión de Virtual Connect.

Redes compatibles

Los módulos de interconexión de Virtual Connect de los receptáculos admiten los siguientes tipos de redes de centros de datos:

- Ethernet para las redes de datos, incluidas las redes etiquetadas, sin etiquetar o de túnel.
- Fibre Channel para las redes de almacenamiento, que pueden ser conexiones Fibre Channel Fabric attach (con un conmutador SAN) y conexiones Fibre Channel Direct attach (de conexión directa o Flat SAN) con sistemas de almacenamiento 3PAR compatibles.
- Fibre Channel sobre Ethernet (FCoE) para redes de almacenamiento cuyo tráfico de almacenamiento se lleva a través de una VLAN Ethernet dedicada.

Interconexiones lógicas

Una interconexión lógica es el conjunto de interconexiones físicas y sus enlaces, e incluye lo siguiente:

- Enlaces ascendentes a las redes del centro de datos conforme a las asignaciones de sus conjuntos de enlaces ascendentes
- Enlaces descendentes a los servidores
- Redes internas
- Enlaces de apilamiento (conexiones entre ellos)

Más información

Capítulo 1, «Información acerca de HPE OneView»
Migración de una configuración de Virtual Connect a HPE OneView

1.14 Funciones de HPE Smart Update Tools

HPE Smart Update Tools (SUT) es una utilidad de sistema operativo para HPE OneView que permite que un administrador lleve a cabo actualizaciones de controladores y firmware en línea. SUT consulta HPE OneView cada cinco minutos en busca de solicitudes nuevas, las procesa y le da un estado a HPE OneView. HPE OneView publica el proceso en la sección **Firmware** de la página **Server Profile** (Perfil de servidor). SUT instala las actualizaciones en el orden correcto y se asegura de que se cumplan todas las dependencias antes de iniciar una actualización. Cuando hay dependencias no satisfechas, SUT evita la instalación y avisa al administrador de HPE OneView de que la instalación no puede continuar debido a una dependencia.

Características principales:

- Actualizaciones combinadas de controladores, software y firmware.
- Generación de informes de cumplimiento en el panel de HPE OneView basada en el estado recibido de SUT.
- Aumento al máximo posible el tiempo de funcionamiento al reducir al mínimo el número de reinicios necesarios para la activación.
- Capacidad de efectuar el almacenamiento provisional de firmware y tareas de desarrollo fuera de la ventana de mantenimiento real, de forma que un reinicio durante la ventana de mantenimiento activa actualizaciones tanto de firmware como de controladores.
- Roles de usuario múltiples:
  - Administrador de infraestructuras de HPE OneView, que define el estado deseado mediante las opciones de firmware del perfil de servidor
  - Administrador de SUT que utiliza SUT para actualizar el firmware y el software del servidor
- Control manual y distintos niveles de automatización:
  - Actualizaciones a petición o manuales
  - Semiautomática, cuando el almacenamiento provisional es automático o la instalación y el almacenamiento provisional son automáticos.
  - Actualización completamente automática

  NOTA: SUT requiere HPE iLO 2.30 y versiones posteriores para funcionar correctamente. Si HPE OneView gestiona el firmware del servidor, HPE OneView actualiza automáticamente el firmware de iLO para permitir que SUT proceda.

Más información

Apéndice D, «Instalación de HPE Smart Update Tools con HPE Insight Control server provisioning»

2 Conceptos básicos sobre el modelo de recursos

HPE OneView utiliza un modelo de recursos que reduce la complejidad y simplifica la gestión del centro de datos. Este modelo ofrece recursos lógicos, como plantillas, grupos y conjuntos, que, cuando se aplican a los recursos físicos, proporcionan una estructura común para todo el centro de datos.

La interfaz de usuario distingue entre los recursos físicos y virtuales mediante el uso de ciertas acciones. Por ejemplo:

- Es posible *crear*, *eliminar*, o copiar un recurso lógico, pero no un recurso físico
- Es posible *agregar* o *quitar* un recurso físico

Información general de alto nivel

- Diagrama de resumen del modelo de recursos (página 46)

Recursos de servidor

- Plantillas de perfiles de servidor (página 63)
- Perfiles de servidor (página 62)
- Conexiones (página 47)
- Plantillas de conexión (página 48)
- Hardware de servidor (página 60)
- Tipos de hardware de servidor (página 62)

Recursos de aprovisionamiento de red

- Grupos de receptáculos (página 50)
- Tipos de receptáculos (página 51)
- Receptáculos (página 50)
- Tipos de interconexiones (página 52)
- Interconexiones (página 51)
- Receptáculos lógicos (página 53)
- Grupos de interconexiones lógicas (página 55)
- Interconexiones lógicas (página 53)
- Logical switches (Conmutadores lógicos) (página 56)
- Logical switch groups (Grupos de conmutadores lógicos) (página 57)
- Conmutadores (página 65)
- Conjuntos de enlaces ascendentes (página 66)

Recursos de red

- Redes (página 57)
- Conjuntos de redes (página 57)

Recursos de almacenamiento

- Sistemas de almacenamiento (página 65)
- Pools de almacenamiento (página 64)
- Volúmenes (página 67)
- Plantillas de volumen (página 68)
- Administradores de SAN (página 59)
- Redes SAN (página 60)

Recursos del dispositivo

- Dispositivo (página 46)
- Dominios (página 49)

Recursos de gestión de energía y refrigeración del centro de datos

- Centros de datos (página 48)
- Bastidores (página 59)
- Dispositivos de suministro de energía (página 58)
- Equipos no gestionados (página 66)

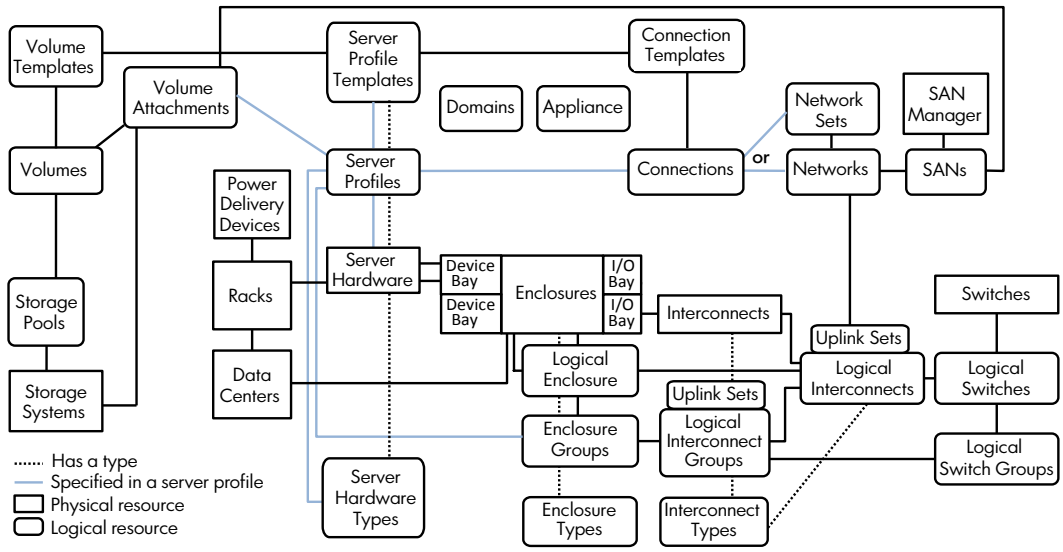
Más información

- Para obtener una lista completa de recursos, consulte la *Referencia de la API de REST de HPE OneView* en la ayuda en línea.
- Para obtener información sobre el uso de HPE OneView, consulte el resto de los capítulos de esta guía y la ayuda en línea.

2.1 Diagrama de resumen del modelo de recursos

En la figura siguiente se resumen algunos de los recursos más utilizados y se muestran las relaciones entre ellos.

Figura 2 Diagrama de resumen del modelo de recursos



La interfaz de usuario y las API de REST están organizadas por recursos. La documentación de la interfaz de usuario y las API de REST también está organizada por recursos.

La lista completa de recursos se incluye en la *Referencia de la API de REST de HPE OneView* de la ayuda en línea.

En las secciones siguientes se presentan los recursos mostrados en la Figura 2: Diagrama de resumen del modelo de recursos (página 46).

Más información

Conceptos básicos sobre el modelo de recursos (página 45)

2.2 Dispositivo

El recurso de dispositivo define los detalles de configuración específicos del dispositivo HPE OneView (a diferencia de los recursos gestionados por HPE OneView).

Relación con otros recursos

Un recurso de dispositivo está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Un único dominio
- Cero o más instancias de los demás recursos del diagrama de resumen (página 46)

Pantallas de la interfaz de usuario y recursos de la API de REST

Varios recursos de la API de REST están relacionados con el dispositivo y con la configuración del dispositivo. Consulte los recursos de las siguientes categorías de la *Referencia de la API de REST de HPE OneView* de la ayuda en línea:

Pantalla de la interfaz de usuario	Recurso de la API de REST

Settings (Configuración)	• Configuración de hora, regional y zona horaria del dispositivo
	`appliance/configuration/timeconfig/locales`
	`appliance/configuration/time-locale`
	• Cadena de comunidad de lectura del dispositivo
	`appliance/device-read-community-string`
	• Restablecimiento del dispositivo a la configuración de fábrica
	`dispositivo`
	• Actualización o uso de parche en el firmware del dispositivo
	`appliance/firmware`
	• Estado de los componentes del dispositivo
	`appliance/health-status`
	• Configuración y obtención de la información de red del dispositivo
	`appliance/network-interfaces`
	• Apagado o reinicio de un dispositivo
	`appliance/shutdown`
	• Generación y descarga de soporte de volcados de soporte de un dispositivo
	`appliance/support-dumps`
	• Destinos de captura en el dispositivo de gestión
	`appliance/trap-destinations`

Licencia de OneView	• Estado del contrato de licencia de usuario final (CLUF) y datos relacionados `appliance/eula`

Más información

Gestión del dispositivo (página 321)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.3 Conexiones

Una conexión es la representación lógica de una conexión entre un servidor y una red o un conjunto de redes. Las conexiones se pueden configurar en los perfiles de servidor. Una conexión especifica lo siguiente:

- La red o el conjunto de redes al que se va a conectar el servidor
- Reemplazos de configuración (tales como un cambio en el ancho de banda preferido) que deben hacerse en la configuración predeterminada de la red o el conjunto de redes que se ha especificado
- Orden de arranque

Relación con otros recursos

Un recurso de conexión está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Un único recurso de perfil de servidor.
- Un único recurso de plantilla de conexión.
- Un único recurso de red o conjunto de redes. Los recursos que están disponibles para una conexión dependen de la configuración de la interconexión lógica del receptáculo que contiene el hardware de servidor.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recursos de la API de REST
Server Profiles (Perfiles de servidor)	`connections` y `server-profiles`

Más información

Acerca de los perfiles de servidor (página 179)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.4 Plantillas de conexión

Una plantilla de conexión define características de configuración predeterminadas, tales como el ancho de banda preferido y el ancho de banda máximo, para una red o un conjunto de redes. Cuando se crea una red o un conjunto de redes, HPE OneView crea una plantilla de conexión predeterminada para la red o el conjunto de redes.

Relación con otros recursos

Un recurso de plantilla de conexión está asociado a cero o más recursos de conexión. Un recurso de conexión está asociado a la plantilla de conexión adecuada para un tipo de red o de conjunto de redes.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST	Notas
No hay	`connection-templates`	La interfaz de usuario no muestra ni hace referencia a las plantillas de conexión, pero estas determinan los valores predeterminados que se muestran para la conexión cuando se selecciona una red o un conjunto de redes.

Más información

Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.5 Centros de datos

En HPE OneView, un centro de datos representa un área físicamente contigua en la que se encuentran los bastidores que contienen los equipos informáticos, tales como servidores, receptáculos y dispositivos. Un centro de datos se crea para describir una parte de una sala de informática para resumir un entorno y sus requisitos térmicos y eléctricos. Un recurso de centro

de datos a menudo es una parte de un centro de datos completo, y puede incluir equipos que no están gestionados por HPE OneView. Al representar la distribución física de los equipos del centro de datos, incluidos los dispositivos no gestionados, puede utilizar la información detallada de supervisión proporcionada para la planificación del espacio y para determinar los requisitos de energía y refrigeración.

En HPE OneView puede:

- Ver un modelo en 3D del diseño del centro de datos que incluye un sistema con códigos de colores para ayudarle a identificar las áreas que están demasiado calientes o demasiado frías.
- Ver los datos del historial de temperaturas.
- Localizar con más facilidad dispositivos específicos para realizar en ellos tareas de servicio técnico.

Relación con otros recursos

Un recurso de centro de datos está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más bastidores

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Centros de datos	`datacenters`

Más información

Gestión del centro de datos (página 276)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.6 Dominios

El recurso de dominio describe el dominio de gestión del dispositivo. Todos los recursos físicos y lógicos gestionados por el dispositivo forman parte de un único dominio de gestión.

Relación con otros recursos

Un recurso de dominio está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Un único dispositivo
- Cero o más instancias de los demás recursos del diagrama de resumen (página 46)

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST	Notas
No hay	`dominios`	La interfaz de usuario no muestra ni hace referencia a los dominios, pero el recurso de dominio proporciona información acerca de los límites, como el número total de redes que se pueden agregar al dispositivo. Puede utilizar la API de REST `domains` para obtener información sobre el dominio.

Más información

Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.7 Receptáculos

Un receptáculo es una estructura física con compartimentos de dispositivo que admiten elementos de servidor, conexión de red y almacenamiento. Estos elementos constitutivos comparten la infraestructura común de gestión, refrigeración y alimentación del receptáculo.

El receptáculo proporciona las conexiones de hardware entre los enlaces descendentes de interconexión y los servidores instalados. Las interconexiones del receptáculo proporcionan los enlaces ascendentes físicos a las redes del centro de datos.

Cuando se agrega un receptáculo para gestionarlo, HPE OneView detecta y agrega todos los componentes que contiene el receptáculo, incluyendo las interconexiones y servidores que tenga instalados.

Relación con otros recursos

Un recurso de receptáculo está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Un receptáculo lógico
- Un único grupo de receptáculos
- Cero o más interconexiones físicas
- Una o varias interconexiones lógicas y uno o varios grupos de interconexiones lógicas (a través de la asociación del receptáculo con un grupo de receptáculos e interconexiones)
- Cero o un recurso de bastidor
- Cero o más dispositivos de suministro de energía

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Receptáculos	`receptáculos`

Más información

Gestión de receptáculos (página 235)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.8 Grupos de receptáculos

Un grupo de receptáculos es una plantilla que define una configuración coherente para un receptáculo lógico. La conectividad de red de un grupo de receptáculos se define mediante el grupo de interconexiones lógicas asociado con el grupo de receptáculos.

Mediante el uso de grupos de receptáculos, se pueden agregar rápidamente muchos receptáculos y configurarlos con receptáculos lógicos idénticos.

Relación con otros recursos

Un recurso de grupo de receptáculos está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más receptáculos lógicos

- Cero o más perfiles de servidor
- Cero o más grupos de interconexiones lógicas

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Enclosure Groups (Grupos de receptáculos)	`enclosure-groups`

Más información

Gestión de grupos de receptáculos (página 255)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.9 Tipos de receptáculos

Un tipo de receptáculo define las características de un modelo específico de hardware de receptáculo de Hewlett Packard Enterprise, como un receptáculo HPE BladeSystem c7000.

Relación con otros recursos

Un recurso de tipo de receptáculo está asociado a cero o más recursos de receptáculos.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST	Notas
Ninguna	Ninguno	La interfaz de usuario no hace referencia al tipo de receptáculo, pero HPE OneView utiliza el tipo de receptáculo cuando se agrega uno. El recurso de REST `enclosures` incluye un atributo `enclosureType`.

Más información

Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.10 Interconexiones

Una interconexión es un recurso físico que permite la comunicación entre el hardware del receptáculo y las redes LAN Ethernet y SAN Fibre Channel del centro de datos. Un módulo Virtual Connect FlexFabric de 10 Gb y 24 puertos es un ejemplo de interconexión compatible. Para obtener una lista de las bases de datos admitidas, consulte la ***Matriz de compatibilidad de HPE OneView***.

Una interconexión tiene los siguientes tipos de puertos:

Tipo de puerto	Descripción
Enlaces ascendentes	Los enlaces ascendentes son puertos físicos que conectan la interconexión con las redes del centro de datos. Por ejemplo, el puerto X2 de un módulo Virtual Connect FlexFabric de 10 Gb y 24 puertos es un enlace ascendente.
Enlaces descendentes	Los enlaces descendentes son puertos físicos que conectan la interconexión con el hardware de servidor a través del plano medio del receptáculo.
Enlaces de apilamiento	Los enlaces de apilamiento son puertos físicos internos o externos que unen interconexiones para proporcionar rutas redundantes para el tráfico Ethernet entre los servidores y las redes del centro de datos. Los enlaces de apilamiento se basan en la configuración del grupo de interconexiones lógicas asociado.

En el modelo de recursos:

Relación con otros recursos

Un recurso de interconexión está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Un único receptáculo
- Cero o más interconexiones lógicas y, a través de esa interconexión lógica, uno o varios grupos de interconexiones lógicas

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recursos de la API de REST
Interconnects (Interconexiones)	`interconnects`, `interconnect-types` y `logical-interconnects`

Más información

Gestión del hardware de interconexión del receptáculo (página 209)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.11 Tipos de interconexiones

El recurso de tipo de interconexión define las características de un modelo de interconexión como las siguientes:

- Capacidades de enlace descendente y el número de puertos de enlace descendente
- Capacidades de enlace ascendente y el número de puertos de enlace ascendente
- Versiones de firmware compatibles

Relación con otros recursos

Un recurso de tipo de interconexión está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más interconexiones

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST	Notas
Interconexiones	`interconnect-types`	La interfaz de usuario no muestra ni hace referencia específicamente al recurso de tipo de interconexión, pero HPE OneView utiliza la información cuando se agrega o se gestiona una interconexión con la pantalla **Interconnects** (Interconexiones).

Más información

Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.12 Receptáculos lógicos

Un receptáculo lógico representa una vista lógica de un único receptáculo con un grupo de receptáculos que actúa como plantilla. Si la configuración prevista en el receptáculo lógico no coincide con la configuración real del receptáculo, el receptáculo lógico pasa a ser incoherente.

Cuando se agrega un receptáculo c7000, se crea automáticamente un receptáculo lógico.

Relación con otros recursos

Un recurso de receptáculo lógico está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Un receptáculo y, a través del receptáculo, un grupo de receptáculos

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Logical Enclosures (Receptáculos lógicos)	`logical-enclosures`

Más información

Gestión de receptáculos lógicos (página 256)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.13 Interconexiones lógicas

Una interconexión lógica es una sola entidad que representa múltiples interconexiones físicas

Una interconexión lógica es una sola entidad administrativa que consta de la configuración de un conjunto de interconexiones de un receptáculo. Esta configuración incluye:

- Interconexiones, que son necesarias para que el receptáculo pueda conectarse a las redes del centro de datos.
- Conjuntos de enlaces ascendentes, que asignan las redes del centro de datos a los puertos de enlace ascendente físicos. Si no se definen conjuntos de enlaces ascendentes, la interconexión lógica no se puede conectar a las redes del centro de datos, y los servidores conectados a los enlaces descendentes de la interconexión lógica no se pueden conectar a las redes del centro de datos.

- Puertos de enlace descendente, que se conectan con los servidores del receptáculo a través del plano medio del receptáculo. Una interconexión lógica incluye todos los enlaces descendentes físicos de todas las interconexiones que pertenecen a ella. Los enlaces descendentes conectan las interconexiones con los servidores físicos. El conjunto de enlaces descendentes que comparten el acceso a un conjunto común de redes se denominan enlaces descendentes lógicos.
- Redes internas, que se utilizan para las comunicaciones de servidor a servidor sin tráfico saliente por los enlaces ascendentes.
- Enlaces de apilamiento, si se usan, que unen las interconexiones, bien a través de las conexiones interiores del receptáculo o de cables externos entre los puertos del frontal de las interconexiones.
- La línea de base de firmware, que especifica la versión de firmware que deben utilizar todas las interconexiones que pertenecen a la interconexión lógica. La línea de base de firmware de las interconexiones físicas se gestiona desde la interconexión lógica.

El administrador de red configura varias rutas entre los compartimentos de servidor y las redes

El administrador de red puede asegurarse de que cada compartimento de servidor de un receptáculo tiene dos rutas independientes a una red Ethernet del centro de datos mediante la creación de una interconexión lógica que cumpla las condiciones siguientes:

- La interconexión lógica tiene al menos dos interconexiones que están unidas por enlaces de apilamiento o definidas en grupos de interconexiones lógicas independientes.
- La interconexión lógica tiene al menos un conjunto de enlaces ascendentes que incluye enlaces ascendentes a la red desde al menos dos interconexiones físicas.

HPE OneView detecta e informa de una configuración o estado en el que solo hay una ruta (no hay rutas redundantes) a una red o en el que no hay rutas a una red.

El administrador de servidores no está obligado a conocer los detalles acerca de las configuraciones de interconexión

Debido a que una interconexión lógica se gestiona como una sola entidad, el administrador de servidores está aislado de los detalles de las configuraciones de interconexión. Por ejemplo, si el administrador de la red configura la interconexión lógica para asegurar el acceso redundante desde cada compartimento de servidor del receptáculo hasta cada red Ethernet del centro de datos, el administrador de servidores solo debe asegurarse de que un perfil de servidor incluye dos conexiones a una red o a un conjunto de redes que incluya esa red.

Relación con otros recursos

Un recurso de interconexión lógica está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más interconexiones. Para que una interconexión lógica pueda utilizarse, debe incluir al menos una interconexión. Si no tiene ninguna interconexión, el receptáculo y su contenido no tienen ningún enlace ascendente a las redes del centro de datos.
- Uno o varios grupos de interconexiones lógicas asociados a un grupo de receptáculos, que definen la configuración inicial de las interconexiones lógicas.
- Cero o más conjuntos de enlaces ascendentes, que asocian cero o más puertos de enlace ascendente a cero o más redes.
- Cero o un receptáculo lógico.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST	Notas
Logical Interconnects (Interconexiones lógicas)	`logical-interconnects` y `logical-downlinks`	La API de REST `logical-downlinks` se usa para obtener información sobre el conjunto común de redes y capacidades disponibles para un enlace descendente.

Más información

Gestión de interconexiones lógicas y grupos de interconexiones lógicas (página 211)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.14 Grupos de interconexiones lógicas

El grupo de interconexiones lógicas es una plantilla que define la configuración física y lógica de las interconexiones configuradas conjuntamente para formar una interconexión lógica. Esta configuración incluye lo siguiente:

- Los tipos de interconexiones, las configuraciones de interconexión y las capacidades de enlace descendente de interconexión
- Los puertos de interconexión utilizados para los enlaces de apilamiento
- Los conjuntos de enlaces ascendentes, que asignan puertos de enlace ascendente a redes Ethernet o Fibre Channel
- Las redes disponibles en función de los conjuntos de enlaces ascendentes y las redes internas

En el modelo de recursos:

- Uno o varios grupos de interconexiones lógicas están asociados a un grupo de receptáculos en lugar de a un receptáculo específico.
- Puede crear un grupo de interconexiones lógicas de forma automática durante una operación de adición de receptáculos, o independientemente de las operaciones de adición de estos.

  Si agrega un receptáculo sin especificar un grupo de receptáculos existente, HPE OneView crea tanto un grupo de receptáculos como un solo grupo de interconexiones lógicas basado en las interconexiones físicas de ese receptáculo. A continuación, puede editar ese grupo de receptáculos y ese grupo de interconexiones lógicas.

  Si desea tener varios grupos de interconexiones lógicas por cada receptáculo, cree los grupos de interconexiones lógicas antes de agregar el receptáculo, o edite los grupos de interconexiones lógicas para quitar las interconexiones de un grupo de interconexiones lógicas y agregarlos a otro.

- Los conjuntos de enlaces ascendentes definidos por el grupo de interconexiones lógicas establecen la configuración inicial de los conjuntos de enlaces ascendentes de cada interconexión lógica del grupo de interconexiones lógicas. Si se cambian los conjuntos de enlaces ascendentes para un grupo de interconexiones lógicas existente:
  - La nueva configuración del conjunto de enlaces ascendentes solo se aplica a los receptáculos que se agregan después del cambio de configuración.
  - Se informa de las interconexiones lógicas existentes que no son coherentes con el grupo de interconexiones lógicas. En ese caso, puede solicitar que las interconexiones lógicas existentes se actualicen con la nueva configuración.

Después de crear una interconexión lógica y asociarla a un grupo de interconexiones lógicas, sigue estando asociada a ese grupo e informa si su configuración difiere de la del grupo. En ese caso, puede cambiar la configuración de la interconexión lógica para que coincida con el grupo.

Relación con otros recursos

Un recurso de grupo de interconexiones lógicas está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más interconexiones lógicas
- Cero o más grupos de receptáculos

Los conjuntos de enlaces ascendentes definidos por el grupo de interconexiones lógicas especifican la configuración inicial de los conjuntos de enlaces ascendentes de cada interconexión lógica del grupo.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Logical Interconnect Groups (Grupos de interconexiones lógicas)	`logical-interconnect-groups`

Más información

Gestión de interconexiones lógicas y grupos de interconexiones lógicas (página 211)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.15 Logical switches (Conmutadores lógicos)

Un conmutador lógico se agrega a HPE OneView como conmutador lógico gestionado o supervisado. El conmutador lógico puede estar formado por un máximo de dos conmutadores físicos de la parte superior del bastidor (externos al receptáculo c7000) configurados en un único dominio de apilamiento.

La conectividad limita a un conmutador lógico por cada interconexión lógica. Las interconexiones de una interconexión lógica no se pueden conectar a más de un conmutador lógico.

Un conmutador lógico se basa en una configuración de grupo de conmutadores lógicos. Si el conmutador lógico cambia a un estado `Inconsistent with group` (Incoherente con el grupo) (debido a cambios en el conmutador lógico o en el grupo de conmutadores lógicos), actualice la configuración del conmutador lógico basándose en el grupo de conmutadores lógicos para volver a un estado coherente.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Logical Switches (Conmutadores lógicos)	`logical-switches`

Más información

Gestión de conmutadores lógicos (página 290)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.16 Logical switch groups (Grupos de conmutadores lógicos)

Un grupo de conmutadores lógicos es una plantilla para la creación de conmutadores lógicos. Los conmutadores lógicos son una agregación de hasta dos conmutadores físicos de la parte superior del bastidor.

Una vez que se crea a partir de un grupo de conmutadores lógicos, un conmutador lógico sigue estando asociado a su grupo de conmutadores lógicos. Cualquier cambio en la coherencia entre el grupo de conmutadores lógicos y sus conmutadores lógicos asociados se supervisa y se muestra en la pantalla del conmutador lógico asociado en HPE OneView.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Logical Switch Groups (Grupos de conmutadores lógicos)	`logical-switch-groups`

Más información

Gestión de grupos de conmutadores lógicos (página 293)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.17 Redes

Una red representa una red Fibre Channel, Ethernet o Fibre Channel sobre Ethernet (FCoE) del centro de datos.

Relación con otros recursos

Un recurso de red está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más conexiones
- Cero o un conjunto de enlaces ascendentes por cada interconexión lógica
- Para las redes Ethernet, etiquetadas cero o más conjuntos de redes

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Networks (Redes)	`fc-networks`, `ethernet-networks` o `fcoe-networks`

Más información

Gestión de redes y recursos de red (página 201)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.18 Conjuntos de redes

Un conjunto de redes representa un conjunto de redes Ethernet etiquetadas identificadas por un nombre único. Los conjuntos de redes se utilizan para simplificar las configuraciones de perfiles de servidor y las plantillas de perfiles de servidor. Cuando una conexión de un perfil de servidor especifica un conjunto de redes, se puede acceder a cualquiera de las redes del conjunto. Además, si se añaden o quitan redes de un conjunto de redes, los perfiles de servidor que

especifican el conjunto de redes están aislados de los cambios. Un uso común de los conjuntos de redes es actuar como una red troncal entre varias VLAN y un vSwitch (conmutador virtual).

En el modelo de recursos:

- Un conjunto de redes puede contener cero o más redes Ethernet etiquetadas.
- Una red Ethernet etiquetada puede ser miembro de cero o más conjuntos de redes.
- Una conexión de un perfil de servidor puede especificar una red o un conjunto de redes.
- Un conjunto de redes no puede pertenecer a un conjunto de enlaces ascendentes.

Se aplican otras reglas de configuración.

Relación con otros recursos

Un recurso de conjunto de redes está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más conexiones y, a través de ellas, cero o más perfiles de servidor
- Cero o más redes Ethernet

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Network Sets (Conjuntos de redes)	`network-sets`

Más información

Acerca de los conjuntos de redes (página 202)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.19 Dispositivos de suministro de energía

Un dispositivo de suministro de energía es un recurso físico que proporciona energía procedente de la fuente de suministro eléctrico del centro de datos a los componentes del bastidor. Los objetos de dispositivos de distribución de energía se crean para describir el suministro eléctrico de uno o varios componentes del bastidor. Los dispositivos de suministro de energía pueden incluir tomas de alimentación eléctrica, paneles de disyuntores, circuitos de derivación, PDU, barras de salida, tomas y dispositivos UPS.

Para obtener una lista completa de los dispositivos de suministro de energía, consulte la ayuda en línea sobre los detalles de pantalla para la pantalla **Power Delivery Devices** (Dispositivos de suministro de energía).

Relación con otros recursos

Un recurso de dispositivo de suministro eléctrico está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más bastidores
- Cero o más equipos no gestionados

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Dispositivos de suministro de energía	`power-devices`

Más información

Gestión de energía (página 275)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.20 Bastidores

Un bastidor es una estructura física que contiene equipos informáticos, tales como receptáculos, servidores, dispositivos de suministro de energía y dispositivos no gestionados de un centro de datos. Cuando se describen la ubicación física, el tamaño y los límites térmicos de los equipos de los bastidores, se habilitan las funciones de planificación del espacio y la energía, y de análisis energético del centro de datos.

Relación con otros recursos

Un recurso de bastidor está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o un centros de datos
- Cero o más receptáculos
- Cero o más instancias de hardware de servidor (para servidores HPE ProLiant DL)
- Cero o más equipos no gestionados
- Cero o más dispositivos de suministro de energía

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Bastidores	`bastidores`

Más información

Gestión de energía (página 275)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.21 Administradores de SAN

El recurso de los **administradores de SAN** le permite incluir en la gestión de HPE OneView los sistemas que gestionan redes SAN. Cuando se agrega un administrador de SAN a HPE OneView, las SAN que gestiona pasan a estar disponibles para asociarse con redes de HPE OneView que pueden conectarse a los perfiles de servidor.

En el modelo de recursos:

- Los administradores de SAN no están asociados directamente con los recursos de HPE OneView. Las SAN que gestionan (conocidas como SAN gestionadas) se pueden asociar con redes de HPE OneView, que se pueden configurar en los perfiles de servidor.

Relación con otros recursos

El recurso de administradores de SAN está asociado con los siguientes recursos en el diagrama de resumen de modelo de recursos (página 46):

- Una SAN gestionada en un administrador de SAN puede estar asociada con una red de HPE OneView, que puede, a su vez, estar asociada con un perfil de servidor.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Administradores de SAN	`device-managers`

Más información

Administradores de SAN (página 284)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.22 Redes SAN

Los administradores de SAN detectan las **SAN** y empiezan a gestionarse cuando se asocian con redes de HPE OneView. Las conexiones de perfiles de servidor con volúmenes a través de las SAN configuran automáticamente el servidor, la división por zonas de las SAN y los sistemas de almacenamiento para que el servidor pueda acceder al volumen.

Las **SAN** se ponen a disposición de HPE OneView cuando se agrega el administrador de SAN al que pertenecen.

En el modelo de recursos:

- Las SAN están asociadas con el administrador de SAN en el que residen.
- Las SAN pueden asociarse con una o varias redes Fibre Channel (FC) o Fibre Channel sobre Ethernet (FCoE).

Relación con otros recursos

El recurso de las SAN está asociado con los siguientes recursos en el diagrama de resumen del modelo de recursos (página 46):

- Una SAN gestionada en un administrador de SAN puede asociarse con una o varias redes Fibre Channel (FC) o Fibre Channel sobre Ethernet (FCoE).

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Redes SAN	`fc-sans`

Más información

Redes SAN (página 286)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.23 Hardware de servidor

El hardware de servidor representa una instancia de hardware de servidor, como un blade de servidor HPE ProLiant BL460c Gen8 físico instalado en un receptáculo o un servidor de montaje en bastidor HPE ProLiant DL380p físico.

Para obtener información sobre los modelos de hardware de servidor compatibles, consulte la ***Matriz de compatibilidad de HPE OneView***.

Relación con otros recursos

Un recurso de hardware de servidor está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o un perfil de servidor. Si un servidor no tiene un perfil de servidor asignado, no se podrán realizar acciones que requieran el recurso de perfil de servidor, tales como la gestión de firmware o la conexión a las redes del centro de datos. No obstante, sí se puede:
  - Añadir el hardware de servidor gestionado a HPE OneView, lo que incluye la actualización automática del firmware del servidor a la versión mínima necesaria para gestionarlo con HPE OneView.

    NOTA: Si se intenta añadir servidores supervisados cuya versión de firmware es inferior a la mínima requerida por HPE OneView, se producirá un error y el firmware deberá actualizarse fuera de HPE OneView, por ejemplo, con Smart Update Manager.
  - Ver los datos de inventario.
  - Encender o apagar el servidor.
  - Iniciar la consola remota de iLO.
  - Supervisar la energía, la refrigeración y la utilización.
  - Supervisar el estado y las alertas.
- Un único tipo de hardware de servidor.
- Si el hardware de servidor es un blade de servidor, un único compartimento de dispositivo de un receptáculo. Esta asociación también se aplica a los blades de servidor de altura completa, que ocupan dos compartimentos de dispositivo, pero solamente están asociados al compartimento superior.
- Si el hardware de servidor es un servidor de montaje en bastidor, cero o un recurso de bastidor y cero o más dispositivos de suministro de energía.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST	Notas
Hardware de servidor	`server-hardware`	Se utiliza el recurso de hardware de servidor, y no el recurso de perfil de servidor, para llevar a cabo acciones tales como apagar o encender el servidor, reiniciarlo e iniciar la consola remota de HPE iLO. Puede iniciar la consola remota de iLO a través de la interfaz de usuario. Las API de REST no incluyen una API para iniciar la consola remota de iLO.

Más información

Gestión del hardware de servidor (página 169)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.24 Tipos de hardware de servidor

Un tipo de hardware de servidor captura información acerca de la configuración física del hardware de servidor y define los parámetros que están disponibles para los perfiles de servidor asignados a ese tipo de hardware de servidor. Por ejemplo, el tipo de hardware de servidor para el blade de servidor HPE ProLiant BL460c Gen8 incluye un conjunto completo de valores predeterminadas del BIOS para la configuración de hardware de ese blade de servidor.

Cuando se agrega un chasis a HPE OneView, HPE OneView detecta los servidores instalados en el chasis y crea un tipo de hardware de servidor para cada una de las distintas configuraciones de servidor que detecta. Cuando se agrega un modelo nuevo de servidor de montaje en bastidor, HPE OneView crea un nuevo tipo de hardware de servidor para esa configuración de servidor.

Relación con otros recursos

Un recurso de tipo de hardware de servidor está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más perfiles de servidor
- Cero o más plantillas de perfiles de servidor
- Cero o más servidores del tipo definido por ese tipo de hardware de servidor

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Server Hardware Types (Tipos de hardware de servidor)	`server-hardware-types`

Más información

Acerca de los tipos de hardware de servidor (página 175)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.25 Perfiles de servidor

Los perfiles de servidor capturan los aspectos clave de la configuración del servidor en un solo lugar, y permiten el aprovisionamiento de hardware de infraestructura convergente de forma rápida y coherente siguiendo las prácticas recomendadas de cada organización.

Un perfil de servidor puede contener la información siguiente sobre la configuración de hardware de servidor:

- Información básica de identificación del servidor
- Versiones de firmware
- Conexiones con redes Ethernet, conjuntos de redes Ethernet, redes FCoE y redes Fibre Channel
- Almacenamiento local
- Almacenamiento SAN
- Parámetros de arranque
- Configuración del BIOS
- UUID (identificadores exclusivos universales) físicos o virtuales, direcciones MAC (control de acceso a medios) y direcciones WWN (nombre World Wide)

Relación con otros recursos

Un perfil de servidor está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o una plantilla de perfil de servidor.
- Cero o más recursos de conexión. Los recursos de conexión se utilizan para especificar la conexión entre el servidor y una red o un conjunto de redes. Si no se especifica al menos una conexión, el servidor no se podrá conectar a las redes del centro de datos. Las redes y los conjuntos de redes que están disponibles para una conexión de perfil de servidor dependen de la configuración de la interconexión lógica del receptáculo que contiene el hardware de servidor.
- Cero o un recurso de hardware de servidor.
- Un único recurso de tipo de hardware de servidor.
- Un único recurso de grupo de receptáculos.

  Para permitir la portabilidad de los perfiles de servidor, un perfil de servidor se asocia a un recurso de grupo de receptáculos en lugar de a un recurso de receptáculos. Debido a que los receptáculos del grupo de receptáculos están configurados de manera idéntica, puede asignar un perfil de servidor a cualquier hardware de servidor adecuado, independientemente del receptáculo y del compartimento del grupo de receptáculos que contenga ese hardware de servidor.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Perfiles de servidor	`server-profiles`

Más información

Gestión de perfiles de servidor (página 178)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.26 Plantillas de perfiles de servidor

Las plantillas de perfiles de servidor sirven para supervisar, marcar y actualizar perfiles de servidor en HPE OneView.

Una plantilla de perfil de servidor define el origen de la configuración de:

- Versiones de firmware
- Conexiones con redes Ethernet, conjuntos de redes Ethernet y redes Fibre Channel
- Almacenamiento local
- Almacenamiento SAN
- Parámetros de arranque
- Configuración del BIOS
- Afinidad del perfil

Relación con otros recursos

Una plantilla de perfil de servidor está asociada al siguiente recurso en el diagrama de resumen de recursos (página 46):

- Cero o más recursos de perfil de servidor.
- Cero o más recursos de conexión.
- Un único recurso de tipo de hardware de servidor.
- Un único recurso de grupo de receptáculos.

  Para permitir la portabilidad de los perfiles de servidor, un perfil de servidor se asocia a un recurso de grupo de receptáculos en lugar de a un recurso de receptáculos. Debido a que los receptáculos del grupo de receptáculos están configurados de manera idéntica, puede asignar un perfil de servidor a cualquier hardware de servidor adecuado, independientemente del receptáculo y del compartimento del grupo de receptáculos que contenga ese hardware de servidor.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Server Profile Templates (Plantillas de perfiles de servidor)	`server-profile-templates`

Más información

Gestión de plantillas de perfiles de servidor (página 190)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.27 Pools de almacenamiento

Un pool de almacenamiento existe en un sistema de almacenamiento y contiene volúmenes. Los pools de almacenamiento se crean en un sistema de almacenamiento mediante el software de gestión para dicho sistema. Después de agregar un pool de almacenamiento a HPE OneView, puede agregar volúmenes existentes o crear otros nuevos.

En el modelo de recursos:

- Existe un pool de almacenamiento en solo un sistema de almacenamiento.
- Un pool de almacenamiento puede contener cero o más volúmenes.
- Un pool de almacenamiento se puede asociar cero o más plantillas de volumen.

Relación con otros recursos

El recurso de pool de almacenamiento está asociado con los siguientes recursos en el diagrama de resumen de modelo de recursos (página 46):

- Un sistema de almacenamiento, y a través de él, cero o más volúmenes, que se pueden conectar a cero o más perfiles de servidor

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Storage Pools (Pools de almacenamiento)	`storage-pools`

Más información

Pools de almacenamiento (página 283)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.28 Sistemas de almacenamiento

Puede conectar sistemas de almacenamiento compatibles a HPE OneView para gestionar los volúmenes y pools de almacenamiento.

En el modelo de recursos:

- Un sistema de almacenamiento puede tener o no tener pools de almacenamiento.
- Un sistema de almacenamiento puede tener o no tener volúmenes en cada pool de almacenamiento.

Relación con otros recursos

El recurso del sistema de almacenamiento se asocia con los siguientes recursos en el diagrama de resumen de modelo de recursos (página 46):

- Cero o más pools de almacenamiento y, a través de ellos, cero o más volúmenes.
- Cero o más perfiles de servidor, a través de cero o más volúmenes.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Sistemas de almacenamiento	`storage-systems`

Más información

Sistemas de almacenamiento (página 281)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.29 Conmutadores

Los conmutadores proporcionan a una estructura unificada y convergente sobre Ethernet para el tráfico de LAN y SAN. Esta unificación permite la consolidación de la red y un mayor uso de la infraestructura y el cableado, lo que reduce el número de adaptadores y cables necesarios y elimina conmutadores redundantes.

Una configuración de receptáculos, blades de servidor y dispositivos de otros fabricantes — por ejemplo, Cisco Fabric Extender para módulos HPE BladeSystem y conmutadores de la parte superior del bastidor Cisco Nexus— aporta escalabilidad para gestionar blades de servidor y una mayor demanda de ancho de banda desde cada servidor con la redundancia de acceso a capa.

HPE OneView proporciona una supervisión mínima (solo estado y alimentación) de los conmutadores y sus interconexiones asociadas. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener la lista completa de dispositivos admitidos.

Relación con otros recursos

Un conmutador de la parte superior del bastidor Cisco Nexus está asociado con interconexiones, en concreto, el extensor de estructura Cisco para los módulos de BladeSystem dentro de un receptáculo, como se muestra en el diagrama de resumen de recursos (página 46).

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Conmutadores	`conmutadores`

Más información

Gestión de conmutadores (página 289)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.30 Equipos no gestionados

Un equipo no gestionado es un recurso físico que se encuentra en un bastidor o que consume energía, pero que actualmente no está gestionado por HPE OneView. Algunos equipos no gestionados son equipos no compatibles que no pueden ser gestionados por HPE OneView.

Todos los equipos conectados a una unidad Intelligent Power Distribution Unit (iPDU) que utilicen una conexión Intelligent Power Discovery (IPD) se añaden a HPE OneView como equipos no gestionados.

Otros equipos que no son compatibles con IPD, tales como conmutadores KVM, routers o monitores y teclados de montaje en bastidor, no se agregan a la lista de equipos no gestionados de forma automática. Para incluir estos equipos en HPE OneView, puede agregarlos manualmente y describir sus nombres, posiciones en el bastidor y requisitos de energía.

Relación con otros recursos

Un recurso de equipo no gestionado está asociado a los siguientes recursos en el diagrama de resumen de recursos (página 46):

- Cero o más bastidores
- Cero o más dispositivos de suministro de energía

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST	Notas
Unmanaged Devices (Equipos no gestionados)	`unmanaged-devices`	Puede ver, añadir o editar las propiedades de los equipos no gestionados usando la interfaz de usuario o las API de REST. Para eliminar un equipo no gestionado, debe utilizar la API de REST.

Más información

Acerca de los equipos no gestionados (página 174)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.31 Conjuntos de enlaces ascendentes

Un conjunto de enlaces ascendentes asigna redes del centro de datos a los puertos de enlace ascendente de las interconexiones. Los enlaces ascendentes deben proceder de interconexiones físicas que son miembros de la interconexión lógica a la que pertenece el conjunto de enlaces ascendentes. Un conjunto de enlaces ascendentes forma parte de una interconexión lógica. Para cada interconexión lógica:

- Un conjunto de enlaces ascendentes no puede incluir un conjunto de redes.

- Una red puede pertenecer a un conjunto de enlaces ascendentes por cada grupo de interconexiones lógicas.
- Un conjunto de enlaces ascendentes puede contener una red Fibre Channel.
- Un conjunto de enlaces ascendentes puede contener varias redes Ethernet.
- Un conjunto de enlaces ascendentes puede contener una o varias redes FCoE, pero los enlaces ascendentes deben estar dentro de una sola interconexión compatible con FCoE.
- Las redes internas permiten la conectividad entre servidores dentro de la interconexión lógica. Las redes internas se crean agregando redes existentes a las redes internas y no asociándolas con un conjunto de enlaces ascendentes. Si se agrega una red interna a un conjunto de enlaces ascendentes, la red se quita automáticamente de las redes internas.

Relación con otros recursos

Un conjunto de enlaces ascendentes forma parte de una interconexión lógica o de un grupo de interconexiones lógicas.

Los conjuntos de enlaces ascendentes definidos por un grupo de interconexiones lógicas especifican la configuración de los conjuntos de enlaces ascendentes utilizados por las interconexiones lógicas que pertenecen al grupo. Si los conjuntos de enlaces ascendentes de una interconexión lógica no coinciden con los conjuntos de enlaces ascendentes del grupo de interconexiones lógicas, HPE OneView le avisará de que la interconexión lógica no es coherente con su grupo.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Logical Interconnects (Interconexiones lógicas) o **Logical Interconnect Groups (Grupos de interconexiones lógicas)**.	`uplink-sets`

Más información

Acerca de los conjuntos de enlaces ascendentes (página 213)
Gestión de interconexiones lógicas y grupos de interconexiones lógicas (página 211)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.32 Volúmenes

Un volumen es un disco virtual asignado de un pool de almacenamiento. Un perfil de servidor puede definir la conexión de un servidor con volumen.

En el modelo de recursos:

- Existe un volumen en un único pool de almacenamiento que, a su vez, existe en un solo sistema de almacenamiento.
- Un volumen puede conectarse a uno, varios o ningún perfil de servidor.

Relación con otros recursos

El recurso de volúmenes está asociado con los siguientes recursos en el diagrama de resumen de modelo de recursos (página 46):

- Un pool de almacenamiento y, a través de él, un sistema de almacenamiento
- Cero, uno o varios perfiles de servidor a través de conexiones de volúmenes

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Volumes (Volúmenes)	`storage-volumes`

Más información

Volúmenes (página 283)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

2.33 Plantillas de volumen

En una plantilla de volumen se definen los valores de volúmenes creados a partir de ella. Utilice plantillas de volumen para crear varios volúmenes con la misma configuración.

En el modelo de recursos:

- Puede asociarse una plantilla de volumen con un pool de almacenamiento.

Relación con otros recursos

Un recurso de plantilla de volumen se asocia con los siguientes recursos en el diagrama de resumen de modelo de recursos (página 46):

- Un pool de almacenamiento, que puede tener cero, una o varias plantillas de volumen asociadas a él

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Volume Templates (Plantillas de volumen)	`storage-volume-templates`

Más información

Plantillas de volumen (página 284)
Diagrama de resumen del modelo de recursos (página 46)
Conceptos básicos sobre el modelo de recursos (página 45)

3 Información sobre las funciones de seguridad del dispositivo

La mayoría de las directivas y prácticas de seguridad de un entorno convencional pueden aplicarse en un entorno virtualizado. No obstante, en un entorno virtualizado, estas directivas pueden requerir algunas modificaciones y adiciones.

Actualmente solo se admiten los protocolos TLS (Transport Layer Security) para la GUI, la API de REST y el acceso al bus de mensajes. Cualquier referencia a "SSL" en la documentación debe interpretarse como si mencionara los protocolos "TLS".

3.1 Protección del dispositivo

CATA (Comprehensive Applications Threat Analysis) es una potente herramienta de evaluación de calidad de la seguridad de diseñada para reducir sustancialmente el número de defectos de seguridad latentes. El diseño del dispositivo se basó en los principios de CATA y se sometió a revisión siguiendo las directrices de CATA.

Los factores siguientes contribuyen a proteger (reforzar la seguridad) del dispositivo y su sistema operativo:

- Se siguieron las prácticas recomendadas de las directrices de seguridad del sistema operativo.

  El sistema operativo del dispositivo reduce su vulnerabilidad ejecutando solo los servicios necesarios para proporcionar funcionalidad. El sistema operativo del dispositivo aplica controles de acceso obligatorios internamente.

  - El dispositivo mantiene un cortafuegos que permite el tráfico en puertos específicos y bloquea todos los puertos no utilizados. Consulte «Puertos necesarios para HPE OneView» (página 81) para conocer la lista de puertos de red utilizados.
  - Los servicios principales del dispositivo solo se ejecutan con los privilegios necesarios; *no* se ejecutan como usuarios con privilegios.
  - El cargador de arranque del sistema operativo está protegido por contraseña. Alguien que intente arrancar en modo monousuario no puede poner en peligro el dispositivo.
- El dispositivo está diseñado para funcionar por completo en una LAN de gestión aislada. El acceso a la LAN de producción no es necesario.
- El dispositivo obliga a cambiar la contraseña en el primer inicio de sesión. La contraseña predeterminada *no puede* utilizarse de nuevo.
- El dispositivo es compatible con certificados autofirmados y certificados emitidos por una entidad emisora de certificados.

  El dispositivo se configura inicialmente con un certificado autofirmado. Como administrador de infraestructuras, puede generar una CSR (solicitud de firma de certificado) y, tras recibir el certificado, cargarlo en el dispositivo. Esto asegura la integridad y la autenticidad de la conexión HTTPS con el dispositivo.
- Todas las operaciones del explorador y las llamadas a la API de REST utilizan HTTPS. Todos los cifrados SSL (Secure Sockets Layer) débiles están desactivados.
- El dispositivo admite la actualización segura. Hewlett Packard Enterprise firma digitalmente todas las actualizaciones para asegurar la integridad y la autenticidad.
- Los archivos de copia de seguridad y los registros de transacciones están cifrados.

- Los volcados de soporte se cifran de forma predeterminada (como administrador de infraestructuras), pero tiene la opción de no cifrarlos. Los volcados de soporte se cifrados automáticamente cuando los crea un usuario con otro rol.
- A los usuarios del sistema operativo no se les permite acceder al dispositivo.
- Hewlett Packard Enterprise sigue de cerca los boletines de seguridad relacionados con las amenazas a los componentes de software del dispositivo y, si es necesario, publica actualizaciones de software.

3.2 Prácticas recomendadas para el mantenimiento de un dispositivo seguro

En la siguiente tabla se muestra una lista parcial de prácticas recomendadas de seguridad que Hewlett Packard Enterprise recomienda en entornos físicos y virtuales. La existencia de distintas directivas de seguridad y prácticas de implementación dificultan la tarea de proporcionar una lista completa y definitiva.

Tema	Práctica recomendada
Cuentas	• Limite el número de cuentas locales. Integre el dispositivo con una solución de directorio de empresa como Microsoft Active Directory u OpenLDAP.
Certificados	• Utilice los certificados firmados por una entidad emisora de certificados de confianza (CA), si es posible. HPE OneView utiliza certificados para la autenticación y para establecer relaciones de confianza. Uno de los usos más comunes de los certificados es cuando se establece una conexión desde un explorador web a un servidor web. La autenticación en el nivel de equipo se lleva a cabo como parte del protocolo HTTPS con SSL. También puede usar certificados para autenticar dispositivos cuando configure un canal de comunicación. El dispositivo es compatible con certificados autofirmados y certificados emitidos por una CA. El dispositivo está configurado en un principio con los certificados autofirmados para el servidor web y el software del agente de mensajes. Hewlett Packard Enterprise recomienda a los clientes examinar las necesidades de seguridad (es decir, realizar una evaluación de los riesgos) y tener en cuenta el uso de los certificados firmados por una entidad emisora de certificados de confianza. Para el nivel más alto de seguridad, Hewlett Packard Enterprise recomienda que utilice certificados firmados por una entidad emisora de certificados de confianza: ◦ Lo ideal es utilizar el certificado emitido por una entidad emisora de certificados existente de su empresa e importar los certificados de confianza. El certificado CA raíz de confianza debe desplegarse en los exploradores del usuario que se pondrá en contacto con los sistemas y dispositivos que tendrán que realizar la validación de certificados. ◦ Si su empresa no dispone de su propia entidad emisora de certificados, considere la posibilidad de utilizar una CA externa. Existen muchas empresas de otros fabricantes que proporcionan certificados de confianza. Trabaje con la CA externa para disponer de los certificados generados para sistemas y dispositivos específicos y, a continuación, importe los certificados de confianza en los componentes que utilizan. Como administrador de infraestructuras, puede generar una CSR (solicitud de firma de certificado) y, tras recibir el certificado, cargarlo en el servidor web del dispositivo. Esto asegura la integridad y la autenticidad de la conexión HTTPS con el dispositivo. También es posible cargar certificados para el agente de mensajes y base de datos. Para obtener más información, consulte «Uso de una entidad emisora de certificados».

Tema	Práctica recomendada
Red	• Hewlett Packard Enterprise recomienda la creación de una LAN de gestión privada y conservarla separada de las LAN de producción, utilizando VLAN o cortafuegos (o ambos). ◦ LAN de gestión Conecte todos los dispositivos del procesador de gestión, incluidos los Onboard Administrators, iLO e iPDU con el dispositivo HPE OneView y con la LAN de gestión. Conceda acceso a las LAN de gestión solo al personal autorizado: los administradores de infraestructuras, administradores de red y administradores de servidores. ◦ LAN de producción Conecte todas las NIC para los dispositivos gestionados a la LAN de producción. • No conecte sistemas de gestión (por ejemplo, el dispositivo, la iLO y el Onboard Administrator) directamente a Internet. Si necesita acceso entrante a Internet, utilice una VPN (red privada virtual) corporativa que proporcione protección mediante cortafuegos. Para el acceso a Internet saliente (por ejemplo, para Remote Support), utilice un proxy web seguro.
Servicios no esenciales	• El dispositivo está preconfigurado de modo que los servicios no esenciales se han eliminado o desactivado en su entorno de gestión. Asegúrese de que continúa reduciendo al mínimo los servicios al configurar hosts, sistemas de gestión y dispositivos de red (incluyendo los puertos de red que no se usan) para reducir significativamente el número de maneras en que su entorno puede ser atacado.
Contraseñas	• Para las cuentas locales del dispositivo, cambie las contraseñas periódicamente de acuerdo con sus directivas de contraseñas. • Asegúrese de que las contraseñas incluyen al menos tres de estos tipos de caracteres: ◦ Carácter numérico ◦ Carácter alfabético en minúsculas ◦ Carácter alfabético en mayúsculas ◦ Carácter especial
Roles	• Defina y asigna claramente los roles a los usuarios en función del acceso que necesitan para llevar a cabo sus tareas. El rol de administrador de infraestructuras debe reservarse para el acceso más alto.
Gestión de servicios	• Considere el uso de prácticas y procedimientos, como los definidos por *Information Technology Infrastructure Library* (ITIL). Para obtener más información, consulte la página web siguiente: **http://www.itil-officialsite.com/home/home.aspx**

Tema	Práctica recomendada
Actualizaciones	• Asegúrese de que dispone de un proceso para determinar si hay actualizaciones de software y de firmware disponibles y para instalar actualizaciones para todos los componentes del entorno de forma periódica.
Entorno virtual	• Informe a los administradores sobre los cambios en sus roles y responsabilidades en un entorno virtual. • Restrinja el acceso a la consola del dispositivo solo para los usuarios autorizados. Para obtener más información, consulte «Restricción del acceso a la consola» (página 83). • Si en su entorno se utiliza un sistema IDS (Intrusion Detection System), asegúrese de que dicho sistema tiene visibilidad sobre el tráfico de red en el conmutador virtual. • Desactive el modo promiscuo en el hipervisor y cifre el tráfico que pasa por la VLAN para disminuir el efecto de cualquier análisis de protocolos sobre el tráfico de la VLAN. **NOTA:** En la mayoría de los casos, si se desactiva el modo promiscuo en el hipervisor, no se puede utilizar en un invitado de VM (máquina virtual). El invitado de VM puede activar el modo promiscuo, pero no funcionará. • Mantenga una zona de confianza, por ejemplo, una DMZ (zona desmilitarizada) que sea independiente de las máquinas de producción. • Asegúrese de que existen los controles de acceso adecuados a los dispositivos Fibre Channel. • Utilice el enmascaramiento de LUN tanto en los hosts de almacenamiento como de producción. • Asegúrese de que los LUN se definen en la configuración del host, en vez de detectarlos. • Utilice la distribución en zonas permanente (que restringe la comunicación a través de una estructura) basándose en los WWN (nombres internacionales) de puerto, si es posible. • Asegúrese de que la comunicación con los WWN se realiza en el ámbito de los puertos del conmutador.

3.3 Creación de sesiones de inicio de sesión

Una sesión de inicio de sesión se crea cuando se inicia sesión en el dispositivo a través del explorador o algún otro cliente (por ejemplo, mediante la API de REST). Las solicitudes adicionales al dispositivo utilizan el identificador de sesión, que debe estar protegido, ya que representa al usuario autenticado.

Una sesión es válida hasta que se finaliza o se agota el tiempo de espera de la misma (por ejemplo, si una sesión está inactiva por un período de tiempo mayor que el valor del tiempo de inactividad de la sesión).

3.4 Autenticación para el acceso al dispositivo

El acceso al dispositivo requiere autenticación con un nombre de usuario y contraseña. Las cuentas de usuario se configuran en el dispositivo o en un directorio de la empresa. Todo el acceso (con el explorador y las API de REST), incluyendo la autenticación, se realiza a través de SSL para proteger las credenciales durante la transmisión por la red.

3.5 Control del acceso de los usuarios autorizados

El acceso al dispositivo se controla mediante roles, que describen lo que le está permitido hacer a un usuario autenticado en el dispositivo. Cada usuario debe tener asociado, como mínimo, un rol.

3.5.1 Especificación de las cuentas y los roles de usuarios

A cada cuenta de inicio de sesión de usuario del dispositivo se le debe asignar un rol, que determina qué se le permite realizar al usuario.

Para obtener información sobre cada rol y las capacidades que permiten estos roles, consulte «Acerca de los roles de usuario».

Para obtener más información sobre cómo agregar, eliminar y modificar cuentas de usuario, consulte la ayuda en línea.

3.5.2 Correspondencia de roles de SSO para iLO y OA

El dispositivo permite el SSO (inicio de sesión único) en iLO y OA (Onboard Administrator) sin almacenar las credenciales de iLO u OA creadas por el usuario. En la tabla siguiente se describe la correspondencia de roles entre el dispositivo, iLO y OA.

Rol del dispositivo	SSO para los roles de iLO	SSO para los roles de OA
Administrador de infraestructuras	Admin	Admin
Administrador de servidores	Admin	Admin
Administrador de la red	Usuario	Usuario
Solo lectura	Usuario	Usuario
Administrador de copia de seguridad	Nada	Nada
Administrador de almacenamiento	Usuario	Usuario

Roles del dispositivo

Consulte «Acerca de los roles de usuario».

Roles de iLO

- Los privilegios de administrador permiten asignar todos los derechos administrativos para las tareas de inicio de sesión, el reinicio del servidor y la consola remota.
- Los privilegios de usuario tienen restricciones de acceso, en función de la dirección IP, el nombre DNS o la hora.

Roles de OA

- Los privilegios de administrador permiten crear o editar todas las cuentas de usuario de un receptáculo.
- Los privilegios de operador otorgan acceso pleno a la información y control total de los compartimentos a los que se tiene acceso.

  NOTA: No se pueden configurar los compartimentos permitidos mediante SSO.

- Los privilegios de usuario permiten el acceso pleno a la información, pero no ofrecen capacidad de control.

3.5.3 Asignación de interacciones entre el dispositivo e iLO, OA y la iPDU

El dispositivo realiza tareas de configuración en el iLO, el OA y la iPDU. En la tabla siguiente se resume el modo en que el dispositivo interactúa con ellos.

Para obtener información sobre el cortafuegos, consulte «Puertos necesarios para HPE OneView».

Protocolo o interacción	Descripción	iLO		OA		iPDU	
		Uso	Configuración	Uso	Configuración	Uso	Configuración
NTP	Configura NTP		✓		✓		
SNMP	Activa y configura SNMP para recopilar información	✓	✓	✓	✓	✓	✓
Capturas SNMP	Activa y configura las capturas SNMP que se envían al dispositivo	✓	✓	✓	✓	✓	✓
HTTPS (RIBCL/SOAP/JSON)[1]	Recopila información (el protocolo específico puede variar, pero todos utilizan SSL)	✓		✓		✓	
Consola remota	Establece un enlace desde la interfaz de usuario a la consola remota de iLO	✓					
SSH	No se utiliza						
Telnet	No se utiliza						
Respuesta XML	Recopila información genérica sobre el sistema	✓		✓			
SSO	Activa y configura un certificado SSO para el acceso a la UI. Consulte en «Correspondencia de roles de SSO para iLO y OA» los privilegios que se conceden.	✓	✓	✓	✓		
Cuenta de usuario del dispositivo (_HPOneViewAdmin)	Configura y gestiona el sistema con una cuenta de usuario de nivel de administrador (y una contraseña generada aleatoriamente)	✓	✓			✓	✓

[1] SSL cifra el tráfico en la red, pero no autentica el certificado del sistema remoto.

3.6 Protección de las credenciales

Las contraseñas de las cuentas de usuario locales se almacenan usando un hash "con sal"; es decir, que se combinan con una cadena aleatoria y, a continuación, se almacena el hash del valor combinado. Un hash es un algoritmo de un solo sentido que asigna una cadena a un valor único de modo que la cadena original no se pueda recuperar partiendo del hash.

Las contraseñas se enmascaran en el explorador. Cuando se transmiten entre el dispositivo y el explorador a través de la red, las contraseñas se protegen mediante SSL.

Las contraseñas de las cuentas de usuario locales deben tener un mínimo de ocho caracteres y al menos un carácter en mayúsculas. El dispositivo no impone reglas de complejidad adicionales a las contraseñas. La seguridad y la caducidad de las contraseñas se controlan mediante la directiva de seguridad del sitio (consulte «Prácticas recomendadas para el mantenimiento de un dispositivo seguro» (página 70)). Si integra un servicio de directorio de autenticación externo (también conocido como un directorio de empresa) con el dispositivo, el servicio de directorio se encarga de que se cumplan las directrices de seguridad y caducidad de las contraseñas.

3.7 Conceptos básicos sobre el registro de auditoría

El registro de auditoría contiene un registro de las acciones realizadas por cada usuario en el dispositivo.

Para descargar el registro de auditoría, debe disponer de privilegios de administrador de infraestructuras.

Para obtener información sobre cómo descargar el registro de auditoría desde la interfaz de usuario, consulte «Descarga de los registros de auditoría».

Supervise los registros de auditoría, ya que las entradas antiguas se borran periódicamente para evitar que su tamaño sea demasiado grande. Descargue los registros de auditoría periódicamente para conservar un historial de auditoría a largo plazo.

Cada usuario tiene un ID de inicio de sesión único para cada sesión, por lo que es posible seguir el rastro de un usuario mediante el registro de auditoría. Algunas acciones las realiza el dispositivo y puede que no tengan un ID de inicio de sesión.

A continuación se muestra el detalle de una entrada de auditoría:

Token	Descripción
Date/time (Fecha/hora)	La fecha y hora del evento
Internal component ID (Identificador de componente interno)	El identificador exclusivo de un componente interno
Reserved (Reservado)	El identificador de la organización. Reservado para uso interno.
User domain (Dominio del usuario)	El nombre del dominio de inicio de sesión del usuario
User name/ID (Nombre/Identificador de usuario)	El nombre del usuario
Session ID (Identificador de sesión)	El identificador de sesión de usuario asociado al mensaje
Task ID (Identificador de tarea)	El URI del recurso de tarea asociado al mensaje
Client host/IP (Nombre de host/IP del cliente)	La dirección IP del cliente (explorador) identifica el dispositivo cliente que inició la solicitud

Token	Descripción
Result (Resultado)	El resultado de la acción, que puede ser uno de los valores siguientes: • SUCCESS • FAILURE • SOME_FAILURES • CANCELED • KILLED
Action (Acción)	Descripción de la acción, que puede ser uno de los valores siguientes: • ADD • MODIFY • DELETE • ACCESS • RUN • LIST • ENABLE • DISABLE • SAVE • SETUP • UNSETUP • DEPLOY • START • DONE • KILLED • CANCELED • LOGIN • LOGOUT • DOWNLOAD_START
Severity (Nivel de gravedad)	Descripción de la gravedad del evento, que puede ser uno de los valores siguientes, que se enumeran por orden de importancia creciente: • INFO • NOTICE • WARNING • ERROR • ALERT • CRITICAL
Resource category (Categoría del recurso)	Para obtener información de categoría de la API de REST, consulte la *Referencia de la API de REST de HPE OneView* en la ayuda en línea.
Resource URI/name (URI/Nombre del recurso)	El URI/nombre del recurso asociado a la tarea
Message (Mensaje)	El mensaje de salida que aparece en el registro de auditoría

Entradas de la consola de mantenimiento

El registro de auditoría incluye entradas para estos eventos de la consola de mantenimiento:

- Entradas en las que no se requiere ningún inicio de sesión
- Inicios de sesión correctos
- Inicios de sesión incorrectos
- Intentos de autorización de desafío-respuesta incorrectos
- Intentos de reinicio del dispositivo
- Intentos de apagado del dispositivo
- Intentos de restablecer la contraseña del administrador
- Inicios y cierres de la consola de servicios

3.8 Elección de una directiva para el registro de auditoría

Elija una directiva para descargar y examinar el registro de auditoría.

El registro de auditoría contiene un registro de las acciones realizadas por cada usuario en el dispositivo. A medida que crece el tamaño del registro de auditoría, la información antigua se va eliminando. Para mantener un historial de auditoría a largo plazo, debe descargar y guardar el registro de auditoría periódicamente.

Para obtener más información sobre el registro de auditoría, consulte «Conceptos básicos sobre el registro de auditoría» (página 75).

3.9 Acceso al dispositivo a través de SSL

Todo el acceso al dispositivo se realiza a través de HTTPS (HTTP sobre SSL), que cifra los datos a través de la red y ayuda a garantizar la integridad de estos. Para obtener una lista de paquetes de cifrado compatibles, consulte *Algorithms for securing the appliance* (Algoritmos para proteger el dispositivo) en la ayuda en línea.

3.10 Gestión de certificados desde el explorador

El dispositivo se autentica a través de SSL mediante un certificado. El certificado incluye una clave pública y el dispositivo conserva la clave privada correspondiente que está vinculada de manera exclusiva con cada clave pública.

NOTA: En esta sección se analiza la gestión de certificados desde la perspectiva del explorador. Para obtener información sobre cómo utiliza el certificado un cliente distinto del explorador (como cURL), consulte la documentación de dicho cliente.

El certificado también contiene el nombre del dispositivo, que sirve al cliente SSL para identificar el dispositivo.

El certificado consta de los campos siguientes:

- **Common Name (CN) (Nombre común [CN])**

  Este nombre es obligatorio. De forma predeterminada, contiene el nombre de host completo del dispositivo.

- **Alternative Name (Nombre alternativo)**

  Este nombre es opcional, pero Hewlett Packard Enterprise recomienda indicarlo, porque admite varios nombres (incluidas las direcciones IP) para minimizar las advertencias de discrepancia de nombres del explorador.

  De forma predeterminada, este campo se rellena con el nombre de host completo (si se usa DNS), un nombre de host corto y la dirección IP del dispositivo.

  NOTA: Si introduce nombres en el campo **Alternative Name** (Nombre alternativo), uno de ellos debe ser la entrada del **Common Name** (Nombre común).

Estos nombres pueden cambiarse al crear manualmente un certificado autofirmado o una solicitud de firma de certificado.

3.10.1 Certificado autofirmado

El certificado predeterminado generado por el dispositivo está autofirmado; es decir, no ha sido emitido por una entidad emisora de certificados de confianza.

De manera predeterminada, los exploradores no confían en los certificados autofirmados, ya que no tienen información previa sobre ellos. El explorador mostrará una advertencia para permitir al usuario verificar el contenido del certificado autofirmado antes de aceptarlo.

3.10.2 Uso de una entidad emisora de certificados

Utilice una CA (entidad emisora de certificados) de confianza para simplificar la gestión de certificados de confianza; la CA emite certificados que usted importa posteriormente. Si el explorador está configurado para confiar en la CA, también serán de confianza todos los certificados firmados por ella. Una CA puede ser interna (su organización se encarga de su uso y mantenimiento) o externa (otra entidad se encarga de su uso y mantenimiento).

Puede importar un certificado firmado por una CA y usarlo en vez del certificado autofirmado. Los pasos generales son los siguientes:

1. Genere una CSR (solicitud de firma del certificado).
2. Copie la CSR y envíesela a la CA, siguiendo las instrucciones de la CA.
3. La CA autentica al solicitante.
4. La CA le envía el certificado, de acuerdo con sus procedimientos.
5. Importe el certificado.

Para obtener información sobre cómo generar la CSR e importar el certificado, consulte la ayuda de la interfaz de usuario.

3.10.3 Creación de una solicitud de firma de certificado

El dispositivo usa un certificado para la autenticación con SSL. El certificado incluye una clave pública y el dispositivo conserva la clave privada correspondiente que está vinculada de manera exclusiva con la clave pública.

Una entidad emisora de certificados (CA) es una organización de confianza que emite un certificado que permite confiar en el host a quienes también confían en ella. En síntesis, la CA responde por el host.

Para obtener información sobre la creación de un certificado autofirmado, consulte «Creación de un certificado autofirmado» (página 79).

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras.
- Recopilar la información que la CA requiera para la solicitud.
- Obtener la contraseña de seguridad de la CA.

Cómo crear una solicitud de firma de certificado

1. En el menú principal, seleccione **Settings** (Configuración).
2. Seleccione **Actions→Create certificate signing request** (Acciones > Crear una solicitud de firma de certificado).
3. Proporcione los datos que se solicitan en la pantalla.
4. Haga clic en **OK** (Aceptar).
5. Copie los datos de la solicitud de certificado del cuadro de diálogo y envíeselos a la CA. La CA determina cómo y dónde deben enviarse los datos de la solicitud de certificado.
6. Haga clic en **OK** (Aceptar).

Pasos siguientes: cuando reciba el certificado de la CA, impórtelo. Consulte Importación un certificado.

1. Envíe la solicitud de firma de certificado a la CA. La CA determina cómo y dónde debe enviarse la solicitud.
2. La CA autentica al solicitante.
3. Importe el certificado.

3.10.4 Creación de un certificado autofirmado

El dispositivo usa un certificado para la autenticación con SSL. El certificado incluye una clave pública y el dispositivo conserva la clave privada correspondiente que está vinculada de manera exclusiva con la clave pública.

Un certificado autofirmado indica que un host responde por sí mismo, lo que, en algunos casos, puede ser adecuado. De forma predeterminada, los exploradores no confían en los certificados autofirmados y muestran un mensaje de advertencia.

Una alternativa más segura es un certificado emitido por una entidad emisora de certificados. Para obtener información sobre estos certificados, consulte «Creación de una solicitud de firma de certificado» (página 78).

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras

Cómo crear un certificado autofirmado

1. En el menú principal, seleccione **Settings** (Configuración).
2. Haga clic en **Security** (Seguridad).
3. Seleccione **Actions→Create self-signed certificate** (Acciones > Crear un certificado autofirmado).
4. Proporcione los datos que se solicitan en la pantalla.
5. Introduzca la información opcional que considere necesario.
6. Haga clic en **OK** (Aceptar).
7. Compruebe que se ha creado el certificado. La información del certificado se muestra en la pantalla.

3.10.5 Importación un certificado

Después de enviar una solicitud de firma de certificado a la CA y recibirlo, debe importarlo.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras.
- Asegúrese de que no haya otros usuarios conectados al dispositivo.

Cómo importar un certificado

1. En el menú principal, seleccione **Settings** (Configuración).
2. Haga clic en **Security** (Seguridad).
3. Seleccione **Actions→Import Certificate** (Acciones > Importar certificado).
4. Copie el texto del certificado y péguelo en el cuadro correspondiente.
5. Haga clic en **OK** (Aceptar).
6. Cuando el servidor web del dispositivo se reinicie y se vuelva a conectar, inicie sesión en el dispositivo.

3.10.6 Visualización de la configuración del certificado

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras, administrador de copia de seguridad o solo lectura

Cómo visualizar la configuración del certificado

1. Vaya desde el menú principal a la pantalla **Settings** (Configuración).
2. Seleccione **Overview→Security→Certificate** (Información general > Seguridad > Certificado).

3.10.7 Descarga e importación de un certificado autofirmado

Si descarga e importa un certificado autofirmado, evitará la advertencia del explorador.

En un entorno seguro, nunca es apropiado descargar e importar un certificado autofirmado, a menos que haya validado el certificado y conozca el dispositivo específico y confíe en él.

En un entorno con menor seguridad, podría ser aceptable descargar e importar el certificado del dispositivo si conoce y confía en el emisor del certificado. Sin embargo, Hewlett Packard Enterprise no recomienda esta práctica.

Microsoft Internet Explorer y Google Chrome comparten un almacén de certificados común. Un certificado descargado con Internet Explorer puede importarse con Google Chrome y con Internet Explorer. Del mismo modo, un certificado descargado con Google Chrome también puede importarse con los dos exploradores. Mozilla Firefox tiene su propio almacén de certificados, y estos deben descargarse e importarse únicamente con dicho explorador.

Los procedimientos para la descarga e importación de un certificado autofirmado difieren en cada explorador.

Descarga de un certificado autofirmado con Microsoft Internet Explorer

1. Haga clic en el área **Error de certificado**.
2. Haga clic en **Ver certificado**.
3. Haga clic en la ficha **Detalles**.
4. Compruebe el certificado.
5. Seleccione **Copiar en archivo.**
6. Utilice el Asistente para la exportación de certificados para guardar el certificado en un archivo X.509 con codificación base 64.

Importación de un certificado autofirmado con Microsoft Internet Explorer

1. Seleccione **Herramientas→Opciones de Internet**.
2. Haga clic en la ficha **Contenido**.
3. Haga clic en **Certificados**.
4. Haga clic en **Importar**.
5. Utilice el Asistente para importación de certificados.
   a. Cuando se le pida el almacén de certificados, seleccione **Place** (Colocar).
   b. Seleccione el almacén **Entidades de certificación raíz de confianza**.

3.10.8 Comprobación de un certificado

Puede comprobar la autenticidad del certificado viéndolo con el explorador.

Después de iniciar sesión en el dispositivo, seleccione **Settings (Configuración)→Security (Seguridad)** para ver el certificado. Tome nota de estos atributos para compararlos:

- Huellas digitales (en especial)
- Nombres
- Número de serie
- Fechas de validez

Compare esta información con el certificado que se muestra en el explorador, es decir, cuando se navega desde fuera del dispositivo.

3.11 Clientes distintos del explorador

El dispositivo es compatible con una amplia gama de diferentes API de REST. Cualquier cliente, no solo un explorador, puede emitir solicitudes para las API de REST. El emisor de la llamada

debe asegurarse de que toma las medidas de seguridad adecuadas con respecto a la confidencialidad de las credenciales, lo que incluye:

- El token de sesión, que se utiliza para solicitudes de datos.
- Las respuestas además del cifrado de las credenciales durante la transmisión a través de HTTPS.

3.11.1 Contraseñas

Es probable que las contraseñas se muestren y se almacenen con texto sin cifrar en un cliente como `cURL`.

Tenga cuidado para evitar que usuarios no autorizados:

- Vean las contraseñas que se muestran
- Vean los identificadores de sesión
- Tengan acceso a los datos guardados

3.11.2 Conexión SSL

El cliente debería especificar HTTPS como protocolo para garantizar que se utilice SSL en la red para proteger datos confidenciales. Si el cliente especifica HTTP, será redirigido a HTTPS asegurarse de que se utiliza SSL.

El certificado del dispositivo, requerido por el cliente, permite realizar la conexión SSL correctamente. Una manera sencilla de obtener un certificado consiste en acceder al dispositivo mediante un explorador; para obtener más información sobre cómo obtener un certificado con un explorador, consulte «Gestión de certificados desde el explorador» (página 77) .

3.12 Puertos necesarios para HPE OneView

HPE OneView requiere que se pongan determinados puertos a disposición del dispositivo para gestionar servidores, receptáculos e interconexiones.

Tabla 1 Puertos necesarios para HPE OneView

Número de puerto	Protocolo	Uso	Descripción
22	TCP	Entrante y saliente	Se utiliza para SSH y SFTP. SSH es necesario para comunicarse con los módulos de interconexión Ethernet y FlexFabric de VC. SFTP es necesario llevar a cabo acciones como las actualizaciones de firmware y los volcados de soporte.
80	TCP	Entrante	Se utilizan para la interfaz HTTP. Por lo general, este puerto redirige al puerto 443, que proporciona el acceso necesario para iLO.
123	UDP	Entrante	HPE OneView actúa como servidor NTP. iLO y el Onboard Administrator requieren acceso.
123	UDP	Saliente	Se utiliza como cliente NTP para sincronizar la hora del dispositivo.
161	UDP	Saliente	Admite llamadas SNMP GET para obtener datos sobre el estado de un servidor a través de iLO. También se utiliza para las iPDU.
162	UDP	Entrante	Se utiliza para admitir las capturas SNMP desde los dispositivos iLO, Onboard Administrator e iPDU. Este puerto también se utiliza para supervisar el reenvío de capturas y las interconexiones de VC.

Tabla 1 Puertos necesarios para HPE OneView *(continuación)*

Número de puerto	Protocolo	Uso	Descripción
443	TCP	Entrante	Se utiliza para la interfaz HTTPS con la interfaz de usuario y las API.
443	TCP	Saliente	Se utiliza para el acceso SSL seguro a iLO y al Onboard Administrator. Se utiliza para las comunicaciones Redfish, RIBCL, SOAP e iPDU.
2162	UDP	Entrante	Se utiliza como un puerto de captura SNMP alternativo.
5671	TCP	Entrante	Permite que las secuencias de comandos o las aplicaciones externas se conecten al SCMB (State-Change Message Bus) y supervisen sus mensajes.
17988	TCP	Saliente	Se utiliza para el acceso a Virtual Media en el iLO desde HPE OneView.
17990	TCP	Explorador a iLO	Proporciona acceso con el explorador a la consola remota.

3.13 Control del acceso a la consola del dispositivo

Utilice el software de gestión del hipervisor para restringir el acceso al dispositivo, lo que evita que usuarios no autorizados obtengan acceso a las funciones de acceso de servicio y de restablecimiento de contraseña. Consulte «Restricción del acceso a la consola» (página 83).

Los usos propios de la consola son:

- Solucionar problemas de configuración de la red.
- Restablecer la contraseña del administrador del dispositivo
- Activar el acceso de servicio para un representante autorizado de soporte técnico in situ.

La consola virtual del dispositivo se muestra en una consola gráfica, mientras que el restablecimiento de contraseña y el acceso para los servicios de Hewlett Packard Enterprise utilizan una consola no gráfica.

Cambio de una consola a otra (VMware vSphere y Microsoft Hyper-V)

1. Abra la consola del dispositivo virtual.
2. Pulse y mantenga pulsadas las teclas **Ctrl+Alt**.
3. Pulse y suelte la barra espaciadora (solo para VMware vSphere).
4. Pulse **F1** para seleccionar la consola no gráfica o **F2** para seleccionar la consola gráfica.

Cambio de una consola a otra (KVM)

1. Abra Virtual Machine Manager.
2. En la barra de menús, seleccione **Send Key (Enviar clave)**→**Ctrl+Alt+F1** para la consola no gráfica o seleccione **Send Key (Enviar clave)**→ **Ctrl+Alt+F2** para la consola gráfica.

3.13.1 Activar o desactivar el acceso a los servicios autorizados

Cuando inicie por primera vez el dispositivo, tendrá la posibilidad de habilitar o deshabilitar el acceso de los representantes autorizados de soporte técnico in situ. De forma predeterminada, los representantes autorizados de soporte técnico in situ pueden acceder al sistema a través de la consola del dispositivo y diagnosticar los problemas que ha notificado.

El acceso de soporte es un shell de nivel raíz que permite al representante autorizado de soporte técnico in situ depurar cualquier problema del dispositivo y obtener una contraseña de un solo uso mediante un mecanismo de desafío/respuesta similar al del restablecimiento de contraseña.

Una vez realizada la configuración inicial del dispositivo, un administrador de infraestructuras puede activar o desactivar el acceso a los servicios en cualquier momento mediante el procedimiento siguiente:

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras

Activación o desactivación del acceso a los servicios autorizados

1. En el menú principal, seleccione **Settings** (Configuración).
2. Haga clic en el icono **Edit** (Editar) en el panel **Security** (Seguridad).

   Se abre la ventana **Edit Security** (Editar seguridad).
3. Seleccione la configuración adecuada para el **Service console access** (Acceso a la consola de servicios):
   - **Disabled** (Desactivado) para impedir el acceso a la consola.
   - **Enabled** (Activado) para permitir el acceso a la consola.
4. Haga clic en **OK** (Aceptar).

También puede utilizar una API de REST `/rest/appliance/settings` para activar o desactivar el acceso a los servicios.

NOTA: Hewlett Packard Enterprise le recomienda que active el acceso. En caso contrario, el representante autorizado de soporte técnico no podrá acceder al dispositivo para solucionar problemas.

3.13.2 Restricción del acceso a la consola

Puede restringir el acceso de la consola al dispositivo virtual a través de las prácticas de gestión seguras propias del hipervisor.

Para VMware vSphere, esta información está disponible en la página web de VMware:

http://www.vmware.com

En concreto, busque los temas relacionados con el privilegio Console Interaction de vSphere y las prácticas recomendadas para la gestión de roles y permisos de VMware.

Para Microsoft Hyper-V, restrinja el acceso a la consola a través de acceso basado en roles. Para obtener información, consulte la página web de Microsoft:

http://www.microsoft.com

3.14 Archivos que puede descargar desde el dispositivo

Puede descargar los siguientes archivos de datos desde el dispositivo:

- Volcado de soporte

  De forma predeterminada, todos los datos del volcado de soporte están cifrados y solo puede acceder a ellos un representante autorizado de soporte técnico.
- Archivo de copia de seguridad

  Todos los datos del archivo de copia de seguridad están en un formato propietario. Hewlett Packard Enterprise recomienda que cifre el archivo de acuerdo con la directiva de seguridad de su organización.
- Registros de auditoría

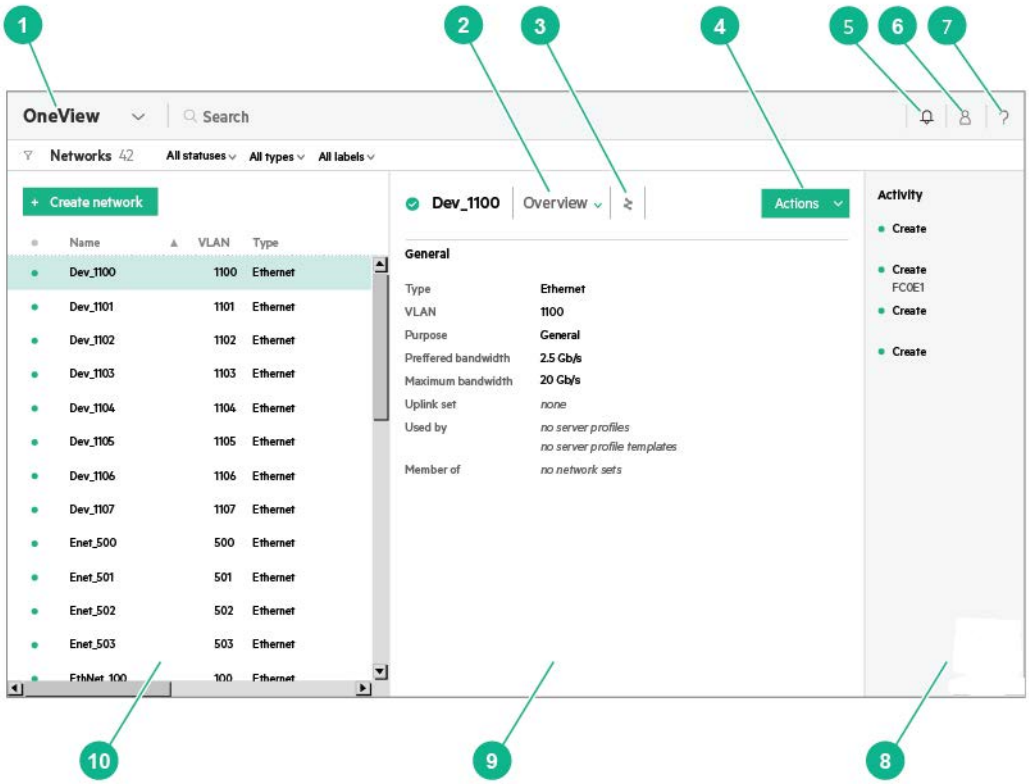
  Los identificadores de sesión no se registran; solo se registran los identificadores de inicio de sesión correspondientes. Las contraseñas y otros datos privados no se registran.

4 Navegación por la interfaz gráfica de usuario

4.1 Acerca de la interfaz gráfica de usuario

Para conocer los nombres de las zonas, los iconos y los controles comunes de una pantalla de la interfaz de usuario, consulte las descripciones correspondientes que aparecen después de la imagen.

Figura 3 Topografía de la pantalla



1 Menú principal de HPE OneView: es el menú principal para navegar por los recursos. Haga clic en el icono ❯ o haga clic en cualquier lugar en el área para expandir el menú.

2 Selector de **Vista**: permite controlar la información que se muestra sobre un recurso, y así poder centrarse únicamente en lo que interese en cada momento.

3 Icono de la vista Map (Mapa): proporciona una representación gráfica de las relaciones entre el recurso seleccionado y los demás recursos. Para ver estas relaciones, seleccione el icono ⚟ o la vista **Map** (Mapa) en el selector de vista.

4 Menú **Actions** (Acciones): proporciona las acciones que pueden ejecutarse en el recurso actual. Las acciones incluyen, entre otras: adición, creación, eliminación, borrado y edición de una instancia de

6 Control Session (Sesión): indica quién ha iniciado sesión en el dispositivo y la duración de cada sesión. También le permite editar cierta información de la cuenta del usuario, en función de sus credenciales de usuario.

7 Control Help (Ayuda): expande (u oculta) una barra lateral que da acceso a la ayuda de la interfaz de usuario y la API de REST, al CLUF y a la Oferta por escrito, así como al **foro de usuarios en línea de HPE OneView**.

8 Barra lateral **Activity** (Actividad): muestra las últimas alertas y actividades de tareas para el recurso actual. Utilice el icono de control Activity (Actividad) para abrir (o cerrar) esta barra lateral.

9 Panel **Details** (Detalles): proporciona toda la información conocida sobre la instancia de recurso seleccionada. Para ver los

recurso. Si no tiene los permisos necesarios para realizar una acción, esta no aparecerá en el menú **Actions** (Acciones).

5 Control Activity (Actividad): expande (u oculta) una barra lateral con la actividad reciente relacionada con el dispositivo, los recursos o los usuarios (desde el inicio de sesión y la ventana del explorador actuales).

detalles relativos a una instancia de recurso en particular, haga clic en su nombre en el panel principal.

10 Panel **Master** (Principal): contiene todas las instancias de recursos que se han configurado en el dispositivo. En algunos casos, un icono de estado indica el estado general del recurso.

Además de los componentes de la pantalla mostrados en la Figura 3, «Topografía de la pantalla», cada pantalla de la interfaz de usuario tiene un área de notificaciones que le notifica cuando un evento o actividad requiere su atención.

Algunas pantallas también tienen una barra lateral de filtros que le permite controlar el tipo de información que se muestra en el panel principal.

4.2 Barra lateral de actividad

4.2.1 Acerca de la barra lateral de actividad

La barra lateral de **Activity** (Actividad) muestra las tareas iniciadas durante la sesión actual. La tarea más reciente se muestra en primer lugar.

Las notificaciones de tareas suministran información (incluyendo mensajes de finalización, en curso y error) acerca de las tareas que se han iniciado.

La barra lateral **Activity** (Actividad) se diferencia de la pantalla **Activity** (Actividad) en que solo muestra la actividad reciente. Por el contrario, la pantalla **Activity** (Actividad) muestra todas las actividades y le permite verlas en una lista, ordenarlas y filtrarlas. Para obtener más información, consulte «Acerca de la pantalla de actividad» (página 340).

Haga clic en una actividad para mostrar más detalles.

4.2.2 Detalles de la barra lateral de actividad

La barra lateral **Activity** (Actividad) muestra las actividades de tareas generadas durante la sesión actual.

Componente	Descripción
	Muestra la actividad de tareas recientes de la tarea generada durante el inicio de sesión. Cuando se cierra la barra lateral **Activity** (Actividad), se muestra el número de notificaciones de alerta o tareas aún no visualizadas junto al icono de actividad.
Actividad	Describe la alerta o tarea y el recurso afectado. Un icono de estado general indica el estado actual del recurso asociado con la actividad.

4.2.3 Expansión o contracción de la barra lateral de actividad

Requisitos previos

- Privilegios mínimos necesarios: administrador de red, administrador de servidores, administrador de infraestructuras, administrador de copia de seguridad, solo lectura

Ampliar o controlar la barra lateral de filtro de actividad

1. Utilice el icono de alfiler derecho () para ampliar la **barra lateral de filtro de actividad**.

   Utilice el icono de alfiler izquierdo () para contraer la **barra lateral de filtro de actividad**.

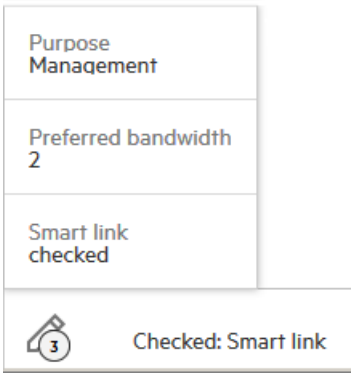
2. Seleccione una actividad para que se muestren más detalles.

Paso siguiente: filtrar actividades.

4.3 Seguimiento de auditorías

El control de cambios ofrece un historial de los cambios que realiza en un cuadro de diálogo, como una acción agregada. Haga clic en en la esquina inferior izquierda del cuadro de diálogo para ver los cambios.

Figura 4 Vista ampliada del seguimiento de auditorías

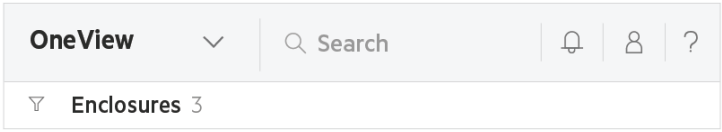


4.4 Barra superior y menú principal

El menú principal es el primer método para navegar a los recursos y las acciones que se pueden realizar con ellos.

Para expandir el menú principal, haga clic dentro del área del menú principal de la barra superior.

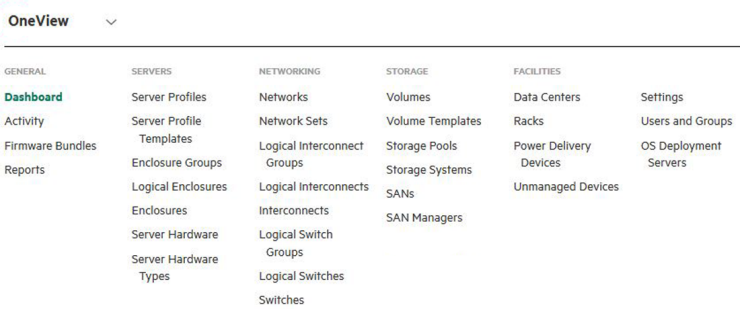
Figura 5 Barra superior



El menú principal proporciona acceso a los recursos; cada pantalla de recurso contiene un menú **Actions** (Acciones).

- Si no tiene autorización para acceder a un recurso, ese recurso no aparecerá en el menú principal.
- Si no tiene los permisos necesarios para realizar una acción, esta no aparecerá en el menú **Actions** (Acciones).

Figura 6 Menú principal expandido



4.5 Exploradores

Para obtener información general sobre el uso de los exploradores, consulte los temas siguientes:

- «Prácticas recomendadas del explorador para un entorno seguro»
- «Configuración y funciones de uso habitual del explorador»
- «Requisitos del explorador»
- «Configuración del explorador para las unidades de medida americanas o del sistema métrico»

4.5.1 Prácticas recomendadas del explorador para un entorno seguro

Práctica recomendada	Descripción
Utilice exploradores compatibles	Consulte la ***Matriz de compatibilidad de HPE OneView*** para asegurarse de que el explorador y la versión del explorador que utiliza son compatibles, y la configuración y los complementos del explorador son correctos.
Cierre la sesión del dispositivo antes de cerrar el explorador	En el explorador, el identificador de sesión del usuario autenticado se guarda en una cookie. Aunque la cookie se elimina cuando se cierra el explorador, la sesión sigue siendo válida en el dispositivo hasta que se cierre. Al cerrar la sesión se garantiza que se invalida la sesión en el dispositivo. **NOTA:** Si cierra el explorador, todas las sesiones abiertas se invalidarán en 24 horas.
No utilice enlaces cuyo origen o destino esté fuera de la interfaz de usuario del dispositivo	Cuando esté conectado al dispositivo, evite hacer clic en enlaces cuyo origen o destino esté fuera de la interfaz de usuario del dispositivo, como los enlaces que reciba en mensajes de correo o por mensajería instantánea. El contenido situado fuera de la interfaz de usuario del dispositivo podría contener código malicioso.
Utilice un explorador diferente para acceder a sitios fuera del dispositivo	Cuando tenga iniciada una sesión en el dispositivo, no utilice la misma instancia del explorador (por ejemplo, otra fichas en el mismo explorador) para navegar por otros sitios web. Por ejemplo, para garantizar un entorno de navegación independiente, utilice Firefox para la interfaz de usuario del dispositivo y utilice Chrome para navegar fuera del dispositivo.

4.5.2 Configuración y funciones de uso habitual del explorador

Función	Descripción
Resolución de pantalla	Para un rendimiento óptimo, el tamaño mínimo de pantalla es de 1280 × 1024 píxeles para los monitores de escritorio y de 1280 × 800 para las pantallas de portátiles. El tamaño mínimo de pantalla admitido es de 1024 × 768 píxeles.
Idioma	Los idiomas admitidos son: inglés de Estados Unidos, japonés y chino simplificado.
Cerrar ventana	Puede cerrar las ventanas del explorador en cualquier momento. Si se cierra la ventana con una sesión iniciada, la sesión se invalida pasadas 24 horas.
Copiar y pegar	Puede seleccionar y copiar la mayor parte del texto, con la excepción del texto de las imágenes. Puede pegar texto en los cuadros de entrada de texto.
Buscar en una pantalla	Pulse **Ctrl+F** para buscar texto en la pantalla actual.
Historial local	Haga clic con el botón derecho en el botón **Atrás** del explorador para ver el historial de la ficha activa. Utilice esta función para determinar cómo llegó a la pantalla actual.

Función	Descripción
Botones Back (Atrás) y Forward (Adelante)	Puede utilizar los botones **Back** (Atrás) y **Forward** (Adelante) en el explorador para navegar por la interfaz de usuario. **NOTA:** Los cuadros de diálogo emergentes no se consideran pantallas. Si hace clic en el botón **Back** (Atrás) mientras se muestra un cuadro de diálogo emergente, volverá a la pantalla anterior. Si hace clic en el botón **Forward** (Adelante) para ir a un cuadro de diálogo emergente, en su lugar irá a la pantalla con el enlace al cuadro de diálogo emergente. Se exceptúan las pantallas a las que puede acceder directamente desde el menú **Actions** (Acciones). Si utiliza los botones de navegación del explorador con estas pantallas, perderá los cambios sin guardar realizados en dichas pantallas.
Marcadores	Puede crear marcadores para las pantallas de uso común. Puede enviar estos enlaces a otros usuarios, que deberán iniciar sesión y tener la autorización adecuada para acceder a la pantalla.
Abrir pantallas en una nueva ficha o ventana	En el dispositivo, haga clic con el botón derecho en un hiperenlace a un recurso o una pantalla para abrir el enlace en una nueva ficha o ventana. **NOTA:** Si hace clic con el botón derecho en un enlace mientras se encuentra en una pantalla de edición, las acciones que realice en la otra pantalla no actualizarán de forma automática el formulario de la primera pantalla.
Actualizar el explorador	Si hace clic en el botón **Actualizar** del explorador para actualizar una pantalla en la que ha añadido información pero no la ha guardado, perderá la información.
Acercar o alejar	Utilice la función de acercar o alejar para aumentar o disminuir el tamaño del texto.

4.5.3 Requisitos del explorador

El dispositivo cuenta con requisitos específicos del explorador que pueden afectar a su uso. Estos son los exploradores compatibles:

- Microsoft Internet Explorer: versión 10 y versión 11
- Mozilla Firefox: ESR versión 17, Personal edition (última versión)
- Google Chrome (la versión más reciente)

4.5.4 Configuración del explorador para las unidades de medida americanas o del sistema métrico

Para configurar el modo en que se visualizan las unidades de medida, (sistema métrico o sistema americano), cambie los parámetros regionales de la configuración de idioma del explorador.

Las unidades del sistema métrico se utilizan para todas las regiones excepto la de Estados Unidos. Especifique el código de región correspondiente a Estados Unidos si desea unidades tradicionales de Estados Unidos. Especifique cualquier otro código de región si desea unidades del sistema métrico.

Tabla 2 Configuración de unidades de medida del sistema americano o métrico

Explorador	Procedimiento
Google Chrome	1. Haga clic en el icono de menú de Google. 2. Seleccione **Configuración→Mostrar opciones avanzadas** 3. Desplácese hacia abajo hasta **Idiomas** y haga clic en **Configuración de idioma y de introducción de texto** 4. Haga clic en **Añadir** y, a continuación, seleccione el idioma que desea utilizar. 5. Reinicie el explorador para aplicar los cambios.
Microsoft Internet Explorer	La configuración regional y las regiones del explorador se derivan de la configuración de Windows. 1. Seleccione **Herramientas+Opciones de Internet+General (ficha)+Idiomas→Preferencias de idioma**. 2. Especifique sus propias etiquetas de idioma. Haga clic en el botón **Agregar** en el cuadro de diálogo **Preferencias de idioma** y, a continuación, introduzca su etiqueta de idioma en el cuadro **Definido por el usuario**. 3. Haga clic en **Aceptar**. 4. Reinicie el explorador para aplicar los cambios.
Mozilla Firefox	La configuración regional del explorador y de las regiones se derivan de la versión de Firefox que está ejecutando. 1. Seleccione **Herramientas→Opciones→Contenido→Idiomas→Seleccionar**. 2. Seleccione el idioma que desee y haga clic en **Aceptar**. 3. Reinicie el explorador para aplicar los cambios.

4.6 Funciones de los botones

Los botones de la interfaz de usuario tienen la misma función, tanto si aparecen en las pantallas como en los cuadros de diálogo.

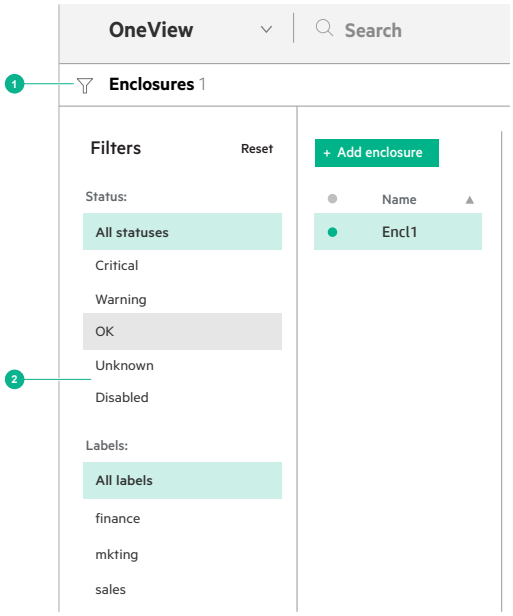
Tabla 3 Botones estándar de la interfaz de usuario

Botón	Descripción
Add (Agregar) y **Add +** (Agregar +)	Agrega elementos del entorno del centro de datos . para la supervisión o la gestión • **Add** (Agregar) agrega un solo elemento y cierra la pantalla o el cuadro de diálogo. • **Add +** (Agregar +) permite agregar otro elemento en el mismo cuadro de diálogo.
Create (Crear) y **Create +** (Crear +)	Crea construcciones lógicas utilizadas por el dispositivo (por ejemplo, perfiles de servidor, plantillas de interconexión lógica y conjuntos de redes). • **Create** (Crear) crea un solo elemento y cierra la pantalla o el cuadro de diálogo. • **Create +** (Crear +) permite crear otro elemento en la misma sesión.
Close (Cerrar)	Cierra una pantalla o un cuadro de diálogo y vuelve a la pantalla anterior.
Cancel (Cancelar)	Descarta los cambios no guardados en una pantalla o un cuadro de diálogo y, a continuación, cierra la pantalla o el cuadro de diálogo.
OK (Aceptar)	Confirma y guarda las entradas y, a continuación, cierra la pantalla o el cuadro de diálogo.

4.7 Barra lateral de filtros

Algunas pantallas de recursos tienen una barra lateral **Filters** (Filtros) que permite controlar la cantidad y el tipo de información que se muestra en el panel de detalles.

Figura 7 Barra lateral de filtros



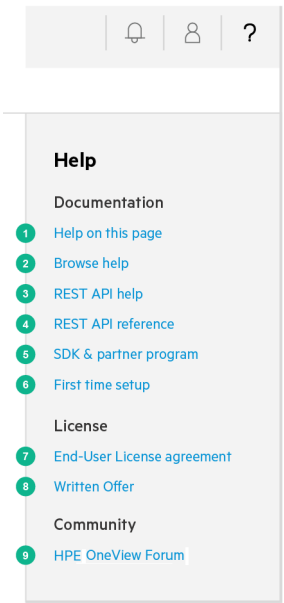
1 Control de posición: al hacer clic en él, cambia entre la barra lateral **Filters** y la barra superior **Filters** (Filtros). Cuando está abierta la barra superior de filtros, los encabezados de filtros se muestran en la pantalla debajo del título del recurso. Cuando se encuentre en la vista de la barra superior, haga clic en el nombre del filtro para acceder a las opciones correspondientes.

2 Los criterios de filtrado le permiten refinar la información que se muestra para un recurso en el panel principal.

4.8 Barra lateral de ayuda

Haga clic en ? en la barra superior para abrir la barra lateral de ayuda. La barra lateral de ayuda proporciona hiperenlaces que dan acceso al sistema de ayuda, el código abierto utilizado en el producto, el programa para socios, los procedimientos de configuración inicial, el contrato de licencia, la oferta por escrito y el foro de usuarios en línea.

Figura 8 Barra lateral de ayuda



1. Abre la ayuda contextual para la pantalla actual en una nueva ventana o ficha del explorador.
2. Abre el nivel superior del contenido de ayuda en una nueva ventana del explorador, lo que le permite navegar por toda la tabla de contenido de la ayuda de la interfaz de usuario.
3. Abre el nivel superior del contenido de la referencia de la API de REST en una nueva ventana del explorador, lo que le permite navegar por toda la tabla de contenido de la referencia de la API de REST.
4. Abre en una nueva ventana del explorador la página web del programa para socios Composable Infrastructure.
5. Se abre en una nueva ventana del explorador la ayuda de configuración inicial, que lo guiará a través de las tareas de configuración inicial para que el dispositivo reconozca los recursos del centro de datos e incluirlos en la gestión.
6. Muestra el Contrato de licencia de usuario final (CLUF).
7. Muestra la Oferta por escrito, que describe los productos de código abierto utilizados por HPE OneView.
8. Abre en una nueva ventana del explorador el **foro de usuarios en línea** donde puede compartir sus experiencias en el uso de HPE OneView, y plantear o contestar preguntas.

4.9 Pantallas de estado del dispositivo

Si se dan determinadas condiciones y situaciones, las pantallas de estado ofrecerán recomendaciones para realizar acciones correctivas o sugerencias y consejos de solución de problemas. Si aparecen dichas pantallas, consulte los temas siguientes para obtener más información.

4.9.1 Starting (Iniciando)

El dispositivo se está iniciando o reiniciando

En principio, se muestra un icono rotativo seguido de una barra de progreso. La barra de progreso avanza conforme se van activando las aplicaciones web del dispositivo. Al finalizar el proceso, se muestra la pantalla de inicio de sesión.

4.9.2 Oops (¡Vaya!)

Se produjo un error grave en el dispositivo que no se pudo recuperar.

El error podría solucionarse reiniciando el dispositivo.

El mensaje de error le aconsejará crear un archivo de volcado de soporte y ponerse en contacto con su representante autorizado de soporte técnico.

4.9.3 Updating the appliance (Actualizando el dispositivo)

Hay una actualización del dispositivo en curso.

El dispositivo se reiniciará cuando se actualice y se mostrará una pantalla de inicio de sesión. Este reinicio no afectará al funcionamiento de los sistemas gestionados.

4.9.4 Temporarily unavailable (No disponible temporalmente)

El dispositivo está fuera de línea o no responde.

Esta pantalla también se muestra después de apagar el dispositivo.

4.9.5 Resetting (Restableciendo)

Actualmente se está restableciendo la configuración predeterminada de fábrica del dispositivo.

La operación de restablecimiento de la configuración predeterminada de fábrica ofrece la opción de conservar o eliminar la configuración de red del dispositivo. Si se elimina, deberá volver a establecer la configuración de red.

Una vez completada la operación de restablecimiento, tendrá que determinar la dirección IP que debe utilizar en la ventana del explorador para poder iniciar una sesión en el dispositivo. Realice una de las acciones siguientes para configurar el dispositivo:

- Restaure el dispositivo a partir de un archivo de copia de seguridad. Consulte «Restauración de un dispositivo a partir de un archivo de copia de seguridad» (página 316).
- Configurar el dispositivo manualmente. Consulte «Configuración inicial de los recursos en HPE OneView» (página 137).

Más información

«Sobre la operación de restauración de fábrica»

4.9.6 Espera

En estos momentos, el dispositivo está esperando los recursos:

- Para que estén disponibles mientras se reinicia.

  Cuando dichos recursos están disponibles, aparece la pantalla de estado **Starting** (Inicio).

- Para que estén disponibles mientras se actualiza.

  Cuando dichos recursos están disponibles, aparece la pantalla de estado **Updating** (Actualizando).

- En modo inactivo mientras se cierra.

  Aparecerá la pantalla de estado **Temporarily unavailable** (No disponible temporalmente).

También existe la posibilidad de que el dispositivo haya detectado algún error. En este caso, aparecerá la pantalla de estado **Oops** (Vaya).

4.10 Descripciones de los iconos

utiliza iconos como controles para el usuario y para mostrar el estado actual de los recursos y las actividades.

- «Iconos de estado y de gravedad»
- «Iconos de control del usuario»
- «Iconos informativos»

4.10.1 Iconos de estado y de gravedad

Icono grande	Icono pequeño	Recurso	Actividad	Tarea
		Crítico	Crítico	Fallo/Interrupción
		Advertencia	Advertencia	Advertencia
		Correcto	Informativo	Correcta
		Desactivado		Cancelada

Icono grande	Icono pequeño	Recurso	Actividad	Tarea
		Desconocido		
		El icono giratorio **en curso** indica que se está aplicando un cambio o se está ejecutando una tarea. Puede aparecer junto a cualquiera de los estados de los recursos. Por ejemplo:		

4.10.2 Iconos de control del usuario

Icono	Nombre	Acción
	Expandir menú	Expande un menú para mostrar todas las opciones
	Ver detalles	Identifica un título que tiene más información. Al hacer clic en el título cambia la vista para mostrar los detalles
	Expandir	Expande un elemento de lista contraído
	Contraer	Contrae un elemento del lista expandido
	Editar	Habilita la función de edición
	Eliminar o quitar	Elimina la entrada actual
	Buscar	Busca el texto que especificó en la casilla **Search** (Buscar). Esto es especialmente útil para encontrar tipos de recursos o recursos específicos por nombre.
	Fijar	La flecha de la izquierda expande o contrae la barra lateral **Filters** (Filtros) La flecha de la derecha expande o contrae la barra lateral **Activity** (Actividad) o la barra lateral **Help** (Ayuda)
	Ordenar	Determina si los elementos se muestran en orden ascendente o descendente

4.10.3 Iconos informativos

Icono	Nombre	Descripción
	Mapa	Proporciona una representación gráfica de las relaciones entre el recurso actual y los demás recursos
	Control de actividad	Proporciona una historia reciente de las tareas y alertas iniciadas por el usuario y el dispositivo

Icono	Nombre	Descripción
	Control de la sesión	Muestra el nombre de inicio de sesión y la duración de su sesión actual. También proporciona un vínculo que puede utilizar para cerrar sesión en el dispositivo. Para cambiar el nombre completo, la contraseña y la información de contacto, haga clic en el icono de edición, que se encuentra junto al nombre de inicio de sesión.
	Control de ayuda	• Cuando el icono se encuentre en la parte superior del cuadro de diálogo, puede hacer clic en él para abrir la ayuda contextual para ese tema en otra ventana o ficha. • En la barra superior, este icono expande o contrae la barra lateral **Help** (Ayuda), donde puede navegar por la documentación de ayuda o encontrar ayuda sobre la pantalla que se muestra actualmente. La barra lateral de ayuda proporciona lo siguiente: ◦ Un hiperenlace **Help on this page** (Ayuda sobre esta página) para acceder a la ayuda contextual para la pantalla actual ◦ Un hiperenlace **Browse help** (Buscar en la ayuda) para acceder a la totalidad del sistema de ayuda ◦ Vínculos que puede utilizar para mostrar el CLUF (Contrato de licencia de usuario final) y la Oferta por escrito. ◦ Un enlace al **Foro de HPE OneView**, un foro en línea que permite a los clientes y socios compartir sus experiencias y hacer preguntas relacionadas con el uso de HPE OneView. Tanto los miembros de la comunidad como los representantes de Hewlett Packard Enterprise son bienvenidos para ayudar a responder las preguntas.

4.11 Detalles de la pantalla de etiquetas

La vista **Labels** (Etiquetas) le permite ver las etiquetas para un recurso. Pueden utilizarse etiquetas para organizar los recursos en grupos. por ejemplo, puede que desee identificar los servidores utilizados principalmente por el equipo financiero o los sistemas de almacenamiento asignados a la división de Asia Pacífico. Puede filtrar y buscar etiquetas en todos los tipos de recursos o dentro de un recurso determinado.

4.12 Detalles de la pantalla de la vista de mapa

La vista **Map** (Mapa) permite examinar la configuración y entender las relaciones entre los recursos lógicos y físicos del centro de datos. Esta vista le da una visibilidad inmediata de los recursos, desde cada una de las redes Ethernet, Fibre Channel y FCoE, hasta los receptáculos, bastidores y el centro de datos físico de nivel superior.

La vista **Map** (Mapa) se ha diseñado para que sea altamente interactiva y útil incluso a escala.

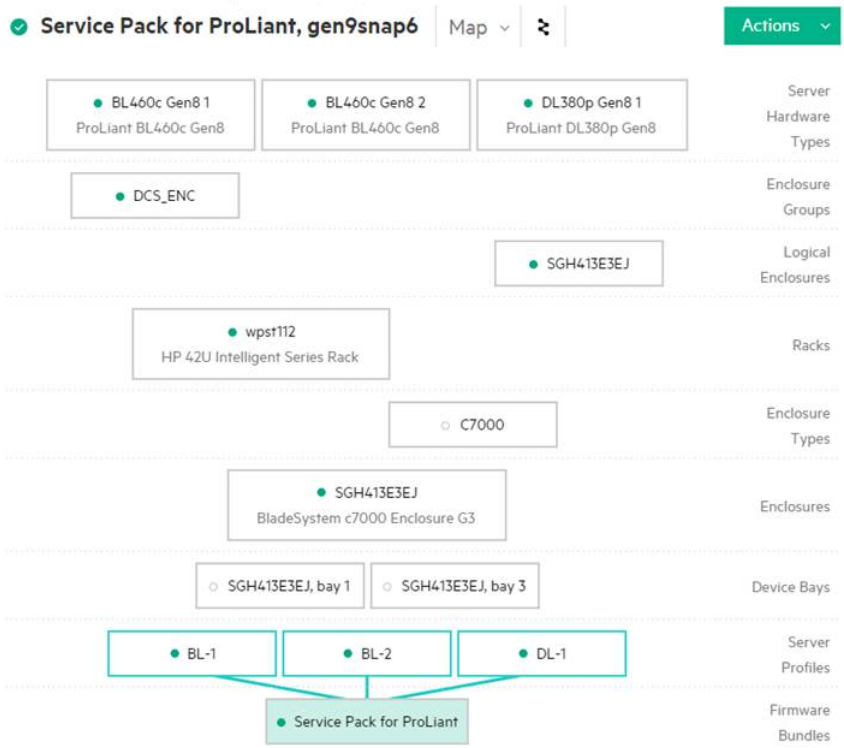
Para abrir la vista de relaciones de un recurso, realice una de las acciones siguientes:

- Seleccione **Map** (Mapa) en el selector de vista.
- Seleccione el icono .

Proporcionar el contexto de un recurso puede ser útil para solucionar problemas con el recurso. Al observar la vista **Map** (Mapa), se puede determinar si cualquier aspecto relacionado con el recurso también presenta algún problema.

Un icono de estado indica el estado general del recurso y proporciona un método rápido para detectar errores.

Figura 9 Ejemplo de vista Map (Mapa)



El recurso seleccionado se encuentra en el centro de la vista **Map** (Mapa). Todo lo que está por encima del recurso es un antecesor; todo lo que está por debajo del recurso es un descendiente.

Una línea de conexión entre los cuadros indica una relación directa, como la de los servidores con su receptáculo. Pase el puntero por encima de cualquier recurso para ver sus relaciones directas con otros recursos. Otros elementos pueden estar relacionados indirectamente con el recurso, tales como los grupos de interconexiones lógicas y los perfiles de servidor.

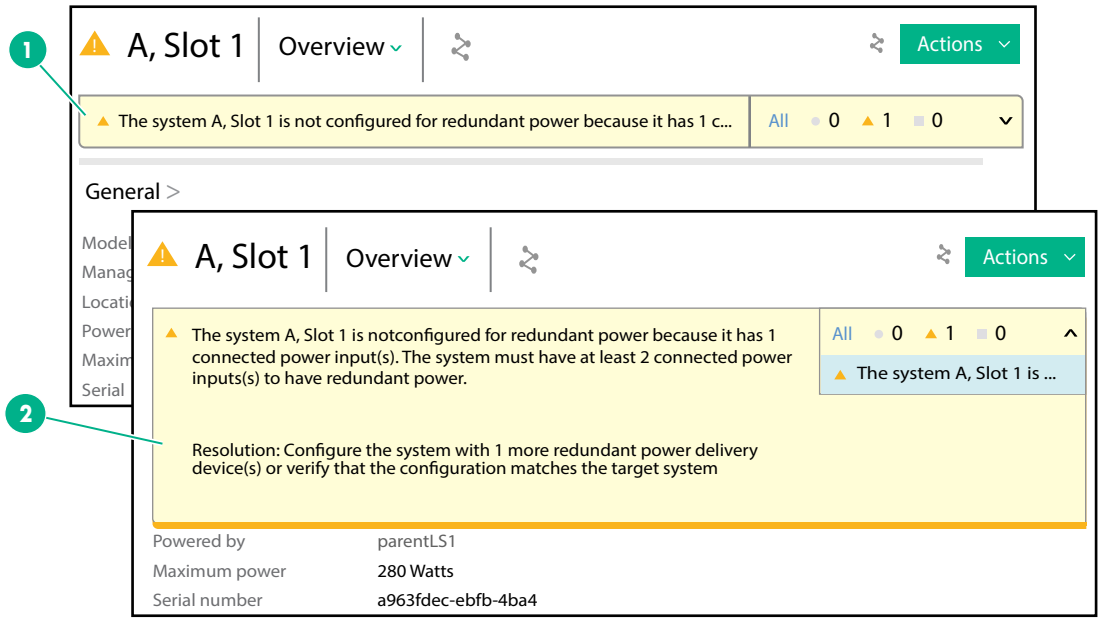
Haga clic en cualquier recurso que aparece en una vista de relación para abrir su vista **Map** (Mapa) específica.

4.13 Área de notificaciones

El área de notificaciones de la pantalla de la interfaz de usuario de un recurso aparece cuando una actividad (una alerta o una tarea) ha afectado al recurso, lo que podría requerir su atención.

De forma predeterminada, en el área de notificaciones aparece una línea de información. Haga clic en cualquier lugar del cuadro amarillo para expandir el área de notificaciones y ver más información relacionada con la actividad. Haga clic de nuevo para cerrar el área de notificaciones.

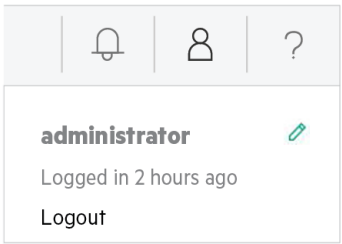
Figura 10 Área de notificaciones



1. Un área de notificaciones contraída (valor predeterminado). Seleccione **All** (Todo) para ver todas las actividades relacionadas con el recurso.
2. Un área de notificaciones expandida, que ofrece soluciones a alertas críticas o de advertencia que requieren su atención, con enlaces a los **Details** (Detalles), cuando están disponibles.

4.14 Cierre de sesión en el dispositivo

1. Haga clic en el icono Control de la sesión de la barra superior.
2. Seleccione **Logout** (Cerrar sesión).



4.15 Organización de los recursos en grupos mediante la asignación de etiquetas

Las etiquetas identifican los recursos para que pueda organizarlos en grupos. Cuando etiquete los recursos, podrá verlos rápidamente haciendo búsquedas por etiquetas.

Requisitos previos

- Privilegios necesarios: privilegios de edición para el recurso

Agregar una nueva etiqueta a un recurso

1. En el menú principal, seleccione el recurso y, a continuación, seleccione la instancia de recurso que desea etiquetar.
2. Seleccione **Labels** (Etiquetas) en el selector de vista.
3. Seleccione el icono .

4. Siga estas pautas para crear un nombre de etiqueta:
   - Las etiquetas no distinguen entre mayúsculas y minúsculas, pero se muestran como se han introducido.
   - Las etiquetas deben ser alfanuméricas y tener un máximo de 80 caracteres. Las etiquetas pueden contener espacios.
5. Haga clic en **Agregar**.

   Se muestras las nuevas etiquetas.
6. Haga clic en **OK** (Aceptar) para agregar las etiquetas a este recurso.

Agregar una etiqueta existente a un recurso

1. En el menú principal, seleccione la categoría del recurso y, a continuación, seleccione la instancia de recurso que desea etiquetar.
2. Seleccione **Labels** (Etiquetas) en el selector de vista.
3. Seleccione el icono .
4. Determine si desea buscar todas las etiquetas o una etiqueta concreta.
   - Para buscar todas las etiquetas para este tipo de recurso, haga clic en . Desplácese por la lista para encontrar la etiqueta que desea.
   - Para buscar una etiqueta concreta, en el cuadro **Name** (Nombre), escriba un nombre de etiqueta existente o una parte del nombre y, a continuación, haga clic en .
5. Seleccione la etiqueta existente y haga clic en **Add** (Agregar).
6. Haga clic en **OK** (Aceptar) para agregar la etiqueta al recurso.

Borrado de una etiqueta de un recurso

1. En el menú principal, seleccione el recurso y, a continuación, seleccione la instancia de recurso de la que desea borrar una etiqueta.
2. Seleccione **Labels** (Etiquetas) en el selector de vista.
3. Seleccione el icono .
4. Haga clic en el icono **Delete** (Eliminar) × de la etiqueta que desea eliminar de este recurso.
5. Haga clic en **OK** (Aceptar) para eliminar la etiqueta del recurso.

Búsqueda de recursos por etiqueta

1. Haga clic en el cuadro de **Smart Search** (Búsqueda inteligente) y escriba **`labels:`** seguido del nombre de la etiqueta.

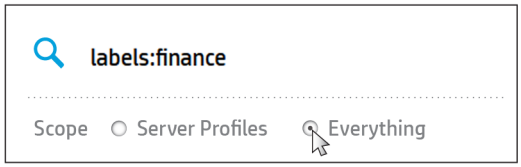
SUGERENCIA: Introduzca palabras o nombres completos como criterios de búsqueda. Es posible que si usa partes de palabras o nombres no obtenga los resultados esperados.

Para buscar una etiqueta con un espacio, escriba el nombre de etiqueta entre comillas. Por ejemplo, **`labels:"División Asia Pacífico"`**.

2. Determine si desea buscar una etiqueta concreta para el tipo de recurso o busque una etiqueta entre todos los tipos de recursos.
   - Para buscar una etiqueta para un tipo de recurso concreto:
     a. Seleccione el **Scope** (Ámbito) para el tipo de recurso.
     b. Pulse **Intro**.

     Aparecerán los recursos que compartan dicha etiqueta.

- Para buscar una etiqueta entre todos los tipos de recursos:
  a. Seleccione **Everything** (Todo) para el **Scope** (Ámbito).



  a. Pulse **Intro**.

  En una página de resultados de la búsqueda aparecerán las mejores coincidencias para todos los tipos de recursos.

  b. Haga clic en una instancia de recurso (hipervínculo) en la página de resultados para ir al recurso en cuestión.

  Aparecerá la vista **Overview** (Información general) del recurso.

4.15.1 Visualización de recursos por etiqueta

En la mayoría de las pantallas, puede filtrar la vista de instancias de recursos por su etiqueta.

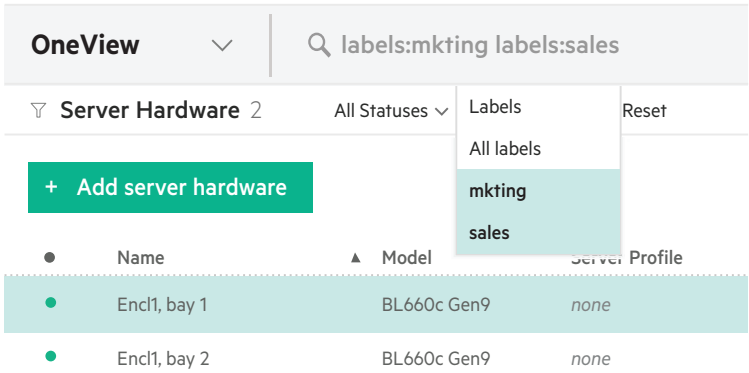
El filtro por defecto es **All labels** (Todas las etiquetas), que muestra todas las instancias de recursos.

Para filtrar la vista en base a una o varias etiquetas, selecciónelas en el menú **Labels** (Etiquetas). Se muestran todas las instancias de recursos con dichas etiquetas.

Para borrar los filtros de etiqueta seleccionados, seleccione **All labels** (Todas las etiquetas).

NOTA: Se muestran hasta 100 etiquetas para el recurso. Si no ve la etiqueta que está buscando, consulte "Organizing resources into groups by assigning labels" (Organización de recursos en grupos asignándoles etiquetas) en la ayuda en línea.

Filtrado de recursos mediante etiquetas

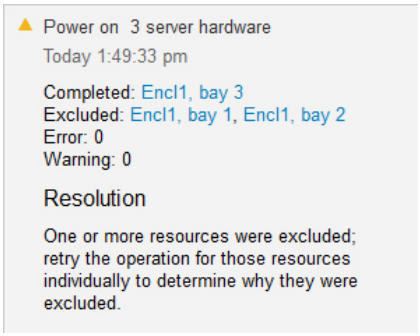


4.16 Realización de una acción en varios recursos a la vez

Para algunas acciones, se pueden seleccionar varios recursos. De esta forma, no tendrá que realizar la accion en cada uno de ellos por separado. Por ejemplo, puede encender varios blades de servidor con una sola operación. Cada acción realizada con una instancia de un recurso se registra individualmente en la pantalla **Activity** (Actividad).

Si la acción no se puede realizar en una instancia de un recurso determinado, dicho recurso se excluye de la acción. Por ejemplo, si intenta encender un servidor que ya esté encendido, no se realiza la acción en dicho servidor. Al abrirse la «Barra lateral de actividad» para una

acción, se muestran los resultados. En este ejemplo, se muestra que se ha encendido un servidor y que se excluyeron dos:



Si se excluye algún recurso la acción, aparecerá un icono de advertencia o estado crítico. Los recursos se excluyen cuando no es posible realizar la acción; por ejemplo, si se intenta eliminar un perfil de servidor para un servidor que está encendido. Si se excluyen de varios recursos, seleccione un único recurso y vuelva a intentar de nuevo la acción para determinar por qué se ha excluido ese recurso.

Utilice las combinaciones de teclas siguientes para seleccionar varios recursos en el panel principal:

- Para seleccionar un intervalo contiguo de objetos, seleccione el primer recurso en el intervalo y mantenga pulsada la tecla **Mayús** mientras selecciona el último recurso del intervalo.
- Para seleccionar objetos individuales, pulse **Ctrl** y manténgalo pulsado mientras los selecciona.

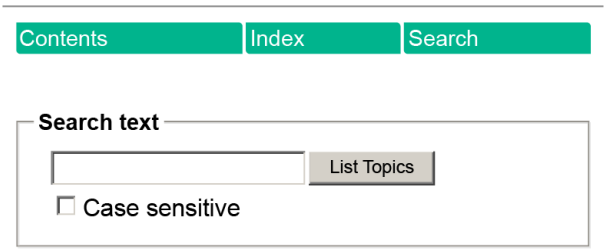
Utilice la tecla **Ctrl** para anular la selección de cualquier objeto seleccionado anteriormente.

4.17 Búsqueda en los temas de ayuda

1. En cualquier pantalla, haga clic en el icono ? de la barra superior para abrir la barra lateral de ayuda.
2. En la barra lateral **Help** (Ayuda), seleccione **Help on this page** (Ayuda sobre esta página).

   La ayuda contextual aparece en una ventana independiente del explorador.
3. En la nueva ventana del explorador en la que aparece la ayuda, haga clic en **Search** (Buscar) en la parte superior del panel de navegación izquierdo, junto a los enlaces **Contents** (Contenido) e **Index** (Índice).

   Figura 11 Cuadro de búsqueda de la ayuda de la interfaz de usuario



4. Escriba el término que desea buscar en el cuadro **Search** (Buscar).
5. Pulse **Intro** o haga clic en **List Topics** (Lista de temas) para iniciar el proceso de búsqueda.

   Los resultados de la búsqueda se presentan como enlaces a las secciones en las que aparece el término de búsqueda.

6. Examine los resultados de la búsqueda y localice el título o títulos de sección que mejor coincidan con lo que está buscando, y haga clic en el enlace para ver el contenido. El término de búsqueda aparece resaltado en amarillo cada vez que aparece para que pueda identificarlo fácilmente.

Más información

«Funciones y limitaciones de la búsqueda en la ayuda»

4.17.1 Funciones y limitaciones de la búsqueda en la ayuda

Características

Diferenciación entre mayúsculas y minúsculas.	De forma predeterminada, la búsqueda distingue entre mayúsculas y minúsculas. La casilla de verificación de diferenciación entre mayúsculas y minúsculas le permite buscar haciendo coincidir las mayúsculas o minúsculas de la palabra o frase que escriba.
Coincidencias de frases y palabras completas	Puede buscar palabras completas o con guiones. La búsqueda de frases le permite buscar documentos que contengan una frase exacta escribiendo el texto a buscar entre comillas dobles (`"`). No incluya caracteres especiales en el texto de búsqueda en la búsqueda de una frase.
Caracteres comodín	La función comodín le permite cambiar letras sueltas, o secuencias de letras, dentro de la palabra a buscar. Utilice un signo de interrogación (`?`) para sustituir un solo carácter. Utilice un asterisco (`*`) para representar varios (o cero) caracteres.
Caracteres pegados con el teclado	Puede que cuando escriba una palabra clave a buscar, le sea útil copiarla desde otra ventana, para ello, haga clic con el botón derecho en el cuadro de texto y seleccione **Paste** (Pegar).
Operadores booleanos	Esta función le permite combinar palabras clave con operadores booleanos para producir resultados más relevantes. Utilice un carácter de espacio para el Y booleano. Utilice `OR` u `or` para el booleano O. Utilice un carácter de guion (`-`) para NO.
Completar automáticamente	La función de completar automáticamente supervisa lo que está escribiendo y, tras escribir los primeros caracteres, muestra una lista de palabras sugeridas. Si una de dichas palabras coincide con la que intentaba escribir, puede seleccionarla de la lista.
Resaltar	El resaltado de la búsqueda resalta las palabras clave o frase buscadas en los documentos resultantes.
Búsqueda aproximada	Como si de un corrector ortográfico se tratara, la búsqueda aproximada intenta corregir el texto de búsqueda mal escrito y sugiere el texto corregido.

Búsqueda por proximidad	La búsqueda por proximidad busca documentos en los que dos o más ocurrencias de palabras estén separadas como mucho por diez palabras. Los operadores de búsqueda de proximidad son `NEAR` (cerca) y `FBY` (que significa “seguido de”). Estos operadores se pueden escribir en mayúsculas o minúsculas.
Búsqueda de sinónimos	Esta función sugiere enlaces a sinónimos de la palabra clave.

Limitaciones

Caracteres especiales	La búsqueda de palabras no admite los caracteres especiales. La función de búsqueda no devuelve temas ni entradas del índice que contienen caracteres especiales, como el símbolo de copyright, por ejemplo. El carácter de barra diagonal (`\`) no está permitido en el interior de una frase.
Guion	La función de búsqueda no devuelve temas ni entradas del índice que contienen guiones.
Palabras comunes	La función de búsqueda no devuelve palabras comunes, por ejemplo, `una`, `un` y `el`.
Initials (Iniciales)	La función de búsqueda no devuelve temas ni entradas del índice que contienen iniciales, tales como `L.P.`.
Búsquedas booleanas	Los nombres de los operadores booleanos deben escribirse en inglés. Los operadores booleanos AND (Y) u OR (O) no se pueden combinar en un texto de búsqueda. Los operadores NOT (NO) deben estar al final de la cadena de búsqueda.
Búsquedas por proximidad	Los operadores de proximidad deben escribirse en inglés.

Más información

«Búsqueda en los temas de ayuda»

4.18 Búsqueda de recursos

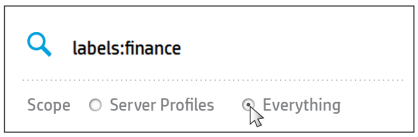
En la barra superior de cada pantalla se incluye la función **Smart Search** (Búsqueda inteligente), que permite encontrar información específica sobre los recursos, como los nombres de determinados recursos, números de serie, WWN (World Wide Name) y direcciones IP y MAC.

En general, se puede buscar todo lo que aparece en el panel principal para un recurso.

Smart Search hace que la localización de los recursos sea sencilla, lo que permite realizar un inventario o llevar a cabo acciones con un conjunto determinado de equipos.

Tal vez esté buscando todos los recursos de un receptáculo determinado o tiene que encontrar un servidor con una dirección MAC determinada. La búsqueda inteligente le proporciona al instante la información que está buscando.

El comportamiento de búsqueda predeterminado se centra en el recurso que está viendo actualmente. Sin embargo, para ampliar el ámbito de la búsqueda a todos los recursos, debe seleccionar la opción de buscar en **Everything** (Todo), que busca en todos los recursos.

Búsqueda en el recurso actual	Búsqueda en todos los recursos
1. Haga clic en el cuadro **Smart Search** (Búsqueda inteligente).  2. Escriba el texto que desea buscar y pulse **Intro**. Los resultados de búsqueda se centran en su ubicación actual en la interfaz de usuario.	1. Haga clic en el cuadro **Smart Search** (Búsqueda inteligente).  2. Seleccione **Everything** (Todo).  3. Escriba el texto que desea buscar y pulse **Intro**.

Es posible que algunos recursos no incluyan la opción de elegir entre el recurso actual o todos, en cuyo caso la búsqueda predeterminada se realiza en todos.

Cuando se empieza a escribir, se proporcionan sugerencias de búsqueda basadas en la coincidencia de patrones y en los criterios de búsqueda introducidos previamente.

- Puede seleccionar una sugerencia (la pantalla muestra datos que contienen esa selección) o hacer clic en **Enter** (Intro).
- Si el término de búsqueda es un recurso, se filtra la lista de recursos del panel principal para que coincida con el término.

SUGERENCIA:

- Introduzca palabras o nombres completos como criterios de búsqueda. Es posible que si usa partes de palabras o nombres no obtenga los resultados esperados.
- Si introduce un término de búsqueda de varias palabras, los resultados contendrán todas las palabras introducidas.
- Encierre un término de búsqueda entre comillas dobles (″) si el término de búsqueda contiene espacios.

Cuando encuentre lo que busca en los resultados de búsqueda, que están organizados por tipo, seleccione el elemento al que desea acceder.

NOTA: La función **Smart Search** (Búsqueda inteligente) no busca en el sistema de ayuda. Para saber cómo buscar en la ayuda de la interfaz de usuario y de la API de REST, consulte «Búsqueda en los temas de ayuda».

La selección del filtro más reciente se muestra en el cuadro **Smart Search** (Búsqueda inteligente).

Tabla 4 Búsqueda y filtrado avanzados mediante propiedades

Ejemplo de sintaxis de filtrado avanzado	Resultados de búsqueda

Por nombre de modelo:
`model:"BladeSystem c7000 Enclosure G2"`
`model:"ProLiant BL460c Gen8"`
`model:"VC 8Gb 20-Port FC Module"`
	Todo el hardware que coincide con el nombre y el número de modelo.

Por nombre o dirección: `name:enclosure10`	Un receptáculo denominado `enclosure10`.
`name:"192.0.2.0, PDU 1"`	Un dispositivo de suministro de energía denominado `192.0.2.0, PDU 1`.
`name:"192.0.2"`	Una lista de máquinas físicas cuyas direcciones IP comienzan por `192.0.2`.
`name:"mysystem"`	Una lista de máquinas físicas cuyo nombre de host es `mysystem`.
Por estado: `status:Critical`	Todos los recursos que se encuentran en un estado crítico. Para otros valores de estado, consulte «Niveles de gravedad de las actividades».
Por recurso asociado: `Associated resource category:Networks"`	All Networks (Todas las redes)
Por rol de usuario: `roles:"network administrator"`	Todos los usuarios (por nombre) que tienen asignada la función de administrador de la red. Para otros valores para rol, consulte «Acerca de los roles de usuario».
Por propietario: `owner:Administrator`	Todos los recursos y mensajes cuyo propietario es el administrador de infraestructuras.
Por fecha: `created:<7d`	Creado durante los últimos 7 días.
Perfeccionamiento de los resultados mediante la combinación de propiedades:	

Un carácter de espacio que separa dos objetos del mismo tipo funciona como un OR lógico.
`model:"ProLiant BL460c Gen8"`
`model:"ProLiant BL460c Gen9"`
	Todo el hardware ProLiant BL460c Gen8 y ProLiant BL460c Gen9.

`status:Critical status:Warning`	Todos los recursos que se encuentran en un estado crítico o de advertencia.
Un carácter de espacio que separa dos objetos de tipos distintos funciona como un AND. `owner:Administrator firmware`	Todas las actividades cuyo propietario es el administrador y que están relacionadas con el firmware.
`NTP status:critical`	Todos los mensajes críticos relacionados con NTP.

Tabla 4 Búsqueda y filtrado avanzados mediante propiedades *(continuación)*

Ejemplo de sintaxis de filtrado avanzado	Resultados de búsqueda
`status:unknown state:locked owner:Administrator`	Todos los mensajes cuyo estado se desconoce o está bloqueado y cuyo propietario es el administrador.
Combinación de operaciones AND y OR El operador `OR` (O) resulta útil para la especificación de objetos similares. El operador `AND` (Y) resulta útil para la combinación de objetos diferentes.	
`status:critical OR status:disabled`	Todos los mensajes con el estado Critical (Crítico) o Warning (Advertencia).
`name:host.example.com status:Critical status:Warning`	Todos los mensajes cuyo estado es crítico o advertencia y que están relacionados con el recurso `host.example.com`.
`associatedresourcecategory:network OR associatedresourcecategory:Network sets`	Todos los mensajes que pertenecen a las categorías de recursos Network (Red) o Network Sets (Conjuntos de redes)
`associatedresourcecategory:power-devices AND status:warning OR status:critical`	Todos los mensajes Critical (Crítico) o Warning (Advertencia) para la categoría de recursos de dispositivos de alimentación.
Operación NOT `status:Warning NOT model:"ProLiant BL465c G7"`	Todos los mensajes cuyo estado es advertencia, excepto aquellos que se aplican al modelo ProLiant BL465c G7 **NOTA:** Solo se puede usar NOT una vez en cada consulta. Los operadores NOT adicionales se consideran texto.

4.18.1 Borrado del cuadro de búsqueda inteligente

El cuadro **Smart Search** (Búsqueda inteligente) conserva las opciones de filtro. Utilice este procedimiento para borrarlas antes de introducir un parámetro de búsqueda.

Borrado del cuadro de búsqueda inteligente

1. En el menú principal, vaya a la pantalla **Activity** (Actividad).
2. Haga clic en **Reset** (Restablecer) en el **encabezado de la actividad** o en la **barra lateral de filtro de actividad**.

4.19 Visualización de recursos según su estado

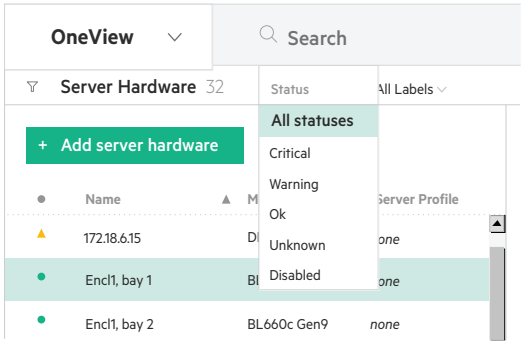
En la mayoría de las pantallas, puede filtrar la vista de las instancias de recursos en función de su estado, lo que podría ser útil para tareas de solución de problemas o de mantenimiento.

El filtro predeterminado es **All statuses** (Todos los estados), que significa que se muestran todos los miembros del recurso, independientemente de su estado.

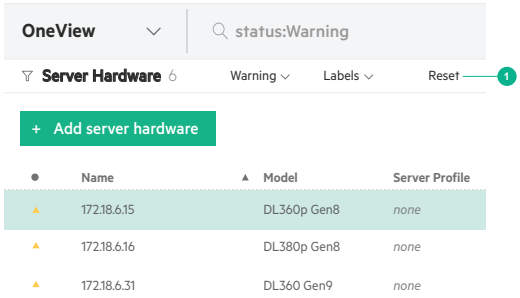
Para filtrar esa vista basándose en un estado específico, seleccione el estado que desea ver en el menú **Status** (Estado).

Para obtener más información sobre los iconos de estado y su significado, consulte «Descripciones de los iconos».

Figura 12 Filtrado de las instancias de los recursos por su estado



4.19.1 Restablecimiento de la vista de estado



1 Para volver a la vista predeterminada, **All statuses** (Todos los estados), haga clic en el enlace **Reset** (Restablecer).

5 Uso de las API de REST y otras interfaces de programación

REST (Representational State Transfer) es un servicio web que utiliza operaciones CRUD (creación, lectura, actualización y eliminación) básicas que se llevan a cabo en los recursos mediante los métodos `POST`, `GET`, `PUT` y `DELETE` del protocolo HTTP. Para obtener más información acerca de los conceptos de REST, consulte **http://en.wikipedia.org/wiki/Representational_state_transfer**.

El dispositivo tiene una arquitectura orientada a recursos que proporciona una interfaz REST uniforme. Cada recurso tiene un URI (Uniform Resource Identifier) y representa un dispositivo físico o una construcción lógica. Puede utilizar las API de REST para manipular los recursos.

5.1 Operaciones con recursos

Las API de RESTful no tienen estado. El gestor de recursos mantiene como representación de los recursos el estado que se devuelve para los recursos. El cliente mantiene el estado de la aplicación y podría manipular el recurso localmente, pero hasta que no se use un método `PUT` o `POST`, el recurso, tal como lo conoce el gestor de recursos, no cambia.

Operación	Método de HTTP	Descripción
Create (Creación)	`POST` URI del recurso (carga = datos del recurso)	Crea nuevos recursos. Una solicitud `POST` síncrona devuelve el recurso recién creado. Un solicitud `POST` asíncrona devuelve un URI `TaskResource` en el encabezado `Location`. Este URI realiza el seguimiento del progreso de la operación `POST`.
Read (Lectura)	`GET` URI del recurso	Devuelve las representaciones del recurso solicitado
Update (Actualización)	`PUT` URI del recurso (carga = datos de actualización)	Actualiza un recurso existente
	`PATCH` URI del recurso (carga = datos de actualización)	Actualiza una parte del recurso. Por ejemplo, cuando solo se necesita actualizar un campo del recurso.
Delete (Eliminación)	`DELETE` URI del recurso	Elimina el recurso especificado

5.2 Códigos de devolución

Código de devolución	Descripción
2*xx*	Operación correcta
4*xx*	Error del lado del cliente con el mensaje de error devuelto
5*xx*	Se ha devuelto un error del dispositivo con mensaje

NOTA: Si se produce un error, lo que se indica mediante un código de devolución 4*xx* o 5*xx*, se devuelve un `ErrorMessage`. El modelo de recurso esperado no se devuelve.

5.3 Formato de los URI

Todos los URI hacen referencia a recursos. El cliente no tiene que crear ni modificar los URI. El URI de un recurso es estático y utiliza el formato `https://{appl}/rest/categoría del recurso/ID del recurso`, donde:

`https://{dispositivo}`	Dirección del dispositivo
`/rest`	El tipo de URI
`/categoría del recurso`	La categoría del recurso (por ejemplo, `server-profiles`)
`/ID de instancia del recurso`	El identificador de instancia de un recurso determinado (opcional)

5.4 Formato del modelo de recursos

Los recursos son compatibles con JSON (JavaScript Object Notation) para el intercambio de datos mediante una API de REST. Si no se especifica otra cosa en la operación de la API de REST, el valor predeterminado es JSON.

5.5 Inicio de sesión en el dispositivo mediante las API de REST

Cuando inicia sesión en el dispositivo usando la API de REST `login-sessions`, se devuelve un identificador de sesión. Utilice el ID de sesión en todas las operaciones de la API de REST posteriores en el encabezado `auth`. El identificador de sesión es válido durante 24 horas.

Inicio de sesión	Fin de sesión

Operación
`POST`
API
`/rest/login-sessions`
Encabezados de la solicitud
Encabezados de solicitud de la API de REST
Cuerpo de la solicitud
`{"userName":"SuNombreDeUsuario","password":"SuContraseña"}`
NOTA: Este es un ejemplo de un inicio de sesión local en el dispositivo. Si está utilizando un servicio de directorio, debe agregar los siguientes atributos: `authnHost` y `authLoginDomain`.
Respuesta
El `LoginSessionIdDTO` que incluye el identificador de sesión
	Operación
	`DELETE`
	API
	`/rest/login-sessions`
	Encabezados de la solicitud
	`auth:{SuIdDeSesión}`
	Encabezados de solicitud de la API de REST
	Cuerpo de la solicitud
	Ninguno
	Respuesta
	`204 No Content`

5.6 Versión de la API de REST y compatibilidad con versiones anteriores

Para realizar una operación API de REST, se necesita un encabezado `X-API-Version`. Este encabezado de versión corresponde a la versión de la API de REST del software que se está ejecutando en el dispositivo. Para determinar la versión de la API de REST correcta, ejecute `/rest/version`. Esta operación `GET` no requiere un encabezado `X-API-Version`. Si se están ejecutando varios dispositivos en su entorno, es necesario determinar la versión de la API de REST que requiere cada dispositivo.

NOTA: Si la solicitud no incluye un encabezado `X-API-Version`, las API toman la versión 1 como valor predeterminado. Puesto que la mayoría de las API de HPE OneView son como mínimo de la versión 3 o posterior, al llamar a una API sin incluir el encabezado `X-API-Version` es probable que se produzca un error HTTP 404, porque no se encontrará esa versión de la API.

Las solicitudes que se documentan en la ayuda de secuencias de comandos de la API de REST de HPE OneView 3.0 se corresponde con el `número de versión` de 300. Las solicitudes que

especifiquen la versión de la API 200 se comportan como se documenta aquí. Los próximos cambios de la API introducirán números de versión superiores.

Versiones de la API de REST admitidas

Esta versión de HPE OneView es compatible con la nueva versión 300 de la API de REST, además de admitir la versión 3 de la API de REST (mínimo), que se admitía en las revisiones anteriores de HPE OneView.

La documentación de la API de REST de HPE OneView para versiones anteriores de la API de REST está disponible en línea en www.hpe.com/info/oneview/docs y la documentación de la versión actual de las API de REST admitidas se incluyen con la ayuda en línea de esta revisión. También está disponible en línea.

Compatibilidad con versiones anteriores

En la siguiente lista se explica cómo conservar las secuencias de comandos existentes cuando se actualiza a una versión de HPE OneView más reciente, a aprovechar las ventajas de la nueva funcionalidad y a encontrar la versión actual y las anteriores de la documentación de la API de REST de HPE OneView.

- **Evitar la interrupción de las secuencias de comandos**

  Para evitar la interrupción de las secuencias de comandos existentes escritas para una versión específica de la API, utilice el mismo valor de `X-API-Version` para dicha API de REST en concreto. Esto garantiza que se envía el mismo conjunto de datos y que se devuelve en el cuerpo de la respuesta durante las operaciones `PUT` y `POST`.

  NOTA: El conjunto de posibles valores enumerados que se pueden devolver en un atributo de recurso determinado puede aumentar de una revisión a otra (independientemente de la versión de la API). Los clientes deben hacer caso omiso de los valores que no esperen.

  Para mantener la compatibilidad con versiones anteriores, no se reducirá el conjunto de valores enumerados y su significado no se cambiará para una versión de la API determinada.

  NOTA: El índice o SCMB siempre devuelve la versión más reciente de los datos del recurso, independientemente de lo que se envía en el encabezado `X-API-Version` de la solicitud (este encabezado controla el modelo DTO del índice, pero no los datos que contiene). Para obtener una versión específica de los datos de un recurso, lleve a cabo una operación `GET` en el URI del recurso con el encabezado `X-API-Version` que desee.

- **Uso de las nuevas funciones**

  Para poder utilizar las nuevas funciones, debe moverse al nuevo valor `X-API-Version`. Si se configura globalmente el valor `X-API-Version` en sus secuencias de comandos, es probable que al pasarse a la nueva `X-API-Version` varias API de REST se vean afectadas. Para ver una lista de las API de REST que hayan cambiado, consulte las ***Notas de la visión de HPE OneView***.

  Si no necesita utilizar la nueva funcionalidad, puede utilizar un valor anterior de `X-API-Version` para evitar que sus secuencias de comandos existentes se vean afectadas. Hewlett Packard Enterprise le recomienda pasarse a la nueva `X-API-Version`, ya que no se garantiza la compatibilidad con versiones anteriores de una versión a otra; las funciones antiguas dejarán de utilizarse.

  La versión actual de las API de REST se documentan en la *Referencia de la API de REST de HPE OneView* que se incluye en el dispositivo. Para ver las versiones anteriores de la referencia de la API de REST, visite www.hpe.com/info/oneview/docs.

5.7 Operaciones asíncronas frente a síncronas

Una operación síncrona devuelve una respuesta después de que la API de REST termine. Por ejemplo, `POST /rest/server-profiles` devuelve un perfil de servidor que acaba de crear en el cuerpo de la respuesta. Una operación asíncrona, como crear una copia de seguridad de un dispositivo, devuelve la URI de una tarea en el encabezado de respuesta Location (Ubicación). Puede utilizar la URI de la tarea para recuperar el estado actual de la operación y para obtener el recurso asociado cuando se complete la tarea.

- Esto es un comportamiento habitual para todas las API asíncronas.
- No debería depender de ningún otro comportamiento para obtener el estado actual de la operación (como el contenido del cuerpo de la respuesta devuelta), dado que varía de una API a OTRA.

  Consulte la *API Reference* (Referencia de la API) para conocer el comportamiento de cada API en concreto.
- No debería depender de que se produzca ningún otro comportamiento, dado que está sujeto a cambio en el futuro, incluso para la misma versión de la API.

Ejemplo 1 Ejemplo de encabezado de respuesta devuelto desde una llamada REST de copia de seguridad de un dispositivo

```
HTTP/1.1 202 Accepted
Date: Tue, 26 Jan 2016 23:19:14 GMT
Server: Apache
Ubicación: https://<nombre del anfitrión>/rest/tasks/39CE80C4-EF2C-4717-90EA-EF166E83B49F
Content-Length: 0
cache-control: no-cache
```

5.8 Recurso de tarea

Cuando se realiza una operación asíncrona de la API de REST, se devuelve el estado HTTP `202 Accepted`, y se devuelve el URI de un modelo de recursos `TaskResource` en el encabezado `Location` de la respuesta.

A continuación, puede realizar una operación `GET` con el URI del modelo `TaskResource` para sondear el estado de la operación asíncrona. El modelo `TaskResource` también contiene el nombre y el URI del recurso que se ve afectado por la tarea en el atributo `associatedResource`.

Ejemplo de creación de una copia de seguridad del dispositivo

1. Cree una copia de seguridad del dispositivo.

   `/rest/backups`

   En la respuesta se devuelve el URI de un modelo `TaskResource` en el encabezado `Location`.
2. Compruebe el estado de la copia de seguridad mediante el URI del modelo `TaskResource` devuelto en el paso 1.

   `/rest/tasks/{id}`
3. Cuando la tarea alcance el estado `Completed`, utilice el URI de `associatedResource` en el modelo `TaskResource` para descargar el archivo de copia de seguridad.

   `GET {associatedResource URI}`

5.9 Tratamiento de errores

Si se produce un error durante una operación de la API de REST, se devuelve un error 4*xx* (lado del cliente) o 5*xx* (dispositivo) junto con un mensaje de error (modelo de recursos `ErrorMessage`). El mensaje de error contiene una descripción y puede contener acciones recomendadas para corregir el error.

Una operación `POST` correcta de la API de REST devuelve el recurso que se acaba de crear (operación síncrona) o un URI `TaskResource` en el encabezado Location (operación asíncrona).

5.10 Control de concurrencia mediante etags

El cliente utiliza etags para comprobar la versión del modelo de recursos. Esto evita que el cliente pueda modificar (`PUT`) una versión del modelo de recursos que no está actualizada. Por ejemplo, si un cliente realiza una operación `GET` en un perfil de servidor y recibe una etag en el encabezado de la respuesta, modifica el perfil de servidor y, a continuación, actualiza (`PUT`) el modelo de recursos, la etag del encabezado de la solicitud `PUT` debe coincidir con la etag del modelo de recursos. Si las etags no coinciden, la solicitud `PUT` del cliente no se completará y se devolverá un error `412 PRECONDITION FAILED`.

5.11 Consulta de recursos y paginación utilizando parámetros comunes de la API de REST

Consulta a los recursos

Puede utilizar un conjunto de parámetros comunes para personalizar los resultados devueltos por una operación `GET`, como ordenar o filtrar. Cada especificación de la API de REST enumera el conjunto de parámetros comunes disponibles.

Paginación al consultar una colección de recursos

Cuando se realiza una operación de `GET` para recuperar varios recursos (es decir, una operación `GET` en una colección de URI, por ejemplo, `/rest/server-profiles`), los recursos se devuelven en un objeto colección que incluye un array de los recursos, junto con información sobre el conjunto de recursos devuelto. Esta colección de recursos puede verse truncada automáticamente en páginas para mejorar el rendimiento en el caso de que una consulta pueda devolver una gran cantidad de recursos. Los atributos de la colección (descritos más adelante) proporcionan información necesaria para determinar si se ha devuelto el conjunto completo de recursos o si se necesitan consultas adicionales para recuperar más páginas.

Por ejemplo, un objeto de colección incluye una URI de página siguiente y de página anterior. Estos URI indican si hay disponibles más páginas y se pueden recuperar a través de una operación `GET` sobre estos URI. Esto ofrece un modelo sencillo para garantizar que se hayan recuperado todos los recursos en la consulta, ejecutando comandos `GET` iterativos en el atributo `nextPageUri` hasta que este se devuelva vacío o con el valor null (consulte *Ejemplo: devolución de todos los recursos en una consulta de colección específica*).

También posible realizar una consulta de una página específica de recursos por medio de los parámetros de consulta `start` y `count`. Estos parámetros indican el índice del primer recurso que se debe devolver y la cantidad de recursos a devolver en la página, respectivamente.

NOTA: Las consultas en varias páginas de una colección no tienen estado y se basan simplemente en el índice de inicio y el número de recursos devueltos desde ese punto de inicio en el momento en el que se realiza la consulta. Por ejemplo, si se ha añadido o eliminado algún perfil de servidor después de llevarse a cabo una operación `GET` mediante una URI de página siguiente específica a partir de una colección de recursos de perfiles de servidor y se vuelve a realizar una operación `GET`, la página devuelta con la misma URI de página siguiente no puede contener el mismo conjunto de recursos.

Tenga en cuenta también que el conjunto específico de recursos devueltos con parámetro de inicio y de recuento determinado depende en gran medida de los parámetros `filter`, `query` y `sort` enviados en la solicitud, por lo tanto, es importante pasarle siempre los mismos parámetros filter, query y sort en todas las solicitudes de páginas adicionales. Los atributos `nextPageUri` y `prevPageUri` se rellenarán previamente con los parámetros `filter`, `query` y `sort` de la solicitud actual.

Los atributos que se devuelven en todas las operaciones GET llevadas a cabo en una colección de URI, por ejemplo`/rest/server-profile`**:**

`total`	Cantidad total de recursos disponibles en la colección solicitada (incluyendo cualquier filtro). No es necesariamente lo que se ha devuelto.
`count`	Número real de recursos devueltos (en el atributo members).
`start`	Índice, comenzando en cero, del primer elemento devuelto (en el atributo members).
`members`	Array de recursos que devueltos en el conjunto de resultados actual.
`nextPageUri`	URI que se puede utilizar para consultar la página siguiente en el conjunto de resultados (con el mismo valor de `count` especificado en la consulta actual).
`prevPageUri`	URI que se puede utilizar para consultar la página anterior en el conjunto de resultados (con el mismo valor de `count` especificado en la consulta actual).

NOTA: Un atributo `nextPageUri` o `prevPageUri` vacío o nulo indica que se ha alcanzado la última o la primera página (respectivamente) en la consulta. Esto permite que las secuencias de comandos realicen una iteración en `nextPageUri` hasta que el valor sea `null` para recuperar el conjunto completo de recursos en la consulta.

Ejemplo: devolución de todos los recursos en una consulta de colección específica

El número de recursos devueltos en una consulta puede no coincidir con lo especificado en el parámetro `count`. Los clientes siempre deben comprobar los resultados devueltos para determinar si se devolvió o no el conjunto de resultados completo. Los dos motivos por los que no se devuelvan todos los recursos en una consulta son:

- Ha llegado a la última página de la consulta (y simplemente no quedan recursos que volver). Esto también se indica mediante la devolución de un`prevPageUri` con un valor `null`.
- Por cuestiones de rendimiento, el servicio puede truncar automáticamente el conjunto de resultados devuelto, lo que requerirá solicitudes `GET` adicionales (con los parámetros de recuento e inicio adecuados) para poder recuperar el conjunto completo de recursos.

La manera más sencilla de asegurarse de que se recuperaron todos los recursos de una colección específica es realizar siempre solicitudes `GET` iterativas por medio del `nextPageUri` devuelto, hasta que el valor sea `null`. Consulte el siguiente ejemplo en pseudocódigo basado en filtros/consultas y ordenación:

```
currentCollection = doGet("/rest/server-hardware");
allResources = currentCollection.members;
While (currentCollection.nextPageUri) {
currentCollection = doGet(currentCollection.nextPageUri);
allResources.Append(currentCollection.members);
}
```

5.12 State-Change Message Bus

El Bus State-Change Message Bus (SCMB) es una interfaz que utiliza la mensajería asíncrona para notificar a los suscriptores que se han producido cambios en los recursos gestionados, tanto lógicos como físicos. Por ejemplo, puede programar aplicaciones para recibir notificaciones cuando se añade nuevo hardware de servidor al entorno gestionado o cuando cambia el estado de los recursos físicos, sin tener que sondear continuamente el dispositivo para conocer el estado mediante las API de REST. Para obtener más información sobre la recepción de mensajes asíncronos sobre los cambios en el entorno del dispositivo, consulte el Capítulo 28, «Uso de un bus de mensajes para enviar datos a los suscriptores».

5.13 Metric Streaming Message Bus

El bus Metric Streaming Message Bus (MSMB) es una interfaz que utiliza mensajería asíncrona para notificar a los suscriptores las estadísticas más recientes de los recursos gestionados. Puede configurar el intervalo y las estadísticas que desea recibir mediante las API de REST. Para obtener más información, consulte Capítulo 28, «Uso de un bus de mensajes para enviar datos a los suscriptores».

5.14 Análisis y solución de problemas

Puede utilizar las API de REST para capturar datos obtenidos de iLO y de los registros de los sistemas remotos, y hacer que potentes herramientas de análisis y solución de problemas accedan a estos datos y los usen.

5.14.1 Integración de HPE Operations Analytics con HPE OneView

La integración de Operations Analytics con HPE OneView proporciona a los profesionales de TI información de solución de problemas, análisis y planificación de capacidad para los dispositivos gestionados mediante HPE OneView. Mediante las API de REST de HPE OneView, puede capturar datos de registros, estadísticas, alertas e inventarios, e importarlos en Operations Analytics para verlos y representarlos gráficamente.

Las aplicaciones de solución de problemas en tiempo real como Operations Analytics necesitan acceso a los recursos, relaciones, estadísticas, alertas y registros de HPE OneView a intervalos cercanos al tiempo real. A continuación, estos datos se utilizan para señalar problemas y evitar tiempos de inactividad de la infraestructura mediante la previsión de fallos anticipada.

Para obtener información técnica sobre Operations Analytics, consulte los **manuales de HPE Operations Analytics**.

5.15 Herramientas para desarrolladores en un explorador web

Puede utilizar las herramientas para desarrolladores o para depuración en el explorador web para ver las operaciones de la API de REST a medida que se producen en la interfaz de usuario. La interfaz de usuario utiliza las API de REST para todas las operaciones; por lo tanto, cualquier cosa que se puede hacer en la interfaz de usuario se puede hacer utilizando operaciones de la API de REST.

5.16 Bibliotecas de ejemplo de código Python y PowerShell

Hay disponibles bibliotecas de Windows PowerShell y Python en sitios compatibles con Git que puede descargar y utilizar en sus secuencias de comandos API de REST. Estas bibliotecas se

distribuyen bajo la licencia de código abierto MIT, por lo que puede modificar su código fuente según necesite. Cada biblioteca proporciona métodos para enviarle a Hewlett Packard Enterprise comentarios, problemas u otro tipo de intervenciones.

Acerca del control de versiones Git:

Los diseños de repositorio y los flujos de trabajo global utilizan un flujo de trabajo simple y estándar, donde la rama principal es siempre la parte superior del tronco del árbol. Hewlett Packard Enterprise etiqueta cada revisión y solo la divide para solucionar un problema de revisión específica.

Para obtener más información sobre el uso de Git, consulte **http://git-scm.com/book**.

NOTA: Si tiene alguna duda acerca de las secuencias de comandos de la API de REST o de HPE OneView, envíe sus preguntas al foro de la comunidad de usuarios en **http://www.hpe.com/info/oneviewcommunity**.

Biblioteca de PowerShell

La biblioteca de PowerShell se encuentra alojada en GitHub y está disponible aquí: **https://github.com/HewlettPackard/POSH-HPOneView**. Para suscribirse al sitio y supervisar el proyecto, necesita una cuenta válida de Microsoft o GitHub. La descarga de versiones o de código fuente no requiere autenticación.

Para facilitar su uso cuando se actualiza la biblioteca, se proporciona un nuevo instalador.

Puede utilizar un explorador o un cliente Windows GIT para descargar el código fuente y ejemplos. Para descargar el cliente de Windows, consulte **http://windows.github.com/**.

El sitio GitHub ofrece un sistema de seguimiento de problemas mediante el cual se pueden enviar problemas o solicitudes de funciones.

Biblioteca de Python

La biblioteca de Python se encuentra alojada en una página web de GitHub y está disponible aquí: **https://github.com/HewlettPackard/python-hpOneView**.

Para participar en foros relativos al desarrollo, regístrese en la lista pública de correo **https://groups.google.com/forum/#!forum/hp-oneview-python**.

6 Acceso a la documentación y la ayuda

En este capítulo se describe cómo acceder a la ayuda desde el dispositivo, cómo acceder a la biblioteca de información en línea a disposición del público y dónde encontrar ayuda y documentación de referencia sobre la API de REST.

6.1 Ayuda en línea: información conceptual y sobre tareas siempre que la necesite

La ayuda en línea documenta tanto la interfaz de usuario como las API de REST e incluye:

- Información general sobre el dispositivo y sus funciones
- Descripciones de los recursos y las pantallas de la interfaz de usuario
- Instrucciones de inicio rápido para incluir en la gestión el centro de datos
- Instrucciones detalladas para usar la interfaz de usuario para realizar tareas
- Información sobre el uso de secuencias de comandos de la API de REST para realizar tareas
- Referencia *de la API de REST de HPE OneView*
- Información sobre el uso del bus SCMB (State-Change Message Bus) para suscribirse a los mensajes de cambio de estado

Diseño de la ayuda de la API de REST

La ayuda de la API de REST está diseñada de manera que:

- Cada recurso está documentado en su propio capítulo.
- Cada capítulo sobre secuencias de comandos de la API de REST identifica las llamadas a la API de REST que se deben realizar para completar las tareas.
- Cada llamada a la API de REST incluye un enlace a la *Referencia de la API de REST de HPE OneView* desde el cual puede obtener más información acerca de la API, como atributos y parámetros, el esquema del modelo de recursos y ejemplos de JSON (JavaScript Object Notation).

Diseño de la ayuda de la interfaz de usuario

La ayuda en línea de la interfaz de usuario está diseñada de forma que cada recurso está documentado en su propio capítulo. En la parte superior de cada capítulo de la ayuda hay un cuadro de navegación que da acceso a:

- Las tareas que se pueden realizar con la interfaz de usuario
- Una sección **About** (Acerca de) que proporciona información conceptual sobre el recurso
- Una sección de detalles de la pantalla para cada pantalla, que proporciona definiciones de los componentes de la pantalla para ayudarle en la entrada de datos y la toma de decisiones
- Información de solución de problemas por si le surge algún problema
- Enlaces a la ayuda sobre las API de REST relacionadas por si prefiere utilizar las secuencias de comandos de la API de REST para realizar una tarea

6.2 Esta guía de usuario es un complemento de la ayuda en línea

Esta guía de usuario ofrece:

- Información conceptual y descripciones de las tareas que se pueden realizar con la interfaz de usuario o las API de REST. No duplica las instrucciones paso a paso proporcionadas por la ayuda en línea, a menos que la información pueda ser necesaria si la ayuda en línea no está disponible.
- Para los procedimientos que utilizan las API de REST, se indican las API de REST, pero la sintaxis completa y la información de uso se incluye en la *Referencia de la API de REST de HPE OneView* de la ayuda en línea.
- Información de planificación, incluidas las decisiones de configuración que se deben tomar y las tareas que podría ser necesario llevar a cabo antes de instalar un dispositivo, agregar equipos gestionados o realizar cambios de configuración.
- Secciones de inicio rápido que proporcionan instrucciones paso a paso de alto nivel para determinadas tareas que podrían requerir que configure múltiples recursos utilizando la interfaz de usuario o las API de REST.

6.3 Dónde se puede encontrar documentación de HPE OneView

Guías de usuario y otros manuales

Las guías de usuario de HPE OneView y demás manuales están disponibles en la **Biblioteca de información de Hewlett Packard Enterprise**. Consulte «Páginas web» para conocer otras fuentes de información.

Ayuda en línea

Para ver la ayuda en el dispositivo, haga clic en ? para abrir la barra lateral de ayuda. Los enlaces de la barra lateral abren la ayuda en una nueva ventana o ficha del explorador:

- **Help on this page** (Ayuda en esta página) abre la ayuda de la pantalla actual.
- **Browse help** (Navegar por la ayuda) abre la parte superior del sistema de ayuda, donde puede decidir acerca de qué temas de ayuda desea leer.
- **Browse REST API help** (Navegar por la ayuda de la API de REST) abre la ayuda para obtener información de referencia y secuencias de comandos de la API.
- Al hacer clic en ? en una pantalla o cuadro de diálogo se abre una ventana de ayuda contextual para dicho cuadro de diálogo.

NOTA: Para enviar comentarios sobre la documentación de HPE OneView, envíe un correo electrónico a **docsfeedback@hpe.com**.

6.4 Activación de la navegación por los archivos de ayuda de la interfaz de usuario y la API de REST sin usar el dispositivo

Las versiones de los sistemas de ayuda de HPE OneView independientes del dispositivo son útiles para los desarrolladores que escriben secuencias de comandos de la API de REST u otros usuarios que prefieren la comodidad de acceder a la ayuda localmente sin necesidad de iniciar sesión en el dispositivo.

NOTA: También puede examinar la *referencia de la API* en http://www.hpe.com/info/oneview/docs.

Descarga de los archivos HTML de ayuda de la interfaz de usuario y REST

1. Visite la Biblioteca de información empresarial:

   http://www.hpe.com/info/oneview/docs

2. Seleccione el archivo zip de la *ayuda en línea de HPE OneView y la referencia de la API (descarga)* y guárdelo en su equipo o en un directorio local en un servidor web.
3. Use la utilidad que prefiera para extraer el contenido del archivo `.zip`.
4. Vaya al directorio de contenido.
5. Haga doble clic en el archivo `index.html` para abrir el sistema de ayuda de HPE OneView.

Parte II Tareas de planificación

En los capítulos de esta parte se describen las tareas de planificación de la configuración del centro de datos que puede que desee realizar antes de instalar el dispositivo o antes de realizar cambios en la configuración. Al completar estas tareas de planificación, puede crear una configuración de centro de datos que aproveche al máximo las funciones del dispositivo y resulte más fácil de supervisar y gestionar para los administradores.

7 Planificación de los recursos del centro de datos

Además de asegurarse de que su entorno cumple los requisitos previos para la instalación del dispositivo, hay otras tareas de planificación que es posible que desee realizar antes de añadir recursos al centro de datos. Al completar estas tareas de planificación, puede crear una configuración de centro de datos que aproveche al máximo las funciones del dispositivo y resulte más fácil de supervisar y gestionar para los administradores.

7.1 ¿Cuántos centros de datos?

Un recurso de centro de datos del dispositivo representa un área físicamente contigua en la que se encuentran los bastidores que contienen equipos informáticos. Los centros de datos se crean en el dispositivo para describir una planta de un laboratorio o parte de una sala de informática que proporciona una agrupación útil para resumir un entorno y sus requisitos térmicos y eléctricos.

El uso de centros de datos para describir la topología física y los sistemas de alimentación de su entorno es opcional. Si decide crear varios centros de datos, considere la posibilidad de incluir información sobre el centro de datos en los nombres de los demás recursos para que pueda utilizar las capacidades de búsqueda del dispositivo para filtrar los resultados por centro de datos.

7.1.1 ¿Va a gestionar, supervisar o migrar hardware de servidor?

Determine si desea agregar receptáculos a HPE OneView para gestionarlos o supervisarlos, o si desea migrar un receptáculo de Virtual Connect.

Gestionar Si se agrega un servidor gestionado a HPE OneView, ya sea en un receptáculo o en un servidor de montaje en bastidor, se pueden aplicar configuraciones, implementar perfiles de servidor, supervisar el estado de funcionamiento, recopilar estadísticas y alertar a los usuarios cuando se den determinadas situaciones. Para obtener más información, consulte «Acerca de los receptáculos c7000 gestionados» y «Gestión del hardware de servidor». Para gestionar hardware de servidor se necesita la licencia HPE OneView Advanced. Para obtener más información, consulte «Acerca de las licencias».

Supervisar Si se agrega un servidor supervisado a HPE OneView, ya sea en un receptáculo o en un servidor de montaje en bastidor, únicamente se puede supervisar su estado de hardware e inventario. Para obtener más información, consulte «Acerca de los receptáculos c7000 supervisados» y «Acerca del hardware de servidor supervisado». La supervisión del hardware de servidor utiliza una licencia gratuita denominada HPE OneView Standard. Para obtener más información, consulte «Acerca de las licencias».

Migrar Si tiene un receptáculo en Virtual Connect Manager (VCM), puede migrarlo a HPE OneView junto con su información de configuración para que HPE OneView pueda gestionarlo. Para gestionar un receptáculo se requiere una licencia HPE OneView Advanced. Para obtener más información, consulte «Acerca de las licencias». Para obtener más información sobre la migración, consulte «Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión».

7.2 Planificación de la seguridad

Para obtener más información sobre las funciones de seguridad del dispositivo y para obtener información general sobre la protección del este, consulte «Información sobre las funciones de seguridad del dispositivo» (página 69).

7.3 Preparación de los conmutadores de red del centro de datos

Los puertos de conmutación de los conmutadores de la red del centro de datos que se conectan a los módulos de interconexión de Virtual Connect deben configurarse como se describe en «Requisitos de los puertos de conmutación del centro de datos» (página 207). El tráfico de red también debe considerarse como se describe en «Acerca de las configuraciones activo/activo y activo/en espera».

7.4 Planificación para una implementación de doble pila

Los sistemas de gestión de red pueden usar protocolos de comunicaciones IPv4 o IPv4/IPv6 en la misma la infraestructura de red. El protocolo predeterminado es IPv4. La gestión de interconexiones con los protocolos IPv4 y IPv6 proporciona redundancia de dirección de red si la dirección principal IPv4 produce un fallo al conectarse.

Se necesita una configuración de doble pila de comunicación IPv4/IPv6 para que el dispositivo se comunique con las interconexiones de la red de gestión IPv6.

Para configurar un protocolo de doble pila para un receptáculo, utilice el Onboard Administrator para activar IPv6 y los tipos de direcciones IPv6.

NOTA: El acceso SNMP y los destinos de captura SNMP admiten tanto direcciones IPv4 como IPv6.

7.5 Planificación de los nombres de los recursos

En la barra superior de cada pantalla se incluye la función **Smart Search** (Búsqueda inteligente), que le permite encontrar información sobre recursos específicos, como determinados nombres de recursos, números de serie, WWN y direcciones IP y MAC. En general, puede buscarse cualquier cosa que aparezca en un recurso.

La definición de una convención de nomenclatura estándar para redes, conjuntos de redes, receptáculos, grupos de receptáculos, grupos de interconexiones lógicas y conjuntos de enlaces ascendentes hace que resulte sencillo identificarlos, y permite buscar o aplicar filtros a la interfaz de usuario de forma eficiente.

Tenga en cuenta la información siguiente al elegir los nombres de los recursos:

- Para reducir al mínimo la necesidad de realizar cambios de nombres y para que resulte más sencillo identificar los recursos relacionados con la red, procure elegir nombres que incluyan la información siguiente:
  - El propósito del recurso. Por ejemplo:

    `prod` para los recursos de la red de producción
    `dev` para los recursos de la red de desarrollo

  - Para redes etiquetadas, el ID de VLAN

    NOTA: Si está creando simultáneamente varias redes con etiquetas (creación de redes en masa), se adjuntan automáticamente el nombre de la red seguido de un guion bajo (_) y el ID de la VLAN. Por ejemplo, Dev_101.

  - Un identificador para ayudar a distinguir entre los recursos que utilizan el lado izquierdo o el lado derecho del receptáculo. Por ejemplo:

    `izd` y `dch`
    `A` y `B`
    `1` y `2`

- A continuación se indican algunos ejemplos de nombres de red que siguen las convenciones de nomenclatura recomendadas:

  ```
  dev_1105_A
  prod_1102_1
  test_1111_izd
  ```

- Si va a utilizar conexiones con varias redes en los perfiles de servidor, cree conjuntos de redes que contengan todas las redes que se van a utilizar en una misma conexión de perfil. Elija nombres como los siguientes:

  ```
  dev_nset_A
  prodnset_1
  testns_izd
  ```

- Si se cambian los nombres de los conjuntos de enlaces ascendentes, puede que los recursos queden fuera de línea temporalmente (consulte «Cambios de configuración que requieren o dan lugar a la interrupción de la alimentación del dispositivo» (página 127)). Para reducir al mínimo la necesidad de realizar cambios de nombres y para que resulte más sencillo identificar los conjuntos de enlaces ascendentes, elija nombres como los siguientes:

  ```
  devUS_A
  prodUS_1
  testUS_izd
  ```

- El dispositivo no admite el filtrado de recursos, como el hardware de servidor, basado en la ubicación física (nombre del centro de datos). Para filtrar por nombre de centro de datos, elija una convención de nomenclatura que incluya el nombre del centro de datos en el nombre del recurso.
- El dispositivo admite el filtrado de recursos basado en el modelo, por lo que puede buscar hardware de servidor incluso si no ha incluido el número del modelo en el nombre.
- El dispositivo proporciona nombres predeterminados para muchos recursos. Por ejemplo:
  - A los receptáculos se les asigna el nombre `Encl`*`n`*, donde *`n`* es un número que se incrementa en 1 cada vez que se añade un receptáculo.
  - *`nombre_del_receptáculo`*`-LI` es el nombre predeterminado de una interconexión lógica, donde *`nombre_del_receptáculo`* es el nombre del receptáculo.
  - `Datacenter 1` es el nombre que se asigna al centro de datos cuando se inicializa el dispositivo.
  - A los tipos de hardware de servidor se les asignan nombres basados en el modelo de servidor, tales como `BL460c Gen8 1`. Si tiene un tipo estándar de hardware de servidor, puede cambiar el nombre de ese tipo de hardware de servidor para que incluya la palabra `Standard` o algún otro identificador que ayude a los administradores a determinar rápidamente el tipo de hardware de servidor correcto que deben elegir.
- Puede abreviar los nombres de los recursos para acortarlos. Por ejemplo:

Nombre del recurso	Abreviaturas típicas (entre paréntesis, abreviatura en inglés)
Receptáculo	Rc (Encl)
Grupo de receptáculos	GR, Grupo (EG, Group)
Interconexión lógica	IL (LI)

Nombre del recurso	Abreviaturas típicas (entre paréntesis, abreviatura en inglés)
Grupo de interconexiones lógicas	GIL (LIG)
Conjunto de enlaces ascendentes	CEA (US)

Para obtener más información sobre las capacidades de búsqueda del dispositivo, consulte «Búsqueda de recursos» (página 102).

7.6 Planificación de la configuración del dispositivo

En estos temas se trata la configuración del dispositivo.

7.6.1 Requisitos del host y la VM del dispositivo

HPE OneView es un dispositivo virtual que se ejecuta en los hosts de hipervisor compatibles siguientes.

Tabla 5 Versiones e hipervisores admitidos

Hipervisor	Versión
VMware vSphere ESXi	• 5.5 • 5.5 actualización 1 • 5.5 actualización 2 • 5.5 actualización 3 • 6.0 • 6.0 actualización 1 • 6.0 actualización 2
Microsoft Hyper-V	Hyper-V se admite en las siguientes plataformas de Microsoft Windows con el rol Hyper-V instalado: • Windows Server 2012 • Windows Server 2012 R2 • Windows Hyper-V Server 2012 • Windows Hyper-V Server 2012 R2

Los requisitos de la máquina virtual (VM) del dispositivo han cambiado y son los siguientes:

- ProLiant G7–class o CPU posterior.
- Cuatro CPU virtuales de 2–GHz o más,
- 16 GB de memoria.
- 160 GB de espacio en disco de aprovisionamiento grueso.

  Puede ampliar manualmente el disco virtual para aumentar el tamaño del repositorio de firmware de los 12 GB por defecto a 100 GB (se necesitan como mínimo 275 GB de espacio en disco en total). La mejor opción es ampliar el disco virtual durante la instalación del dispositivo. Consulte las instrucciones de instalación o actualización.
- Una conexión con la LAN de gestión. Hewlett Packard Enterprise recomienda tener redes de datos y de gestión independientes.
- El host del hipervisor cumple los requisitos mínimos del sistema:

- ***Minimum system requirements for installing ESXi/ESX (1003661)*** (Requisitos mínimos del sistema para instalar ESXi/ESX [1003661]), base de conocimientos de VMware
- ***Review Prerequisites for Installation*** (Revisión de los requisitos previos para la instalación) (Hyper-V Server 2012, Hyper-V Server 2012 R2), Microsoft TechNet
- ***Install Hyper-V and Configure a Virtual Machine*** (Instalación de Hyper-V y configuración de una máquina virtual) (Windows Server 2012), Microsoft Windows Server

- Para las opciones de gestión de Configure Power (Configuración de la energía) en la configuración del BIOS:
  - Establezca Power Regulator (Regulador de energía) en `Static High Performance Mode` (Modo estático de alto rendimiento de HPE).
  - Establezca Power Profile (Perfil de energía) en `Maximum Performance` (Máximo rendimiento).
- Network Time Protocol (NTP) (Protocolo de tiempo de red) se ha configurado correctamente.

  Para el funcionamiento correcto del dispositivo virtual es necesaria una fuente de tiempo precisa. Existen dos opciones para garantizar la precisión de la hora en el dispositivo virtual utilizando el Network Time Protocol (NTP) Protocolo de tiempo de red):

  NTP en el hipervisor

  Configure el host del hipervisor para utilizar NTP y configure HPE OneView para utilizar el host del hipervisor como su fuente de tiempo.

  NTP en HPE OneView

  Configure HPE OneView para utilizar tres o más servidores NTP.

NOTA: Debe configurar el host del hipervisor para que reserve los recursos mínimos necesarios (reservas o comparticiones). Consulte los siguientes enlaces para obtener instrucciones sobre la reserva de recursos en un host del hipervisor.

- **Configure Memory and Processors** (Configuración de la memoria y los procesadores) (**Microsoft Windows Server**)
- **Allocate CPU Resources** (Asignación de recursos de CPU) y **Allocate Memory Resources** (Asignación de recursos de memoria) (**VMware vSphere ESX y vCenter Server Documentation Center**)

7.6.2 Planificación para alta disponibilidad

Para utilizar HPE OneView en una configuración de alta disponibilidad (HA), consulte la documentación del hipervisor para conocer los requisitos específicos.

VMware vSphere ESXi	**http://www.vmware.com/products/vsphere.html**
Microsoft Hyper-V	**http://technet.microsoft.com/en-us/library/cc753787.aspx**

7.6.3 Redes de datos y de gestión independientes

HPE recomienda tener redes de datos y de gestión independientes. Consulte «Prácticas recomendadas para el mantenimiento de un dispositivo seguro» para obtener más información. Consulte la ***Matriz de compatibilidad de HPE OneView***.

7.6.4 Relojes de tiempo y NTP

HPE recomienda el uso de NTP en el host en el que se instala el dispositivo virtual. Si no se utiliza NTP en el host, HPE recomienda configurar NTP directamente en el dispositivo virtual. No configure NTP en el host y en el dispositivo virtual simultáneamente. Además, el reloj del host de la VM debe tener la hora correcta.

7.6.5 Direcciones IP

Debe especificar el tipo de direcciones IP que se usan y cómo se asignan al dispositivo, ya sea asignándolas usted manualmente o mediante un servidor DHCP (Dynamic Host Configuration Protocol):

El dispositivo admite la configuración de direcciones tanto IPv4 como IPv6 como dirección IP del dispositivo. El dispositivo no admite una configuración únicamente IPv6; puede ser una configuración solo IPv4 o una configuración de modo dual (tanto IPv4 como IPv6). Consulte «Planificación para una implementación de doble pila» para obtener más información.

Dispositivo de VM

En un dispositivo de VM, las direcciones IP se pueden asignar de dos maneras: manualmente por parte del usuario (IP estática) o asignarse por DHCP (Dynamic Host Configuration Protocol). DHCP no se admite para la asignación de direcciones IP a dispositivos a menos que se utilicen reservas de DHCP.

8 Planificación de los cambios de configuración

En este capítulo se identifican los cambios de configuración que podrían dar lugar a que un recurso quede fuera de línea temporalmente o que podrían requerir que se realicen cambios en varios recursos.

8.1 Cambios de configuración que requieren o dan lugar a la interrupción de la alimentación del dispositivo

Dispositivo

Si se pone fuera de línea el dispositivo, los recursos gestionados no se ven afectados, sino que siguen funcionando mientras el dispositivo se encuentra en ese estado.

En un clúster de dispositivos, HPE OneView se desconecta de forma temporal mediante una operación de espera de la activación. HPE OneView reanuda el funcionamiento cuando el dispositivo en espera se convierte en el dispositivo activo.

Cuando se instala una actualización del dispositivo, este se reinicia y se pone fuera de línea.

Receptáculos

El Onboard Administrator (OA) se pone fuera de línea automáticamente durante la actualización del firmware de un receptáculo.

Interconexiones e interconexiones lógicas

- Las conexiones de los perfiles de servidor con las redes de un conjunto de enlaces ascendentes se ponen fuera de línea cuando se elimina el conjunto de enlaces ascendentes.
- Las conexiones de los perfiles de servidor con las redes de un conjunto de enlaces ascendentes pueden interrumpirse durante unos segundos cuando se cambia el nombre de un conjunto de enlaces ascendentes utilizando cualquiera de estos métodos:
  - Cambiar el nombre del conjunto de enlaces ascendentes en la interconexión lógica.
  - Cambiar el nombre del conjunto de enlaces ascendentes en el grupo de interconexiones lógicas y, a continuación, actualizar la interconexión lógica a partir del grupo de interconexiones lógicas.
- Una interconexión se pone fuera de línea cuando:
  - Se actualiza o se activa el firmware de una interconexión lógica. El almacenamiento provisional de firmware no requiere poner fuera de línea las interconexiones.
  - Se actualiza el firmware de un receptáculo y se selecciona la opción de actualizar el receptáculo, la interconexión lógica y los perfiles de servidor.
- Si una interconexión tiene firmware que se ha almacenado provisionalmente pero no se ha activado, cualquier reinicio posterior de esa interconexión activa el firmware, lo que pone la interconexión fuera de línea.
- Puede evitar la pérdida de conectividad de red para los servidores conectados a una interconexión lógica que tiene el modo de apilamiento `Enclosure` (Receptáculo) y el estado de apilamiento `Redundantly Connected` (Conexión redundante) si actualiza el firmware utilizando el método siguiente:
  1. Almacenar provisionalmente el firmware en la interconexión lógica.
  2. Activar el firmware de las interconexiones situadas en los compartimientos del receptáculo con números pares.

3. Esperar hasta que termine la actualización del firmware y las interconexiones estén en el estado `Configured` (Configurada).
4. Activar el firmware de las interconexiones situadas en los compartimientos del receptáculo con números impares.

Redes

- Si intenta eliminar una red que están usando uno o varios perfiles de servidor, el dispositivo le advierte de que la red está en uso. Si elimina la red mientras está en uso, se ponen fuera de línea las conexiones de los perfiles de servidor que especifican la red de forma explícita (en lugar de como parte de un conjunto de redes).

  Si agrega una red con el mismo nombre que la red que ha eliminado, las conexiones que especifican la red de forma explícita (en lugar de como parte de un conjunto de redes) no se actualizan, sino que debe editar cada conexión del perfil de servidor para volver a configurarla de forma que especifique la red que ha añadido. Debido a que es necesario editar el perfil de servidor para editar la conexión, debe apagar el servidor.

- Si intenta eliminar una red que pertenece a un conjunto de redes, el dispositivo le advierte de que la red está asignada al menos a un conjunto de redes. Si elimina esa red y hay otras redes en ese conjunto de redes, la conectividad de los perfiles de servidor con la red eliminada se pone fuera de línea, pero la conectividad con las demás redes del conjunto de redes no se ve afectada.

  Puede agregar una red a un conjunto de redes, incluyendo una red que tiene el mismo nombre que una red que ha eliminado, mientras que las conexiones de los perfiles de servidor con ese conjunto de redes permanecen en línea.

Conjuntos de redes

- Si intenta eliminar un conjunto de redes que están usando uno o varios perfiles de servidor, el dispositivo le advierte de que el conjunto de redes está en uso. Si elimina el conjunto de redes mientras está en uso, las conexiones de los perfiles de servidor con ese conjunto de redes se ponen fuera de línea.
- Si agrega un conjunto de redes con el mismo nombre que el conjunto de redes que ha eliminado, las conexiones que especifican el conjunto de redes no se actualizan, sino que debe editar cada conexión del perfil de servidor para volver a configurarla de forma que especifique el conjunto de redes que ha añadido. Debido a que es necesario editar el perfil de servidor para modificar la conexión, debe apagar el servidor.
- Los perfiles de servidor con conexiones a un conjunto de redes pueden verse afectados cuando se elimina una red del conjunto de redes. Consulte «Redes».

Perfiles de servidor y hardware de servidor

- Antes de editar un perfil de servidor, es posible que deba apagar el hardware de servidor al que está asignado el perfil de servidor. Consulte «Acerca de la edición de perfiles de servidor» para obtener una lista de las modificaciones que se pueden realizar sin necesidad de apagar el hardware de servidor.
- Las actualizaciones de firmware requieren que se edite el perfil de servidor para cambiar la línea de base de firmware. Al igual que con cualquier otra modificación de los perfiles de servidor, debe apagar el hardware de servidor al que está asignado el perfil de servidor antes de editar un perfil de servidor.
- Los perfiles de servidor y el hardware de servidor pueden verse afectados por los cambios en las redes y los conjuntos de redes. Para obtener más información, consulte «Redes» y «Conjuntos de redes».

- Los perfiles de servidor y el hardware de servidor pueden verse afectados por los cambios en los nombres de los conjuntos de enlaces ascendentes. Para obtener más información, consulte «Interconexiones e interconexiones lógicas».

8.2 Cambios de configuración que podrían requerir cambios en varios recursos

- «Adición de una red»
- «Adición de un receptáculo»

8.2.1 Adición de una red

Al agregar una red al dispositivo, puede que sea necesario hacer cambios en la configuración de los siguientes recursos:

- **Redes**. Agregue la red.
- **Conjuntos de redes**. (Opcional) Si la red que está agregando es una red Ethernet, es posible que desee agregarla a un conjunto de redes o crear un conjunto de redes que la incluya.
- **Interconexiones lógicas** y **grupos de interconexiones lógicas**. Para que un servidor conectado a una interconexión lógica acceda a una red, la interconexión lógica debe tener un conjunto de enlaces ascendentes que incluya una conexión con esa red:
  - Puede que sea necesario actualizar varias interconexiones lógicas.
  - Puede hacer cambios en la configuración del grupo de interconexiones lógicas y, a continuación, actualizar cada interconexión lógica desde el grupo.
  - Si los cambios de configuración incluyen la eliminación o el cambio de nombre de un conjunto de enlaces ascendentes, la conectividad del perfil de servidor con la red puede verse afectada. Consulte «Cambios de configuración que requieren o dan lugar a la interrupción de la alimentación del dispositivo» (página 127).
- **Perfiles de servidor**. Si el perfil de servidor no tiene una conexión con un conjunto de redes que incluya esta red, debe añadir conexiones a la red.

Para ver un resumen de las tareas que debe completar cuando añada una red, consulte .

8.2.2 Adición de un receptáculo

Al agregar un receptáculo al dispositivo para gestionarlo, puede que sea necesario hacer cambios en la configuración de los siguientes recursos:

- **Receptáculos**. Agregue el receptáculo que va a gestionar.
- **Grupos de receptáculos**. Cada receptáculo gestionado debe pertenecer a un grupo de receptáculos. Si no elige un grupo de receptáculos existente, debe crear uno cuando agregue el receptáculo.
- **Receptáculos lógicos**. Los receptáculos lógicos sirven para mantener las configuraciones de los receptáculos que están enlazados entre sí. Utilice los receptáculos lógicos para las actualizaciones de firmware, las secuencias de comandos de OA y para hacer que los receptáculos estén al día con los cambios efectuados desde el grupo de receptáculos.
- **Interconexiones lógicas** y **grupos de interconexiones lógicas**. Las interconexiones lógicas y los grupos de interconexiones lógicas definen la conectividad del receptáculo gestionado con la red. Los grupos de receptáculos deben especificar un grupo de interconexiones lógicas. Cuando se crea un grupo del receptáculo, si no se especifica un grupo de interconexiones lógicas existente, se debe crear uno. Para que un servidor

conectado a una interconexión lógica acceda a una red, el grupo de interconexiones lógicas que se crea debe tener un conjunto de enlaces ascendentes que incluya una conexión con esa red.

- **Perfiles de servidor**. No es necesario agregar y asignar perfiles de servidor a los blades de servidor del receptáculo gestionado en el momento de agregar el receptáculo, pero para poder utilizar los blades de servidor de un receptáculo gestionado, deberá asignarles perfiles de servidor. Para acceder a una red, el perfil de servidor debe incluir una conexión con esa red o con un conjunto de redes que incluya esa red.

Para ver un resumen de las tareas que debe realizar cuando añada un receptáculo gestionado y conecte sus blades de servidor a las redes del centro de datos, consulte «Inicio rápido: Adición de un receptáculo c7000 con un solo grupo de interconexiones lógicas y conexión de sus blades de servidor a las redes» (página 149).

9 Planificación de la migración de receptáculos de VCM a HPE OneView

La planificación de la migración de receptáculos gestionados por VCM a receptáculos gestionados por HPE OneView es una parte importante del proceso de migración. Una idea clara sobre lo que se migrará desde Virtual Connect Manager (VCM) y sobre los requisitos de HPE OneView puede ayudarle a asegurarse de que la migración se realizará de forma sencilla y sin problemas. En este capítulo se explican los requisitos y lo que se debe esperar de la migración. Por ejemplo, en «Sobre problemas de bloqueo durante la migración» se muestra una lista parcial de lo que no se migrará.

El proceso de migración automatizada importa la información de configuración de los receptáculos, lo que incluye hardware, dominio de Virtual Connect (VC), redes y perfiles de servidor, con algunas excepciones. La configuración de direcciones MAC y WWN de las conexiones de los perfiles de servidor se conserva y se especifica como definida por el usuario en HPE OneView. Las direcciones nuevas asignadas después de la migración proceden del pool de identificadores de HPE OneView. Consulte "About ID pools" (Acerca de los pools de identificadores) en la ayuda en línea para obtener más información.

Al planificar la migración, tenga en cuenta que Virtual Connect distingue entre mayúsculas y minúsculas, pero HPE OneView no lo hace. Por ejemplo, en Virtual Connect, “Profile1” es distinto de “profile1” y de “PROFILE1”. En HPE OneView, “Profile1” es lo mismo que “profile1” y que “PROFILE1”. Es posible que deba cambiar el nombre de algunos componentes antes de realizar la migración para evitar conflictos de nombre.

9.1 Duración y tipo de migración

Para determinar cuándo realizar una migración, decida si quiere realizar una migración en servicio o sin conexión. Para una sin conexión, tenga en cuenta el tiempo de inactividad necesario para realizar la migración. Para la migración en servicio, tenga en cuenta la infraestructura de software y hardware necesarias para realizar la migración.

El tamaño de la configuración que se va a migrar afecta al tiempo de procesamiento. Las configuraciones de gran tamaño y complejidad tardan más tiempo en procesarse que otras más pequeñas.

9.2 Conceptos básicos sobre el proceso de migración

Un receptáculo gestionado por VCM se puede migrar a HPE OneView para que este lo gestione. La migración puede realizarse a través de la interfaz de usuario de HPE OneView o mediante la API de REST. El proceso básico consta de los pasos que se indican a continuación. Revise este proceso para ver los tipos de problemas que pueden surgir, lo que le ayudará a determinar qué cambios debe realizar en su entorno para llevar a cabo una migración satisfactoria. Consulte «Antes de migrar receptáculos c7000» para obtener más información.

IMPORTANTE: Ejecute `show config -includepoolinfo` desde la línea de comandos de VCM. Haga una copia de seguridad de la configuración de VCM: el dominio de Virtual Connect (VC) y la salida del comando `show config -includepoolinfo`. La copia de seguridad se utiliza si es necesario volver a usar VCM para realizar la gestión. Si se necesita una restauración, necesitará las credenciales predeterminadas de fábrica de la interconexión de VC que se encuentran en la etiqueta.

La salida del comando `show config -includepoolinfo` le permite consultar los detalles específicos del dominio de VC después de migrar el receptáculo a HPE OneView. Para obtener más información, consulte la Guía de usuario de Virtual Connect en **http://www.hpe.com/info/virtualconnect/docs**.

Requisitos previos para realizar una migración

- Privilegios necesarios: administrador de infraestructuras de HPE OneView, administrador de Onboard Administrator (OA) y administrador del dominio de VCM.
- Credenciales de OA y de VCM, así como la dirección IP del OA del receptáculo.
- Para los receptáculos gestionados por VCEM: las credenciales de VCEM para eliminar el dominio de Virtual Connect del grupo de dominios mediante la interfaz web de VCEM o el módulo de HPE PowerShell.
- Copia de seguridad y garantía de la configuración del VCM (incluido el resultado de `show config -includepoolinfo`).
- Consulte la ***Matriz de compatibilidad de HPE OneView*** y compruebe que el receptáculo contiene servidores, módulos de interconexión y tarjetas intermedias compatibles.
- Consulte «Requisitos previos para incluir un receptáculo c7000 en HPE OneView» para conocer los requisitos previos y la preparación que debe realizar.
- Asigne perfiles de servidor antes de la migración o vuelva a crear los perfiles de servidor después de la migración, si corresponde.
- Compruebe la conectividad de red con OA y los iLO en el dominio de Virtual Connect.
- Asegúrese de que todos los módulos de interconexión se encuentran en el receptáculo y están encendidos.

Tarea de migración

Inicie el proceso de compatibilidad y migración

1. Decida si quiere realizar una migración sin conexión o en servicio.
2. Determine si va a migrar el receptáculo a través de laGUI de HPE OneView o la API de REST de HPE OneView.
3. Proporcione las credenciales de OA y VCM y la dirección IP del OA del receptáculo.

HPE OneView comprueba la compatibilidad del receptáculo de gestionado con VCM con HPE OneView y genera un informe de compatibilidad de migración con los problemas. El informe muestra advertencias y problemas de bloqueo (problemas que impedirán la migración).

Solucione los problemas del informe de compatibilidad

4. Revise y solucione los problemas empezando por el principio del informe de compatibilidad. Al resolver primero los problemas que aparecen al principio, es posible que se solucionen otros problemas que aparecen más adelante en el informe.
   - Modifique la configuración en VCM o HPE OneView para resolver todos errores de migración de **bloqueo** indicados en el informe de compatibilidad. Para obtener una lista de algunos de los problemas de bloqueo que pueden surgir, consulte «Sobre problemas de bloqueo durante la migración».
   - Evalúe las **advertencias** en el informe de compatibilidad para determinar si es necesario realizar alguna acción.

     A menos que se especifique lo contrario, las advertencias indican una función que no se migrará a HPE OneView. Antes de continuar, asegúrese de que la función detectada no es crítica para el funcionamiento. Para obtener una lista de algunas de las advertencias que puede encontrar, consulte «Problemas de tipo advertencia».
5. Para resolver un problema, puede ser necesario deshabilitar una función de VCM, cambiar una configuración de VCM o, en algunos casos, cambiar el grupo de interconexiones lógicas de HPE OneView.

Para obtener más información sobre VCM, consulte la Guía de usuario de HPE Virtual Connect para c-Class BladeSystem o la Guía de usuario de la interfaz de línea de comandos de HPE Virtual Connect Manager para c-Class BladeSystem en **https://www.hpe.com/info/virtualconnect/docs**.

Realice la migración

6. Para la migración en servicio, después de resolver todos los problemas de bloqueo, así como las advertencias que desee, ejecute una prueba de compatibilidad final.

   Para la migración sin conexión, después de resolver todos los problemas de bloqueo (excepto el encendido del servidor), así como las advertencias que desee, apague los servidores y ejecute una prueba de compatibilidad final.
7. Si el informe final indica que se han resuelto todos los problemas de bloqueo:
   a. Lea todas las confirmaciones por completo (incluidos los enlaces para obtener más información).
   b. Entienda y acepte las implicaciones de cada confirmación haciendo clic en cada una de ellas.
   c. Continúe con la migración.

      NOTA: Tiene la opción de migrar hasta cuatro dominios de receptáculo individuales de ka VCM a HPE OneView de manera simultánea.

Tareas posteriores a la migración

1. Tras completar con éxito una migración sin conexión, encienda los servidores.
2. Opcional: vuelva a crear los perfiles de servidor en HPE OneView, si los perfiles de servidor no se asignaron a un hardware de servidor antes de la migración. Consulte «Confirmación del perfil de servidor» para obtener más información.
3. Realice estas prácticas recomendadas:
   a. Copia de seguridad de la nueva configuración en HPE OneView.
   b. Compruebe la conectividad de la red y el almacenamiento.
   c. Programe un reinicio en caso de que una de las confirmaciones, por ejemplo una configuración de función virtual de SR-IOV, indique un cambio que afectaría al funcionamiento.

      NOTA: Durante una migración en servicio, algunos cambios no tienen efecto hasta que los servidores se reinician por primera vez después de una migración.

Después de la migración, el receptáculo dejará de estar disponible en el VCM.

9.2.1 Problemas de tipo advertencia

A continuación se incluye una lista parcial de las funciones de Virtual Connect que no son compatibles con HPE OneView. Estas funciones se consideran problemas de tipo *advertencia* y se incluyen en el informe de compatibilidad. La migración puede continuar con estas advertencias, pero debe examinarlas para determinar si son importantes para su entorno. Si se necesita una función en su entorno y el receptáculo contiene blades de servidor ProLiant G6 o posteriores, puede que le convenga supervisar el receptáculo. Consulte «Acerca de los receptáculos c7000 supervisados».

NOTA: Los perfiles sin asignar no se migrarán. Los perfiles se eliminarán de VCM durante la migración. Asigne los perfiles antes de la migración o utilice la salida del comando `show config -includepoolinfo` para recrearlos una vez que el receptáculo se encuentre en HPE OneView.

Advertencias posibles		
• Nombre de host de módulo personalizado • Distintas conexiones USE-BIOS en un perfil • Nombre DNS específico de un módulo	• Grupo de acceso a redes • RADIUS/TACACS+ • Supervisión del tráfico sFlow • SMIS no activado	• Perfiles de servidor sin asignar • Configuración de roles de usuario • Incoherencia entre las capturas SNMP de VCM y la configuración de acceso a SNMP de Ethernet y FC

NOTA: En general, si una función se muestra como una advertencia que no es necesaria para el entorno, continuar implicará que la funcionalidad no se migrará a HPE OneView.

Parte III Inicios rápidos de configuración

En las secciones de inicio rápido que componen esta parte se describen las tareas básicas de configuración de recursos necesarias para incluir rápidamente en la gestión del dispositivo los principales componentes de la infraestructura de hardware. En la Parte IV se documentan tareas adicionales de configuración de recursos y de gestión continuada.

10 Inicio rápido: Configuración inicial de HPE OneView

La configuración inicial de los recursos en HPE OneView es similar a la configuración de recursos durante las tareas habituales de mantenimiento.

Si bien HPE OneView está diseñado para dotar de flexibilidad al orden en que se crean, agregan y editan recursos y equipos, Hewlett Packard Enterprise recomienda utilizar la siguiente secuencia de flujo de trabajo para realizar la configuración inicial o para hacer adiciones o cambios importantes en el entorno.

Para utilizar las API de REST para configurar el dispositivo e incluir por primera vez en entorno en la gestión, consulte la ayuda de la API de REST, que está disponible en la barra lateral de ayuda.

10.1 Configuración inicial de los recursos en HPE OneView

10.1.1 Requisitos previos

- Ha instalado HPE OneView. Para obtener más información, consulte la ***Guía de instalación de HPE OneView***.
- Ha configurado la red del dispositivo.
- Ha iniciado sesión como administrador.

10.1.2 Configuración de recursos en HPE OneView

1. **Agregue usuarios al dispositivo.**

   Cree cuentas de usuario con privilegios específicos y con autenticación local o basada en directorio.

   - Añada un usuario local totalmente autorizado (administrador de infraestructuras)
   - Añada un usuario local con acceso especializado
   - Añada un usuario totalmente autorizado con autenticación por pertenencia a grupos en un directorio de la organización
   - Añada un usuario con acceso basado en roles y autenticación por pertenencia a grupos en un directorio de la organización

     Cree cuentas de usuario asignadas con privilegios predefinidos o especializados con autenticación local o basadas en directorio.

     Consulte la ayuda en línea de **Users and Groups** (Usuarios y grupos) para obtener más información.

2. **Agregue un lote de firmware al repositorio de firmware del dispositivo.**

   Agregue el lote de firmware más reciente al dispositivo.

   Consulte la ayuda en línea **Firmware Budles** (Lotes de firmware) para obtener más información.

3. **Cree redes.**

   Cree redes Ethernet para los datos y redes Fibre Channel sobre Ethernet para el almacenamiento.

   Consulte la ayuda en línea de **Networks** (Redes) para obtener más información.

4. **Cree conjuntos de redes.**

   Cree conjuntos de redes para agrupar redes Ethernet y simplificar la gestión.

Consulte la ayuda en línea sobre **Network Sets** (Conjuntos de redes) para obtener más información.

5. **Cree uno o varios grupos de interconexiones lógicas.**

   Cree uno o varios grupos de interconexiones lógicas para definir las conexiones entre sus redes y los puertos de enlace ascendente de las interconexiones.

   Consulte la ayuda en línea de **Logical Interconnect Groups** (Grupos de informaciones lógicas) para obtener más información.

6. **Cree un grupo de receptáculos.**

   Cree un grupo de receptáculos para definir y mantener configuraciones coherentes y poder detectar y gestionar los dispositivos, como las interconexiones y el hardware de servidor de los receptáculos.

   Consulte la ayuda en línea de **Enclosure Groups** (Grupos receptáculos) para obtener más información.

7. **Agregue receptáculos al dispositivo.**

   Agregue receptáculos al dispositivo para gestionar su contenido y aplicarles actualizaciones de firmware.

   Consulte la ayuda en línea de **Enclosures** (Receptáculos) para obtener más información.

8. **Opcional: Agregue conmutadores al dispositivo.**

   Cree un grupo de conmutadores lógicos para agregar un conmutador de la parte superior del bastidor al dispositivo para proporcionar una estructura unificada y convergente sobre Ethernet de 10 Gigabits para el tráfico de LAN y SAN.

   Consulte la ayuda en línea de **Switches** (Conmutadores) para obtener más información.

9. **Opcional: Agregue sistemas de almacenamiento y pools de almacenamiento.**

   Agregue sistemas de almacenamiento al dispositivo y, a continuación, agregue pools de almacenamiento al dispositivo.

   Consulte la ayuda en línea de **Storage Systems** (Sistemas de almacenamiento) y de **Storage Pools** (Pools de almacenamiento) para obtener más información.

10. **Opcional: Cree volúmenes.**

    Cree volúmenes en los pools de almacenamiento. También puede crear volúmenes mediante la creación de plantillas de volumen.

    Puede agregar volúmenes existentes desde los sistemas de almacenamiento al dispositivo.

    Consulte la ayuda en línea de **Volumes** (Volúmenes) y de **Volume Templates** (Plantillas de volumen) para obtener más información.

11. **Opcional: Agregue un administrador de SAN al dispositivo para gestionar el almacenamiento SAN.**

    Agregue un administrador de SAN para acceder a las SAN que gestiona.

    Consulte la ayuda en línea sobre **SAN Managers** (Administradores de SAN) para obtener más información.

12. **Opcional: Asocie las SAN con redes.**

    Asocie las SAN con redes en HPE OneView.

    Consulte la ayuda en línea sobre **SAN Managers** (Administradores de SAN) para obtener más información.

13. **Cree perfiles de servidor y aplíquelos al hardware de servidor.**

    Cree y aplique perfiles de servidor para definir las configuraciones comunes para el hardware de servidor.

Consulte la ayuda en línea sobre **Server Profiles** (Perfiles de servidor) para obtener más información.

14. **Opcional: Conecte un volumen SAN a un perfil de servidor.**

    Conecte un volumen SAN a un perfil de servidor.

    Consulte la ayuda en línea sobre **Server Profiles** (Perfiles de servidor) para obtener más información.

15. **Guarde la configuración del dispositivo en un archivo de copia de seguridad.**

    Guarde la base de datos y los parámetros de configuración iniciales del dispositivo en un archivo de copia de seguridad para el caso de que, en el futuro, necesite restaurar la configuración actual del dispositivo.

    Consulte la ayuda en línea de **Settings** (Configuración) para obtener más información sobre cómo crear y guardar archivos de copia de seguridad del dispositivo.

10.2 Definición de las dimensiones físicas y los sistemas de alimentación en HPE OneView

La definición de las dimensiones físicas del espacio en el que reside el hardware de conexión de redes y la colocación de receptáculos, dispositivos de suministro eléctrico, hardware de servidor y otros dispositivos de los bastidores en HPE OneView proporciona al dispositivo un diagrama preciso de los dispositivos del centro de datos y sus conexiones físicas. Esto permite al dispositivo proporcionar potentes funciones de gestión y supervisión, como son:

- La pantalla **Data Centers** (Centros de datos) proporciona un modelo en 3D del entorno de TI, que se puede utilizar para la planificación y organización.
- La pantalla **Data Centers** (Centros de datos) muestra datos relativos a la alimentación y la temperatura que le permiten analizar el nivel de consumo eléctrico. El dispositivo informa sobre temperaturas pico en los bastidores y sus componentes para identificar posibles problemas de refrigeración y avisarle de ellos.
- La pantalla **Power Delivery Devices** (Dispositivos de suministro de energía) proporciona datos que le permiten analizar los índices de consumo de energía y los límites de alimentación.

1. **Agregue dispositivos de alimentación.**

   Defina los dispositivos y conexiones de alimentación.

   Consulte la ayuda en línea de **Power Delivery Devices** (Dispositivos de suministro de energía) para obtener más información.

2. **Agregue bastidores y configure su disposición.**

   Agregue bastidores y configure la disposición de los receptáculos, los dispositivos de suministro de energía y otros dispositivos de montaje en bastidor.

   Consulte la ayuda en línea de **bastidores** para obtener más información.

3. **Cree centros de datos y situar bastidores en ellos.**

   Defina la topología física y las características de alimentación y refrigeración de su centro de datos, lo que permite la supervisión de la temperatura y la visualización en 3D.

   Consulte la ayuda en línea de **Data Centers** (Centros de datos) para obtener más información.

11 Inicios rápidos para redes, receptáculos y almacenamiento

11.1 Inicio rápido: Adición de una red y asociación de esta con un servidor existente

En esta sección de inicio rápido se describe el proceso para agregar una red al dispositivo y permitir que los servidores existentes accedan a dicha red.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de red para añadir la red.
- Privilegios necesarios: administrador de infraestructuras o administrador de servidores para cambiar las configuraciones de los perfiles de servidor.
- Los receptáculos y el hardware de servidor se deben haber agregado al dispositivo.
- Todos los puertos de los conmutadores del centro de datos que se conectan con interconexiones de Virtual Connect deben estar configurados como se describe en «Requisitos de los puertos de conmutación del centro de datos» (página 207).

11.1.1 Adición de una red y asociación de esta con un servidor existente

Al agregar una red al dispositivo, puede que tenga que hacer cambios en la configuración de los recursos siguientes:

NOTA: Puede crear configuraciones activo/activo sin necesidad de crear dos redes con el mismo ID de VLAN. Consulte «Inicio rápido: Adición de una configuración de red activo/activo para uno o varios grupos de interconexiones lógicas» para obtener más información.

Recurso	Tarea	Descripción
Redes	**1.** Agregue la red.	• La adición de una red no requiere que se pongan los recursos fuera de línea. • Para obtener más información sobre las redes, consulte «Gestión de redes y recursos de red» (página 201), la ayuda en línea de la pantalla **Networks** (Redes) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las redes y los conjuntos de redes.
Grupos de interconexiones lógicas	**2.** Agregue la red a un conjunto de enlaces ascendentes o a las redes internas.	• Puede agregar la red a un conjunto de enlaces ascendentes existente o crear un conjunto de enlaces ascendentes para la red. • Para cambiar la configuración de un conjunto de enlaces ascendentes no es necesario poner los recursos fuera de línea. • Los cambios de configuración realizados en un grupo de interconexiones lógicas no se propagan automáticamente a las interconexiones lógicas que pertenecen a él. Sin embargo, al cambiar el grupo de interconexiones lógicas, puede actualizarlo para cada interconexión lógica con una sola acción. • Para obtener más información, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnect Groups** (Grupos de interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las interconexiones lógicas y la API de REST para el recurso `uplink-sets`.

Recurso	Tarea	Descripción
Interconexiones lógicas (una o más)	**3.** Realice una de las acciones siguientes: • Agregar la red a un conjunto de enlaces ascendentes o a las redes internas. • Actualice la interconexión lógica a partir del grupo de interconexiones lógicas.	• Para cambiar la configuración de un conjunto de enlaces ascendentes no es necesario poner los recursos fuera de línea. • Los cambios de configuración realizados en un grupo de interconexiones lógicas no se propagan automáticamente a las interconexiones lógicas que pertenecen a él. Para actualizar una interconexión lógica con los cambios realizados en su grupo de interconexiones lógicas, lleve a cabo una de las acciones siguientes: ◦ Seleccione **Logical Interconnects**→**Actions**→**Update from group**. ◦ Utilice las API de REST para volver a aplicar el grupo de interconexiones lógicas. Cuando se actualiza una interconexión lógica a partir de su grupo al agregar una red, no es necesario poner los recursos fuera de línea. • Es posible realizar cambios en una interconexión lógica sin cambiar el grupo de interconexiones lógicas. En este caso, se agrega la red a un conjunto de enlaces ascendentes de la interconexión lógica. Sin embargo, el dispositivo etiqueta la interconexión lógica como incompatible con su grupo. • Para obtener más información, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnects** (Interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las interconexiones lógicas.
Conjuntos de redes	**4.** (Opcional) Agregue la red a un conjunto de redes.	• Solo se aplica a las redes Ethernet. • La adición de una red a un conjunto de redes no requiere que se pongan los recursos fuera de línea. No es necesario actualizar los perfiles de servidor que estén conectados al conjunto de redes. • Para obtener más información sobre los conjuntos de redes, consulte «Gestión de redes y recursos de red» (página 201), la ayuda en línea de la pantalla **Network Sets** (Conjuntos de redes) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las redes y los conjuntos de redes.
Perfiles de servidor y **hardware de servidor**	**5.** Apague el servidor antes de editar el perfil de servidor. **6.** Edite el perfil de servidor para agregar una conexión a la red. **7.** Encienda el servidor después de aplicar el perfil de servidor.	• Para que un servidor se conecte a la red, el perfil de servidor del hardware de servidor debe incluir una conexión a la red o a un conjunto de redes que incluya dicha red. • Si se agrega la red a un conjunto de redes, los perfiles de servidor que tienen conexiones con el conjunto de redes tendrán acceso automáticamente a la red agregada. No es necesario editar estos perfiles de servidor. • Si la red no se agrega a un conjunto de redes, deberá agregar una conexión a la red en los perfiles de servidor que desee conectar con a dicha red. Apague el hardware de servidor antes agregar la conexión a un perfil de servidor. • Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.

11.2 Inicio rápido: Adición de una configuración de red activo/activo para uno o varios grupos de interconexiones lógicas

En esta sección de inicio rápido se describe cómo agregar una configuración activo/activo para un receptáculo.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de red para añadir redes.
- Privilegios necesarios: administrador de infraestructuras o administrador de servidores para cambiar las configuraciones de perfiles de servidor.
- Dos o más interconexiones de Virtual Connect compatibles, de acuerdo con la matriz de compatibilidad correspondiente de la **Biblioteca de información de Hewlett Packard Enterprise**.
- Los receptáculos y los blades de servidor se deben haber agregado al dispositivo.
- Siga las convenciones de nomenclatura recomendadas que se describen en «Requisitos para una configuración activo/activo».

11.2.1 Adición de una configuración de red activo/activo para uno o varios grupos de interconexiones lógicas

Para cada módulo de interconexión de Virtual Connect al que desee asignar la configuración activo/activo en el dispositivo, asegúrese de cambiar la configuración de los recursos siguientes:

Recurso	Tarea	Descripción
Redes	**1.** Agregue las redes. • Para un grupo de receptáculos con un solo grupo de interconexiones lógicas: **a.** Agregue un par de redes Ethernet para cada VLAN a la que desee conectarse: una red para el primer módulo de interconexión y otra red para el segundo módulo de interconexión que utiliza el mismo ID de VLAN. Por ejemplo, cree `Dev101_A` y `Dev101_B` para VLAN ID 101. • Para una configuración de varios grupos de interconexiones lógicas: **a.** Agregue una red Ethernet que se utilizará en ambos grupos de interconexiones lógicas.	En la pantalla **Networks** (Redes): • En **Name** (Nombre), asígnele nombres a las redes según «Requisitos para una configuración activo/activo» • En **Type** (Tipo), seleccione `Ethernet`. • En **VLAN ID** (ID de VLAN), introduzca el mismo ID en ambas redes. • Asegúrese de que esté seleccionada la opción **Smart link** (Enlace inteligente). • Para obtener más información sobre las redes, consulte «Gestión de redes y recursos de red» (página 201), la ayuda en línea de la pantalla **Networks** (Redes) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las redes y los conjuntos de redes.
Grupos de interconexiones lógicas e **interconexiones lógicas**.		• Puede agregar las redes a un conjunto de enlaces ascendentes existente o crear uno nuevo para las redes. • Los enlaces ascendentes de cada conjunto de enlaces ascendentes deben restringirse a una única interconexión. • No se permiten ID de VLAN duplicados en el mismo un conjunto de enlaces ascendentes. • Para obtener más información, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnects** (Interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los grupos de interconexiones lógicas y la API de REST para el recurso `uplink-sets`. **NOTA:** Si cambia el nombre de un conjunto de enlaces ascendentes en la pantalla de **Logical Interconnect Groups** (Grupos lógicos de interconexión) y, a continuación, selecciona **Actions→Update from group** (Acciones > Actualizar desde el grupo) en la pantalla **Logical Interconnects** (Interconexiones lógicas), se interrumpe brevemente la conectividad.

Recurso	Tarea	Descripción
	2. Cree los conjuntos de enlaces ascendentes. • Para un grupo de receptáculos con un solo grupo de interconexiones lógicas: **a.** Cree un par de conjuntos de enlaces ascendentes para asociar las redes a los puertos de enlace ascendente del módulo de interconexión. **b.** Asigne un conjunto de redes al conjunto de enlaces ascendentes que dispone de puertos en el primer módulo de interconexión. Asigne las otras redes al conjunto de enlaces ascendentes que dispone de puertos en el segundo módulo de interconexión. Por ejemplo, el puerto de enlace ascendente X5 se define en ambos conjuntos: `UplinkSet_A` para el compartimento 1 y `UplinkSet_B` para el compartimiento 2. `Dev101_A` se asigna a `UplinkSet_A` y `Dev101_B`, a `UplinkSet_B`. • Para una configuración de varios grupos de interconexiones lógicas: **a.** Cree un conjunto de enlaces ascendentes en el primer grupo de interconexiones lógicas y otro en el segundo, con las mismas redes.	

Recurso	Tarea	Descripción
Conjuntos de redes	**3.** (Opcional) Agregue uno o más pares de conjuntos de redes. Cada conjunto debe incluir solo las redes que se van a utilizar en la misma conexión de perfil de servidor. Por ejemplo, cree un conjunto de redes `DevSet_A` para sus redes de desarrollo `Dev_A`y cree `DevSet_B` para sus redes de desarrollo `Dev_B`.	• La adición de una red a un conjunto de redes no requiere que se pongan los recursos fuera de línea. No es necesario actualizar los perfiles de servidor que estén conectados al conjunto de redes. • No se permiten ID de VLAN duplicados en un conjunto de redes. • Cada conjunto de redes puede tener varias redes. • Para obtener más información sobre los conjuntos de redes, consulte «Gestión de redes y recursos de red» (página 201), la ayuda en línea de la pantalla **Network Sets** (Conjuntos de redes) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las redes y los conjuntos de redes.
Perfiles de servidor y **hardware de servidor**	**4.** Apague el servidor antes de editar el perfil de servidor. **5.** Edite el perfil de servidor para agregar dos conexiones. Asigne un puerto para las redes o conjuntos de redes en un mismo módulo y asígneles un puerto diferente para las redes o conjuntos de redes del otro módulo. Asegúrese de que las redes asociadas con los puertos de enlace ascendente del conjunto de enlaces ascendentes coinciden con las redes asignadas a las conexiones del perfil de los puertos de enlace descendente. Por ejemplo, `Connection1` es LOM1:1-a para `DevSet_A`y `Connection2` es LOM1:1-b para `DevSet_B`. **6.** Encienda el servidor.	• Al agregar una conexión al perfil de servidor, seleccione el puerto físico conectado al módulo con el conjunto de enlaces ascendentes que contiene las redes configuradas para dicha conexión. No seleccione **Auto** (Automático). • Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.

11.3 Inicio rápido: Migración de una configuración activo/en espera a activo/activo

En esta sección de inicio rápido se describe cómo migrar una configuración activo/en espera a una configuración activo/activo para un receptáculo.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de red para añadir redes.
- Privilegios necesarios: administrador de infraestructuras o administrador de servidores para cambiar las configuraciones de perfiles de servidor.
- Dos o más interconexiones de Virtual Connect compatibles, de acuerdo con la matriz de compatibilidad correspondiente de la **Biblioteca de información de Hewlett Packard Enterprise**.
- Los receptáculos y los blades de servidor se deben haber agregado al dispositivo.
- Siga las convenciones de nomenclatura recomendadas que se describen en «Requisitos para una configuración activo/activo».

11.3.1 Migración de una configuración activo/en espera a activo/activo

Para un grupo de receptáculos con un solo grupo de interconexiones lógicas, al realizar la migración de una configuración activo/en espera a una configuración activo/activo, debe realizar los cambios de configuración en los recursos siguientes:

Recurso	Tarea	Descripción
Grupos de interconexiones lógicas	1. Busque el conjunto o conjuntos de enlaces ascendentes que se desea convertir en activo/activo. 2. Anote todas las redes de los conjuntos de enlaces ascendentes.	Para obtener más información, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnect Groups** (Grupos de interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los grupos de interconexiones lógicas.
Redes	3. Cambie el nombre de las redes agregando `<lado>` al nombre de red, como se describe en «Requisitos para una configuración activo/activo» (por ejemplo, `Dev_100_A`). 4. Cree redes Ethernet mediante el mismo identificador de VLAN externa para cada red cuyo nombre haya cambiado en el paso 3 (por ejemplo, `Dev_100_B`).	En la pantalla **Networks** (Redes): • Para **VLAN ID**, utilice el mismo ID de VLAN para todas las redes cuyo nombre haya cambiado en el paso 3. • Asegúrese de que esté seleccionada la opción **Smart link** (Enlace inteligente). • Para obtener más información sobre las redes, consulte «Gestión de redes y recursos de red» (página 201), la ayuda en línea de la pantalla **Networks** (Redes) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las redes y los conjuntos de redes.
Conjuntos de redes	5. (Opcional) Agregar conjuntos de redes para las redes creadas en el paso 4.	• La adición de una red a un conjunto de redes no requiere que se pongan los recursos fuera de línea. No es necesario actualizar los perfiles de servidor que estén conectados al conjunto de redes. • No se permiten ID de VLAN duplicados en un conjunto de redes. • Para obtener más información sobre los conjuntos de redes, consulte «Gestión de redes y recursos de red» (página 201), la ayuda en línea de la pantalla **Network Sets** (Conjuntos de redes) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las redes y los conjuntos de redes.

Recurso	Tarea	Descripción
Grupos de interconexiones lógicas e **interconexiones lógicas**.	6. Determine si todas las interconexiones lógicas tienen puertos de enlace ascendente activos y en espera en los mismos módulos. • Si los enlaces ascendentes en espera se encuentran en el mismo módulo, vaya al paso 7. • Si los enlaces ascendentes en espera están en módulos diferentes, fuerce una conmutación por error de modo que todos los enlaces ascendentes en espera estén en el mismo módulo. Continúe con el paso 7. 7. Edite el conjunto de enlaces ascendentes activo/en espera y elimine los enlaces ascendentes en espera. 8. Cree un segundo conjunto de enlaces ascendentes para los enlaces ascendentes en espera eliminados en el paso 7. 9. Agregue las redes creadas en el paso 4 al nuevo conjunto de enlaces ascendentes. Por ejemplo, `UplinkSet_B` contiene todas las redes `Dev_B` . 10. Seleccione **Actions→Update from group** (Acciones > Actualizar desde el grupo). Los enlaces ascendentes activos mantendrán el tráfico, por lo que no hay ningún tiempo de inactividad.	Para determinar el estado del puerto (activo o en espera), acceda a la pantalla **Logical interconexiones** (Logical interconexiones) y revise el estado de cada puerto en la vista **Uplink Sets** (Conjuntos de enlaces ascendentes). • Hewlett Packard Enterprise recomienda eliminar los enlaces ascendentes en espera desde el conjunto de enlaces ascendentes original para, a continuación, agregarlos al nuevo conjunto de enlaces ascendentes. Este método impide la pérdida de conectividad. Si cambia el nombre de un conjunto de enlaces ascendentes en la pantalla de **Logical Interconnect Groups** (Grupos lógicos de interconexión) y, a continuación, selecciona **Actions→Update from group** (Acciones > Actualizar desde el grupo) en la pantalla **Logical Interconnects** (Interconexiones lógicas), se interrumpe brevemente conectividad. • Para obtener más información, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnects** (Interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las interconexiones lógicas y la API de REST para el recurso `uplink-sets`.

Recurso	Tarea	Descripción
Perfiles de servidor y **hardware de servidor**	11. Apague el servidor antes de editar el perfil de servidor. 12. Edite el perfil de servidor para agregar una conexión para la nueva red o conjunto de redes. 13. Encienda el servidor.	• Cambie todas las conexiones de perfil de servidor asociadas con el puerto de los enlaces ascendentes originales en espera. Asigne al puerto las nuevas redes o conjuntos de redes creados en los pasos 4 o 5. • Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.
Grupos de interconexiones lógicas e **interconexiones lógicas**.	14. Modifique grupo de interconexiones lógicas y cambie el nombre del conjunto de enlaces ascendentes original añadiendo `<lado>` al nombre, como se describen en «Requisitos para una configuración activo/activo» (por ejemplo, `UplinkSet_A`). No realice ningún otro cambio que no sea en el nombre del conjunto de enlaces ascendentes. 15. Seleccione **Actions→Update from group** (Acciones > Actualizar desde el grupo).	• Para obtener más información, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnects** (Interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las interconexiones lógicas y la API de REST para el recurso `uplink-sets`.

11.4 Inicio rápido: Adición de un receptáculo c7000 con un solo grupo de interconexiones lógicas y conexión de sus blades de servidor a las redes

En esta sección de inicio rápido se describe el proceso para agregar un receptáculo a un dispositivo existente con interconexiones de Virtual Connect y permitir que los blades de servidor accedan a las redes existentes en el centro de datos. Los escenarios de este inicio rápido son para una configuración de un solo grupo de interconexiones lógicas en cada receptáculo (totalmente apilado). Para ver un inicio rápido de una configuración de varios grupos de interconexiones lógicas en cada receptáculo, consulte “Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos” en la ***Guía de usuario de HPE OneView***.

Los pasos a seguir para añadir un receptáculo y asegurarse de que sus blades de servidor están conectados con las redes del centro de datos dependen de si utiliza un grupo de receptáculos existente o necesita definir la conectividad con la red mediante la configuración de grupos de receptáculos e interconexiones lógicas con sus conjuntos de enlaces ascendentes.

Para que un blade de servidor de un receptáculo se conecte con una red del centro de datos, es necesario asegurarse de que están configurados varios recursos. Para obtener una lista completa de los recursos y de las razones por las que son necesarios, consulte «Lista de comprobación: Conexión de un servidor a una red del centro de datos» (página 249).

Los grupos de interconexiones lógicas, sus conjuntos de enlaces ascendentes y sus grupos de receptáculos asociados pueden crearse de varias formas:

- Es posible crearlos antes de añadir el chasis a HPE OneView.
- Es posible crearlos durante la operación de adición del receptáculo. Durante la operación de adición del receptáculo, HPE OneView detecta las interconexiones instaladas en el receptáculo y crea los grupos basándose en el hardware existente en el receptáculo. La

configuración de los grupos debe completarse antes de completar la operación de adición del receptáculo.

11.4.1 Escenario 1: Adición de un receptáculo c7000 para gestionarlo en un grupo de receptáculos existente

La forma más rápida de agregar un receptáculo para gestionarlo con HPE OneView consiste en especificar un grupo de receptáculos existente. Cuando se agrega un receptáculo a un grupo de receptáculos existente, el receptáculo se configura como los demás receptáculos del grupo, incluyendo las conexiones de red. Este escenario crea un solo grupo de interconexiones lógicas para el receptáculo. Para crear un grupo de interconexiones lógicas para un receptáculo, consulte “Acerca de la configuración de varios grupos de interconexiones lógicas” en la ***Guía de usuario de HPE OneView***.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores.
- La configuración de hardware de las interconexiones del receptáculo debe coincidir con la configuración esperada por el grupo de interconexiones lógicas que está asociado con el grupo de receptáculos.
- Los conjuntos de enlaces ascendentes del grupo o los grupos de interconexiones lógicas deben incluir conexiones a las redes a las que se desea acceder.
- Todos los puertos de los conmutadores del centro de datos que se conectan a los módulos de interconexión de Virtual Connect (VC) deben estar configurados como se describe en «Requisitos de los puertos de conmutación del centro de datos» (página 207).
- Las redes y los conjuntos de redes, si los hay, deben haberse agregado HPE OneView. Para agregar redes o conjuntos de redes, consulte «Inicio rápido: Adición de una red y asociación de esta con un servidor existente» (página 141) o «Gestión de redes y recursos de red» (página 201).
- Consulte en «Requisitos previos para incluir un receptáculo c7000 en HPE OneView» los requisitos previos y la preparación que debe completar antes de agregar un receptáculo.
- Consulte en «Requisitos previos para incluir el hardware de servidor en un dispositivo» los requisitos previos y la preparación que debe completar antes de agregar un servidor.

Proceso

Recurso	Tarea	Descripción
Receptáculos	**1.** Agregue el receptáculo.	• Seleccione **Add enclosure for management** (Agregar receptáculo para gestionarlo). • Especifique un grupo de receptáculos existente. • Seleccione una línea de base de firmware y una opción de licencias HPE OneView Advanced. • Para obtener más información acerca de los receptáculos, consulte «Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos» (página 235), la ayuda en línea de la pantalla **Enclosures** (Receptáculos) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los receptáculos.
Perfiles de servidor	**2.** Realice una de las acciones siguientes: • Cree un perfil de servidor manualmente o desde una plantilla de perfil de servidor y asígneselo al hardware de servidor. • Copie un perfil de servidor y asígneselo al hardware de servidor y, a continuación, modifíquelo según sea necesario. **3.** Encienda el hardware de servidor.	Para que un blade de servidor se conecte a una red del centro de datos, debe tener asignado un perfil de servidor, y ese perfil de servidor debe incluir una conexión a la red o a un conjunto de redes que incluya dicha red: • Si existe un perfil de servidor que coincida con la forma en que desea configurar el hardware de servidor, puede copiarlo y asignárselo al hardware de servidor. • De lo contrario, debe crear o copiar y modificar un perfil de servidor que incluya al menos una conexión a la red o a un conjunto de redes que contenga dicha red. • Los perfiles de servidor contienen mucha más información de configuración que las conexiones con las redes. Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.

11.4.2 Escenario 2: Definición de la conectividad de red antes de agregar un receptáculo c7000 para gestionarlo

En este escenario, se configura el grupo de interconexiones lógicas, incluyendo sus conjuntos de enlaces ascendentes, y el grupo de receptáculos antes de agregar el receptáculo para gestionarlo. Después de definir estas configuraciones, el proceso es el mismo que agregar un receptáculo a un grupo de receptáculos existente. Este escenario crea un solo grupo de interconexiones lógicas para el receptáculo. Para crear una configuración de varios grupos de interconexiones lógicas en cada receptáculo, consulte “Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos” en la ***Guía de usuario de HPE OneView***.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores.
- La configuración de hardware de las interconexiones del receptáculo debe coincidir con la configuración esperada por el grupo de interconexiones lógicas que va a crear.
- Todos los puertos de los conmutadores del centro de datos que se conectan a los módulos de interconexión de Virtual Connect (VC) deben estar configurados como se describe en «Requisitos de los puertos de conmutación del centro de datos» (página 207).

- Las redes y los conjuntos de redes, si los hay, deben haberse agregado HPE OneView. Para agregar redes o conjuntos de redes, consulte «Inicio rápido: Adición de una red y asociación de esta con un servidor existente» (página 141) o «Gestión de redes y recursos de red» (página 201).
- Consulte en «Requisitos previos para incluir un receptáculo c7000 en HPE OneView» los requisitos previos y la preparación que debe completar antes de agregar un receptáculo.
- Consulte en «Requisitos previos para incluir el hardware de servidor en un dispositivo» los requisitos previos y la preparación que debe completar antes de agregar un servidor.

Proceso

Recurso	Tarea	Descripción
Grupos de interconexiones lógicas	**1.** Cree un grupo de interconexiones lógicas como mínimo.	• Los conjuntos de enlaces ascendentes se agregan durante la creación de un grupo de interconexiones lógicas. Asegúrese de que al menos uno de los conjuntos de enlaces ascendentes que agrega incluye un puerto de enlace ascendente a las redes del centro de datos a las que desea acceder. • Para obtener más información acerca de los grupos de interconexiones lógicas, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnect Groups** (Grupos de interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los grupos de interconexiones lógicas.
Grupos de receptáculos	**2.** Cree un grupo de receptáculos.	• Puede crear un grupo de receptáculos con grupos de interconexiones lógicas desde el principio, o puede crear uno que no especifique grupos de interconexiones lógicas y agregarlos más adelante. • Para obtener más información acerca de los grupos de receptáculos, consulte «Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos» (página 235), la ayuda en línea de la pantalla **Enclosure Groups** (Grupos de receptáculos), o la ayuda sobre secuencias de comandos de la API de REST relacionada de los grupos de receptáculos.

Recurso	Tarea	Descripción
Receptáculos	**3.** Agregue el receptáculo.	• Seleccione **Add enclosure for management** (Agregar receptáculo para gestionarlo). • Especifique el grupo de receptáculos que ha creado. • Seleccione una línea de base de firmware y una opción de licencias HPE OneView Advanced. • Para obtener más información acerca de los receptáculos, consulte «Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos» (página 235), la ayuda en línea de la pantalla **Enclosures** (Receptáculos) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los receptáculos.
Perfiles de servidor y **hardware de servidor**	**4.** Realice una de las acciones siguientes: • Cree un perfil de servidor manualmente o desde una plantilla de perfil de servidor y asígneselo al hardware de servidor. • Copie un perfil de servidor y asígneselo al hardware de servidor y, a continuación, modifíquelo según sea necesario. **5.** Encienda el hardware de servidor.	Para que un blade de servidor se conecte a una red del centro de datos, debe tener asignado un perfil de servidor, y ese perfil de servidor debe incluir una conexión a la red o a un conjunto de redes que incluya dicha red: • Si existe un perfil de servidor que coincida con la forma en que desea configurar el hardware de servidor, puede copiarlo y asignárselo al hardware de servidor. • De lo contrario, debe crear o copiar y modificar un perfil de servidor que incluya al menos una conexión a la red o a un conjunto de redes que contenga dicha red. • Los perfiles de servidor contienen mucha más información de configuración que las conexiones con las redes. Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.

11.4.3 Escenario 3: Definición de la conectividad de red al agregar el receptáculo para gestionarlo

En este escenario, se configuran el grupo de interconexiones lógicas, incluyendo sus conjuntos de enlaces ascendentes, y el grupo de receptáculos durante la operación de adición del receptáculo. HPE OneView detecta las interconexiones instaladas en el chasis y le pregunta si desea crear un grupo de interconexiones lógicas y un grupo de chasis basándose en el hardware existente en el chasis. Este escenario crea un solo grupo de interconexiones lógicas para el receptáculo. Para ver un inicio rápido de una configuración de varios grupos de interconexiones lógicas en cada receptáculo, consulte “Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos” en la ***Guía de usuario de HPE OneView***.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores.
- Todos los puertos de los conmutadores del centro de datos que se conectan a los módulos de interconexión de Virtual Connect (VC) deben estar configurados como se describe en «Requisitos de los puertos de conmutación del centro de datos» (página 207).
- Las redes y los conjuntos de redes, si los hay, deben haberse agregado HPE OneView. Para agregar redes o conjuntos de redes, consulte «Inicio rápido: Adición de una red y asociación de esta con un servidor existente» (página 141) o «Gestión de redes y recursos de red» (página 201).

- Consulte en «Requisitos previos para incluir un receptáculo c7000 en HPE OneView» los requisitos previos y la preparación que debe completar antes de agregar un receptáculo.
- Consulte en «Requisitos previos para incluir el hardware de servidor en un dispositivo» los requisitos previos y la preparación que debe completar antes de agregar un servidor.

Proceso

Recurso	Tarea	Descripción
Receptáculos	**1.** Agregue el receptáculo.	• Seleccione **Add enclosure for management** (Agregar receptáculo para gestionarlo). • Seleccione **Create new enclosure group** (Crear nuevo grupo de receptáculos). • Seleccione un nombre de grupo de receptáculos. • Seleccione una línea de base de firmware y una opción de licencias HPE OneView Advanced. • Para obtener más información acerca de los receptáculos, consulte «Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos» (página 235), la ayuda en línea de la pantalla **Enclosures** (Receptáculos) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los receptáculos.
Grupos de interconexiones lógicas	**2.** Seleccione **Create new logical interconnect group** (Crear nuevo grupo de interconexiones lógicas). **3.** Edite el grupo de interconexiones lógicas predeterminado.	• Durante la operación de adición del receptáculo, seleccione **Create new logical interconnect group** (Crear nuevo grupo de interconexiones lógicas). Después de hacer clic en **Add** (Agregar), HPE OneView detecta las interconexiones del receptáculo, crea un grupo de interconexiones lógicas predeterminado y abre una pantalla de edición para ese grupo de interconexiones lógicas. • El nombre del grupo de interconexiones lógicas predeterminado es el nombre del grupo de receptáculos que ha introducido seguido por `interconnect group`. Por ejemplo, si ha especificado `DirectAttachGroup` para el nombre del grupo de receptáculos, el nombre predeterminado del grupo de interconexiones lógicas es `DirectAttachGroup interconnect group`. • Los conjuntos de enlaces ascendentes se agregan durante la modificación del grupo de interconexiones lógicas. Asegúrese de que al menos uno de los conjuntos de enlaces ascendentes que agrega incluye un puerto de enlace ascendente a las redes del centro de datos a las que desea acceder. • Para obtener más información acerca de los grupos de interconexiones lógicas, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnect Groups** (Grupos de interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los grupos de interconexiones lógicas.
Perfiles de servidor y **hardware de servidor**		Para que un blade de servidor se conecte a una red del centro de datos, debe tener asignado un perfil de servidor, y ese perfil de servidor debe incluir una conexión a la red o a un conjunto de redes que incluya dicha red: • Si existe un perfil de servidor que coincida con la forma en que desea configurar el hardware de servidor, puede copiarlo y asignárselo al hardware de servidor. • De lo contrario, debe crear o copiar y modificar un perfil de servidor que incluya al menos una conexión a la red o a un conjunto de redes que contenga dicha red. • Los perfiles de servidor contienen mucha más información de configuración que las conexiones con las redes. Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.

Recurso	Tarea	Descripción
	4. Realice una de las acciones siguientes: • Cree un perfil de servidor manualmente o desde una plantilla de perfil de servidor y asígneselo al hardware de servidor. • Copie un perfil de servidor y asígneselo al hardware de servidor y, a continuación, modifíquelo según sea necesario. **5.** Encienda el hardware de servidor.	

11.5 Inicio rápido: Adición de un receptáculo c7000 con varios grupos de interconexiones lógicas y conexión de su hardware de servidor a las redes

En esta sección de inicio rápido se describe el proceso para agregar un receptáculo con varios grupos de interconexiones lógicas para que el hardware de servidor pueda acceder a las redes existentes del centro de datos. Para conocer las ventajas que ofrece la configuración de varios grupos de interconexiones lógicas, consulte «Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos».

Para configurar un receptáculo que no esté apilado, configure varios grupos de interconexiones lógicas, de forma que cada interconexión esté en un grupo de interconexiones lógicas distinto (lo que a su vez define las interconexiones lógicas) antes de agregar el receptáculo. También puede configurar un receptáculo parcialmente apilado en el que haya más de una interconexión asociada a un grupo de interconexiones lógicas.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores.
- Las interconexiones seleccionadas en los grupos de interconexiones lógicas deben coincidir con las interconexiones que contiene el receptáculo.
- Todos los puertos de los conmutadores del centro de datos que se conectan con interconexiones de Virtual Connect (VC) deben estar configurados como se describe en «Requisitos de los puertos de conmutación del centro de datos» (página 207).
- Consulte en «Requisitos previos para incluir un receptáculo c7000 en HPE OneView» los requisitos previos y la preparación que debe completar antes de agregar un receptáculo.
- Consulte en «Requisitos previos para incluir el hardware de servidor en un dispositivo» los requisitos previos y la preparación que debe completar antes de agregar un servidor.

Adición de un receptáculo c7000 con varios grupos de interconexiones lógicas y conexión de su hardware de servidor a las redes

Recurso	Tarea	Descripción
Redes y **conjuntos de redes**	1. Agregue las redes. 2. (Opcional) Agregue las redes a conjuntos.	• La adición de una red no requiere que se pongan los recursos fuera de línea. • Para obtener más información sobre las redes, consulte «Gestión de redes y recursos de red» (página 201).
Grupos de interconexiones lógicas	3. Cree un grupo de interconexiones lógicas para cada interconexión que desee situar en un grupo distinto.	• Puede crear un grupo de interconexiones lógicas con más de una interconexión lógica • Los conjuntos de enlaces ascendentes se agregan durante la creación de un grupo de interconexiones lógicas. Asegúrese de que al menos uno de los conjuntos de enlaces ascendentes que agrega incluye un puerto de enlace ascendente a las redes del centro de datos a las que desea acceder. • Los grupos de interconexiones lógicas crean las interconexiones lógicas cuando se agrega el receptáculo. • Para obtener más información acerca de los grupos de interconexiones lógicas, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnect Groups** (Grupos de interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los grupos de interconexiones lógicas.
Grupos de receptáculos	4. Cree un grupo de receptáculos.	• Incluya los grupos de interconexiones lógicas que ha creado en el grupo de receptáculos. • Para obtener más información acerca de los grupos de receptáculos, consulte «Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos» (página 235), la ayuda en línea de la pantalla **Enclosure Groups** (Grupos de receptáculos), o la ayuda sobre secuencias de comandos de la API de REST relacionada de los grupos de receptáculos.

Recurso	Tarea	Descripción
Receptáculos	**5.** Agregue el receptáculo.	• Seleccione **Add enclosure for management** (Agregar receptáculo para gestionarlo). • Especifique el grupo de receptáculos que ha creado. • Seleccione una línea de base de firmware y una opción de licencias. • Para obtener más información acerca de los receptáculos, consulte «Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos» (página 235), la ayuda en línea de la pantalla **Enclosures** (Receptáculos) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los receptáculos.
Perfiles de servidor y **hardware de servidor**	**6.** Realice una de las acciones siguientes: • Cree un perfil de servidor manualmente o desde una plantilla de perfil de servidor y asígneselo al hardware de servidor. • Copie un perfil de servidor y asígneselo al hardware de servidor y, a continuación, modifíquelo según sea necesario. **7.** Encienda el hardware de servidor.	Para que un blade de servidor se conecte a una red del centro de datos, debe tener asignado un perfil de servidor, y ese perfil de servidor debe incluir una conexión a la red o a un conjunto de redes que incluya dicha red: • Si existe un perfil de servidor que coincida con la forma en que desea configurar el hardware de servidor, puede copiarlo y asignárselo al hardware de servidor. • De lo contrario, debe crear o copiar y modificar un perfil de servidor que incluya al menos una conexión a la red o a un conjunto de redes que contenga dicha red. • Los perfiles de servidor contienen mucha más información de configuración que las conexiones con las redes. Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.

11.6 Inicio rápido: Adición de un servidor de montaje en bastidor HPE ProLiant DL para gestionarlo

En esta sección de inicio rápido se describe el proceso para agregar un servidor de montaje en bastidor para gestionarlo.

Las funciones admitidas por el dispositivo varían según el modelo del servidor. Para obtener información sobre las funciones admitidas para los servidores HPE ProLiant DL, consulte «Funciones de gestión del hardware de servidor» (página 170).

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores.
- El servidor debe estar conectado a una toma de suministro eléctrico activa.
- Consulte en «Requisitos previos para incluir el hardware de servidor en un dispositivo» los requisitos previos y la preparación que debe completar antes de agregar un servidor.

11.6.1 Adición de un servidor de montaje en bastidor HPE ProLiant DL para gestionarlo

Recurso	Tarea	Descripción
Hardware de servidor	1. Agregue el servidor utilizando la pantalla **Server Hardware** (Hardware de servidor) o las API de REST para el recurso `server-hardware`. 2. Encienda el servidor.	• Cuando agregue un servidor, debe proporcionar la información siguiente: ◦ Especifique **Managed** (Gestionado). ◦ El nombre del host o la dirección IP de iLO. ◦ El nombre de usuario y la contraseña de una cuenta de iLO con privilegios de administrador. ◦ Un tipo de licencia para el hardware de servidor. Para obtener más información acerca del hardware de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Hardware (Hardware de servidor)** o la ayuda sobre secuencias de comandos de la API de REST relacionada con el hardware de servidor. • Si la configuración de este servidor es distinta de la de los demás servidores del dispositivo, el dispositivo añade automáticamente un tipo de hardware de servidor para este modelo. • Debido a que este es un servidor de montaje en bastidor: ◦ No se puede utilizar el dispositivo para aprovisionar ninguna red para este servidor. ◦ Las funciones admitidas por el dispositivo varían según el modelo del servidor. Para obtener información sobre las funciones admitidas para los servidores HPE ProLiant DL, consulte «Funciones de gestión del hardware de servidor» (página 170).

11.7 Inicio rápido: Configuración de un receptáculo c7000 y un blade de servidor para la conexión directa con un sistema de almacenamiento HPE 3PAR

En esta sección de inicio rápido se describe el proceso para agregar y configurar un receptáculo de modo que sus servidores puedan conectarse a un sistema de almacenamiento HPE 3PAR que está conectado directamente (Flat SAN) con el receptáculo mediante interconexiones Virtual Connect FlexFabric.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de red para añadir las redes.
- Privilegios necesarios: administrador de infraestructuras o administrador de servidores para añadir receptáculos y perfiles de servidor.
- El sistema de almacenamiento HPE 3PAR debe estar instalado y configurado, y los cables deben estar conectados al receptáculo que se va a utilizar.
- Consulte en «Requisitos previos para incluir un receptáculo c7000 en HPE OneView» los requisitos previos y la preparación que debe completar antes de agregar un receptáculo.

- Consulte en «Requisitos previos para incluir el hardware de servidor en un dispositivo» los requisitos previos y la preparación que debe completar antes de agregar un servidor.

11.7.1 Configuración de un receptáculo c7000 y un blade de servidor para la conexión directa con un sistema de almacenamiento HPE 3PAR

Recurso	Tarea	Descripción
Redes	**1.** Agregue las redes Fibre Channel Direct attach.	• Al añadir las redes desde la pantalla **Networks** (Redes): ◦ Para **Type** (Tipo), seleccione `Fibre Channel` ◦ En **Fabric type** (Tipo de estructura), seleccione `Direct attach` (De conexión directa) • Para obtener más información sobre las redes, consulte «Gestión de redes y recursos de red» (página 201), la ayuda en línea de la pantalla **Networks** (Redes) o la ayuda sobre secuencias de comandos de la API de REST relacionada con las redes y los conjuntos de redes.
Grupos de interconexiones lógicas	**2.** Cree un grupo de interconexiones lógicas que defina los conjuntos de enlaces ascendentes para las conexiones de red Direct attach.	• Elija un nombre para el grupo de interconexiones lógicas que le ayude a distinguir los grupos de interconexiones lógicas que tienen conexiones con redes Fibre Channel Direct attach de los demás grupos de interconexiones lógicas. • Los conjuntos de enlaces ascendentes se agregan durante la creación del grupo de interconexiones lógicas. Asegúrese de que los conjuntos de enlaces ascendentes utilizan los puertos de enlace ascendente del receptáculo que están conectados físicamente al servidor de almacenamiento HPE 3PAR. • Para obtener más información acerca de los grupos de interconexiones lógicas, consulte «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209), la ayuda en línea de la pantalla **Logical Interconnect Groups** (Grupos de interconexiones lógicas) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los grupos de interconexiones lógicas.
Grupos de receptáculos	**3.** Cree un grupo de receptáculos.	• Elija un nombre que le ayude a distinguir los receptáculos que usan conexiones Fibre Channel Direct attach de los receptáculos que utilizan conexiones Fibre Channel Fabric attach.

Recurso	Tarea	Descripción
Receptáculos	**4.** Agregue el receptáculo.	• Seleccione **Add enclosure for management** (Agregar receptáculo para gestionarlo). • Seleccione el grupo de receptáculos que ha agregado en el paso anterior. • Seleccione una línea de base de firmware y una opción de licencias HPE OneView Advanced. • Para obtener más información acerca de los receptáculos, consulte «Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos» (página 235), la ayuda en línea de la pantalla **Enclosures** (Receptáculos) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los receptáculos.
Perfiles de servidor	**5.** Realice una de las acciones siguientes: • Cree un perfil de servidor y asígneselo al hardware de servidor. • Copie un perfil de servidor, modifíquelo según sea necesario y, a continuación, asígneselo al hardware de servidor. **6.** Después de configurar el sistema de almacenamiento HPE 3PAR, encienda el hardware de servidor.	• Para que un blade de servidor se conecte al sistema de almacenamiento HPE 3PAR, debe tener asignado un perfil de servidor, y ese perfil de servidor debe incluir por lo menos una conexión a la red Fibre Channel Direct attach que está conectada al sistema de almacenamiento. • Por ejemplo, si las redes que ha agregado son `Direct A` y `Direct B`, asegúrese de que el perfil de servidor tiene una conexión con la red `Direct A` y una conexión con la red `Direct B`. • Habilite el almacenamiento SAN mediante el perfil de servidor, además de otros valores de configuración. Debe agregar sistemas de almacenamiento, agregar volúmenes de almacenamiento y, a continuación, conectarlos al crear el perfil. Para obtener más información acerca de los perfiles de servidor, consulte «Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor» (página 169), la ayuda en línea de la pantalla **Server Profiles** (Perfiles de servidor) o la ayuda sobre secuencias de comandos de la API de REST relacionada con los perfiles de servidor.

11.8 Inicio rápido: Configuración de un HPE 5900 para gestionarlo con HPE OneView

Para agregar un HPE 5900 al dispositivo como administrador de SAN, debe configurar el conmutador como se describe en este documento. Los procedimientos siguientes describen cómo configurar un HPE 5900 mediante el software del conmutador para poder agregarlo a HPE OneView.

Consulte también:

- El capítulo *SAN Managers* (Administradores de SAN) de la **ayuda de la interfaz de usuario**
- El capítulo *SAN Managers* (Administradores de SAN) de la **ayuda de secuencias de comandos de la API de REST**

Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener más información sobre los administradores de SAN admitidos.

NOTA: En un entorno de conmutador conectado en cascada, todas las operaciones de zona y de alias de zona deben realizarse desde un único conmutador que se agrega como administrador de SAN (gestor de dispositivos) en HPE OneView. Las zonas y los alias de zona creados mediante otros conmutadores de la estructura no podrán verse en HPE OneView.

Tabla 6 Activación de SSH y creación de un usuario de SSH

✓	Configuración
	Active SSH en el HPE 5900 y cree un usuario de SSH (denominado `a5900` con la contraseña `sanlab1` en este ejemplo) en el HPE 5900 mediante el software del HPE 5900: **1.** `system-view` **2.** `public-key local create rsa` **3.** `public-key local create dsa` **4.** `ssh server enable` **5.** `user-interface vty 10 15` **6.** `authentication-mode scheme` **7.** `quit` **8.** `local-user a5900 class manage` **9.** `password simple sanlab1` **10.** `service-type ssh` **11.** `authorization-attribute user-role network-admin` **12.** `quit` **13.** `ssh user a5900 service-type stelnet authentication-type password`

Tabla 7 Creación de un usuario de SNMPv3

✓	Configuración

	El 5900 dispone de una vista predefinida denominada `ViewDefault`. Esta vista da acceso a la MIB `iso`, pero no a las MIB `snmpUsmMIB`, `snmpVasmMIB` ni `snmpModules.18`. Los siguientes pasos muestran cómo asignar un usuario de SNMP v3 con permiso de lectura predeterminado.
	Cree un usuario de SNMPv3 con permisos de lectura predeterminados
	Utilice este procedimiento si desea que el usuario tenga el nivel de acceso predeterminado.
	1. Escriba `system-view` en el HPE 5900 emitiendo el comando:
	`system-view`
	2. Cree un grupo (denominado `DefaultGroup` en este ejemplo) y establezca el permiso `Readview` en `ViewDefault`:
	`snmp-agent group v3 DefaultGroup privacy read-view ViewDefault`
	3. Cree un usuario de SNMPv3 (denominado `defaultUser` y con la contraseña de autenticación MD5 `authPass123` y la contraseña de privacidad AES-128 `privPass123` en este ejemplo) y añádalo al grupo creado en el paso 1:
	`snmp-agent usm-user v3 defaultUser DefaultGroup simple authentication-mode md5 authPass123 privacy-mode aes128 privPass123`
	4. Guarde los cambios:
	`save`
	NOTA: HPE OneView admite los siguientes protocolos de privacidad:
	• AES-128
	• DES-56

11.9 Inicio rápido: Configuración de un conmutador Cisco para agregarlo como administrador de SAN para gestionarlo con HPE OneView

Para agregar un conmutador Cisco al dispositivo como administrador de SAN, debe configurar el conmutador como se describe en este documento. Los procedimientos siguientes describen cómo configurar un administrador de SAN Cisco mediante el software del conmutador para poder agregarlo a HPE OneView.

Consulte también:

- El capítulo *SAN Managers* (Administradores de SAN) de la **ayuda de la interfaz de usuario**

- El capítulo *SAN Managers* (Administradores de SAN) de la **ayuda de secuencias de comandos de la API de REST**

Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener más información sobre los administradores de SAN admitidos.

NOTA: En un entorno de conmutador conectado en cascada, todas las operaciones de zona y de alias de zona deben realizarse desde un único conmutador que se agrega como administrador de SAN (gestor de dispositivos) en HPE OneView. Las zonas y los alias de zona creados mediante otros conmutadores de la estructura no podrán verse en HPE OneView.

Tabla 8 Creación de un usuario de SNMPv3 con permisos de escritura

✓	Configuración
	1. Entre en el modo de configuración con el comando config t **2.** Cree el usuario con la autenticación y la privacidad necesarias snmp-server user <nombre de usuario> auth <modo de autenticación, SHA o MD5> <contraseña de autenticación> priv <protocolo de privacidad, AES128, DES> <contraseña de priv> <nombre de rol/grupo> Ejemplo 1, creación de un usuario AUTHPRIV con SHA y AES128, y adición al grupo network-admin (conmutador)#snmp-server user AuthPrivUser auth sha authString123 priv aes-128 privString123 network-admin Ejemplo 2, creación de un usuario AUTHPRIV con MD5 y DES, y adición al grupo network-admin (conmutador)#snmp-server user AuthPrivUser auth md5 authString123 priv privString123 network-admin **3.** Opcional: para crear un rol para el usuario, utilice los comandos siguientes role name <nombre del rol> rule 1 permit read-write Ejemplo 3, creación de un usuario AUTHNOPRIV con MD5 y adición a un nuevo rol/grupo (conmutador)#role name newRole (conmutador)#rule 1 permit read-write (conmutador)#snmp-server user AuthUser auth md5 authString123 newRole **NOTA:** • Cisco solo admite los usuarios AUTHPRIV y AUTHNOPRIV. El usuario de SNMP puede agregarse al grupo/rol network-admin que existirá en el conmutador o es posible crear un rol y asignar el usuario a este rol. • HPE OneView admite los protocolos de autenticación siguientes: ◦ SHA ◦ MD5 • HPE OneView admite los siguientes protocolos de privacidad: ◦ AES-128 ◦ DES-56

11.10 Inicio rápido: configure la dirección MAC del hardware de servidor vinculante para los perfiles de servidor FCoE

Para configurar una SAN de modo que las conexiones del volumen del perfil de servidor sean visibles para el hardware de servidor, tiene que realizar una configuración vinculante para cada hardware de servidor.

11.10.1 Requisitos previos

- Pretende conectar volúmenes a hardware de servidor usando FCoE.
- Ha configurado al menos una conexión FCoE en un perfil de servidor.

11.10.2 Configuración de la dirección MAC del hardware de servidor vinculante para los perfiles de servidor FCoE

1. En el menú principal, seleccione **Server Profiles** (Perfiles de servidor).
2. En el panel principal, seleccione el perfil de servidor que especifica el hardware de servidor con una conexión FCoE.
3. En el selector **View** (Vista), seleccione **Connections** (Conexiones).
4. Para cada conexión que quiera vincular con una interfaz vfc, haga clic en el expansor para mostrar los detalles de la conexión. Tome nota de la dirección MAC de la conexión.
5. Utilice SSH para vincular la dirección MAC del hardware de servidor con la interfaz vfc de la vSAN. Consulte «Adding a FCoE volume in a multi-hop FCoE environment» (Cómo agregar un volumen FCoE en un entorno FCoE de múltiples saltos) en el ***FCoE Cookbook para HP Virtual Connect*** para obtener información sobre la vinculación de direcciones MAC del hardware de servidor con interfaces vfc en la vSAN.

Parte IV Configuración y gestión

En los capítulos de esta parte se describen las tareas de configuración y gestión para el dispositivo y los recursos que gestiona.

12 Prácticas recomendadas

Hewlett Packard Enterprise recomienda las prácticas que se describen a continuación para HPE OneView:

- «Prácticas recomendadas para la gestión de un dispositivo de VM»
- «Prácticas recomendadas para el mantenimiento de un dispositivo seguro»
- «Prácticas recomendadas para realizar una copia de seguridad de un dispositivo»
- «Prácticas recomendadas para la restauración de un dispositivo»
- «Prácticas recomendadas para migran un receptáculo de VCM a HPE OneView.»
- «Prácticas recomendadas para gestionar el firmware»
- «Prácticas recomendadas para la supervisión del estado con la interfaz de usuario del dispositivo»

13 Gestión de hardware de servidor, perfiles de servidor y plantillas de perfiles de servidor

La gestión de servidores con el dispositivo implica la interacción con distintos recursos del dispositivo:

- Un perfil de servidor captura la configuración completa del servidor en un solo lugar, lo que permite replicar de forma coherente nuevos perfiles de servidor y modificarlos rápidamente para reflejar los cambios del entorno de su centro de datos.
- Un perfil de servidor permite gestionar el hardware de servidor.
- Una plantilla de perfil de servidor proporciona un mecanismo para almacenar la configuración de un perfil de servidor. Todos los parámetros de configuración de un perfil de servidor están presentes en la plantilla de perfil de servidor.
- Una instancia de hardware de servidor es un servidor físico, como un blade de servidor HPE ProLiant BL460c Gen8, instalado en un receptáculo o un servidor de montaje en bastidor HPE ProLiant DL380p.
- Un tipo de hardware de servidor define las características de un modelo de servidor y un conjunto de opciones de hardware específico, como las tarjetas intermedias.
- Una conexión, que se asocia con un perfil de servidor, conecta un servidor con las redes del centro de datos.

Los perfiles de servidor proporcionan la mayor parte de las funciones de gestión de los servidores, pero el hardware de servidor y los perfiles de servidor son independientes entre sí:

- Un servidor físico, que es una instancia de hardware de servidor, puede o no tener asignado un perfil de servidor.
- Un perfil de servidor puede estar asignado a una instancia de hardware de servidor o a ningún hardware de servidor en concreto.

La combinación del hardware de servidor y el perfil de servidor que tiene asignado es lo que constituye un servidor completo en el dispositivo.

Debe utilizar el recurso de hardware de servidor para agregar servidores físicos al dispositivo cuando instale un servidor de montaje en bastidor. Los blades de servidor se añaden al dispositivo automáticamente cuando se agrega un receptáculo o se instala un blade de servidor en un receptáculo existente.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Server Profiles (Perfiles de servidor)	`server-profiles` y `connections`
Server Profile Templates (Plantillas de perfiles de servidor)	`server-profile-templates`
Server Hardware (Hardware de servidor)	`server-hardware`
Server Hardware Types (Tipos de hardware de servidor)	`server-hardware-types`

13.1 Gestión del hardware de servidor

El hardware de servidor representa una instancia de hardware de servidor, como un blade de servidor físico instalado en un receptáculo o servidor de montaje en bastidor físico. Un tipo de

hardware de servidor captura información acerca de la configuración física del hardware de servidor y define los parámetros que están disponibles para los perfiles de servidor asignados a ese tipo de hardware de servidor.

13.1.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de servidores

13.1.2 Tareas para el hardware de servidor

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Obtener información sobre el hardware de servidor.
- Encender y apagar un servidor.
- Reiniciar un servidor.
- Recopile datos de soporte remoto para el hardware de servidor.
- Inicie la consola remota iLO para gestionar los servidores de forma remota.
- Agregar o editar un servidor de montaje en bastidor.
- Agregar un servidor a un receptáculo existente.
- Reclamar un servidor que actualmente gestiona otro dispositivo.
- Quitar un servidor de la gestión.
- Quitar un servidor de un receptáculo existente.
- Actualizar la conexión entre el dispositivo y el hardware de servidor.
- Ver actividades.

13.1.3 Funciones de gestión del hardware de servidor

El dispositivo admite las siguientes funciones del hardware de servidor cuando este se agrega como gestionado.

Función	**Hardware de servidor admitido**		
	HPE ProLiant BL G7[1]	**HPE ProLiant BL y WS Gen8 y HPE ProLiant BL y WS Gen9**	**HPE ProLiant DL Gen8 y HPE ProLiant DL Gen9**
Encendido o apagado del servidor	✓	✓	✓
Visualización de los datos de inventario	✓	✓	✓
Supervisión de la energía, la refrigeración y la utilización[2]	✓	✓	✓
Supervisión del estado y las alertas	Con la instalación y configuración manual de agentes SNMP **NOTA:** Los agentes SNMP no están disponibles en ESXi	✓	✓

Función	Hardware de servidor admitido		
	HPE ProLiant BL G7[1]	HPE ProLiant BL y WS Gen8 y HPE ProLiant BL y WS Gen9	HPE ProLiant DL Gen8 y HPE ProLiant DL Gen9
Inicio de la consola remota de iLO	✓	✓	✓
SSO (single sign-on) a la interfaz web de iLO	✓	✓	✓
Actualización automática del firmware (iLO) a la versión mínima admitida cuando se añade al dispositivo	✓	✓	✓
Visualización y edición de bastidores	✓	✓	✓
Detección automática del tipo de hardware de servidor	✓	✓	✓
Funciones de los perfiles de servidor			
Configuración del BIOS		✓	✓[3]
Firmware		✓	✓
Conexiones a las redes	✓	✓	
Orden de arranque[4]	✓	✓	✓[3]
Almacenamiento local[5]		✓	✓[6]
Almacenamiento SAN	✓	✓	

[1] El dispositivo podría informar de un estado no admitido para algunos modelos de blades de servidor ProLiant G7 de doble ancho y doble densidad, lo que significa que el dispositivo no puede gestionarlos.

[2] No todos los servidores admiten la supervisión de la energía, la refrigeración y la utilización.

[3] No se admite el servidor HPE ProLiant DL580 Gen8.

[4] Debido a una limitación en las ROM de servidor Gen9 BL con fecha 27/08/2014 o anterior, si el modo de arranque está configurado como UEFI o UEFI optimizado, no es posible configurar el dispositivo de arranque principal. Si se selecciona la orden Manage boot (Gestionar el arranque), en el perfil correspondiente aparecerá una advertencia avisando de esta situación.

[5] Solo se admite con la controladora de matriz integrada. Las unidades M.2 se admiten en configuraciones concretas. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener más información.

[6] El almacenamiento local se admite para determinados modelos del hardware de servidor HPE ProLiant DL Gen9. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener una lista de los modelos que admiten el almacenamiento local.

13.1.4 Funciones de supervisión del hardware de servidor

Cuando se supervisa hardware de servidor, el dispositivo admite las funciones siguientes.

Función	Hardware de servidor supervisado			
	HPE ProLiant BL y DL G6 (con iLO 2)	HPE ProLiant BL y DL G7	HPE ProLiant BL y DL Gen8 y Gen9	HPE ProLiant XL Gen9 **NOTA:** El chasis Apollo no se detecta.
Encendido o apagado del servidor	✓	✓	✓	✓
Supervisión de la energía, la refrigeración y la utilización[1]		✓	✓	✓

Función	Hardware de servidor supervisado			
	HPE ProLiant BL y DL G6 (con iLO 2)	**HPE ProLiant BL y DL G7**	**HPE ProLiant BL y DL Gen8 y Gen9**	**HPE ProLiant XL Gen9** **NOTA:** El chasis Apollo no se detecta.
Supervisión del estado y las alertas	Con la instalación y configuración manual de agentes SNMP **NOTA:** Los agentes SNMP no están disponibles en ESXi 5.x y 6.x.	Con la instalación y configuración manual de agentes SNMP **NOTA:** Los agentes SNMP no están disponibles en ESXi 5.x y 6.x.	✓	✓
Inicio de la consola remota de iLO		✓	✓	✓
Remote Support			✓	
SSO (single sign-on) a la interfaz web de iLO		✓	✓	✓
Detección automática del tipo de hardware de servidor		✓[2]	✓	

[1] No todos los servidores admiten la supervisión de la energía, la refrigeración y la utilización.

[2] Los servidores ProLiant DL G7 no disponen de detección del tipo de hardware de servidor.

13.1.5 Requisitos previos para incluir el hardware de servidor en un dispositivo

Modelo de hardware de servidor

El hardware de servidor debe ser un modelo compatible según la ***Matriz de compatibilidad de HPE OneView***.

El hardware de servidor debe estar conectado a una toma de suministro eléctrico activa.

El hardware de servidor debe tener un ID de producto y un número de serie válidos para poder gestionarlo con HPE OneView.

Firmware de iLO

La versión de firmware de iLO (Integrated Lights-Out) debe cumplir los requisitos mínimos indicados en la ***Matriz de compatibilidad de HPE OneView***.

Direcciones IP

Se requiere la configuración de IPv4.

Los iLO del hardware de servidor de montaje en bastidor deben tener una dirección IP.

Cuentas de usuario locales

Los iLO deben estar configurados para usar cuentas de usuario locales.

13.1.6 Acerca del hardware de servidor

Un recurso de hardware de servidor representa una instancia de servidor que se gestiona o supervisa mediante HPE OneView.

Es posible aplicar la configuración a un recurso de hardware de servidor gestionado asignándole un perfil de servidor.

Existen distintas formas de agregar servidores a HPE OneView.

Gestionado HPE OneView gestiona el servidor, lo que le permitirá aplicar configuraciones, asignar perfiles de servidor, supervisar el estado de funcionamiento, recopilar estadísticas y alertar a los usuarios cuando se den determinadas situaciones. Los blades de servidor que se encuentren en un receptáculo gestionado se agregarán automáticamente como gestionados. Los servidores gestionados requieren una licencia HPE OneView Advanced o HPE OneView Advanced w/o iLO.

Supervisado HPE OneView supervisa el hardware únicamente a efectos de inventario y de estado del hardware. El servidor puede gestionarse fuera de HPE OneView. Los blades de servidor que se encuentren en un receptáculo supervisado se agregarán como supervisados. Los servidores supervisados utilizan una licencia gratuita denominada HPE OneView Standard.

13.1.6.1 Cómo gestiona el dispositivo el hardware no compatible

El hardware no compatible es cualquier equipo de hardware que el dispositivo no puede gestionar. Los equipos no compatibles son similares a los equipos no gestionados en que todos los equipos no compatibles no están gestionadas por el dispositivo. La diferencia consiste en que puede incluir los equipos no gestionados en la gestión del dispositivo si toma las medidas adecuadas o los configura correctamente. El hardware no compatible nunca puede gestionarse mediante el dispositivo.

El dispositivo detecta el hardware no compatible y muestra el nombre del modelo y otra información básica que se obtiene del equipo de hardware con fines de inventario. El dispositivo también controla el espacio físico que ocupan los equipos de hardware no compatibles en los receptáculos y los bastidores.

Para tener en cuenta el espacio que ocupa un equipo de hardware, el dispositivo de gestión representa el hardware no compatible de la misma forma en que representa los equipos no gestionados.

La acción disponible para el hardware no compatible es **Remove** (Quitar).

13.1.6.2 Acerca del hardware de servidor supervisado

Se pueden agregar servidores de montaje en bastidor o blades de servidor para poder hacer el inventario del hardware y supervisarlo. Esto es útil cuando se dispone de servidores que ya han sido implementados.

La supervisión permite controlar la alimentación, la refrigeración, la utilización y el estado del hardware. Puede encender y apagar el servidor o la consola remota de iLO y examinar el inventario. También obtendrá notificaciones por correo electrónico, el reenvío de capturas SNMP y soporte opcional 9 horas al día, cinco días a la semana, durante 1 año.

La función de supervisión está disponible para todos los servidores ProLiant G6 y posteriores con iLO 2, iLO 3 o iLO 4. Si HPE OneView supervisa un servidor, usted puede gestionar los receptáculos, los perfiles de servidor y la infraestructura de Virtual Connect mediante VCM o VCEM. No puede gestionar perfiles de servidor para el hardware de servidor supervisado en HPE OneView.

Una ventaja de la supervisión del hardware de servidor es que la funcionalidad básica de supervisión e inventario puede llevarse a cabo con una licencia gratuita denominada HPE OneView Standard.

OneView puede configurar los servidores' iLO para que envíen sus registros del sistema a un destino remoto. Consulte la documentación de *HPE OneView REST API Reference* (Referencia de la API de REST de HPE OneView) de la operación PATCH en /rest/serverhardware para obtener información adicional sobre cómo realizar una operación de registro del sistema.

Para agregar un blade de servidor para supervisarlo, consulte «Adición de un receptáculo c7000 para supervisar el hardware».

13.1.6.3 Acerca del hardware de servidor no compatible

El dispositivo no puede gestionar el hardware de servidor no compatible. Sin embargo, es posible colocar hardware de servidor no compatible en receptáculos o bastidores. La adición en el dispositivo de hardware de servidor no compatible permite hacerse una idea del espacio físico que ocupa este en un receptáculo o bastidor para fines de planificación o inventario.

El dispositivo muestra información básica sobre el hardware de servidor no compatible que obtiene de iLO o el OA.

Cuando el dispositivo detecta hardware de servidor no compatible, coloca el hardware en el estado `Unsupported` (No compatible). Puede realizar una operación remove (quitar) para quitar del dispositivo el hardware de servidor no compatible.

NOTA: Los servidores DL no compatibles solo se pueden agregar a través de una iPDU inteligente.

13.1.6.4 Acerca de los equipos no gestionados

Un equipo no gestionado es un equipo, como un servidor, receptáculo, conmutador KVM (teclado, vídeo y ratón), monitor/teclado de montaje en bastidor o un router, que ocupa un espacio en un bastidor y/o consume energía, pero que no está gestionado por el dispositivo de gestión.

Los equipos no gestionados se crean automáticamente para representar los equipos que están conectados a una unidad Intelligent Power Distribution Unit (iPDU) utilizando conexiones Power Discovery Services. Los receptáculos BladeSystem y los servidores de la serie ProLiant DL se muestran con el estado `unmanaged` (no gestionado) o `unsupported` (no compatible) en las pantallas **Enclosures** (Receptáculos) y **Server Hardware** (Hardware de servidor) del panel principal, respectivamente. Estos se representarán como receptáculos y servidores no gestionados y, como tal, se incluirán en la lista de recursos **Unmanaged Devices** (Equipos no gestionados).

Al crear un equipo no gestionado, debe proporcionar su nombre, descripción del modelo, altura en ranuras U y requisitos máximos de energía. Estos valores se utilizan para el análisis de la capacidad de enfriamiento y energía, y permiten generar alertas para identificar los posibles problemas de energía y refrigeración.

Debido a que no hay comunicación con un equipo no gestionado, este se muestra con el estado `disabled` (desactivado), a menos que haya alertas generadas por el dispositivo de gestión para identificar problemas que deben solucionarse.

A efectos de la configuración de energía, se supone que los equipos no gestionados tienen dos conexiones de alimentación para admitir alimentación redundante. Estas se identifican como fuente de alimentación 1 y 2. Si un equipo no gestionado no admite alimentación redundante, conecte solo la fuente de alimentación 1 y, a continuación, desactive la alerta sobre la falta de alimentación redundante en el equipo.

Para los equipos que no se detectan a través de conexiones Power Discovery Services, puede agregar manualmente estos equipos en el dispositivo de gestión para poder realizar su seguimiento, inventario y gestión de energía.

13.1.7 Tareas para los tipos de hardware de servidor

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Editar el nombre o la descripción del tipo de hardware de servidor.
- Eliminar un tipo de hardware de servidor.

13.1.8 Acerca de los tipos de hardware de servidor

Un tipo de hardware de servidor define la configuración física del hardware de servidor y define los parámetros disponibles para los perfiles de servidor que se van a asignar a ese tipo de hardware de servidor. Por ejemplo, el tipo de hardware de servidor para el blade de servidor HPE ProLiant BL460c Gen8 incluye una lista completa de parámetros de configuración del BIOS y los valores predeterminados para ese modelo.

El dispositivo crea tipos de hardware de servidor según el hardware de servidor que detecte. El tipo de hardware de servidor se utiliza cuando se crea un perfil de servidor para mostrar los valores que se encuentran disponibles.

13.1.9 Cómo cambia el iLO a consecuencia de la gestión de HPE OneView

Cuando el dispositivo gestiona hardware de servidor, el iLO del servidor experimenta estos cambios en la configuración:

- Se crea una cuenta de gestión (_HPOneViewadmin) que puede visualizarse en las pantallas **Overview** (Información general) y **User Administration** (Administración de usuarios) del iLO.
- Se activa SNMP y el dispositivo se añade como destino de captura SNMP.

  NOTA: La supervisión del estado no se activa en el iLO3 del hardware de servidor ProLiant G6 o ProLiant G7 hasta que no se instalan los agentes de gestión en el sistema operativo y **se configura el servicio SNMP** con la misma cadena de comunidad de lectura de SNMP que se muestra en la pantalla Settings (Configuración).

- Se activa NTP y el dispositivo se convierte en la fuente de tiempo NTP del hardware de servidor.
- Se instala un certificado del dispositivo para permitir las operaciones de inicio de sesión único.
- El firmware de iLO se actualiza a las versiones mínimas indicadas en la ***Matriz de compatibilidad de HPE OneView*** para los servidores gestionados.
- La zona horaria de iLO se establece en `Atlantic/Reykjavik`, tal como recomienda la documentación de iLO.

  La configuración de la zona horaria determina el modo en que el iLO ajusta la hora UTC para obtener la hora local y cómo se ajusta al horario de verano. Para que las entradas del registro de eventos de iLO y el IML muestren la hora local correcta, debe especificar en qué zona horaria está ubicado el servidor.

  Si desea que el iLO utilice la hora proporcionada por el servidor SNTP sin ajustarla, configure el iLO para que utilice una zona horaria que no aplique un ajuste con respecto a la hora UTC. Además, esa zona horaria tampoco debe aplicar el horario de verano.

  Hay varias zonas horarias que cumplen este requisito. Por ejemplo, la zona horaria `Atlantic/Reykjavik`. Esta zona horaria no está ni al este ni al oeste del meridiano de Greenwich y la hora no cambia en primavera ni en otoño.

Más información

«Activación de la supervisión del estado para los servidores heredados»
«Acerca de la configuración de SNMP»

13.1.10 Inicio de la consola de iLO para gestionar servidores de forma remota

La consola remota de iLO solo está disponible para los servidores que tienen una licencia de iLO. La consola le permite conectarse de forma remota al servidor para realizar las acciones siguientes:

- Acceder a una pantalla en el servidor físico para instalar o utilizar el sistema operativo (Windows o Linux)
- Encender, apagar o reiniciar un servidor
- Montar soportes de instalación en CD/DVD desde un cliente remoto para permitir la instalación de un sistema operativo

La interfaz de usuario web de iLO expone estas funciones de iLO:

- Supervisión de energía
- Encendido o apagado
- Consola remota
- Datos de estado
- Creación de cuentas
- Seguridad
- Otras tareas de gestión de iLO

La consola remota de iLO se inicia desde la pantalla **Server Hardware** (Hardware de servidor) o **Server Profiles** (Perfiles de servidor). Los pasos necesarios para iniciar la consola remota de iLO dependen del sistema operativo (Windows o Linux) y el explorador (Internet Explorer, Chrome o Firefox) del cliente.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores

Cómo iniciar la consola de iLO para gestionar servidores de forma remota

1. En el menú principal, seleccione una de las opciones siguientes:
   - **Server Hardware** (Hardware de servidor) y, a continuación, seleccione un servidor
   - **Server Profiles** (Perfiles de servidor) y, a continuación, seleccione un perfil de servidor
2. Seleccione **Actions→Launch console** (Acciones > Iniciar consola).
   - **Cliente Windows con Internet Explorer, Chrome o Firefox**

     La consola de iLO es una aplicación binaria de Windows que se instala en cada equipo cliente la primera vez que se inicia la consola. Una vez finalizada la instalación inicial, haga clic en el botón **My installation is complete — Launch console** (Mi instalación se ha completado — Iniciar consola) para iniciar la consola remota. Después de instalar la consola, se puede iniciar directamente desde el menú **Actions** (Acciones).

     NOTA: La instalación de la aplicación ofrece la mejor experiencia de usuario de HPE OneView.

     La acción inicial **Launch console** (Iniciar consola) solicita una instalación e intentará abrir el instalador. El número de cuadros de diálogo que aparecen durante la instalación depende del explorador.

     - En Internet Explorer, haga clic en **Ejecutar** cuando se le indique.

       Si se intenta realizar la acción **Launch console** (Iniciar consola) y no se producen errores durante la instalación, pero no se muestra la consola, mantenga pulsada la tecla **Mayús** y, a continuación, seleccione **Actions→Launch console** (Acciones

> Iniciar consola) para volver a instalar la consola remota como se describe en «Reinstalación de la consola remota».

- En Chrome, al hacer clic en **Install software** (Instalar el software), el archivo del instalador de la consola remota integrada de HPE iLO se muestra en la esquina inferior izquierda del explorador. Haga clic en este nombre de archivo para comenzar la instalación.

  Si se intenta realizar la acción **Launch console** (Iniciar consola) y no se producen errores durante la instalación, pero no se muestra la consola, mantenga pulsada la tecla **Mayús** y, a continuación, seleccione **Actions→Launch console** (Acciones > Iniciar consola) para volver a instalar la consola remota como se describe en «Reinstalación de la consola remota».

- En Firefox, haga clic en el botón **Guardar archivo** cuando Firefox intente abrir el instalador por primera vez y, a continuación, haga doble clic en el archivo del instalador cuando se muestre en el cuadro de diálogo **Descargas** para comenzar la instalación.

  Si intenta realizar una acción **Launch console** (Iniciar consola) durante la instalación y recibe una notificación, mantenga pulsada la tecla **Mayús** y, a continuación, seleccione **Actions→Launch console** (Acciones > Iniciar consola) para volver a instalar la consola remota como se describe en «Reinstalación de la consola remota».

- **Cliente Windows con el complemento de Java**

  Si no está ejecutando Internet Explorer, también puede iniciar un complemento de Java para la consola de iLO haciendo clic en el enlace **Launch** (Iniciar) en el cuadro de diálogo **Install software** (Instalar el software). Esto está pensado para los casos en que se usa una estación de trabajo de Windows en la que no se permite instalar ningún software. El cuadro de diálogo **Install software** (Instalar el software) no se muestra nunca con Internet Explorer, por lo que no se puede iniciar la consola de Java.

  NOTA: La consola del complemento de Java abre una ventana emergente. Hewlett Packard Enterprise recomienda desactivar el bloqueador de ventanas emergentes del explorador.

- **Cliente Linux con cualquier explorador**

  Los clientes Linux inician la consola del complemento de Java con autenticación de inicio de sesión único directamente en el iLO. Esta consola requiere tener instalado JRE en el cliente; en caso contrario, que se le pedirá que lo instale. El número de cuadros de diálogo que se muestran durante la instalación depende del explorador.

13.1.11 Activación de la supervisión del estado para los servidores heredados

Los sistemas de gestión de redes utilizan SNMP (Simple Network Management Protocol) para supervisar los equipos conectados a la red. El dispositivo utiliza SNMP para recuperar la información de los equipos gestionados. Los equipos gestionados utilizan SNMP para enviar notificaciones asíncronas (que se denominan capturas) al dispositivo.

Se especifica una cadena de comunidad de lectura que sirve como credencial para comprobar el acceso a los datos de SNMP en los equipos gestionados. El dispositivo envía la cadena de comunidad de lectura a los receptáculos (a través de sus OA) y a los servidores (a través de sus procesadores de gestión de iLO). Algunos equipos más antiguos requieren configuración manual en el sistema operativo del host.

Instalación de los agentes SNMP del host del sistema operativo para blades de servidor HPE ProLiant

Para que el dispositivo supervise el estado de los blades de servidor HPE ProLiant G6 y HPE ProLiant G7, debe ajustar la configuración de SNMP del servidor y de iLO 3.

1. Instale el sistema operativo host en el servidor.
2. Instale el subsistema SNMP en el servidor.
3. Configure SNMP en el host para utilizar la cadena de comunidad y el destino de captura del dispositivo.
4. Utilice el SPP más reciente para instalar el conjunto de agentes de gestión de Hewlett Packard Enterprise y los controladores asociados. Se le pedirán el destino de captura y la cadena de comunidad SNMP.
5. Cuando el conjunto de agentes de gestión de Hewlett Packard Enterprise y los controladores asociados estén instalados y en funcionamiento, agregue el blade de servidor HPE ProLiant G6 y HPE ProLiant G7 al dispositivo.

   Si instala los agentes y los controladores después de agregar el blade de servidor G7, es posible que tenga que actualizar el blade de servidor G7 desde la interfaz de usuario o con las API de REST.

NOTA: Si cambia la cadena de comunidad de lectura del dispositivo, debe volver a configurar los agentes SNMP del host del sistema operativo de todos los blades de servidor HPE ProLiant G6 y HPE ProLiant G7 para que utilicen la nueva cadena de comunidad de lectura. El dispositivo no puede propagar esta actualización al sistema operativo del host.

13.2 Gestión de perfiles de servidor

Los servidores se representan y gestionan a través de sus perfiles de servidor. Un perfil de servidor recoge en un solo lugar los aspectos fundamentales de la configuración de un servidor, como niveles de firmware, configuración del BIOS, conectividad de red, configuración del orden de arranque, configuración de iLO e identificadores únicos.

13.2.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de servidores

13.2.2 Tareas para los perfiles de servidor

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para las siguientes tareas:

- Obtener información acerca de un perfil de servidor.
- Agregar un volumen SAN a un perfil de servidor.
- Arrancar desde un volumen SAN conectado.
- Crear y aplicar un perfil de servidor o una plantilla de perfil de servidor.
- Copiar, editar o eliminar un perfil de servidor.
- Instalar un lote de firmware utilizando un perfil de servidor.
- Conectar el servidor a las redes del centro de datos añadiendo una conexión a un perfil de servidor.
- Gestionar el almacenamiento local de un servidor.
- Gestionar el almacenamiento SAN conectando volúmenes SAN nuevos o existentes al perfil de servidor.

- Gestionar los parámetros de arranque de un servidor.
- Gestionar la configuración del BIOS de un servidor.
- Gestionar los identificadores virtuales o físicos del hardware de servidor.
- Migrar un perfil de servidor existente.
- Mover un perfil de servidor a otro servidor.
- Encender y apagar el hardware de servidor al que está asignado el perfil de servidor.
- Especificar identificadores y direcciones al crear un perfil de servidor.
- Actualizar el firmware con un perfil de servidor.
- Actualizar la configuración del perfil partiendo de la plantilla de perfil de servidor.
- Ver actividades.

13.2.3 Acerca de los perfiles de servidor

- «Captura de configuraciones recomendadas»
- «Acerca de la edición de perfiles de servidor»
- «Acerca del traslado de perfiles de servidor»
- «Acerca de la migración de perfiles de servidor»
- «Uso de perfiles de servidor para controlar el comportamiento de eliminación y sustitución»
- «Acerca de la asignación de un perfil de servidor a un compartimento de dispositivo vacío»
- «Acerca de las conexiones de perfiles de servidor»
- «Sobre las conexiones del perfil de servidor y el cambio de los tipos de hardware de servidor»
- «Acerca de los perfiles de servidor y el almacenamiento local»
- «Acerca de la conexión de volúmenes SAN a un perfil de servidor»

13.2.3.1 Captura de configuraciones recomendadas

Después de configurar el centro de datos, puede crear perfiles de servidor para aprovisionar cientos de servidores tan fácilmente como si fueran solo uno. Un perfil de servidor es la configuración para una instancia de servidor. Los perfiles de servidor y las plantillas de perfiles de servidor capturan la configuración completa del servidor en un solo lugar, lo que permite replicar nuevos perfiles de servidor y modificarlos para reflejar los cambios de un centro de datos.

Un perfil de servidor incluye:

- Información básica de identificación del servidor
- Configuración de conectividad para redes Ethernet, conjuntos de redes y redes Fibre Channel y FCoE
- Versiones de firmware
- Configuración de almacenamiento local
- Configuración de almacenamiento SAN
- Parámetros de arranque
- Configuración del BIOS

Cuando se crea un perfil de servidor, se puede especificar el hardware de servidor al que quiere aplicar el perfil. Si el hardware de servidor aún no está instalado, déjelo sin asignar. Por lo

general, se capturan las configuraciones recomendadas en una plantilla de perfil de servidor y, a continuación, se crean perfiles de servidor individuales. Al igual que las plantillas de máquina virtual (VM), los perfiles le permiten crear una línea de base de aprovisionamiento para los tipos de hardware de servidor de un receptáculo.

Cuando crea un perfil de servidor, se diseña para un tipo de hardware de servidor y un grupo de receptáculos (para blades de servidor), tanto si el perfil está asignado como si no lo está. Solo se puede asignar un único perfil al hardware de servidor.

De forma predeterminada, el perfil de servidor controla el comportamiento de arranque del servidor. El tipo de hardware de servidor determina las opciones disponibles, que puede seleccionar en el perfil de servidor. Si es necesario, se puede seleccionar el modo de arranque y la directiva de arranque PXE. También se puede especificar el orden en que el hardware de servidor intentará arrancar. Los servidores HPE ProLiant Gen9 admiten tanto el BIOS heredado como UEFI para configurar el proceso de arranque, mientras que los servidores HPE ProLiant Gen8 solo admiten el modo BIOS heredado. Para obtener más información sobre UEFI, consulte **UEFI FAQs** (Preguntas más frecuentes sobre UEFI) en **Unified Extensible Firmware Interface Forum**.

Si selecciona que se debe gestionar la configuración del BIOS a través del dispositivo, podrá ver todas las configuraciones, solo las que se han modificado o solo las que son diferentes de los valores predeterminados. Los parámetros de configuración del BIOS que se muestran dependen del hardware de servidor admitido.

La aplicación de secciones de un perfil de servidor al hardware de servidor es un proceso secuencial. La pantalla muestra la sección que se está aplicando actualmente, seguida por otras secciones que se hayan aplicado correctamente. Si se debe volver a aplicar un perfil de servidor debido a un error, solo se vuelven a aplicar las secciones sin configurar y las que no hayan sido aplicadas previamente. Por ejemplo, si se realiza correctamente una actualización del firmware, pero falla la parte del BIOS siguiente de la operación de aplicación, el firmware no se aplica una segunda vez cuando se vuelve el aplicar el perfil. Esto ayuda a evitar actualizaciones largas e innecesarias para el perfil.

Práctica recomendada: realice las tareas de gestión de los perfiles de servidor en un receptáculo cada vez

Para obtener el mejor rendimiento posible, cree, elimine, edite, copie o mueva los perfiles de servidor del hardware de servidor de un receptáculo antes de gestionar los perfiles de servidor de otro receptáculo.

13.2.3.2 Acerca de la edición de perfiles de servidor

Edite un perfil de servidor para cambiar la configuración asociada con dicho perfil. Puede editar un perfil de servidor en cualquier momento después de crearlo. También puede editar un perfil de servidor con una condición de `Error` para corregirlo.

Cuando se edita un perfil de servidor, cambia el estado del servidor. El dispositivo analiza los cambios y determina las acciones para actualizar el servidor. Por ejemplo, si se cambia la configuración del BIOS pero no la línea de base de firmware, no se actualiza el firmware. Solo se aplican los cambios solicitados.

NOTA: Si se cambia la configuración o el estado del servidor mediante otras herramientas distintas del dispositivo, los cambios no se detectan ni se gestionan. Estos cambios se podrían sobrescribir la próxima vez que se modifique el perfil.

Cuando modifique un perfil de servidor, tenga en cuenta lo siguiente:

- La modificación de un perfil es una operación asíncrona. Los cambios en el nombre y la descripción surten efecto de inmediato, pero es posible que otros cambios tarden más en completarse. Si un perfil está asociado a una plantilla de perfil de servidor, los cambios pueden hacer que el perfil deje de estar sincronizado con la plantilla. Consulte «Acerca de la validación de coherencia de los perfiles de servidor» para obtener más información.

- Los nombres de los perfiles deben ser únicos.
- Al anular la asignación de un perfil de servidor que tiene configurado almacenamiento local, se corre el riesgo de perder el contenido de la unidad lógica. Para conservar la unidad lógica, extraiga físicamente las unidades de disco o haga una copia del contenido de la unidad lógica para poder reasignar el perfil posteriormente.
- La configuración del BIOS se gestiona mediante el perfil de servidor, y la configuración del servidor se sobrescribe cuando se le aplica el perfil de servidor.
- No se puede cambiar entre identificadores virtuales y físicos para los elementos siguientes, a menos que se elimine y se vuelva a crear la conexión del perfil:
  - Número de serie/UUID
  - Dirección MAC
  - WWN

Para editar la configuración de algunos ajustes de perfil de servidor, es necesario que el hardware esté apagado; mientras que para otros, el hardware de servidor puede permanecer encendido. Puede editar los siguientes ajustes con el hardware de servidor encendido:

- Nombre del perfil
- Descripción del perfil
- Afinidad del perfil
- Ancho de banda solicitado de una conexión existente
- Red y conjunto de redes de una conexión existente, excepto cuando la conexión es de arranque

  NOTA: No se puede cambiar una conexión existente entre una red o un conjunto de redes Ethernet y una red Fibre Channel.

  Una red Fibre Channel solo se puede cambiar por otra red Fibre Channel de la misma interconexión.

- Crear, conectar y editar volúmenes de almacenamiento.

  NOTA: Si el servidor está configurado para arrancar desde la ruta de almacenamiento, dicha ruta no se puede desactivar.

- Firmware y controladores del sistema operativo mediante HPE Smart Update Tools
- Firmware únicamente mediante HPE Smart Update Tools

El perfil no puede modificarse mientras el hardware de servidor está encendido si las modificaciones anteriores no se aplicaron correctamente, a menos que el fallo se debiera únicamente al almacenamiento SAN.

13.2.3.3 Acerca del traslado de perfiles de servidor

Puede mover un perfil de servidor a otro componente de hardware de servidor si, por ejemplo, quita un componente de hardware de servidor y lo sustituye por otro similar. La operación de traslado le permite cambiar con rapidez el destino de hardware sin reconstruir el perfil de servidor completo.

Si no puede mover un perfil de servidor directamente al nuevo hardware de servidor, puede cambiarlo a `unassigned` (sin asignar). Esto le permite conservar los perfiles de servidor que actualmente no están asignados a ningún servidor.

IMPORTANTE: Si mueve un perfil de blade de servidor a otro receptáculo y el perfil está configurado para arrancar desde un dispositivo de almacenamiento Direct attach, debe actualizar manualmente la conexión de arranque del perfil para especificar el WWPN que se utiliza para el dispositivo de almacenamiento que está conectado directamente al receptáculo de destino.

Cada receptáculo se conecta a un puerto diferente del dispositivo de almacenamiento Direct attach, por lo que el WWPN para ese dispositivo de almacenamiento es distinto para cada receptáculo. Si no especifica el WWPN y el LUN correctos para el dispositivo, el servidor no arranca correctamente desde ese destino de arranque.

IMPORTANTE: Cuando se mueve un perfil de servidor a un servidor distinto y el perfil está gestionando almacenamiento local interno, se deben trasladar manualmente los discos físicos desde el servidor original al servidor nuevo para conservar los datos.

13.2.3.4 Acerca de la migración de perfiles de servidor

Es posible asignar perfiles de servidor existentes al nuevo hardware cuando se actualiza o se agrega hardware a un entorno. Por ejemplo, cuando se actualiza hardware de servidor, puede cambiar el tipo de hardware de servidor y, como consecuencia, un perfil de servidor asignado es posible que ya no coincida con la nueva configuración de hardware. En este caso, se puede editar el perfil de servidor existente para actualizar el tipo de hardware de servidor y es necesario volver a crear un perfil de servidor potencialmente complejo desde el principio.

La posibilidad de editar perfiles de servidor existentes y cambiar el tipo de hardware de servidor y el grupo de receptáculos le permite llevar a cabo tareas como:

- Agregar o quitar una tarjeta intermedia de un servidor
- Mover el hardware de servidor de un receptáculo a otro receptáculo con una configuración diferente
- Mover perfiles de servidor a servidores con adaptadores distintos, generaciones de hardware distintas y modelos de hardware distintos
- Mover cargas de trabajo a configuraciones de receptáculos o servidores distintas

En un perfil de servidor existente, haga clic en el enlace **Change** (Cambiar) situado junto a la configuración de **Server hardware type** (Tipo de hardware de servidor) o **Enclosure group** (Grupo de receptáculos) para cambiar estos valores.

Si cambia el tipo de grupo de hardware de servidor o el grupo de receptáculos, pueden verse afectados otros parámetros dentro de un perfil de servidor. Para la mayoría de los atributos siguientes, la configuración se conserva sin cambios, siempre que el tipo de hardware de servidor o el grupo de receptáculos seleccionado admita la configuración existente. Si los parámetros de configuración no son compatibles con el tipo de hardware de servidor o el grupo de receptáculos seleccionado, sus valores se eliminan. Existen las excepciones que se indican a continuación.

Afinidad	Permanece inalterada si es compatible, o se elimina (si la configuración nueva es un servidor de montaje en bastidor).
Firmware	Permanece inalterado si es compatible; si no, se elimina.
Conexiones	La mayoría de los parámetros permanecen inalterados si son compatibles, aunque los puertos se establecerán en `Auto`. Los valores de configuración no compatibles se eliminan.
Almacenamiento local	Permanece inalterado si es compatible; si no, se elimina.
Almacenamiento SAN	Los valores de configuración permanecen inalterados si son compatibles, o se eliminan las rutas de almacenamiento o todas las configuraciones de SAN (si la configuración nueva es un servidor de montaje en bastidor).

Parámetros de arranque	Los valores siempre se ajustan de acuerdo con la configuración nueva.
BIOS	Permanece inalterado si es compatible, o se elimina si el perfil se migra a un modelo de servidor diferente.

13.2.3.5 Uso de perfiles de servidor para controlar el comportamiento de eliminación y sustitución

En un perfil de servidor, el control **Affinity** (Afinidad) establece el comportamiento de eliminación y sustitución para los blades de servidor. Si aplica un perfil de servidor a un blade de servidor y posteriormente se retira este del compartimento de dispositivo, la configuración de **Affinity** (Afinidad) controla si se vuelve a aplicar el perfil de servidor cuando se introduce un blade de servidor en el compartimiento vacío. Los perfiles de servidor para los servidores de bastidor no son afines.

Valor de afinidad	Descripción
Compartimento de dispositivo	El perfil de servidor que se asigna al compartimento de dispositivo (vacío) se aplica a cualquier blade de servidor que se introduzca en el compartimento, siempre que el tipo de hardware de servidor del blade de servidor introducido coincida con el tipo de hardware de servidor especificado en el perfil de servidor. La afinidad del compartimento de dispositivo es el valor predeterminado.
Compartimento de dispositivo + hardware de servidor	El perfil de servidor asignado al compartimento del dispositivo (vacío) no se aplica si se inserta un servidor diferente en el compartimiento. El número de serie y el tipo de hardware de servidor del blade de servidor insertado deben coincidir con los valores del perfil de servidor. La afinidad entre el perfil de servidor y el hardware de servidor se establece cuando se cumple una de las condiciones siguientes: • El perfil de servidor está asignado al hardware de servidor de un compartimento de dispositivo. • El perfil de servidor está asignado a un compartimento de dispositivo vacío y posteriormente se inserta en el compartimiento un blade de servidor cuyo tipo de hardware de servidor coincide. La edición de un perfil de servidor restablece su afinidad del hardware de servidor. Si asigna el perfil de servidor a un compartimento de dispositivo ocupado, el hardware de servidor del compartimento se asocia con el perfil. Si el perfil de servidor está sin asignar o asignado a un compartimento para dispositivos vacío, se borra cualquier asociación actual.

13.2.3.6 Acerca de la asignación de un perfil de servidor a un compartimento de dispositivo vacío

Puede asignar un perfil de servidor a un compartimento vacío. El perfil de servidor se aplica automáticamente al hardware de servidor cuando el servidor que se inserta en el compartimiento cumple los criterios siguientes:

- El compartimento del receptáculo no está asignado por otro perfil de servidor (por ejemplo, no se puede asignar un perfil al compartimento 9 si se ha asignado un perfil para un tipo de hardware de servidor de altura completa al compartimento 1). Esto se comprueba cuando se asigna el perfil.
- El tipo de hardware de servidor del hardware coincide con el tipo de hardware de servidor especificado en el perfil de servidor.

Al crear el perfil de servidor, seleccione la afinidad **Device bay** (Compartimento de dispositivo) o **Device bay + server hardware** (Compartimento de dispositivo + Hardware de servidor). Si selecciona la afinidad **Device bay + server hardware** (Compartimento de dispositivo + Hardware de servidor) para un compartimento vacío, el UUID se establece cuando se inserta un tipo de hardware de servidor que coincide en el compartimento.

13.2.3.7 Acerca de las conexiones de perfiles de servidor

El número máximo de conexiones compatibles con un perfil depende de la cantidad total de puertos virtuales definidos por el tipo de hardware de servidor y el grupo de receptáculos asociado con el perfil. El número total de puertos virtuales se determina al multiplicar al número de puertos virtuales por adaptador FlexFabric por el número de adaptadores FlexFabric definido por el tipo de hardware de servidor. El número máximo de conexiones es 50, o el número total de puertos virtuales (más dos para las conexiones sin asignar), el que sea mayor.

13.2.3.8 Sobre las conexiones del perfil de servidor y el cambio de los tipos de hardware de servidor

Cuando se cambia el tipo de hardware de servidor de un perfil de servidor con conexiones implementadas, el nuevo tipo de hardware de servidor debe definir los puertos necesarios para permitir la asignación automática de puertos de todas las conexiones implementadas en ese momento. Si el nuevo tipo de hardware de servidor no tiene suficiente capacidad de puertos, la asignación automática de puertos falla cuando se aplica a un servidor y provoca el fallo de la operación de edición del perfil. Para evitar este problema, realice una de las acciones siguientes:

- Elimine conexiones para que el número restante pueda asignarse automáticamente.
- Edite las conexiones y establezca la asignación de puertos en `None` (Ninguna) para que dichas conexiones no se implementen.

13.2.3.9 Acerca de los perfiles de servidor y el almacenamiento local

Puede gestionar el almacenamiento local en el hardware de servidor con los perfiles de servidor.

- «Unidades lógicas e identificadores exclusivos»
- «Acerca de la controladora y el nivel de RAID»
- «Niveles de RAID y número de unidades físicas»
- «Sobre el almacenamiento local y las controladoras de almacenamiento integradas»

NOTA: Cuando el perfil de servidor que especifica las unidades se borra o no se asigna, HPE OneView no borra los datos de las unidades físicas. Puede que sea posible acceder a los datos, por lo que si desea asegurarse de que no se puede acceder a los datos, borre todos los datos confidenciales antes de eliminar el perfil de servidor o la configuración de almacenamiento local.

13.2.3.9.1 Unidades lógicas e identificadores exclusivos

Si configura unidades lógicas nuevas en un perfil de servidor o importa las unidades lógicas existentes del hardware de servidor, HPE OneView almacenará un identificador único para cada unidad lógica en la configuración del perfil de servidor cuando se aplique este.

Cada vez que se aplique posteriormente el perfil de servidor, HPE OneView comprobará la existencia del identificador en las unidades físicas del hardware de servidor asignado. Si no se encuentra el identificador, la operación de aplicación fallará para garantizar que si el perfil de servidor se vuelve a asignar a un nuevo hardware de servidor, las unidades físicas estén insertadas correctamente.

HPE OneView borra el identificador actual durante la operación de aplicación de un perfil de servidor si se cumple cualquiera de las condiciones siguientes:

- Se ha seleccionado **Re-initialize internal storage** (Reinicializar el almacenamiento interno).
- La **unidad lógica** se ha eliminado del perfil de servidor.
- La controladora de almacenamiento está configurada como **managed manually** (gestionada manualmente).

13.2.3.9.2 Acerca de la controladora y el nivel de RAID

Puede utilizar RAID para definir las unidades lógicas o HBA para presentar unidades directamente a la controladora. Los niveles de RAID que admite la controladora se definen en las especificaciones de cada controladora. Debe comprobar las especificaciones de cada controladora para comprobar los niveles de RAID que admite. Los niveles de RAID admitidos dependen del tipo de hardware de servidor de la configuración del servidor físico. Asegúrese de tener suficientes unidades físicas presentes para el nivel de RAID seleccionado.

NOTA: Aunque algunas controladoras admiten RAID 50 y RAID 60, HPE OneView no los admite. Para utilizar RAID 50 o RAID 60, configure el controlador como **manage manually** (gestionar manualmente) en HPE OneView.

Más información

«Niveles de RAID y número de unidades físicas»

13.2.3.9.3 Niveles de RAID y número de unidades físicas

Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener información sobre el número de unidades admitidas por el hardware de servidor específico.

RAID 0	1 unidad como mínimo, en incrementos de 1.
RAID 1	Requiere 2 unidades.
RAID 10	Requiere 4 unidades, en incrementos de 2.
RAID 1 ADM	Requiere 3 unidades.
RAID 5	3 unidades como mínimo, en incrementos de 1.
RAID 6	4 unidades como mínimo, en incrementos de 1.

13.2.3.9.4 Sobre el almacenamiento local y las controladoras de almacenamiento integradas

- HPE OneView no es consciente de la configuración de almacenamiento local existente en la controladora de almacenamiento integrada, a menos que se importe el almacenamiento local al aplicar un perfil de servidor al hardware de servidor.
- La opción de importación no es una garantía de que no se perderá ningún dato. Por ejemplo, si el servidor se encuentra en modo HBA, debe cambiarlo al modo RAID para poder importarlo, y ese cambio en el modo de controladora puede provocar la pérdida de datos.
- Una vez que se crea una unidad lógica y se aplica al hardware de servidor, dicha unidad lógica ya no se puede modificar.

Si bien al eliminar o cancelar la asignación de un perfil de servidor no se eliminan directamente los datos de almacenamiento local del hardware de servidor, los datos pueden perderse si en el futuro se aplica al hardware de servidor un perfil de servidor que contiene cambios efectuados en la configuración de almacenamiento local. En la tabla siguiente se describe cómo conservar los datos al efectuar cambios en el hardware o el perfil.

Tabla 9 Cambios en el hardware de servidor/perfil de servidor conservando los datos de almacenamiento local integrados

Cambio en el hardware de servidor	Procedimiento	Resultado
Traslado del perfil de servidor de un hardware de servidor a otro	**Traslado de unidades físicas a un hardware de servidor nuevo** 1. Cancele la asignación del perfil de servidor del hardware de servidor actual. 2. Extraiga físicamente las unidades de almacenamiento local del hardware de servidor. 3. Introduzca las unidades locales en el nuevo hardware de servidor. 4. No seleccione **Re-initialize internal storage** (Reinicializar el almacenamiento interno) cuando aplique el perfil de servidor al nuevo hardware de servidor.	• El dispositivo comprueba que las unidades físicas se han insertado correctamente validando el identificador exclusivo guardado.
Asignación de un perfil de servidor a hardware de servidor que tiene configurado el almacenamiento local	**A. Importación de unidades y datos existentes** 1. Elimine o cancele la asignación del perfil de servidor actual. 2. Seleccione **Import existing logical drives** (Importar las unidades lógicas existentes) cuando aplique el nuevo perfil de servidor.	• El identificador exclusivo se conserva. • Las unidades lógicas y los datos existentes se importan.
	B. Creación de copias de seguridad y copia de datos 1. Haga una copia de seguridad de los datos. 2. Elimine o cancele la asignación del perfil de servidor. 3. Seleccione **Re-initialize internal storage** (Reinicializar el almacenamiento interno) cuando aplique el nuevo perfil de servidor. 4. Copie los datos de la copia de seguridad en la nueva unidad lógica del hardware de servidor.	• Se crea una nueva unidad lógica con un nuevo identificador exclusivo. • Los datos de copia de seguridad se copian en la nueva unidad lógica.

13.2.3.10 Acerca de la conexión de volúmenes SAN a un perfil de servidor

Los volúmenes se asocian con los perfiles de servidor a través de conexiones de volúmenes. La conexión de un volumen a un perfil de servidor concede al hardware de servidor que está asignado al perfil de servidor acceso al espacio de almacenamiento de un sistema de almacenamiento.

En el momento de crear o editar un perfil de servidor, puede conectar un volumen existente o crear dinámicamente un nuevo volumen para conectarlo.

Los volúmenes recién creados se pueden marcar como permanentes, de manera que continúen existiendo cuando se eliminen del perfil o si se elimina el perfil. En caso contrario, un volumen no permanente se elimina cuando se elimina el perfil de servidor.

Las propiedades de conexión de un volumen pueden configurarse mediante el perfil de servidor. Por ejemplo, es posible activar y desactivar rutas de almacenamiento desde el servidor al almacenamiento SAN.

Destinos de almacenamiento

Dentro de un perfil de servidor, los puertos de destino de almacenamiento para la conexión de volúmenes se pueden asignar automáticamente; también pueden asignarse manualmente los puertos disponibles. Los puertos de destino que se asignen automáticamente pertenecerán al mismo grupo de puertos. Los puertos de destino que se asignan manualmente pueden pertenecer al mismo grupo de puertos o a otros. Los grupos de puertos se crean cuando se añade un sistema de almacenamiento a HPE OneView.

La selección manual de destinos solo se admite para rutas Fabric attach, no para rutas Direct attach.

Volúmenes HPE 3PAR existentes

En los sistemas 3PAR StoreServ Storage, un VLUN *host sees* (visible para el host) solo permite ver un volumen a un host específico y un VLUN *matched set* (conjunto coincidente) solo permite ver el volumen a un host específico en un puerto específico.

Para volver a utilizar una configuración *host sees* (visible para el host) en HPE OneView al agregar un volumen 3PAR existente a un perfil, tendrá que introducir el valor exacto del LUN tal como está configurado en el array 3PAR.

En HPE OneView, utilice la opción de LUN **Manual** para agregar el valor exacto del LUN en el cuadro de diálogo **Add Volume** (Agregar volumen). Para volver a usar la conectividad de extremo a extremo para el volumen, especifique manualmente lo siguiente:

- Valor del LUN (que coincida con el LUN en el sistema de almacenamiento 3PAR)
- Puertos de destino

Asimismo, para conectar (exportar) un volumen 3PAR como *host sees* (visible para el host), todas las rutas de almacenamiento con destino a ese volumen deben activarse o desactivarse conjuntamente. Algunas rutas no se pueden activar mientras haya algunas desactivadas. Para obtener más información, descargue la *HPE 3PAR StoreServ Storage Concepts Guide* (Guía de conceptos de HPE 3PAR StoreServ Storage) desde la biblioteca de información de almacenamiento de HPE **http://www.hpe.com/info/storage/docs**.

13.2.3.11 Acerca de la validación de coherencia de los perfiles de servidor

La comprobación de coherencia consiste en validar un perfil de servidor para asegurarse de que coincide con la configuración de su plantilla de perfil de servidor correspondiente. El

dispositivo supervisa el perfil de servidor y la plantilla de perfil de servidor, los compara, y comprueba la coherencia de los puntos siguientes.

Sección del perfil	Comprobación de coherencia
General	• Server hardware type (Tipo de hardware de servidor) • Enclosure group (Grupo de receptáculos) • Affinity (Afinidad) **NOTA:** Las incoherencias en el tipo de hardware de servidor y el grupo de receptáculos deben corregirse manualmente; es decir, hay que editar el perfil y cambiar el tipo de hardware y el grupo de receptáculos para que coincidan con la plantilla.
Firmware	Si el firmware no se gestiona mediante la plantilla de perfil de un servidor, no se comprueba la coherencia de la configuración de firmware del perfil de servidor. En caso contrario, se comprueba la coherencia de los elementos siguientes. • Firmware baseline (Línea de base de firmware) • Installation method (Método de instalación) **NOTA:** El firmware instalado a la fuerza solo se compara si la línea de base de firmware es incoherente. En caso contrario, no se comprueba la coherencia del firmware instalado a la fuerza.
Conexiones	Las conexiones se comparan para detectar si hay conexiones adicionales o si faltan. Para las conexiones similares, se comprueban las diferencias de los atributos siguientes. • Port (Puerto) • Network (Red) • Requested bandwidth (Ancho de banda solicitado) • Connection boot settings (Configuración de arranque de la conexión) **NOTA:** Las conexiones adicionales del perfil de servidor cuya identificación de puerto sea `None` (Ninguna) no se consideran incoherentes.
Local Storage (Almacenamiento local)	Si el almacenamiento local no se gestiona mediante la plantilla de perfil de servidor, no se comprueba la coherencia de la configuración de almacenamiento local del perfil de servidor. En caso contrario, se comprueba la coherencia de los elementos siguientes. • Controller model (Modelo de controladora) • Logical drives (Unidades lógicas) **NOTA:** Las incoherencias en el almacenamiento local no se solucionan automáticamente mediante **Update from Template** (Actualizar desde la plantilla). Deben corregirse manualmente.
SAN Storage (Almacenamiento SAN)	Si el almacenamiento SAN no se gestiona mediante la plantilla de perfil de servidor, no se comprueba la coherencia de la configuración de almacenamiento SAN del perfil de servidor. En caso contrario, para los volúmenes cuyo tipo de uso compartido es `private` (privado), el perfil requiere el mismo número de volúmenes privados definido en la plantilla de perfil de servidor procedentes de los mismos pools de almacenamiento, y que los números de LUN permanezcan coherentes. Las diferencias en el número de volúmenes privados, su grupo de almacenamiento o en un número de LUN se marcarán como incoherencias. Para que sigan siendo coherentes los volúmenes cuyo tipo de uso compartido es `shared` (compartido), el perfil debe conectarse a todos los volúmenes compartidos asociados a la plantilla de perfil de servidor cuyos números de LUN y rutas de almacenamiento coincidan. Se pueden conectar volúmenes compartidos adicionales sin que se produzca un estado de coherencia. Para mantener la coherencia, el tipo de sistema operativo del host designado en un perfil debe coincidir con la plantilla de perfil de servidor. **NOTA:** Los elementos conectados adicionales en el perfil de servidor no provocan incoherencias.

Sección del perfil	Comprobación de coherencia
Boot Settings (Parámetros de arranque)	Si los parámetros de arranque no se gestionan mediante la plantilla de perfil de servidor, no se comprueba la coherencia de los parámetros de arranque del perfil de servidor. En caso contrario, todas las configuraciones deben coincidir con la plantilla de perfil de servidor.
BIOS Settings (Configuración del BIOS)	Si la configuración del BIOS no se gestiona mediante la plantilla de perfil de servidor, no se comprueba la coherencia de la configuración del BIOS del perfil de servidor. En caso contrario, toda la configuración debe coincidir con la plantilla de perfil de servidor.
Advanced (Opciones avanzadas)	La opción «Hide unused FlexNICs» (Ocultar las FlexNIC que no se utilizan) debe coincidir con la plantilla de perfil de servidor.

Si las configuraciones coinciden, el campo **Consistency state** (Estado de coherencia) del perfil de servidor se establece en `Consistent` (Coherente) y se considera que existe compatibilidad.

Cualquier incoherencia da como resultado una alerta para el perfil de servidor, y el campo **Consistency state** (Estado de coherencia) se establece en `Inconsistent with template` (Incoherente con la plantilla).

13.2.4 Cuándo utilizar un perfil de servidor

Un perfil de servidor permite llevar a cabo las siguientes tareas:

- Gestionar la configuración del hardware de servidor por separado del hardware de servidor en sí.
- Volver a aplicar fácilmente la configuración al hardware de servidor si el hardware de servidor está en mantenimiento se sustituye.
- Definir la configuración del servidor antes de la instalación del hardware de servidor.
- Capturar partes importantes de la configuración del servidor en un solo lugar, lo que simplifica y acelera en gran medida la configuración del servidor.

Según el entorno de hardware, puede configurar muchos de los siguientes ajustes, o todos ellos.

- **Firmware** (opcional):
  - Especificar la versión del Service Pack para ProLiant (SPP) y el método de instalación para instalar el firmware y las controladoras mientras el servidor está encendido (las actualizaciones se aplican sobre la red de gestión).
  - Especificar la instalación del firmware sin controladoras independientemente de si el servidor está encendido o apagado (el hardware de servidor se encenderá para instalar el firmware).
  - Se admite para los servidores Gen8 y DL.
- **Configuración de BIOS** (opcional):
  - Especificar la configuración de BIOS a aplicar en el hardware de servidor seleccionado.
  - Se admite para los servidores Gen8 y DL.
- **Orden de arranque** (opcional):
  - Especificar el orden de arranque de BIOS o UEFI a aplicar en el hardware de servidor seleccionado.
  - Se admite para los servidores G7, Gen8 y DL.
- **Configuración de almacenamiento local** (opcional):
  - Configurar las unidades de disco conectadas directamente a la Smart Array integrada controladas con un nivel de RAID concreto para crear un volumen lógico.

- Configurar varios volúmenes lógicos, según el número de controladoras de disco compatibles con el hardware de servidor.
- Especificar la configuración de almacenamiento local para servidores Gen8 y DL.

- **Conexiones** (obligatorio para Virtual Connect):
  - Describir a qué redes Ethernet y SAN de Fibre Channel puede acceder el hardware de servidor.
  - Describir las opciones de configuración de arranque.
  - Virtual Connect permite virtualizar las MAC y WWN, de manera que las MAC y WWN presentadas a las redes se mantienen constantes aún cuando los componentes de hardware subyacentes cambian.
- **Conexiones de almacenamiento** (requiere Virtual Connect):
  - Describe los volúmenes de StoreServ a los que puede acceder el servidor y admite la creación de nuevos volúmenes de StoreServ, a los que se puede acceder con Fibre Channel o FCoE.
  - Describe los volúmenes de StoreServ para automatizar la presentación de los volúmenes al hardware de servidor para eliminar la necesidad de tener que configurar manualmente la división por zonas.

Más información

Matriz de compatibilidad de HPE OneView
«Cuándo utilizar una plantilla de perfil de servidor»

13.3 Gestión de plantillas de perfiles de servidor

Una plantilla de perfil de servidor sirve como referencia estructural para crear un perfil de servidor. Todos los parámetros de configuración de un perfil de servidor están presentes en la plantilla de perfil de servidor. Este tipo de plantilla define el origen centralizado para la configuración de firmware, las conexiones, el almacenamiento local, el almacenamiento SAN, el arranque, el BIOS, la afinidad del perfil, y si las FlexNIC que no se utilizan permanecen ocultas.

13.3.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de servidores

13.3.2 Tareas para las plantillas de perfiles de servidor

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Crear una plantilla de perfil de servidor.
- Copiar, editar o eliminar una plantilla de perfil de servidor.
- Actualizar la configuración del perfil partiendo de la plantilla de perfil de servidor.
- Actualizar el firmware con una plantilla de perfil de servidor.

13.3.3 Acerca de las plantillas de perfiles de servidor

Las plantillas de perfiles de servidor proporcionan un mecanismo para almacenar las configuraciones de un perfil de servidor. Por lo general, se capturan las configuraciones

recomendadas en una plantilla de perfil de servidor y, a continuación, se crean e implementan perfiles de servidor a partir de ellas.

13.3.3.1 Acerca de la creación de una plantilla de perfil de servidor

Puede crear una o varias plantillas para almacenar las configuraciones de todos los parámetros de un perfil de servidor. Cuando se crea una plantilla de perfil de servidor, se puede especificar el tipo de hardware de servidor y el grupo de receptáculos. No se puede cambiar el tipo de hardware de servidor ni el grupo de receptáculos después de crear la plantilla. Todos los perfiles generados a partir de la misma plantilla tendrán el mismo tipo de hardware de servidor y el mismo grupo de receptáculos.

Las conexiones siempre se asignan a los puertos; es decir, una plantilla de perfil de servidor guardada nunca tendrá conexiones con `Port=Auto`. No se pueden configurar conexiones con `Port=None`.

No se puede agregar un volumen privado existente. Para obtener más información sobre la creación de una plantilla de perfil de servidor, consulte los detalles de la pantalla Server Profile Template (Plantilla de perfil de servidor) en la ayuda en línea.

13.3.3.2 Acerca de la edición de una plantilla de perfil de servidor

Edite una plantilla de perfil de servidor para cambiar la configuración asociada a la plantilla. Se puede editar una plantilla de perfil de servidor en cualquier momento después de crearla. También se puede editar una plantilla de perfil de servidor que tiene una condición de `Error` para corregirla.

Cuando se edita una plantilla de perfil de servidor, el dispositivo analiza los cambios y actualiza la configuración de la plantilla. A continuación, se evalúa la coherencia de todos los perfiles de servidor creados a partir de la plantilla y se proporciona una notificación que indica el número de perfiles que se verán afectados por el cambio. Dichos perfiles se marcan como no coherentes. Puede utilizar la opción **Update from template** (Actualizar desde la plantilla) de los perfiles de servidor para aceptar todos los cambios de la plantilla.

NOTA: El hardware de servidor debe estar apagado para realizar la actualización desde una plantilla, a menos que los cambios realizados se puedan efectuar en línea, como por ejemplo, los relacionados con las redes y el ancho de banda de red.

Cuando modifique una plantilla de perfil de servidor, tenga en cuenta lo siguiente:

- Los nombres de las plantillas de perfil de servidor deben ser exclusivos.
- No se puede cambiar entre los identificadores virtuales y físicos para los siguientes elementos:
  - Número de serie/UUID
  - Dirección MAC
  - WWN

13.3.4 Cuándo utilizar una plantilla de perfil de servidor

Una plantilla de perfil de servidor permite llevar a cabo las siguientes tareas:

- Gestionar la configuración del hardware de servidor por separado del hardware de servidor en sí.
- Volver a aplicar fácilmente la configuración al hardware de servidor si el hardware de servidor está en mantenimiento se sustituye.
- Definir la configuración del servidor antes de la instalación del hardware de servidor.

- Capturar partes importantes de la configuración del servidor en un solo lugar, lo que simplifica y acelera en gran medida la configuración del servidor.

Según el entorno de hardware, puede configurar muchos de los siguientes ajustes del perfil de servidor, o todos ellos.

Las plantillas de perfiles de servidor son útiles ya que permiten:

- Gestionar varios perfiles de servidor con la misma configuración.
- Generar fácilmente nuevos perfiles de servidor a partir de la plantilla.
- Controlar los cambios en la configuración para varios servidores a la vez. HPE OneView comprueba la conformidad en todos los perfiles de servidor que hacen referencia a la plantilla.
- Resolver automáticamente los problemas de conformidad con la acción **Update from Template** (Actualización desde plantilla). La configuración del perfil de servidor se ajusta para que coincida con la plantilla de perfil de servidor.

Más información

Matriz de compatibilidad de HPE OneView

13.4 Información adicional

- «Conceptos básicos sobre el modelo de recursos» (página 45)
- «Acerca de los receptáculos» (página 236)
- «Gestión de licencias» (página 193)
- «Solución de problemas de hardware de servidor» (página 438)
- «Solución de problemas de perfiles de servidor» (página 441)

14 Gestión de licencias

Las licencias se gestionan desde la pantalla **Settings (Configuración)** o utilizando las API de REST.

14.1 Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)	`licenses`

14.2 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

14.3 Tareas para licencias

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar una clave de licencia al pool de licencias del dispositivo.
- Especificar una directiva de licencias durante la adición de un receptáculo.
- Especificar un tipo de licencia durante la adición de un servidor de montaje en bastidor.
- Ver la información de estado de las licencias a través de gráficos de licencias.
- Ver una lista del hardware de servidor al que se ha asignado un tipo de licencia determinado.

14.4 Acerca de las licencias

En este tema se describen los tipos de licencias, cómo se adquieren, cómo se entregan y cómo determinar las licencias disponibles.

- «Tipos de licencias»
- «Adquisición u obtención de licencias»
- «Entrega de licencias»
- «Formato de clave de licencia»
- «Licencias y estadísticas de utilización»
- «Escenarios de asignación de licencias»
- «Información sobre licencias»

14.4.1 Tipos de licencias

14.4.1.1 Licencias de hardware de servidor

Existen los siguientes tipos de licencias para gestionar o supervisar hardware en HPE OneView.

Licencias para hardware gestionado

Las siguientes licencias de HPE OneView Advanced tienen las características que se indican a continuación y además permiten la integración con otros productos. Para obtener más información, consulte «Integración con otro software de gestión».

`HPE OneView Advanced` — Proporciona una licencia HPE OneView Advanced y una licencia iLO Advanced.

Esta licencia se ha creado para el hardware de servidor y los receptáculos que se van a gestionar con HPE OneView. Consulte «Adquisición u obtención de licencias» para obtener más información.

`HPE OneView Advanced w/o iLO`

Proporciona exclusivamente una licencia HPE OneView Advanced.

Esta licencia se ha creado para el hardware de servidor que se va a gestionar con HPE OneView. Esta licencia es para los servidores cuyos iLO ya disponen de licencia o para hardware de servidor para el que no se requiere una licencia de iLO. Consulte «Adquisición u obtención de licencias» para obtener más información.

Una licencia HPE OneView Advanced w/o iLO permite utilizar todas las funciones del hardware de servidor del dispositivo, con las siguientes excepciones:

- El hardware de servidor que no tiene una licencia iLO Advanced no muestra los datos de utilización.
- Los servidores de montaje en bastidor que no tienen una licencia iLO Advanced no pueden acceder a la consola remota.

Si desea ver ejemplos, consulte «Escenarios de asignación de licencias».

Licencia para hardware supervisado

`HPE OneView Standard`

Proporciona una licencia HPE OneView Standard para todo el hardware de servidor supervisado.

Esta licencia se selecciona automáticamente:

- para el receptáculo cuando se añade un receptáculo supervisado
- para el servidor cuando se añade un servidor supervisado
- para todos los blades de servidor ProLiant G6 o para los blades de servidor BL680c G7 cuando se agrega un receptáculo gestionado

HPE OneView no gestiona el hardware que se ejecuta con una licencia HPE OneView Standard. Consulte «Acerca de los receptáculos c7000 supervisados» para obtener más información.

Cuando se agrega un receptáculo o un servidor de montaje en bastidor al dispositivo, se debe especificar una de estas licencias. Si desea ver ejemplos, consulte «Escenarios de asignación de licencias».

Más información

«Sobre la licencia HPE OneView Advanced para gestionar hardware de servidor»
«Sobre la licencia HPE OneView Standard para supervisar hardware de servidor»

14.4.1.2 Otras licencias

14.4.1.2.1 Licencias de interconexión

Licencia de gestión de HPE OneView B22HP FEX

La licencia de gestión de HPE OneView B22HP FEX permite seguir supervisando los entornos de los conmutadores Cisco Nexus 5k y 6k ToR cuando se conectan con interconexiones Cisco

Fabric Extender en un receptáculo. Esta licencia también permite suministrar conexiones de perfil de servidor Ethernet y FCoE a los puertos de enlace descendente de Cisco Fabric Extender y asignar VLAN.

NOTA: La licencia de gestión de HPE OneView B22HP FEX no se aplica actualmente en HPE OneView. Puede recuperar la clave y agregarla al pool de licencias de HPE OneView para hacer un seguimiento del recuento de licencias. Las licencias no se asignan automáticamente desde el pool.

Más información

«Adquisición u obtención de licencias»

14.4.1.2.2 Contrato de licencia de usuario final (CLUF)

El dispositivo incluye un CLUF (Contrato de licencia de usuario final) que debe aceptar antes de utilizarlo por primera vez. Puede ver al CLUF desde la barra lateral de ayuda.

14.4.2 Sobre la licencia HPE OneView Advanced para gestionar hardware de servidor

Este tema proporciona información sobre las licencias de hardware de servidor, incluidos los blades de servidor y los servidores de montaje en bastidor. Esta sección solo se aplica a las licencias HPE OneView Advanced y HPE OneView Advanced w/o iLO.

El dispositivo utiliza licencias basadas en los servidores, pero los blades de servidor y los servidores de montaje en bastidor se gestionan de manera diferente. Las licencias de los blades de servidor se gestionan en el ámbito del receptáculo y las licencias de los servidores de montaje en bastidor se gestionan en el ámbito del servidor. Cuando se agrega un receptáculo, se especifica una directiva de licencias para todos los blades de servidor del receptáculo. Cuando se agrega un servidor de montaje en bastidor, se especifica un tipo de licencia para ese servidor. Tanto *directiva* como *tipo* pueden referirse a cualquiera de las dos licencias: `HPE OneView Advanced` o `HPE OneView Advanced w/o iLO` (HPE OneView Advanced sin iLO).

Una licencia `HPE OneView Advanced w/o iLO` permite utilizar todas las funciones del hardware de servidor del dispositivo, con las siguientes excepciones:

- El hardware de servidor que no tiene una licencia iLO Advanced no muestra los datos de utilización.
- Los servidores de montaje en bastidor que no tienen una licencia iLO Advanced no pueden acceder a la consola remota.

NOTA: El dispositivo aplica las licencias integradas al hardware de servidor gestionado en que se encuentran.

14.4.2.1 Licencias de blades de servidor en el nivel de receptáculo

Una directiva de licencias para blades de servidor en el ámbito del receptáculo es una forma eficiente de gestionar la asignación de licencias para todos los servidores de un receptáculo.

Cuando se agrega un receptáculo al dispositivo, se debe elegir una directiva de licencias de hardware de servidor. Así se establece la directiva de licencias para todo el hardware de servidor del receptáculo. No se puede cambiar la directiva de un receptáculo a menos que se quite y se vuelva a agregar el receptáculo.

Para obtener más información acerca de cómo el dispositivo gestiona las licencias de receptáculos, consulte «Acerca de las licencias».

NOTA: Una licencia integrada en un blade de servidor gestionado anulará la directiva de licencias del receptáculo. Si se agrega un blade de servidor gestionado con una licencia integrada, el dispositivo asigna la licencia integrada a ese servidor, independientemente de la directiva de licencias del receptáculo. Se hace caso omiso de las licencias integradas en el hardware de servidor supervisado.

Comportamiento de la directiva de asignación de licencias del receptáculo

Al agregar un receptáculo gestionado al dispositivo:

- Debe elegir una directiva de asignación de licencias: `HPE OneView Advanced` o `HPE OneView Advanced w/o iLO` (HPE OneView Advanced sin iLO).
- Se añade una licencia integrada en el OA (Onboard Administrator) al pool de licencias del dispositivo.
- Si el blade de servidor no tiene una licencia integrada, el dispositivo intenta asignar una licencia del pool.
- Si no hay suficientes licencias para cumplir la directiva, se muestra una notificación que le indica cómo abordar el problema.
- Si agrega blades de servidor al receptáculo después de añadirlo al dispositivo, el hardware de servidor utilizará la directiva de licencias del receptáculo.
- No hay garantía de que una licencia de OA integrada se aplique a los blades de servidor del receptáculo que contiene la licencia integrada.
- Las licencias integradas en el iLO de un servidor se agregan al dispositivo y se aplican automáticamente al hardware de servidor en el que están integradas.
- Si el hardware de servidor tiene una licencia permanente iLO Advanced existente, el dispositivo asigna una licencia `HPE OneView Advanced w/o iLO`, independientemente del tipo de licencia que se elija.
- Para cambiar la directiva de licencias de hardware de servidor de un receptáculo, debe quitar el receptáculo de la gestión y volver a agregarlo con la nueva directiva de licencias.
- Cuando se agrega hardware de servidor al dispositivo, la licencia iLO Advanced que forma parte de la licencia `HPE OneView Advanced` se aplica al iLO del hardware de servidor.
- Si un blade de servidor no tiene una licencia de iLO y no hay un número suficiente de licencias del tipo seleccionado disponibles, el dispositivo intentará aplicar una licencia de iLO de demostración al blade de servidor.

14.4.2.2 Sobre la gestión de licencias de servidores de montaje en bastidor

La asignación de licencias de los servidores de montaje en bastidor se gestiona en el ámbito del servidor.

Cuando se agrega un servidor de montaje en bastidor al dispositivo, se debe elegir un tipo de licencia. No puede cambiar el tipo de licencia de un servidor de montaje en bastidor a menos lo quite y vuelva a agregarlo.

NOTA: Las licencias integradas tienen prioridad sobre el tipo de licencia que se elija. Si se añade un servidor de montaje en bastidor para gestionarlo con una licencia integrada, el dispositivo asigna la licencia a ese servidor de montaje en bastidor, independientemente del tipo de licencia que se elija.

El uso de la consola remota no está permitido si el servidor de montaje en bastidor no tiene una licencia de iLO.

Comportamiento de la asignación de licencias de los servidores de montaje en bastidor

Cuando se agrega un servidor de montaje en bastidor gestionado al dispositivo:

- Es necesario elegir un tipo de licencia: `HPE OneView Advanced` o `HPE OneView Advanced w/o iLO` (HPE OneView Advanced sin iLO).
- Una licencia integrada en el iLO del servidor de montaje en bastidor se agrega al dispositivo y se aplica al servidor de montaje en bastidor automáticamente.
- Si el hardware de servidor tiene una licencia permanente iLO Advanced existente, el dispositivo asigna una licencia `HPE OneView Advanced w/o iLO`, independientemente del tipo de licencia que se elija.
- Si el servidor de montaje en bastidor no tiene una licencia integrada, el dispositivo intenta asignar una licencia del pool de licencias.
- Si no hay suficientes licencias disponibles, se muestra una notificación que le indica cómo abordar el problema.
- La licencia iLO Advanced que forma parte de la licencia `HPE OneView Advanced` se aplica al iLO cuando se agrega un servidor de montaje en bastidor.
- Para cambiar el tipo de licencia de un servidor de montaje en bastidor que no tenga una licencia integrada, debe quitar de la gestión el servidor de montaje en bastidor y, a continuación, volver a agregarlo con el nuevo tipo de licencia.

14.4.3 Sobre la licencia HPE OneView Standard para supervisar hardware de servidor

La licencia HPE OneView Standard se aplica solo a los servidores y receptáculos supervisados, y no se puede aplicar a los servidores gestionados. La licencia HPE OneView Standard se aplica de forma automática al añadir hardware de servidor o receptáculos para supervisarlos.

La licencia HPE OneView Standard se aplica automáticamente cuando se agrega un receptáculo para gestionarlo que contiene blades de servidor ProLiant G6 o blades de servidor BL680c G7. Estos servidores se agregan en un estado `managed` (supervisado).

Para obtener más información, consulte «Escenarios de asignación de licencias».

14.4.4 Adquisición u obtención de licencias

La adquisición de licencias integradas en el software y el hardware en fábrica ofrece la mejor experiencia, ya que la licencia se entrega en el hardware y HPE OneView agrega automáticamente las licencias al pool de licencias cuando detecta el hardware.

Si adquiere licencias no integradas, debe activarlas y registrarlas en el portal de licencias de Hewlett Packard Enterprise en **My HPE Licensing**. Después de registrar las licencias, agregue las claves de licencia al dispositivo. Si desea ver ejemplos, consulte «Escenarios de asignación de licencias».

Más información

«Tipos de licencias»

14.4.5 Entrega de licencias

Licencias de hardware de servidor

El modo en que se entregan las licencias depende del modo en que se adquieren. Los métodos de entrega para las licencias HPE OneView Advanced y HPE OneView Advanced w/o iLO son:

- Integrada en el iLO del hardware de servidor (software adquirido integrado con el hardware)
- Integrada en el OA del receptáculo (lote de licencias incluido en el receptáculo para 16 servidores)
- Independiente, no integrada (adquirida por separado del hardware)

Más información

«Sobre la licencia HPE OneView Advanced para gestionar hardware de servidor»

14.4.6 Formato de clave de licencia

Para HPE OneView Advanced y HPE OneView Advanced w/o iLO, el formato de clave compatible es:

<*cadena de clave de cifrado*> "<*anotación*>"_<*cadena de clave de cifrado opcional*>

La cadena de clave de cifrado se prevé que sea una serie de bloques de números/caracteres separados por espacios. La anotación incluye campos separados por espacios que representa un número de pedido de ventas de Hewlett Packard Enterprise, un número de producto, una descripción del producto y un EON (número de pedido de concesión). La cadena de clave de licencia de iLO Advanced, en caso de estar presente, utiliza el formato: *xxxxx-xxxxx-xxxxx-xxxxx-xxxxx* y va precedida por un guion bajo (_). La licencia de `HPE OneView Advanced w/o iLO` no incluye la cadena de clave de licencia de iLO Advanced.

Clave de ejemplo de `HPE OneView Advanced`:

ABKE C9MA T9PY 8HX2 V7B5 HWWB Y9JL KMPL K6ND 7D5U UVQW JH2E ADU6 H78V ENXG TXBA KFVS D5GM ELX7 DK2K HKK9 DXLD QRUF YQUE BMUF AQF2 M756 9GVQ QZWD LY9B V9ZF BG2B JKTG 2VCB LK4U R4UR V886 3C9X MQT3 G3AD LVKK 5LRG E2U7 GHA3"Order1 Number2 HPE OneView_Example_License EON3"_35T9X-ZQR9V-716S8-TD48P-JLBTW

14.4.7 Licencias y estadísticas de utilización

El dispositivo recopila e informa de las estadísticas de utilización para el hardware de servidor que tiene una licencia iLO Advanced, incluidos los servidores y los receptáculos supervisados. Las estadísticas de utilización no están disponibles para el hardware de servidor que no tiene una licencia iLO Advanced.

14.4.8 Escenarios de asignación de licencias

La manera en la que el dispositivo gestiona las asignaciones de licencias depende de lo siguiente:

- Si el receptáculo o el hardware de servidor tiene una licencia integrada
- El tipo de licencia elegido al agregar el receptáculo o el hardware de servidor
- Si hay licencias disponibles en el pool de licencias del dispositivo (para el hardware de servidor que carece de una licencia integrada)

En la tabla siguiente se describe el modo en que el dispositivo gestiona la asignación de licencias para las diferentes acciones del usuario.

Tabla 10 Escenarios de asignación de licencias

Acción del usuario	Directiva o tipo de licencia	Resultado	Notas
Agregar un receptáculo gestionado con una licencia `HPE OneView Advanced` o `HPE OneView Advanced w/o iLO` integrada.	La licencia integrada tiene prioridad sobre la directiva de licencias de receptáculos que haya seleccionado.	Las licencias integradas del OA se agregan al pool del dispositivo y se aplican al hardware de servidor que no tiene licencia.	Debido a que las licencias integradas de un receptáculo se sitúan en un pool, estas licencias están disponibles para que el dispositivo se las aplique a cualquier servidor gestionado.
Agregar hardware de servidor gestionado con una licencia `HPE OneView Advanced` o `HPE OneView Advanced w/o iLO` integrada.	Las licencias integradas se aplican al hardware de servidor, independientemente del tipo de licencia que se seleccione.	Las licencias integradas se asignan al hardware de servidor en el que residen.	
Agregar hardware de servidor gestionado con una licencia iLO Advanced existente y permanente.	Se asignará al hardware de servidor una licencia `HPE OneView Advanced w/o iLO`, independientemente de la directiva o el tipo de licencia.	**Licencias `HPE OneView Advanced w/o iLO` disponibles en el pool** El dispositivo asigna una licencia al hardware de servidor. **Sin licencias `HPE OneView Advanced w/o iLO` disponibles en el pool** El dispositivo muestra una advertencia para indicar que no hay suficientes licencias para cumplir la directiva.	
Agregar hardware de servidor o un receptáculo gestionado sin una licencia integrada.	Cualquiera	**Licencias disponibles en el pool** El dispositivo asigna una licencia al hardware de servidor. **Sin licencias disponibles en el pool** El dispositivo muestra una advertencia para indicar que no hay suficientes licencias para cumplir la directiva.	Después del período de prueba de 60 días, aparece un mensaje que le avisa cuando no hay suficientes licencias para el número de instancias de hardware de servidor gestionadas.
Agregar un receptáculo gestionado con servidores ProLiant G6 o Proliant BL680 G7.	Cualquiera	A los servidores G6 se les asignará una licencia `HPE OneView Standard` y a los demás servidores la licencia `HPE OneView Advanced` o `HPE OneView Advanced w/o iLO` que se especifique.	
Agregar un receptáculo para supervisar el hardware	Se asignará una licencia `HPE OneView Standard` a todo el hardware de servidor del receptáculo.	**Licencia `HPE OneView Standard`** El dispositivo asigna automáticamente esta licencia al agregar un receptáculo para supervisar el hardware. Se hace caso omiso de las licencias integradas en el hardware de servidor supervisado.	
Quitar un receptáculo supervisado	`HPE OneView Standard`	La licencia deja de estar asignada al hardware de servidor.	

Tabla 10 Escenarios de asignación de licencias *(continuación)*

Acción del usuario	Directiva o tipo de licencia	Resultado	Notas
Quitar hardware de servidor gestionado.	`HPE OneView Advanced` (aplicada al hardware de servidor).	La licencia permanece asignada al hardware de servidor.	Si se vuelve a agregar el hardware de servidor, se le asignará la misma licencia. Si se quita hardware de servidor que tiene licencias asignadas, puede que el número de servidores con licencia que se muestran en los gráficos de licencias sea mayor que el número de servidores gestionados realmente, porque todavía se están contando las licencias asignadas al hardware de servidor.
Quitar hardware de servidor gestionado.	`HPE OneView Advanced w/o iLO` o `HPE OneView Advanced` (la licencia todavía no se ha aplicado al servidor).	La licencia deja de estar asignada al hardware de servidor.	

14.4.9 Información sobre licencias

La información básica sobre las licencias indica si el dispositivo tiene suficientes licencias para el hardware de servidor gestionadas en el entorno.

En la vista **Licenses** (Licencias) de la pantalla **Settings** (Configuración), puede ver lo siguiente:

- El número de licencias disponibles
- El número de servidores con licencia
- El número de licencias necesarias para alcanzar la conformidad (cuando todo el hardware de servidor dispone de licencia)

14.5 Información adicional

- «Solución de problemas de licencias»

15 Gestión de redes y recursos de red

En este capítulo se describe el modo de configurar y gestionar redes y recursos de red para los receptáculos y blades de servidor gestionados por el dispositivo.

NOTA: Las funciones de red que se describen en este capítulo únicamente se aplican a los receptáculos y blades de servidor. El dispositivo no supervisa ni gestiona las funciones ni el hardware de red de los servidores de montaje en bastidor ni de los equipos de red situados fuera de los receptáculos.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Networks (Redes)	`connection-templates`, `ethernet-networks`, `fc-networks` y `fcoe-networks`
Network Sets (Conjuntos de redes)	`network-sets`

15.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de red

15.2 Tareas para redes

Puede gestionar redes Fibre Channel, Ethernet y FCoE desde la pantalla **Networks** (Redes) de la interfaz de usuario o utilizando las API de REST.

15.2.1 Tareas para redes Fibre Channel

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar y eliminar una SAN Fibre Channel.
- Editar la configuración de una SAN Fibre Channel.
- Asociar una red a una SAN gestionada.

15.2.2 Tareas para redes Ethernet

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar, editar (cambiar la configuración de red) y la eliminar una red.
- Agregar una red túnel o no etiquetada.
- Agregar, editar y eliminar un conjunto de redes.

15.2.3 Tareas para redes FCoE

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar, editar (cambiar la configuración de red) y la eliminar una red.

15.3 Acerca de las redes

Las interconexiones de HPE Virtual Connect de los receptáculos admiten los siguientes tipos de redes de centros de datos:

- Fibre Channel para las redes de almacenamiento, lo que incluye tanto conexiones Fibre Channel (FC) Fabric attach (SAN) como conexiones Direct attach (Flat SAN o de conexión directa).
- Ethernet para las redes de datos, incluidas las redes etiquetadas, sin etiquetar o de túnel.
- Fibre Channel sobre Ethernet (FCoE) para redes de almacenamiento cuyo tráfico de almacenamiento se lleva a través de una VLAN Ethernet dedicada.

IMPORTANTE: Las funciones de red que se describen en esta sección únicamente se aplican a los receptáculos y servidores. El dispositivo no supervisa ni gestiona las funciones ni el hardware de red de los servidores de montaje en bastidor ni de los equipos de red situados fuera de los receptáculos.

Sobre la creación de redes

Antes de crear redes, tenga en cuenta los límites máximos de conexiones de red. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener más información.

Antes de crear una conexión en un perfil de servidor, debe:

- Crear al menos una red
- Agregar la red a un grupo de interconexiones lógicas
- Asignar a la red a las redes internas o a un conjunto de enlaces ascendentes

Puede crear las redes antes de agregar un receptáculo, lo que se denomina aprovisionamiento previo.

Sobre el aprovisionamiento de redes

Una red Ethernet se aprovisiona en una interconexión cuando la red se asocia a un conjunto de enlaces ascendentes o a las redes internas de una interconexión lógica.

Una red FC o FCoE se aprovisiona en una interconexión cuando la red se asocia a un conjunto de enlaces ascendentes de una interconexión lógica.

Para poder implementarlas en una conexión de perfil de servidor, las redes Ethernet y FCoE deben estar aprovisionadas en una interconexión lógica y ser coherentes con el grupo de interconexiones lógicas.

15.4 Acerca de los conjuntos de redes

Un conjunto de redes es una serie de redes Ethernet etiquetadas que forman un grupo al que se asigna un nombre para simplificar la creación de perfiles de servidor. Los conjuntos de redes son útiles en entornos virtuales en los que cada conexión de perfil de servidor debe tener acceso a varias redes. Utilice los conjuntos de redes en las conexiones del perfil de servidor para que todas las redes del puerto de enlace descendente de una conexión estén disponibles. Los conjuntos de redes definen cómo se entregarán los paquetes al servidor cuando la conexión Ethernet del servidor se asocie al conjunto de redes. Los conjuntos de redes también le permiten definir una red troncal VLAN y asociarla con una conexión de servidor.

En lugar de asignar una única red a una conexión en un perfil de servidor, puede asignar un conjunto de redes a esa conexión.

- Gracias al uso de los conjuntos de redes, puede implementar rápidamente cambios en el entorno de red para varios servidores. Por ejemplo, suponga que tiene 16 servidores

conectados a un conjunto de redes. Para añadir una nueva red a los 16 servidores, solo tiene que agregarla al conjunto de redes en lugar de a cada servidor por separado.

- Puede crear un conjunto de redes para sus redes de producción y uno para sus redes de desarrollo.
- Puede configurar un hipervisor con un vSwitch (conmutador virtual) para acceder a varias VLAN mediante la creación de un conjunto de redes como una red troncal que incluya dichas redes.

Requisitos de los conjuntos de redes

- Todas las redes de un conjunto de redes deben ser redes Ethernet y deben tener identificadores de VLAN externa exclusivos. Las redes túnel y no etiquetadas son redes simples, por lo que no utilizan conjuntos de redes.
- Todas las redes de un conjunto de redes deben estar configuradas en el mismo dispositivo.
- Una red puede pertenecer a varios conjuntos de redes.
- Todas las redes de un conjunto de redes deben agregarse a los conjuntos de enlaces ascendentes o las redes internas del grupo de interconexiones lógicas (y sus interconexiones lógicas) para poder utilizarlas en los perfiles de servidor con conexiones a la interconexión lógica.
- Un conjunto de redes puede estar vacío (si no contiene ninguna red) o puede contener una o varias de las redes configuradas en el grupo de interconexiones lógicas y la interconexión lógica. Los conjuntos de redes vacíos permiten crear conjuntos de redes en la configuración antes de crear las propias redes, o eliminar todas las redes de un conjunto antes de agregar sus sustitutas. Sin embargo, si a un perfil de servidor se le agrega una conexión a un conjunto de redes vacío, el servidor no puede conectarse a ninguna red del centro de datos utilizando esa conexión.

Creación, edición y eliminación de conjuntos de redes

- Cuando se crea o modifica un conjunto de redes, es posible designar una red para los paquetes sin etiquetar (red sin etiquetar). Si no se designa una red sin etiquetar, se rechazan los paquetes sin etiquetar en la conexión del perfil asociada con este conjunto de redes.
- El tráfico del servidor se debe etiquetar con el ID de VLAN de una de las redes Ethernet del conjunto de redes. El tráfico del servidor sin etiquetar se envía a la red sin etiquetar (si se ha definido una red sin etiquetar) o se rechaza (si no se ha definido una red sin etiquetar).
- La red sin etiquetar puede enviar tráfico etiquetado y sin etiquetar entre el servidor y la interconexión de forma simultánea.

  Cuando se crea o modifica un conjunto de redes, se define el ancho de banda máximo y el ancho de banda preferido para las conexiones con ese conjunto de redes. Un perfil de servidor puede anular el ancho de banda preferido, pero no el ancho de banda máximo.

- Cuando se elimina una red, se elimina automáticamente de todos los conjuntos de redes a los que pertenecía.
- Cuando se elimina un conjunto de redes, las redes que pertenecen al conjunto de redes no se ven afectadas. Sin embargo, los servidores que tienen una conexión con ese conjunto de redes sí se ven afectados debido a que sus conexiones se definen con el conjunto de redes y no con cada una de las redes. Debido a que el conjunto de redes ya no está disponible, el tráfico de red que entra y sale de ese servidor a través de esa conexión se detiene. Cuando se elimina un conjunto de redes, las conexiones de los perfiles de servidor que especificaban ese conjunto de redes se desconectan.
- Cuando se eliminan redes de un conjunto de redes, si se eliminan todas las redes en uso del conjunto de redes, todos los perfiles asignados que utilizan ese conjunto de redes están

en estado de error y las conexiones de los perfiles de servidor pierden la conectividad. Para evitar la pérdida de conectividad, deje al menos una red en el conjunto de redes o bien cancele la asociación del conjunto de redes de todos los perfiles de servidor.

15.5 Acerca de las redes Fibre Channel

Puede utilizar las redes Fibre Channel para conectar con sistemas de almacenamiento.

- «Tipos de redes Fibre Channel»
- «RedesFibre Channel Fabric attach»
- «Redes Fibre Channel Direct attach»

15.5.1 Tipos de redes Fibre Channel

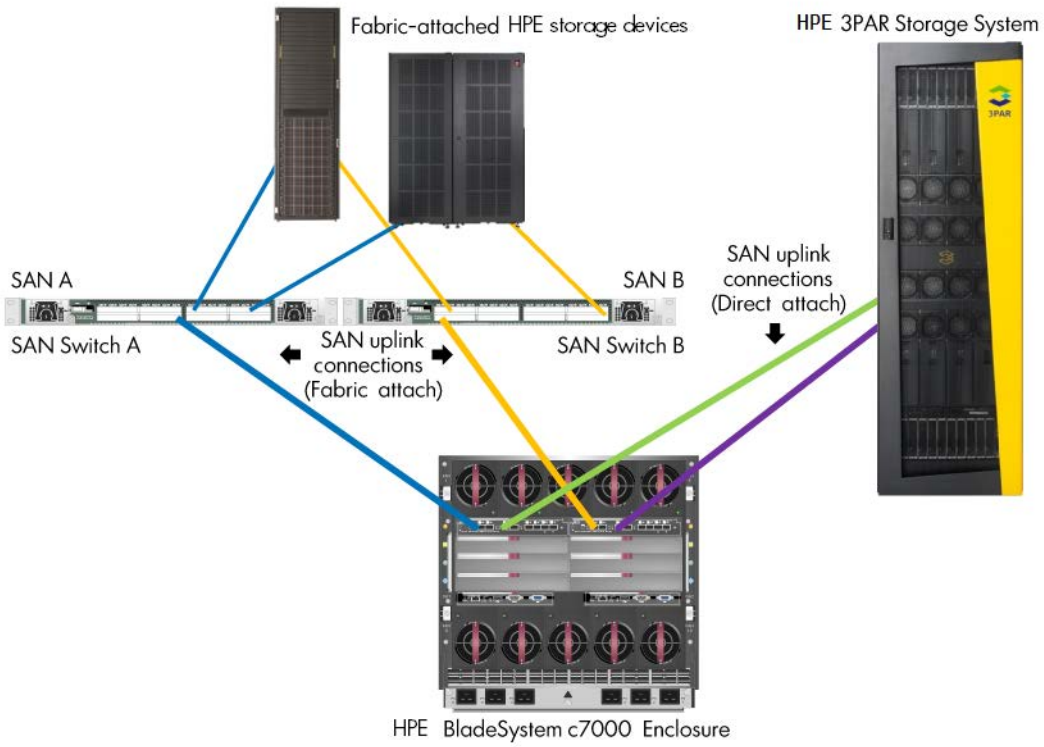
Las interconexiones de Virtual Connect en receptáculos admiten los siguientes tipos de redes Fibre Channel cuando para conectar con sistemas de almacenamiento:

- Redes Fabric attach: las interconexiones del receptáculo se conectan a los conmutadores de la estructura SAN del centro de datos.fabric attach
- Redes Direct attach: también denominadas Flat SAN, son aquellas en las que las interconexiones del receptáculo se conectan directamente a un dispositivo de almacenamiento compatible.

No se puede cambiar el tipo de una red Fibre Channel, pero se puede eliminar la red de HPE OneView y, a continuación, añadir una red de otro tipo.

Una interconexión lógica se puede definir para utilizar almacenamiento Direct attach y almacenamiento Fabric attach al mismo tiempo.

Figura 13 Redes Fibre Channel Direct attach y Fabric attach



15.5.2 RedesFibre Channel Fabric attach

Las infraestructuras SAN suelen utilizar una solución de conmutación Fibre Channel con varios conmutadores SAN que implementan la tecnología NPIV (N-Port ID Virtualization, virtualización de ID de N_port). NPIV utiliza puertos N-port y F-port para crear una estructura SAN Fibre Channel. NPIV permite que varios N_Ports se conecten a un conmutador a través de un solo F_Port, de modo que un servidor puede compartir un único puerto físico con otros servidores, pero solo accede a su almacenamiento asociado en la SAN.

Cuando configure una red Fibre Channel Fabric attach, el puerto que elija para el enlace ascendente desde la interconexión del receptáculo a la SAN de almacenamiento debe ser compatible con NPIV (virtualización de ID de N_port).

Puede utilizar módulos Virtual Connect Fibre Channel para conectar almacenamiento. El dispositivo gestiona hasta seis módulos de Virtual Connect Fibre Channel en los compartimentos de 3 a 8 de un receptáculo. No se admiten módulos Virtual Connect Fibre Channel en los compartimentos 1 y 2.

15.5.3 Redes Fibre Channel Direct attach

La solución Fibre Channel Direct attach, también llamada solución Flat SAN, elimina la necesidad de una conexión desde las interconexiones del receptáculo a un conmutador SAN Fibre Channel. Esto significa que puede conectar las interconexiones del receptáculo directamente al sistema de almacenamiento 3PAR. La solución Fibre Channel Direct attach está disponible para las soluciones de almacenamiento 3PAR que utilizan interconexiones FlexFabric.

Los servidores que se conectan a una red Fibre Channel Direct attach tienen acceso a todos los dispositivos conectados a los puertos de enlace ascendente definidos para esa red. Si hay más de una conexión desde un módulo FlexFabric al sistema de almacenamiento, cada servidor puede tener acceso a tantas rutas al LUN (número de unidad lógica) de almacenamiento como conexiones haya con el sistema de almacenamiento 3PAR.

Para las redes Fibre Channel Direct attach, la interconexión del receptáculo no distribuye los inicios de sesión de los servidores entre los puertos de enlace ascendente. La distribución de inicios de sesión de los servidores no se aplica a las redes Fibre Channel Direct attach.

IMPORTANTE: Si no se utiliza el aprovisionamiento de almacenamiento automatizado, cuando migre a un perfil de servidor tendrá que actualizar manualmente la conexión de arranque. Si mueve un perfil de servidor a otro receptáculo y el perfil está configurado para arrancar desde un dispositivo de almacenamiento Direct attach, debe actualizar manualmente la conexión de arranque del perfil para especificar el WWPN (World Wide Port Name) que se utiliza para el dispositivo de almacenamiento que está conectado directamente al receptáculo.

Cada receptáculo se conecta a un puerto diferente del sistema de almacenamiento Direct attach, por lo que el WWPN para ese sistema de almacenamiento es distinto para cada receptáculo. Si no especifica el WWPN y el LUN correctos para el sistema de almacenamiento, el servidor no arrancará correctamente desde el destino de arranque.

15.6 Acerca de las redes Ethernet

Las redes Ethernet se utilizan como redes de datos. Puede crear los tipos de redes Ethernet siguientes:

- Etiquetada
- Sin etiquetar
- Túnel

15.6.1 Acerca de las redes Ethernet etiquetadas

Una red etiquetada utiliza redes LAN virtuales (VLAN), que permiten que varias redes utilicen las mismas conexiones físicas. Al compartir enlaces ascendentes físicos, puede separar flujos de tráfico procedentes de servidores diferentes utilizando el mismo conjunto de enlaces ascendentes.

Las redes Ethernet con etiquetas conectadas a interconexiones del receptáculo requieren de un ID de VLAN.

- Puede agregar varias redes Ethernet que utilicen el mismo ID de VLAN. Esta capacidad es necesaria para interconexiones lógicas que utilizan una configuración activo/activo.
- El nombre de cada red del dispositivo debe ser único.

Redes Ethernet etiquetadas y conjuntos de redes

Puede asignar varias redes Ethernet etiquetadas a un grupo con nombre, que se denomina conjunto de redes. Más adelante, cuando agregue una conexión a un perfil de servidor, puede seleccionar este conjunto de redes para que se puedan seleccionar varias redes mediante esa única conexión. Todo cambio efectuado en un conjunto de redes se aplica a todos los perfiles de servidor que utilizan el conjunto de redes.

15.6.2 Acerca de las redes Ethernet sin etiquetar

Una red sin etiquetar es una única red dedicada sin etiqueta VLAN, que se utiliza para pasar tráfico sin etiquetas VLAN. Los paquetes etiquetados se descartan. El reenvío se realiza en base a la dirección MAC. Quizá desee configurar una red sin etiquetas para el tráfico de almacenamiento iSCSI o configurar redes sin configurar redes VLAN.

15.6.3 Acerca de las redes Ethernet de túnel

Una red de túnel es una única red dedicada con un conjunto exclusivo de puertos de enlace ascendente utilizados para pasar a un grupo de VLAN sin necesidad de cambiar las etiquetas VLAN. Puede ser conveniente utilizar redes túnel si desea expandirse más allá de las 1000 redes por interconexión lógica y 162 redes por puerto de enlace descendente actuales, o si desea controlar los recursos y QoS. Solo puede haber una red túnel con un máximo de 4094 VLAN.

15.6.4 Sobre Smart Link

Smart Link permite que el software del servidor detecte y responda ante una pérdida de conexión de red en los puertos de enlace ascendente de las interconexiones. Con **Smart Link** activado, las interconexiones de Virtual Connect dejarán caer el enlace de Ethernet en todas las conexiones del servidor asociadas con la red en caso de que todos los puertos de enlace ascendente de un conjunto de enlaces ascendentes pierdan la conexión con los conmutadores del centro de datos. Smart Link hace que el sistema operativo detecte un fallo y dirija el tráfico a una ruta alternativa.

Para que la funcionalidad Smart Link funcione según lo previsto, deben instalarse controladores y firmware de NIC válidos compatibles con DCC (Device Control Channel) en el blade de servidor.

Smart Link puede ser útil cuando se usan ciertas directivas de formación de equipos de redes de servidores. Smart Link debe estar activado para las configuraciones activa/activa, apilamiento horizontal y principal-sección.

15.7 Acerca de las redes Fibre Channel sobre Ethernet (FCoE)

Las redes FCoE son una combinación de tecnología Ethernet y Fibre Channel y se utilizan cuando el tráfico de almacenamiento se lleva a través de una VLAN Ethernet dedicada. Al igual que las redes Ethernet etiquetadas, las redes FCoE usan redes VLAN para permitir que varias

redes utilicen la misma conexión física. Consulte la ***Matriz de compatibilidad de HPE OneView*** para conocer el número de redes FCoE que se pueden asignar a una única interconexión y para una única interconexión lógica o grupo de interconexiones lógicas. Al igual que el tráfico FC, el tráfico FCoE no cruza los enlaces de apilamiento.

Las redes FCoE reducen los costes gracias a la:

- Consolidación de cables
- Reducción del número de conmutadores de la estructura SAN
- Consolidación de adaptadores e interconexiones

Requisitos de las redes FCoE

- ID de VLAN asignado, de 2 a 4094
- Conjunto de enlaces ascendentes Ethernet
- Puertos de enlace ascendente compatibles con FCoE y procedentes de un único módulo de interconexión compatible con FCoE

La compatibilidad con FCoE depende de la versión del firmware de Virtual Connect del módulo de interconexión, como se muestra en la tabla siguiente.

Versión del firmware de Virtual Connect	Funcionalidad admitida	Interconexiones admitidas
4.10	Una sola red FCoE en un conjunto de enlaces ascendentes	• Módulo Virtual Connect FlexFabric de 10 Gb y 24 puertos • Módulo Virtual Connect Flex-10/10D para HPE BladeSystem C-class
4.20 o versiones posteriores	• Hasta 32 redes FCoE en un conjunto de enlaces ascendentes • Hasta 32 redes FCoE por cada interconexión (acumulativas entre todos los conjuntos de enlaces ascendentes de la interconexión) • snooping de FIP	• Módulo Virtual Connect FlexFabric de 10 Gb y 24 puertos • Módulo Virtual Connect Flex-10/10D para HPE BladeSystem C-class • Módulo Virtual Connect FlexFabric–20/40 F8, puertos X1–X8
4.30 o versiones posteriores	• Hasta 32 redes FCoE en un conjunto de enlaces ascendentes • Hasta 32 redes FCoE por cada interconexión (acumulativas entre todos los conjuntos de enlaces ascendentes de la interconexión) • snooping de FIP	• Módulo Virtual Connect FlexFabric de 10 Gb y 24 puertos • Módulo Virtual Connect Flex-10/10D para HPE BladeSystem C-class • Módulo Virtual Connect FlexFabric–20/40 F8, puertos X1–X8 y QSFP

15.8 Requisitos de los puertos de conmutación del centro de datos

Aunque puede configurar un conjunto de enlaces ascendentes para recibir tráfico de red entrante sin etiquetar designando una red de ese conjunto de enlaces ascendentes como `Native` (Nativa), el tráfico saliente del conjunto de enlaces ascendentes siempre contiene etiquetas VLAN (excepto para los conjuntos de enlaces ascendentes sin etiquetar).

Los puertos de conmutación de los conmutadores de red del centro de datos que se conectan a las interconexiones de Virtual Connect se deben configurar de la manera siguiente:

- Bordes del árbol de expansión (debido a que las interconexiones de Virtual Connect aparecen ante el conmutador como dispositivos de acceso en lugar de conmutadores).
- Puertos troncales de VLAN (etiquetado) para admitir los ID de VLAN incluidos en el conjunto de enlaces ascendentes que se conecta al puerto del conmutador.

  Por ejemplo, si configura un conjunto de enlaces ascendentes, `prodUS`, que incluye las redes de producción de `prod 1101` a `prod 1104` para que utilicen los puertos X2 de las interconexiones del compartimento 1 y el compartimento 2 del receptáculo 1, los puertos de conmutación del centro de datos que se conectan a dichos puertos X2 deben configurarse para que admitan los ID de VLAN 1101, 1102, 1103 y 1104.
- Si varios enlaces ascendentes de un conjunto de enlaces ascendentes conectan la misma interconexión lógica al mismo conmutador del centro de datos, debe configurar los puertos de conmutación del centro de datos para LACP (Link Aggregation Control Protocol) en el mismo LAG (Link Aggregation Group) para garantizar que todos los enlaces ascendentes del conjunto de enlaces estén activados.

  Defina la frecuencia de los mensajes de control: corta — cada segundo con un tiempo de espera de 3 segundos; o larga — cada 30 segundos con un tiempo de espera de 90 segundos.

También tenga en cuenta el tipo de tráfico de red y si va a crear una configuración activo/en espera o activo/activo.

15.9 Información adicional

- «Conceptos básicos sobre el modelo de recursos» (página 45)
- «Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas» (página 209)
- «Solución de problemas de redes» (página 437)

16 Gestión de interconexiones, interconexiones lógicas y grupos de interconexiones lógicas

Un grupo de interconexiones lógicas actúa como una fórmula para la creación de una interconexión lógica que representa las redes, los conjuntos de enlaces ascendentes, los enlaces de apilamiento y la configuración de interconexión disponibles de un conjunto de interconexiones físicas en un solo receptáculo.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Interconnects (Interconexiones)	`interconexiones`
Logical Interconnects (Interconexiones lógicas)	`logical-interconnects`
Logical Interconnect Groups (Grupos de interconexiones lógicas)	`logical-interconnect-groups`

16.1 Gestión del hardware de interconexión del receptáculo

Cuando se agrega un receptáculo, también se añaden las interconexiones del receptáculo al dominio de gestión, y permanecerán en el dominio mientras el receptáculo forme parte del dominio. Puede gestionar el hardware de interconexión del receptáculo desde la pantalla **Interconnects** (Interconexiones) de la interfaz de usuario o utilizando las API de REST.

16.1.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de red

16.1.2 Tareas para interconexiones

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Añadir o extraer una interconexión física.
- Borrar los contadores de puertos.
- Activar o desactivar puertos de enlace ascendente o puertos de enlace descendente.
- Volver a aplicar una configuración de interconexión.
- Restablecer la protección contra bucles y desbordamiento de pausa.
- Ver las estadísticas de transferencia de datos para los puertos de enlace ascendente y enlace descendente.

16.1.3 Acerca de las interconexiones

Las interconexiones permiten la comunicación entre el hardware de servidor existente en el receptáculo y las redes del centro de datos.

16.1.3.1 Acerca de las interconexiones gestionadas y supervisadas

Las interconexiones se agregan automáticamente cuando se agrega el receptáculo que las contiene al dispositivo.

Gestionadas
: HPE OneView gestiona las interconexiones; lo que permite aplicar configuraciones, recopilar estadísticas y alertar a los usuarios cuando se den determinadas situaciones.

Supervisadas HPE OneView supervisa el hardware únicamente a efectos de inventario y de estado del hardware. Las interconexiones supervisadas no están asociadas con líneas de base de firmware ni con interconexiones lógicas.

De forma predeterminada, el firmware de las interconexiones recién agregadas está sin establecer.

Interconexiones gestionadas

Las interconexiones gestionadas son una parte integrante de un receptáculo, y cada interconexión gestionada pertenece a una interconexión lógica. Cada interconexión lógica está asociada a un grupo de interconexiones lógicas, que a su vez está asociado a un grupo de receptáculos. Para obtener más información sobre las interconexiones lógicas, consulte «Acerca de las interconexiones lógicas» (página 212). Para obtener información sobre la relación que tienen los receptáculos y los grupos de receptáculos con las interconexiones, las interconexiones lógicas y los grupos de interconexiones lógicas, consulte .

Puede actualizar el firmware de las interconexiones gestionadas utilizando un SPP (Service Pack para ProLiant).

16.1.3.2 Acerca de las interconexiones no gestionadas y no compatibles

Interconexiones no gestionadas

Si asigna un grupo de receptáculos (que incluye un grupo de interconexiones lógicas) a un receptáculo que tiene instaladas interconexiones que no coinciden con las del grupo de interconexiones lógicas, el estado de cada interconexión aparece como `unmanaged`. Para poder gestionar una interconexión, la configuración de interconexiones físicas del receptáculo debe coincidir con el grupo de interconexiones lógicas.

Interconexiones no compatibles

El hardware no compatible es el que el dispositivo no puede gestionar.

Para el c7000, si el dispositivo detecta una interconexión que no espera (no está definida en el grupo de interconexiones lógicas) o que no puede gestionar, la coloca en un estado de `inventory` (inventario) y crea un recurso para ella, pero no la incluye en la gestión. Si la ubicación corresponde a la definición del grupo de interconexiones lógicas, asigna a la interconexión un estado `critical` (crítico) y muestra una alerta recomendando la sustitución de la interconexión por un modelo que pueda gestionar. El dispositivo muestra el nombre del modelo de la interconexión no compatible que obtiene del OA (Onboard Administrator).

16.1.3.3 snooping de FIP

Fibre Channel sobre Ethernet (FCoE) se utiliza para transportar datos de almacenamiento de Fibre Channel (FC) por un cable Ethernet dedicado. El protocolo de inicialización de FCoE (FIP) gestiona el proceso de detección e inicio de sesión de FC para las redes FCoE. FIP utiliza un Fibre Channel Forwarder (FCF), que es un conmutador Ethernet capaz de gestionar tráfico FCoE. Un FCF es como un conmutador Fibre Channel con puertos Ethernet.

FIP proporciona una dirección MAC Ethernet que FCoE utiliza para pasar por la red Ethernet. FIP obtiene el ID de Fibre Channel (FC ID) de la red Ethernet, que es necesario en la red Fibre Channel.

El snooping de FIP proporciona datos estadísticos que se pueden utilizar para supervisar, verificar o solucionar problemas de conectividad.

Para obtener una lista de las interconexiones compatibles con el snooping de FIP, consulte la matriz de compatibilidad adecuada en la **Biblioteca de información de Hewlett Packard Enterprise**.

Más información

“*Información adicional sobre el puerto de enlace ascendente*” en la ayuda en línea.

"*Información adicional sobre el puerto de enlace descendente*" en la ayuda en línea

16.1.3.4 Conectividad y sincronización con el dispositivo

El dispositivo analiza el estado de las interconexiones y emite alertas cuando hay un cambio en el estado de una interconexión o un puerto. El dispositivo mantiene la configuración que se especifica en las interconexiones que gestiona.

El dispositivo también realiza un seguimiento el estado de conectividad de las interconexiones. Si el dispositivo pierde la conectividad con una interconexión, se muestra una alerta hasta que se restablece la conectividad. El dispositivo intenta resolver los problemas de conectividad y desactivar la alerta. Si no puede, será necesario resolver los problemas y actualizar manualmente la interconexión para sincronizarla con el dispositivo.

Puede actualizar manualmente la conexión entre el dispositivo y una interconexión desde la pantalla **Interconnects** (Interconexiones). Consulte la ayuda en línea de la pantalla **Interconnects** (Interconexiones) para obtener más información.

16.1.4 Información adicional

- «Interconexiones»
- «Funciones de red»
- «Solución de problemas de las interconexiones»

16.2 Gestión de interconexiones lógicas y grupos de interconexiones lógicas

Una interconexión lógica representa las redes, los conjuntos de enlaces ascendentes y los enlaces de apilamiento disponibles para un conjunto de interconexiones físicas en un único receptáculo. La pantalla **Logical Interconnects** (Interconexiones lógicas) proporciona una vista gráfica de la configuración de las interconexiones lógicas de un receptáculo. Utilice esta pantalla o las API de REST para gestionar los conjuntos de enlaces ascendentes de la interconexión lógica.

Cuando se agrega un receptáculo, se crea una interconexión lógica automáticamente. El grupo de interconexiones lógicas sirve como plantilla para garantizar que todas sus interconexiones lógicas tienen la misma configuración.

16.2.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de red

16.2.2 Tareas para interconexiones lógicas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Añadir, editar o eliminar un conjunto de enlaces ascendentes.
- Cambiar valores de la configuración de Ethernet tales como:
  - Conmutación por error rápida de memoria caché MAC.
  - Intervalos de actualización MAC.
  - Intervalo tiempo de espera de inactividad y snooping de IGMP (Internet Group Management Protocol).
  - Protección contra bucles.

    - Protección contra desbordamientos de pausa.
    - Activación o desactivación del etiquetado Link Layer Discovery Protocol (LLDP)
    - Activación o desactivación de la configuración mejorada tipo-longitud-valor (TLV)
- Configurar un puerto para supervisar el tráfico de red.
- Editar las redes internas
- Activar y desactivar puertos físicos.
- Actualizar el firmware de las interconexiones a través de las interconexiones lógicas.
- Gestionar el acceso SNMP (Simple Network Management Protocol) y los destinos de captura.
- Gestionar la frecuencia de los mensajes de control a través del temporizador LACP.
- Volver a aplicar la configuración de la interconexión lógica a sus interconexiones físicas.
- Redistribuir los inicios de sesión para conmutación por error de enlace ascendente en una red Fibre Channel.
- Actualizar la configuración de la interconexión lógica a partir del grupo de interconexiones lógicas.
- Ver y descargar la tabla de direcciones MAC.
- Definición de la configuración de Quality of Service (QoS) para la interconexión lógica

16.2.3 Tareas para los grupos de interconexiones lógicas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Crear un grupo de interconexiones lógicas
- Editar un grupo de interconexiones lógicas
- Eliminar un grupo de interconexiones lógicas
- Cómo copiar un grupo de interconexiones lógicas
- Activación o desactivación del etiquetado Link Layer Discovery Protocol (LLDP)
- Activación o desactivación de la configuración mejorada tipo-longitud-valor (TLV)
- Definición de la configuración de Quality of Service (QoS) a aplicar a la interconexión lógica

16.2.4 Acerca de las interconexiones lógicas

Una interconexión lógica es una sola entidad administrativa que consta de la configuración de un conjunto de interconexiones de un solo receptáculo e incluye:

- Los conjuntos de enlaces ascendentes, que conectan a las redes del centro de datos.
- La asignación de redes a los puertos de enlace ascendente físicos, que se define mediante los conjuntos de enlaces ascendentes para una interconexión lógica.
- Las redes internas, que se utilizan para las comunicaciones de servidor a servidor sin tráfico saliente por los enlaces ascendentes.
- Los puertos de enlace descendente, que se conectan con los servidores del receptáculo a través del plano medio del receptáculo.
- Las conexiones entre las interconexiones, que se denominan enlaces de apilamiento. Los enlaces de apilamiento pueden ser cables internos (a través del receptáculo) o cables externos entre los puertos externos de las interconexiones.

Consulte la matriz de compatibilidad adecuada en la **Biblioteca de información de Hewlett Packard Enterprise** para conocer el número máximo de redes que se pueden aprovisionar en una interconexión lógica.

Para un administrador de servidores, una interconexión lógica representa las redes disponibles a través de los enlaces ascendentes de la interconexión y las capacidades de enlace descendente de la interconexión a través de las interfaces de un servidor físico. Para un administrador de redes, una interconexión lógica representa una configuración de apilamiento Ethernet, conectividad de la capa de agregación, topología de apilamiento, accesibilidad de redes, estadísticas y herramientas de solución de problemas.

16.2.4.1 Acerca de los conjuntos de enlaces ascendentes

Un conjunto de enlaces ascendentes define una red única dedicada o un grupo de redes y puertos físicos de un conjunto de interconexiones de un receptáculo. Un conjunto de enlaces ascendentes permite conectar las interconexiones a las redes del centro de datos. Un conjunto de enlaces ascendentes permite que varios puertos admitan la agregación de puertos (múltiples puertos conectados a una única interconexión externa) y la conmutación por error de enlaces con un conjunto coherente de redes VLAN.

- Para redes Ethernet etiquetadas, un conjunto de enlaces ascendentes le permite identificar los enlaces ascendentes de interconexión que llevan varias redes por el mismo cable.
- Para no etiquetadas o redes Ethernet túnel, un conjunto de enlaces ascendentes identifica los enlaces ascendentes dedicados a una única red de interconexión.
- Para las redes Fibre Channel, se puede agregar una red a un conjunto de enlaces ascendentes. Fibre Channel no permite tener las redes virtuales o VLAN.
- Para las redes Fibre Channel sobre Ethernet (FCoE), un conjunto de enlaces ascendentes permite transportar varias redes Ethernet etiquetadas y Fibre Channel por el mismo conjunto de cables Ethernet.
- Se permite un conjunto de enlaces ascendentes por módulo de Cisco FEX.

Un conjunto de enlaces ascendentes forma parte de una interconexión lógica. La configuración inicial de los conjuntos de enlaces ascendentes de una interconexión lógica está determinada por la configuración de los conjuntos de enlaces ascendentes del grupo de interconexiones lógicas, pero se pueden cambiar (anular) los conjuntos de enlaces ascendentes para una interconexión lógica determinada.

Los cambios que realice en los conjuntos de enlaces ascendentes de un grupo de interconexiones lógicas no se propagan automáticamente a las interconexiones lógicas existentes. Por ejemplo, para propagar una VLAN recién añadida a un conjunto de enlaces ascendentes de grupos de interconexiones lógicas, debe actualizar por separado cada configuración de interconexión lógica a partir de un grupo de interconexiones lógicas.

Para cada interconexión lógica:

- Puede definir cero o más conjuntos de enlaces ascendentes. Consulte los límites de conexión de red en la ***Matriz de compatibilidad de HPE OneView*** para conocer el número máximo de conjuntos de enlaces ascendentes y el número máximo de tipos de red admitidos en un conjunto de enlaces ascendentes.

  Si no define ningún conjunto de enlaces ascendentes, los servidores del receptáculo no se podrán conectar a las redes del centro de datos.

- Una red solo puede pertenecer a un conjunto de enlaces ascendentes por cada grupo de interconexiones lógicas.
- Un conjunto de enlaces ascendentes con redes Fibre Channel o FCoE solo puede utilizar los enlaces ascendentes de una única interconexión.

- Un conjunto de enlaces ascendentes puede contener una o varias redes Ethernet etiquetadas. Un conjunto de enlaces ascendentes para una red no etiquetada o túnel solo puede contener dicha red.
- Un conjunto de enlaces ascendentes puede contener una o varias redes FCoE, pero los enlaces ascendentes deben estar dentro de una sola interconexión compatible con FCoE.

  Consulte los requisitos de firmware en «Acerca de las redes Fibre Channel sobre Ethernet (FCoE)».
- Dentro de un grupo de interconexiones lógicas o una interconexión lógica, todos los ID de VLAN debe ser exclusivos en todos los conjuntos de enlaces ascendentes y las redes internas.
- Las redes internas permiten la conectividad entre servidores dentro de la interconexión lógica. Las redes internas se crean agregando redes existentes al conjunto de redes internas. Las redes internas pueden agregarse a conjuntos de enlaces ascendentes, lo que las elimina automáticamente del conjunto de redes internas.

  Los módulos de Cisco FEX no admiten redes internas.
- Las redes Ethernet de un conjunto de enlaces ascendentes deben especificarse individualmente y no mediante la selección de un conjunto de redes. El uso de conjuntos de redes en los conjuntos de enlaces ascendentes no se admite por las siguientes razones:
  - La configuración de red se ha creado para que la gestionen los usuarios que tienen el rol de administrador de redes. Debido a que los usuarios que tienen el rol de administrador de redes, pueden crear y editar conjuntos de redes, si se permitiera que los conjuntos de redes fueran miembros de los conjuntos de enlaces ascendentes, podrían ocurrir que los administradores de servidores cambiaran la asignación de redes a los puertos de enlace ascendente sin que lo supiera el administrador de la red.
  - Debido a que una red puede pertenecer a más de un conjunto de redes, si se permitiera que los conjuntos de redes fueran miembros de los conjuntos de enlaces ascendentes, resultaría más difícil garantizar que no hay ninguna red que pertenezca a más de un conjunto de enlaces ascendentes, sobre todo porque las configuraciones de los conjuntos de redes cambian con el tiempo.

16.2.4.2 Acerca de las redes internas

Una red interna es una red que no tiene puertos de enlace ascendente y se utiliza para las comunicaciones entre servidores dentro de una interconexión lógica. Los servidores que se comunican entre sí a través de redes internas lo hacen sin que el tráfico salga por los enlaces ascendentes.

Solo las redes Ethernet etiquetadas, sin etiquetar y de túnel pueden pertenecer a las redes internas.

Si se requiere conectividad de red fuera del receptáculo lógico, la red debe estar en un conjunto de enlaces ascendentes asociado con un enlace ascendente.

NOTA: Una red no está disponible para las conexiones del perfil hasta que se agrega a un conjunto de enlaces ascendentes o de redes internas de un grupo de interconexiones lógicas y a la interconexión lógica asociada.

Adición y eliminación de redes internas

Cada grupo de interconexiones lógicas e interconexión lógica tiene una lista de redes internas que está vacía inicialmente. La adición de una red a la lista de redes internas, tanto en el grupo de interconexiones lógicas como en la interconexión lógica, permite utilizarla en las conexiones

de perfiles de servidor que pueden asignarse a los enlaces descendentes de las interconexiones que pertenecen a la interconexión lógica.

IMPORTANTE: La existencia de redes duplicadas en la lista de redes internas de más de una interconexión lógica puede impedir que se comuniquen los servidores del receptáculo. Por lo tanto, se recomienda definir todas las redes internas en una interconexión lógica del receptáculo.

Puede agregar o quitar redes internas desde la pantalla **Logical Interconnects** (Interconexiones lógicas) o **Logical Interconnect Groups** (Grupos de interconexiones lógicas). Las interconexiones lógicas asociadas heredan la configuración de redes internas creada en el grupo de interconexiones lógicas. Una interconexión lógica puede hacerse coherente con el grupo de interconexiones lógicas principal seleccionando **Actions→Update from group** (Acciones > Actualizar desde el grupo).

Las redes de la lista de redes internas aparecen como redes disponibles para los conjuntos de enlaces ascendentes. Se eliminan automáticamente de la lista de redes internas si se agregan a un conjunto de enlaces ascendentes.

Si se quita una red Ethernet de un conjunto de enlaces ascendentes de una interconexión lógica, automáticamente pasa a formar parte de las redes internas con objeto de que no se pierda la conectividad de red para las conexiones de perfiles de servidor que utilizan la red. Sin embargo, si se quita una red Ethernet de un conjunto de enlaces ascendentes de un grupo de interconexiones lógicas, la red no pasa automáticamente a formar parte de las redes internas. Si desea que la red sea interna, edite el grupo de interconexiones lógicas y agregue la red a las redes internas.

16.2.4.3 Acerca de los enlaces de apilamiento y estado de apilamiento

Enlaces de apilamiento

Los enlaces de apilamiento solo se aplican a las redes Ethernet. Puede conectar todas las interconexiones entre sí a través de los enlaces de apilamiento para que el tráfico Ethernet desde un servidor conectado a una interconexión de enlace descendente pueda llegar a las redes del centro de datos a través de dicha interconexión o a través de un enlace de apilamiento desde dicha interconexión a otra interconexión. Al agregar receptáculos, cree un solo grupo de interconexiones lógicas con una sola interconexión lógica que contenga todas las interconexiones del receptáculo. Esto crea un receptáculo totalmente apilado.

Para configurar un receptáculo no apilado, configure varios grupos de interconexiones lógicas donde cada interconexión esté en un grupo de interconexiones lógicas independiente (y posteriormente separe las interconexiones lógicas) antes de agregar el receptáculo. También puede configurar un receptáculo parcialmente apilado en el que haya más de una interconexión en un grupo de interconexiones lógicas. Consulte «Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos» para obtener más información.

Estado de apilamiento

El dispositivo detecta la topología dentro de un receptáculo de las conexiones entre las interconexiones, y determina la redundancia de las rutas entre los servidores y las redes del centro de datos. El dispositivo proporciona la información sobre redundancia indicando el estado de apilamiento de la interconexión lógica, que es uno de los siguientes:

`Redundantly Connected (Conexión redundante)`	Hay al menos dos rutas independientes entre cualquier par de interconexiones de la interconexión lógica, y hay al menos dos rutas independientes desde cualquier puerto de enlace descendente de cualquier interconexión de la interconexión lógica hasta cualquier otro puerto (de enlace ascendente o enlace descendente) de la interconexión lógica.

`Connected (Conectado)`	Hay una sola ruta entre cualquier par de interconexiones de la interconexión lógica y hay una sola ruta desde cualquier puerto de enlace descendente de cualquier interconexión de la interconexión lógica hasta cualquier otro puerto (de enlace ascendente o enlace descendente) de la interconexión lógica.
`Disconnected (Desconectado)`	Hay al menos una interconexión que no está conectada con las demás interconexiones que pertenecen a la interconexión lógica.
`Not applicable (No aplicable)`	Las interconexiones no admiten el apilamiento o solo hay una interconexión en la interconexión lógica.

16.2.4.4 Creación o eliminación de una interconexión lógica

Creación de una interconexión lógica en un receptáculo

Se agrega una interconexión lógica automáticamente cuando se agrega el receptáculo. Cuando se agrega un receptáculo c7000, ocurre lo siguiente:

- Se crea un receptáculo lógico basado en el grupo de receptáculos definido.
- El dispositivo detecta las interconexiones físicas y sus enlaces de apilamiento, si los hay.
- El dispositivo crea automáticamente una sola interconexión lógica para cada grupo de interconexiones lógicas definido en el grupo de receptáculos.

  NOTA: El número de interconexiones lógicas que se crean depende de cómo se definió el grupo de receptáculos. Consulte Edit a logical interconnect group (Edición de un grupo de interconexiones lógicas) en la ayuda en línea.

- El dispositivo asigna nombres automáticamente a las interconexiones lógicas mediante la convención de nomenclatura siguiente:

  nombre_de_interconexión_lógica-nombre_del_grupo_de_interconexiones_lógicas

- Los datos de las interconexiones lógicas se muestran en la pantalla **Logical Interconnects** (Interconexiones lógicas).

Para obtener más información sobre cómo agregar o modificar interconexiones lógicas, consulte Edit a logical interconnect group (Editar un grupo de interconexiones lógicas) en la ayuda en línea.

Eliminación de una interconexión lógica

Para eliminar una interconexión lógica, deberá quitar el grupo de interconexiones lógicas del grupo de receptáculos de interconexión y, a continuación, llevar a cabo una actualización desde el grupo en el receptáculo lógico. Así se elimina la interconexión lógica del receptáculo lógico.

16.2.5 Acerca de los grupos de interconexiones lógicas

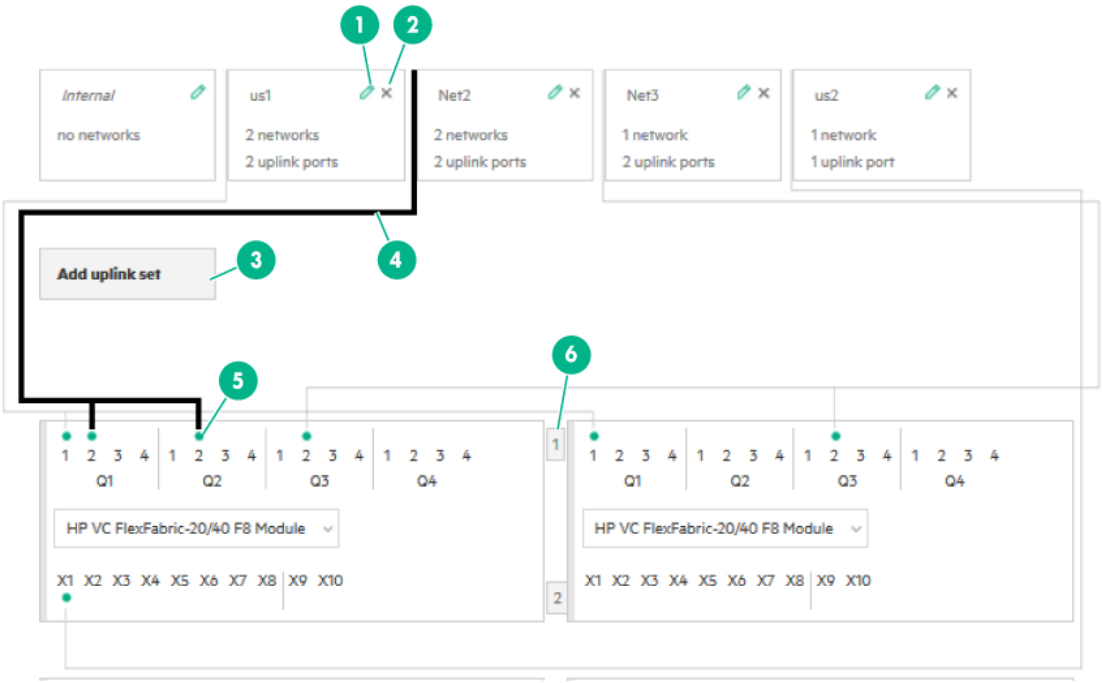
- «Sobre la interfaz gráfica del grupo de interconexiones lógicas»
- «Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos»
- «Sobre la copia de un grupo de interconexiones lógicas»
- «Acerca de los conjuntos de enlaces ascendentes de un grupo de interconexiones lógicas»
- «Sobre el etiquetado Link Layer Discovery Protocol (LLDP)»
- «Sobre la estructura tipo-longitud-valor (TLV) mejorada»

A cada grupo de receptáculos pueden asociarse uno o varios grupos de interconexiones lógicas que se utilizan para definir la configuración de interconexiones lógicas de cada receptáculo que utiliza ese grupo de receptáculos. Las configuraciones de los grupos de interconexiones lógicas incluyen la ocupación de los compartimentos de E/S, los conjuntos de enlaces ascendentes, las redes disponibles basadas en los conjuntos de enlaces ascendentes y las redes internas, y los enlaces descendentes.

Todas las referencias a un grupo de interconexiones lógicas mediante un grupo de receptáculos o interconexión lógica deben eliminarse antes de eliminar el grupo de interconexiones lógicas.

16.2.5.1 Sobre la interfaz gráfica del grupo de interconexiones lógicas

Figura 14 Topografía de la pantalla del grupo de interconexiones lógicas



1. **Icono de edición**: haga clic para editar el objeto asociado, como un conjunto de enlaces ascendentes o redes internas, para cambios en la configuración.
2. **Icono de borrado**: haga clic para eliminar el objeto asociado, como un conjunto de enlaces ascendentes, de la configuración.
3. **Agregar conjunto de enlaces ascendentes**: haga clic para agregar un conjunto de enlaces ascendentes adicional al grupo de interconexiones lógicas.
4. **Conexiones del conjunto de enlaces ascendentes**: ofrece una representación gráfica de la configuración del conjunto de enlaces ascendentes con los puertos de enlaces ascendentes y redes asociadas. Al pasar el ratón por encima del conjunto de enlaces ascendentes o los puertos de enlaces ascendentes se resaltan las
5. **Puerto de enlace ascendente**: el puerto de enlace ascendente asignado y su estado. Al pasar el ratón por encima del puerto se muestra información adicional sobre el mismo.
6. **Número de compartimento del receptáculo**: identifica el compartimento de interconexiones del receptáculo.

conexiones de la configuración.

16.2.5.2 Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos

Es posible asociar varios grupos de interconexiones lógicas con un grupo de receptáculos.

Las ventajas de utilizar varios grupos de interconexiones lógicas en un grupo de receptáculos son:

- Disponer de una separación de "cámara de aire" entre las redes Ethernet para aislar el tráfico de red
- Eliminar la necesidad de cables de apilamiento entre las interconexiones, lo que libera puertos de enlace ascendente para el tráfico con el centro de datos
- Duplicar el número de redes en una configuración activo/activo. Consulte «Acerca de las configuraciones activo/activo y activo/en espera» para obtener más información.

Requisitos de los grupos de interconexiones lógicas

- Las interconexiones situadas en compartimentos adyacentes horizontalmente deben contener el mismo tipo de interconexión o un compartimiento vacío

16.2.5.2.1 Cuándo se crea un grupo de interconexiones lógicas

De forma predeterminada, al agregar un receptáculo se crea automáticamente un solo grupo de interconexiones lógicas que contiene todas las interconexiones del receptáculo, a no ser que se creen los grupos de interconexiones lógicas antes de agregar el receptáculo. Si desea tener varias interconexiones lógicas en un receptáculo:

- Cree grupos de interconexiones lógicas con las interconexiones que desee en cada interconexión lógica.
- Agregue los grupos de interconexiones lógicas a un grupo de receptáculos
- Agregue el receptáculo mediante el grupo de receptáculos.

16.2.5.3 Sobre la copia de un grupo de interconexiones lógicas

Para optimizar la creación de grupos de interconexiones lógicas, puede copiar los grupos de interconexiones lógicas existentes.

Al copiar un grupo de interconexiones lógicas, todos los ajustes, conjuntos de enlaces ascendentes y redes se copian al nuevo grupo. El nuevo grupo no se asocia automáticamente con grupos de receptáculos ni interconexiones lógicas. Tras copiar un grupo de interconexiones lógicas, puede editar el grupo de interconexiones lógicas o asociarlo con un grupo de receptáculos.

Por ejemplo, si tiene un grupo de interconexiones lógicas existente y quiere un nuevo grupo con la misma configuración, pero con una red interna diferente. Copie el grupo de interconexiones lógicas existente y, a continuación, edite el nuevo grupo de interconexiones lógicas para cambiar la red interna.

Más información

“”Copy a logical interconnect group” (Copia de un grupo de interconexiones lógicas) en la ayuda en línea

16.2.5.4 Acerca de los conjuntos de enlaces ascendentes de un grupo de interconexiones lógicas

La parte de los conjuntos de enlaces ascendentes del grupo de interconexiones lógicas define la configuración inicial de los conjuntos de enlaces ascendentes de cada interconexión lógica del grupo de receptáculos. Si cambia los conjuntos de enlaces ascendentes de un grupo de

interconexiones lógicas existente, solo se configurarán con la nueva configuración del conjunto de enlaces ascendentes los receptáculos que agregue después del cambio de configuración. Si se modifican los conjuntos de enlaces ascendentes de un grupo de interconexiones lógicas, el receptáculo lógico y las interconexiones lógicas asociadas a él dejarán de ser coherentes con el grupo de interconexiones lógicas. Seleccione Update from group (Actualizar desde el grupo) para que el receptáculo lógico y la interconexión lógica vuelvan a ser coherentes con los cambios efectuados en el grupo de interconexiones lógicas.

16.2.5.5 Sobre el etiquetado Link Layer Discovery Protocol (LLDP)

La información del Link Layer Discovery Protocol (LLDP) la envían los dispositivos a un intervalo fijo en forma de un marco Ethernet. Cada marco contiene una LLDP Data Unit (LLDPDU). Cada LLDPDU es una secuencia de estructuras de tipo-longitud-valor (TLV).

Marcos de LLDP sin etiquetar

Por defecto, las interconexiones Virtual Connect utilizan marcos LLDP sin etiquetar para anunciar su identidad y aprender sobre sus socios de enlace. LLDP anuncia las direcciones IP de gestión de interconexiones Virtual Connect hacia los puertos de apilamiento de enlaces, enlaces ascendentes y enlaces descendientes. Los marcos LLDP también identifican los enlaces de apilamiento en una interconexión lógica.

La dirección IPv4 (y dirección IPv6 si se habilita) se utilizan como la TLV de la dirección de gestión LLDP.

Marcos de LLDP etiquetados

LLDP también se puede utilizar para comunicarse con un conmutador virtual en el hipervisor mediante el uso de marcos de LLDP etiquetados en los puertos de enlace descendiente. El marco etiquetado contiene el ID de VLAN que identifica el subpuerto del FlexNIC configurado. Esta información se utiliza para crear la topología de la red.

El etiquetado de LLDP se puede habilitar o deshabilitar a través de la interfaz de usuario de HPE OneView o la API de REST.

Más información

“Configuración de la interconexión” en la ayuda en línea
“Cómo habilitar o deshabilitar el etiquetado de LLDP” en la ayuda en línea o la ayuda sobre secuencias de comandos de la API de REST
«Acerca de los grupos de interconexiones lógicas»
«Acerca de las interconexiones lógicas»

16.2.5.6 Sobre la estructura tipo-longitud-valor (TLV) mejorada

La TLV mejorada forma parte del intercambio de información del Link Layer Discovery Protocol (LLDP) entre interconexiones. La TLV mejorada determina qué contiene la `TLV del ID de receptáculo` de los marcos de LLDP enviados por una interconexión.

La TLV mejorada se puede habilitar o deshabilitar a través de la interfaz de usuario de HPE OneView o la API de REST.

Habilite la opción	La `TLV del ID de receptáculo` anuncia el nombre del receptáculo y el número de serie a las otras interconexiones.
Disable (Desactivar)	La `TLV del ID de receptáculo` contiene la dirección MAC del conmutador.

16.2.5.6.1 Valores de la TLV mejorada

Habilitar el formato de la TLV mejorada

- Nombre del sistema (*<nombre del host><número de serie>*BAY:*<número_compartimento>*)
- ID del receptáculo (ENC:*<nombre_receptáculo>*:SERIAL NO:*<número_serie_receptáculo>*
- Descripción de la pieza (*<velocidad_op>*/*<tipo_conector>*)

Deshabilitar el formato de la TLV mejorada

- Nombre del sistema (*<nombre del host>*)
- ID del receptáculo (*<dirección_mac_conmutador>*)
- Descripción de la pieza (*IF-MIB::ifDescr value*), por ejemplo `HPE VC FlexFabric 10Gb/24-puertos Módulo 4.10 X1`

Más información

"Cómo habilitar o deshabilitar la configuración de tipo-longitud-valor (TLV) mejorada" en la ayuda en línea o la ayuda sobre secuencias de comandos de la API de REST
«Acerca de los grupos de interconexiones lógicas»
«Acerca de las interconexiones lógicas»

16.2.6 Sobre el firmware asociado con una interconexión lógica

Todos los componentes de un receptáculo lógico deben utilizar la misma versión de firmware o utilizar versiones de firmware compatibles entre ellas. Puede seleccionar un solo Service Pack para ProLiant (SPP) y aplicarlo a todos los componentes de un receptáculo, lo que reduce al mínimo la posibilidad de tiempo de inactividad debido a la incompatibilidad del firmware. También puede aplicar un SPP a una interconexión lógica, lo hace que hace que todas las interconexiones asociadas tengan la misma línea de base de firmware. De forma predeterminada, esta operación únicamente actualiza el firmware de las interconexiones que ejecutan una versión de firmware distinta e ignora las interconexiones que ejecutan la misma versión de firmware.

La versión del firmware asociada con la interconexión lógica se actualiza automáticamente cuando se agrega un receptáculo y se selecciona un SPP para la línea de base de firmware. También se actualizan el firmware de iLO y del OA. No se producen interrupciones en la red siempre que no se hayan definido o aplicado los perfiles de servidor en el nuevo receptáculo.

Sin embargo, si se selecciona `manage manually` (gestionar manualmente) al agregar el receptáculo, la línea de base de las interconexiones es `Not set` (Sin configurar). Si las actualizaciones de firmware posteriores solo se aplican al receptáculo, la línea de base sigue apareciendo en HPE OneView como `Not set` (Sin configurar). Se puede configurar una actualización de la línea de base para el firmware de las interconexiones lógicas cuando se agrega el receptáculo mediante la pantalla **Enclosures** (Receptáculos), o cuando se actualiza el firmware desde la pantalla **Logical Enclosures** (Receptáculos lógicos) y seleccionando `Enclosure + logical interconnect + server profiles` (Receptáculo + interconexión lógica + perfiles de servidor). Si no se establece nunca una línea de base para la interconexión lógica, el firmware del receptáculo debe gestionarse manualmente.

16.2.6.1 Sobre la actualización del firmware para interconexiones lógicas

Las opciones de activación de firmware permiten mantener la disponibilidad de la red y reducir la probabilidad de que se produzcan averías debidas a errores humanos. También existe la opción de almacenar provisionalmente el firmware para su activación posterior. El firmware almacenado provisionalmente se puede activar en una sola interconexión o en todas ellas.

Cuando actualiza el firmware basado en la interconexión lógica, tiene las siguientes opciones:

Opción	Descripción
Update firmware (stage + activate) (Actualizar el firmware [almacenarlo provisionalmente + activarlo])	Almacena provisionalmente (carga) el firmware seleccionado en la memoria flash secundaria de la interconexión y, a continuación, activa el firmware como línea de base. Al final de esta operación, todas las interconexiones ejecutan la misma línea de base de firmware y son compatibles entre sí. Esta opción y la activación en paralelo afectan a la conectividad desde y hacia los servidores hasta que finaliza la activación, pero tarda menos tiempo en actualizar el firmware. Consulte «Acerca de las opciones para la activación del firmware» para obtener información sobre la activación en paralelo.
Stage firmware for later activation (Almacenar provisionalmente el firmware para activarlo más tarde)	Almacena provisionalmente (carga) el firmware seleccionado en la memoria flash secundaria de la interconexión, pero no lo activa. Puede activar el firmware posteriormente. Esta opción permite la secuenciación manual de la activación del firmware y es el método preferido para reducir al mínimo la interrupción de servicio.
Activate firmware (Activar el firmware)	Activa el firmware seleccionado almacenado provisionalmente.

Cuando se actualiza el firmware basado en las interconexiones lógicas, si hay una o varias interconexiones que ya están ejecutando la versión de firmware deseada, HPE OneView excluye dichas interconexiones de la actualización del firmware.

16.2.6.1.1 Acerca de las opciones para la activación del firmware

Existen las siguientes opciones para activar el firmware de los módulos de interconexión Ethernet y Fibre Channel:

Opción	Descripción
Odd/even (Impar/par)	Activa en primer lugar los módulos de interconexión con números impares 1, 3, 5 y 7 del lado izquierdo, seguidos de los módulos con números pares 2, 4, 6 y 8 del lado derecho.
Serial (En serie)	Activa los módulos de interconexión de uno en uno, comenzando por el compartimento con el número más alto. Este método es el que causa menos perturbaciones.
Parallel (En paralelo)	Activa todos los módulos de interconexión al mismo tiempo. Este método es el más invasivo, y puede provocar interrupciones de conectividad de red y de almacenamiento.

16.2.7 Acerca de las configuraciones activo/activo y activo/en espera

Al determinar la configuración de red Virtual Connect que se va a utilizar (activo/activo o activo/en espera), tenga en cuenta el tipo de tráfico de red del receptáculo. Por ejemplo:

- ¿Va a haber un gran volumen de tráfico servidor a servidor (este/oeste) en el receptáculo?
- ¿El flujo de tráfico del receptáculo será principalmente entrante y saliente (norte/sur)?

Teniendo en consideración los patrones de tráfico de red, puede maximizar el ancho de banda conectado o minimizar el tráfico de servidor a servidor que sale del receptáculo.

Utilice una configuración activo/en espera si el tráfico de red se produce entre sistemas en el mismo receptáculo (este/oeste). Esta configuración reduce al mínimo o elimina las comunicaciones servidor a servidor que dejan el receptáculo.

Utilice una configuración activo/activo si el tráfico de red es entrante y saliente (norte/sur) del receptáculo.

16.2.7.1 Acerca de las configuraciones activo/en espera

Una configuración activo/en espera es una configuración de red Ethernet en la que los servidores del receptáculo tienen dos puertos de NIC conectados a la misma red Virtual Connect. Un conjunto de enlaces ascendentes sencillo tiene enlaces ascendentes en ambas interconexiones. Los enlaces ascendentes de una interconexión están activos; los enlaces ascendentes de la otra están en espera y disponibles en caso de fallo de red o de interconexión. Las comunicaciones entre los servidores no dejan el módulo de interconexión. Para las comunicaciones externas, todos los servidores del receptáculo utilizan el enlace ascendente activo, independientemente de qué NIC esté pasando tráfico de forma activa.

Una configuración activo/en espera:

- Proporciona un ancho de banda predecible.
- No supere ancho de banda del conmutador de la parte superior del bastidor.

Una configuración activo/en espera necesita de los siguientes requisitos:

- Un mínimo de una red Ethernet y un conjunto de enlaces ascendentes para cada ID de VLAN externa que se defina.

16.2.7.2 Acerca de las configuraciones activo/activo

Una configuración activo/activo es una configuración de red Ethernet que permite el tráfico activo en la misma VLAN en varios módulos de interconexión. Las NIC de todos los servidores del receptáculo están conectadas a módulos de Virtual Connect adyacentes. Todos los enlaces ascendentes están activos para reenviar tráfico de red.

Una configuración activo/activo:

- Proporciona un uso completo de todos los puertos de enlace ascendente (no hay ningún puerto de enlace ascendente en el modo en espera).
- Permite que todo el tráfico salga a través del módulo de interconexión conectado al puerto NIC sin pasar por el enlace de apilamiento interno, si se usa el apilamiento.
- Se duplica el ancho de banda disponible mientras se mantiene la redundancia (cuando se combina con Smart Link).

Las redes asociadas con un conjunto de enlaces ascendentes deben incluirse en la conexión del perfil de servidor para el módulo de interconexión. Por ejemplo, si Net_101_A se encuentra en conjunto de enlaces ascendentes US_A, que tiene puertos del módulo de interconexión en el compartimento 1, Net_101_A debe asociarse con el puerto de enlace descendente conectado al módulo de interconexión del compartimento 1 (por ejemplo, LOM1: 1-a).

Al configurar una configuración activo/activo en un receptáculo, determine si dispone de un solo grupo de interconexiones lógicas o de varios grupos de interconexiones lógicas por cada configuración del receptáculo. Para obtener más información, consulte «Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos».

- En una configuración de un solo grupo de interconexiones lógicas, tenga al menos dos módulos de interconexión Ethernet con enlaces de apilamiento en el receptáculo. Todas las interconexiones se definen en una interconexión lógica en el grupo de una sola interconexión lógica. Cuando se establece la configuración activo/activo, todas las redes están disponibles en las dos interconexiones, así como para cualquier servidor conectado a estas interconexiones mediante el uso de enlaces de apilamiento. Las redes se crean en pares para cada VLAN con la que se desea conectar.
- En una configuración de varios grupos de interconexiones lógicas, en la que se define cada interconexión en un grupo de interconexiones lógicas independiente, y posteriormente se separan las interconexiones lógicas, las interconexiones ya no están apiladas. Debido a que puede utilizar la misma red en ambos grupos de interconexiones lógicas, puede crear una configuración activo/activo con el doble de redes disponibles.

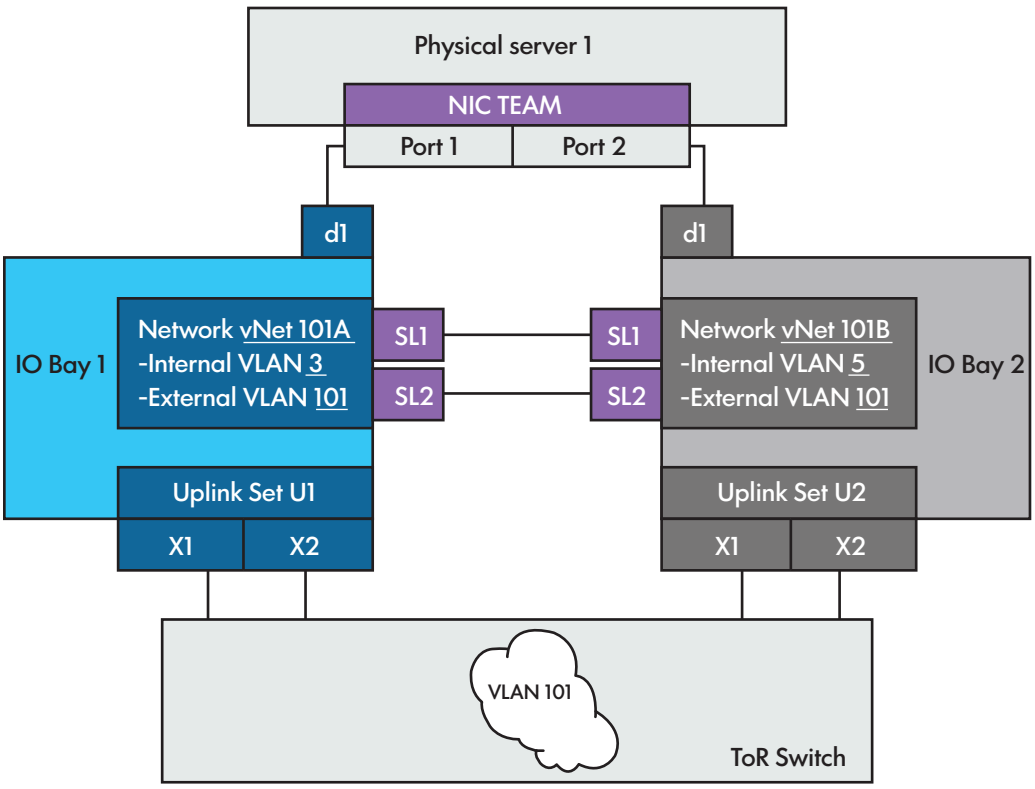
16.2.7.2.1 Requisitos para una configuración activo/activo

Una configuración activo/activo requiere que se configure correctamente el sistema operativo y la formación de equipos de NIC. Una configuración activo/activo también necesita dos módulos Virtual Connect y recursos que cumplan los requisitos siguientes. Para ver un ejemplo de una configuración activo/activo para un grupo de receptáculos con un solo grupo de interconexiones lógicas, consulte «Ejemplo de configuración activo/activo para un solo grupo de interconexiones lógicas».

Recurso	Requisito	Práctica recomendada
Redes	Para una configuración de un solo grupo de interconexiones lógicas, crear un par de redes para cada VLAN que desee conectar. • Al menos una red para el primer módulo de interconexión • Otra red para el segundo módulo de interconexión mediante el mismo ID de VLAN y • **Smart Link** seleccionado en ambas redes. Para una configuración de varios grupos de interconexiones lógicas, puede utilizar la misma red en ambos grupos de interconexiones lógicas.	Para una configuración de un solo grupo de interconexiones lógicas, designe un nombre de red para una red emparejada mediante la convención de nomenclatura `<finalidad>_<ID de VLAN>_<lado>`, donde: • `<finalidad>` puede ser `dev`, `mgmt` o `prod`, por ejemplo. • `<lado>` puede ser `A` o `B`, `1` o `2`, o `right` (derecha) o `left` (izquierda).
Conjunto de enlaces ascendentes	Para una configuración de un solo grupo de interconexiones lógicas, cree un par de conjuntos de enlaces ascendentes para asociar las redes a los puertos de enlace ascendente del módulo de interconexión. • Un conjunto de redes asignado al conjunto de enlaces ascendentes que dispone de enlaces ascendentes en el primer módulo de interconexión • Las demás redes asignadas al conjunto de enlaces ascendentes que dispone de enlaces ascendentes en el segundo módulo de interconexión • Los puertos de enlace ascendente de en cada conjunto de enlaces ascendentes están restringidos a una interconexión Para una configuración de varios grupos de interconexiones lógicas, cree un conjunto de enlaces ascendentes en el primer módulo de interconexión y un conjunto de enlaces ascendentes en el segundo módulo de interconexión con las mismas redes.	Para una configuración de un solo grupo de interconexiones lógicas, asigne nombres a los conjuntos de enlaces ascendentes utilizando la convención de nomenclatura `<nombre del conjunto de enlaces ascendentes>_<lado>`, donde: • `<lado>` puede ser `A` o `B`, `1` o `2`, o `right` (derecha) o `left` (izquierda).

Recurso	Requisito	Práctica recomendada
Conjuntos de redes	Uno o más pares de conjuntos de redes. Cada conjunto debe incluir solo las redes que se van a utilizar en la misma conexión de perfil de servidor. Por ejemplo, si Net_101_A se encuentra en conjunto de enlaces ascendentes US_A, que tiene puertos del módulo de interconexión en el compartimento 1, Net_101_A debe asociarse con el puerto de enlace descendente conectado al módulo de interconexión del compartimento 1 (por ejemplo, LOM1: 1-a)	Para una configuración de un solo grupo de interconexiones lógicas, designe un nombre de conjunto de redes mediante la convención de nomenclatura `<finalidad>_<lado>`, donde: • `<finalidad>` puede ser `dev`, `mgmt` o `prod`, por ejemplo. • `<lado>` puede ser `A` o `B`, `1` o `2`, o `right` (derecha) o `left` (izquierda).
Perfiles de servidor	Puertos físicos a los que desea asignar a la red o los conjuntos de redes. Asigne las conexiones del perfil a los puertos de enlace descendente del mismo módulo de interconexión como enlaces ascendentes del conjunto de enlaces ascendentes. Esto garantiza que las redes asociadas con los puertos de enlace ascendente del conjunto de enlaces ascendentes coinciden con las asignadas a las conexiones del perfil de los puertos de enlace descendente.	

16.2.7.2.2 Ejemplo de configuración activo/activo para un solo grupo de interconexiones lógicas



16.2.8 Acerca de la protección contra bucles

La función de protección contra bucles permite la detección de bucles en los puertos de enlace descendente, que pueden ser puertos lógicos Flex-10 o puertos físicos. Esta función se aplica cuando se está ejecutando el protocolo Device Control Channel (DCC) en el puerto Flex-10.

La protección contra bucles en la red de HPE OneView utiliza dos métodos para detectar los bucles:

1. La interconexión inyecta periódicamente una trama de detección de bucles en la interconexión lógica y analiza los puertos de enlace descendente para detectar la trama de detección devuelta por el bucle. Si se detecta esta trama de detección en los puertos de enlace descendente, el servidor tiene una condición de bucle.
2. La interconexión examina e intercepta las tramas de detección de bucles comunes utilizadas en otros conmutadores, como los Cisco y ProCurve, para evitar que el conmutador de nivel superior resulte afectado.

Cuando está activada la protección contra bucles en la red de la pantalla **Logical Interconnects** (Interconexiones lógicas), y se recibe una trama de detección de bucles en un puerto de enlace descendente, el puerto de enlace descendente se desactiva inmediatamente hasta que se toma una medida administrativa. La medida administrativa conlleva resolver la condición de bucle y borrar la condición de error de protección contra bucles. El estado `loop detected` (bucle detectado) de un servidor se puede borrar editando el servidor y cancelando las asignaciones de todas las redes de la conexión correspondiente al servidor que tiene el estado `loop detected`.

El agente SNMP admite la generación de capturas cuando se detecta o se borra una condición de bucle.

Puede restablecer la protección contra bucles en el menú **Actions** (Acciones) en la pantalla **Interconnects** (Interconexiones).

16.2.9 Acerca de la protección contra desbordamientos de pausa

Las interfaces de conmutador de Ethernet utilizan trama de pausa basada en mecanismos de control de flujo para controlar el flujo de datos. Cuando se recibe una trama de pausa en una interfaz con control de flujo activado, la operación de transmisión se detiene durante la duración de la pausa especificada en la trama de pausa. El resto de tramas cuyo destino es esta interfaz se pondrán en cola. Si se recibe otra trama de pausa antes de que caduque el temporizador de pausa anterior, el temporizador de pausa se actualiza con el nuevo valor de duración de pausa. Si se recibe una secuencia continua de tramas de pausa durante grandes períodos de tiempo, la cola de transmisión de la interfaz continúa creciendo hasta que se agotan todos los recursos en cola. Este estado afecta gravemente a la operación de conmutación de otras interfaces. Además, todas las operaciones de protocolo del conmutador se ven afectadas debido a la incapacidad de transmitir tramas de protocolo. Tanto las tramas de pausa de puerto como las tramas de pausa basadas en prioridad pueden ocasionar el agotamiento de los recursos.

Las interconexiones Virtual Connect proporcionan la capacidad de analizar los puertos de enlace descendente de servidor en busca de desbordamientos de pausa y tomar medidas de protección desactivando el puerto. Virtual Connect 4.31 y las versiones posteriores también supervisan e informan sobre los enlaces ascendentes y los enlaces de apilamiento que presentan desbordamiento de pausa. El intervalo de sondeo predeterminado es de 10 segundos y no lo puede configurar el cliente. El agente SNMP admite la generación de capturas cuando se detecta o se borra una condición de desbordamiento de pausa.

16.2.10 Acerca de la configuración de SNMP

Los sistemas de gestión de redes utilizan SNMP (Simple Network Management Protocol) para supervisar los dispositivos conectados a la red con objeto de detectar situaciones que requieren atención por parte de los administradores. Mediante la configuración de los parámetros de las pantallas **Logical Interconnect Groups** (Grupos de interconexiones lógicas) y **Logical Interconnects** (Interconexiones lógicas), puede permitir que los gestores SNMP de otros fabricantes supervisen (en modo de solo lectura) la información de estado de la red de las interconexiones.

Un gestor SNMP normalmente gestiona un gran número de dispositivos, y cada dispositivo puede tener un gran número de objetos. No resulta práctico que el gestor sondee la información de cada objeto de cada dispositivo. En lugar de ello, cada agente SNMP de dispositivo gestionado envía al gestor sin que este lo solicite un mensaje conocido como captura de evento.

HPE OneView le permite controlar la capacidad de los gestores SNMP de leer los valores de una interconexión. Puede realizar un filtrado del tipo de captura SNMP que se debe capturar y, a continuación, designar el gestor SNMP al que se remitirán las capturas. De forma predeterminada, SNMP está activado sin destinos de captura establecidos.

Cuando se crea una interconexión lógica, hereda la configuración SNMP de su grupo de interconexiones lógicas. Para personalizar la configuración de SNMP en el nivel de interconexión lógica, utilice la pantalla **Logical Interconnects** (Interconexiones lógicas) o las API de REST.

16.2.11 Sobre el módulo de interconexión Virtual Connect FlexFabric–20/40 F8

El módulo Virtual Connect FlexFabric–20/40 F8 para HPE BladeSystem c-Class ofrece varias funciones exclusivas: Para obtener más información, consulte las instrucciones de instalación del *HPE Virtual Connect FlexFabric–20/40 F8 para HPE BladeSystem c-Class* en **http://www.hpe.com/info/qs**.

Requisitos de receptáculos

ATENCIÓN: Para evitar el sobrecalentamiento:

- Asegúrese de que hay 10 ventiladores en el receptáculo.
- No coloque más de seis módulos Virtual Connect FlexFabric–20/40 F8 en un único receptáculo.

16.2.12 Acerca de la calidad de servicio del tráfico de red

La calidad de servicio (Quality of Service, QoS) es un conjunto de los requisitos de servicio que debe cumplir la red para garantizar un nivel de servicio adecuado para la transmisión de datos. El objetivo de QoS es un sistema de entrega garantizado para el tráfico de red.

La función QoS permite a los administradores configurar colas de tráfico para tráfico de red de distinta prioridad, categorizar y dar prioridad al tráfico de entrada, y ajustar la configuración de prioridad del tráfico de salida. Los administradores pueden usar esta configuración para asegurarse de que el tráfico importante recibe la gestión de prioridad máxima mientras que el tráfico menos importante recibe una gestión con una prioridad inferior. El tráfico de red se organiza por categorías y, a continuación, se clasifica. Después de clasificar el tráfico, se le asignan prioridades y se programa para su transmisión.

Para una QoS de extremo a extremo, todos los saltos a lo largo de la ruta deben configurarse con directivas de QoS de clasificación y gestión de tráfico similares. En una directiva de QoS de extremo a extremo, la priorización del tráfico se realiza teniendo en cuenta dos factores.

- En la interconexión, los paquetes van saliendo en función del ancho de banda de la cola asociada. Cuanto mayor sea el ancho de banda, mayor será la prioridad para el tráfico asociado en la cola.
- Las marcas dot1p para tráfico saliente ayudan a conseguir prioridad en los siguientes saltos en la red. Si el tráfico saliente de la cola se marca con un valor dot1p, y dicho valor dot1p está asignado a una cola con mayor ancho de banda en los saltos siguientes, estos paquetes se tratan con mayor prioridad en la red de extremo a extremo.

La configuración de QoS se define en el grupo de interconexiones lógicas y se aplica a la interconexión lógica. Las estadísticas de QoS se recopilan en las interconexiones.

La configuración de QoS solo se aplica en las interconexiones VC Ethernet y VC FlexFabric en receptáculos c7000.

Estado de coherencia de una interconexión lógica con las configuraciones de QoS

La interfaz de usuario muestra únicamente la configuración de QoS que se encuentra activa actualmente y que se aplica a las interconexiones. Asimismo, se guardan dos configuraciones de QoS inactivas para los tipos de configuración **Custom (with FCoE)** (Personalizado [con FCoE]) y **Custom (without FCoE)** (Personalizado [sin FCoE]). Estas son las últimas configuraciones de QoS conocidas para los tipos de configuración correspondientes, que se aplicaron anteriormente al grupo de interconexiones lógicas y a la interconexión lógica asociada.

Cuando se comprueba la coherencia de una interconexión lógica con su grupo de interconexiones lógicas asociado, también se comprueban las configuraciones de QoS inactivas (las configuraciones de QoS inactivas no son visibles en la interfaz de usuario). Aun cuando las configuraciones de QoS sean exactamente iguales entre una interconexión lógica y el grupo de interconexiones lógicas asociado, debido a las incoherencias en las configuraciones de QoS inactivas almacenadas internamente, el estado de coherencia de una interconexión lógica puede aparecer como `Inconsistent` (Incoherente). Realice una actualización desde el grupo para situar el grupo de interconexiones locales y la interconexión lógica en un estado coherente.

16.2.13 Agregar un conjunto de enlaces ascendentes

Cada conjunto de enlaces ascendentes debe tener un nombre exclusivo dentro de la interconexión lógica o el grupo de interconexiones lógicas y debe contener al menos una red. Para obtener más información sobre los conjuntos de enlaces ascendentes, consulte «Acerca de las interconexiones lógicas».

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de red.

Adición de un conjunto de enlaces ascendentes

1. En el menú principal, seleccione **Logical Interconnects** (Interconexiones lógicas) y, a continuación, seleccione la interconexión lógica que desee editar.
2. Seleccione **Actions→Edit** (Acciones > Editar).
3. Haga clic en el botón **Add uplink set** (Agregar conjunto de enlaces ascendentes).
4. Introduzca los datos solicitados en la pantalla. Para obtener más información, consulte Add or edit uplink sets (Agregar o editar conjuntos de enlaces ascendentes) en los detalles de la pantalla Logical Interconnects (Interconexiones lógicas) de la ayuda en línea.
5. Haga clic en **Add networks** (Agregar redes) y seleccione las redes que desea asignar al conjunto de enlaces ascendentes.
6. Haga clic en **Add** (Agregar) o en **Add +** (Agregar +) para agregar otra red.
7. Haga clic en **Add uplink ports** (Agregar puertos de enlace ascendente) y seleccione los puertos de enlace ascendente.
8. Haga clic en **Add** (Agregar) o en **Add +** (Agregar +) para agregar otro puerto.
9. Compruebe que la información que ha introducido es correcta y haga clic en **Create** (Crear).
10. Haga clic en **OK** (Aceptar).
11. Compruebe que el conjunto de enlaces ascendentes se ha creado en el panel de detalles.

16.2.14 Actualización del firmware para las interconexiones lógicas de los receptáculos

Para actualizar el firmware de las interconexiones lógicas, elija una de estas opciones:

- Update firmware (stage + activate) (Actualizar el firmware [almacenarlo provisionalmente + activarlo])
- Stage firmware for later activation (Almacenar provisionalmente el firmware para activarlo más tarde)
- Activate firmware (Activar el firmware)

NOTA: Cuando haya una actualización del firmware de la interconexión lógica en curso, no inicie una actualización del firmware desde el receptáculo lógico de dicha interconexión lógica.

Si dispone de interconexiones Fibre Channel HPE Virtual Connect, consulte “Update the interconnect firmware for HPE Virtual Connect Fibre Channel interconnects” (Actualización del firmware de interconexión de las interconexiones Fibre Channel HP Virtual Connect) en la ayuda en línea.

16.2.14.1 Almacenamiento y activación del firmware para actualización desde una interconexión lógica

Para cargar el firmware y almacenarlo provisionalmente para su activación posterior, realice los pasos siguientes. Para activar firmware que ya está almacenado provisionalmente, consulte “Activate the logical interconnect firmware” (Activar el firmware de la interconexión lógica) en la ayuda en línea.

Requisitos previos

- Privilegios necesarios: administrador de red o administrador de infraestructuras
- Como mínimo un receptáculo con dos interconexiones agregadas configuradas para utilizar Ethernet y como mínimo una interconexión lógica
- Al menos uno o varios SPP compatibles cargados en el dispositivo

Almacenamiento y activación del firmware para actualización desde una interconexión lógica

1. En el menú principal, seleccione **Logical Interconnects** (Interconexiones lógicas).
2. En el panel principal, seleccione la interconexión lógica y, a continuación, realice una de las acciones siguientes:
   - Seleccione **Actions→Update firmware** (Acciones > Actualizar firmware).
   - Seleccione **Update firmware** (Actualizar el firmware) en el panel **Firmware**.
3. En **Update action** (Acción de actualización) seleccione **Update firmware (stage + activate)** (Actualizar el firmware [almacenarlo provisionalmente + activarlo]).
4. En **Firmware baseline** (Línea de base de firmware), seleccione el lote de firmware que desee instalar.
5. Opcional: seleccione **Force installation** (Forzar la instalación) para actualizar el firmware en todas las interconexiones miembro y receptáculos de controladores independientemente de si un miembro ya tiene el firmware actualizado o no.

   Para instalar una versión de firmware más antigua que la versión incluida en el SPP, debe seleccionar la opción **Force installation** (Forzar la instalación) para cambiar el firmware a una versión anterior. Es posible que desee instalar un firmware más antiguo si sabe que el firmware más reciente provoca un problema en su entorno.
6. Seleccione el método de activación del firmware y retardo para las interconexiones en las que activar el firmware.
7. Haga clic en **OK** (Aceptar).
8. Compruebe la versión del firmware asociada con la interconexión lógica y sus interconexiones asociadas en la página **Logical Interconnects** (Interconexiones lógicas= de la vista **Firmware**.

   NOTA: Si el firmware ya está incluido en la línea de base de firmware seleccionada, el firmware no se actualiza y aparece un mensaje en la pantalla Activity (Actividad) indicando que no es necesaria ninguna actualización.

16.2.14.2 Almacenamiento del firmware para una activación posterior para actualización desde una interconexión lógica

Para cargar el firmware y almacenarlo provisionalmente para su activación, realice los pasos siguientes. Para activar firmware que se ha almacenado provisionalmente, consulte “Activate the logical interconnect firmware” (Activar el firmware de la interconexión lógica) en la ayuda en línea.

Requisitos previos

- Privilegios necesarios: administrador de red o administrador de infraestructuras
- Como mínimo un receptáculo con dos interconexiones agregadas configuradas para utilizar Ethernet y como mínimo una interconexión lógica
- Al menos uno o varios SPP compatibles cargados en el dispositivo

Almacenamiento del firmware para una activación posterior para actualización desde una interconexión lógica

1. En el menú principal, seleccione **Logical Interconnects** (Interconexiones lógicas).
2. En el panel principal, seleccione la interconexión lógica y, a continuación, realice una de las acciones siguientes:
   - Seleccione **Actions→Update firmware** (Acciones > Actualizar firmware).
   - Seleccione **Update firmware** (Actualizar el firmware) en el panel **Firmware**.
3. En **Update action** (Acción de actualización) seleccione **Stage firmware for later activation** (Almacenar provisionalmente el firmware para activarlo más tarde).
4. En **Firmware baseline** (Línea de base de firmware), seleccione el lote de firmware que desee instalar.
5. Opcional: seleccione **Force installation** (Forzar la instalación) para actualizar el firmware en todas las interconexiones miembro independientemente de si un miembro ya tiene el firmware actualizado o no.

   Para instalar una versión de firmware más antigua que la versión incluida en el SPP, debe seleccionar la opción **Force installation** (Forzar la instalación). Es posible que desee instalar un firmware más antiguo si sabe que el firmware más reciente provoca un problema en su entorno.
6. Haga clic en **OK** (Aceptar).
7. Compruebe la versión del firmware asociada con la interconexión lógica y sus interconexiones asociadas en la página **Logical Interconnects** (Interconexiones lógicas= de la vista) **Firmware**.

NOTA: Si el firmware ya está incluido en la línea de base de firmware seleccionada, el firmware no se actualiza y aparece un mensaje en la pantalla Activity (Actividad) indicando que no es necesaria ninguna actualización.

16.2.14.3 Activación del firmware para actualización desde una interconexión lógica

Durante el almacenamiento provisional para activarlo más tarde, el firmware se escribe (se carga) en la memoria flash secundaria de la interconexión, pero no se activa. Es necesario activar el firmware almacenado provisionalmente para que se convierta en la nueva línea de base de firmware. Si se produce un fallo durante el almacenamiento provisional en una o varias interconexiones, la operación de actualización del firmware finaliza automáticamente.

En la pantalla **Logical Interconnects** (Interconexiones lógicas), se muestran tanto la línea de base de firmware actual como las versiones de firmware instaladas o almacenadas provisionalmente para cada interconexión.

Requisitos previos

- Privilegios necesarios: administrador de red o administrador de infraestructuras
- Como mínimo un receptáculo con dos interconexiones agregadas configuradas para utilizar Ethernet y como mínimo una interconexión lógica
- Firmware almacenado anteriormente

Activación del firmware para actualización desde una interconexión lógica

1. En el menú principal, seleccione **Logical Interconnects** (Interconexiones lógicas) y, a continuación, seleccione la interconexión lógica cuyo firmware desee gestionar.
2. Seleccione **Actions→Update firmware** (Acciones > Actualizar firmware).
3. En **Update action** (Acción de actualización) seleccione **Activate firmware** (Activar el firmware).
4. Seleccione el método de activación del firmware y retardo para las interconexiones en las que activar el firmware.

   NOTA: En la activación `Odd/Even` (Impar/par) o `Serial` (En serie), los módulos Ethernet se actualizan primero, seguidos de los módulos Fibre Channel. No se comenzará con los módulos Fibre Channel hasta que no estén activados todos los módulos Ethernet.

5. Haga clic en **OK** (Aceptar).
6. Compruebe la pantalla Activity (Actividad) para determinar si se ha completado la acción de actualización del firmware.
7. Para comprobar que la versión de firmware se ha instalado después de activar el firmware, seleccione la vista **Firmware** y compare el número de versión `Installed` (Instalada) y `Baseline` (Línea de base).

16.2.15 Actualización de la configuración de las interconexiones lógicas a partir del grupo de interconexiones lógicas

La comprobación de coherencia es la validación de una interconexión lógica para asegurarse que coincide con la configuración de su grupo de interconexiones lógicas. El dispositivo examina tanto la interconexión lógica como el grupo de interconexiones lógicas, los compara y comprueba si coincide lo siguiente:

Elementos	Comprobación de coherencia
Configuración de interconexiones Ethernet	¿Existen diferencias en las siguientes configuraciones de la interconexión lógica con respecto a la configuración teórica definida por el grupo de interconexiones lógicas? • Activación de la conmutación por error rápida de la memoria caché MAC • Intervalos de actualización de direcciones MAC • Activación de snooping de IGMP • Intervalos de tiempo de inactividad de IGMP • Protección contra bucles • Protección contra desbordamientos de pausa
Conjuntos de enlaces ascendentes	¿Existen diferencias en las asignaciones de puertos o las asociaciones de redes con respecto a la configuración definida por el grupo de interconexiones lógicas? ¿Ha agregado un conjunto de enlaces ascendentes?
Redes internas	¿Existen diferencias en las asignaciones de redes para las comunicación entre servidores con respecto a la configuración definida por el grupo de interconexiones lógicas?

Elementos	Comprobación de coherencia
Asignaciones de interconexiones	¿Se ha editado el grupo de interconexiones lógicas?
Configuración de Quality of Service (QoS) (Calidad de servicio [QoS])	¿Se han editado los requisitos del servicio de red?

Si ambas configuraciones coinciden, el campo **Consistency state** (Estado de coherencia) de la interconexión lógica se establece en `Consistent` (Coherente) y se considera que la interconexión es conforme.

Si hay cualquier incoherencia, se genera una alerta para la interconexión lógica y el campo **Consistency state** (Estado de coherencia) se establece en `Inconsistent with group` (Incoherente con el grupo).

Actualización de la configuración de las interconexiones lógicas a partir del grupo de interconexiones lógicas

Para hacer que una configuración de interconexión `Inconsistent with group` (Incoherente con el grupo) vuelva a ser `Consistent` (Coherente) con el grupo de interconexiones lógicas, debe volver a aplicar la configuración del grupo de interconexiones lógicas.

NOTA: También puede seleccionar **Update from group** (Actualizar desde el grupo) en el receptáculo lógico, ya que una interconexión lógica no coherente da lugar a un receptáculo lógico no coherente.

1. En la pantalla **Logical Interconnects** (Interconexiones lógicas), seleccione **Actions→Update from group** (Acciones > Actualizar desde el grupo).

   NOTA: La opción **Update from group** (Actualizar desde el grupo) no está disponible si el grupo de interconexiones lógicas y la interconexión lógica ya son coherentes (el campo **Consistency state** [Estado de coherencia] está establecido en `Consistent` [Coherente]).

   Las alertas de coherencia se borran automáticamente y la configuración ahora coincide con la del grupo de interconexiones lógicas.

   NOTA: No siempre se puede restablecer la coherencia de una interconexión lógica editando o borrando manualmente la alerta; normalmente se debe seleccionar **Actions→Update from group** (Acciones > Actualizar desde el grupo).

   Si se borra una alerta, puede que cambie el estado del recurso de interconexión lógica (el estado es igual al estado de la alerta más grave que no se haya borrado). Esto es un caso de uso válido si desea que la interconexión lógica no sea coherente, pero quiere que en el panel de control aparezca un estado correcto (de color verde).
2. Marque la casilla de confirmación para confirmar que entiende todas las implicaciones.
3. Haga clic en **Yes, update** (Sí, actualizar) para confirmar.
4. Para comprobar que la actividad es correcta, compruebe que tiene un estado de color verde en el «Área de notificaciones».

   Si la actividad no se realiza correctamente, siga las instrucciones en la resolución propuesta.

16.2.16 Creación de un grupo de interconexiones lógicas

De forma predeterminada, al agregar un receptáculo se crea automáticamente un solo grupo de interconexiones lógicas que contiene todas las interconexiones del receptáculo. Si desea crear varias interconexiones lógicas, cree primero los grupos de interconexiones lógicas con las interconexiones que desee incluir en cada interconexión lógica. Consulte «Acerca de la

configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos» y «Cuándo se crea un grupo de interconexiones lógicas» para obtener más información.

Si quiere utilizar un grupo de interconexiones lógicas existente como plantilla, copie el grupo de interconexiones lógicas en lugar de crear uno nuevo.

Requisitos previos

- Privilegios necesarios: administrador de red o administrador de infraestructuras

Cómo crear un grupo de interconexiones lógicas

1. En el menú principal, seleccione **Logical Interconnect Groups** (Grupos de interconexiones lógicas) y, a continuación, realice una de las acciones siguientes:
   - Seleccione **Actions→Create** (Acciones > Crear).
   - Haga clic en **+ Create logical interconnect group** (+ Crear grupo de interconexiones lógicas).
2. Escriba un nombre para el grupo de interconexiones lógicas.
3. Seleccione elementos en la lista de interconexiones disponibles para cada compartimento. Para obtener más información, consulte Requisitos de los grupos de interconexiones lógicas.
4. Haga clic en el icono **Edit** (Editar) de la zona de redes internas de la vista gráfica.
5. Haga clic en **Add networks** (Agregar redes) para seleccionar entre las redes disponibles.
6. Haga clic en **OK** (Aceptar) cuando termine de agregar redes internas.
7. Haga clic en **Add uplink set** (Agregar conjunto de enlaces ascendentes).
8. Escriba los datos solicitados en la pantalla para cada conjunto de enlaces ascendentes que desea crear. Consulte «Agregar un conjunto de enlaces ascendentes» para obtener más información.
9. Haga clic en **Create** (Crear) para finalizar, o haga clic en **Create +** (Crear +) para crear conjuntos de enlaces ascendentes adicionales.
10. Opcional: desplácese hacia abajo y, si es necesario, introduzca cambios en la configuración de las interconexiones.

    Las interconexiones lógicas creadas a partir del grupo de interconexiones heredan estos valores de configuración. Para obtener más información, consulte los detalles de la pantalla Interconnect settings (Configuración de interconexión) en la ayuda en línea.
11. Opcional: efectúe los cambios necesarios en la configuración de SNMP.

    Las interconexiones lógicas creadas a partir del grupo de interconexiones heredan estos valores de configuración. Para obtener más información, consulte los detalles de la pantalla SNMP en la ayuda en línea.
12. Opcional: efectúe los cambios necesarios en la configuración de la calidad de servicio (QoS).
13. Haga clic en **Create** (Crear) para finalizar, o haga clic en **Create +** (Crear +) para crear grupos de interconexiones lógicas adicionales.
14. Para comprobar que se ha creado el grupo de interconexiones lógicas, busque el grupo en el panel de detalles.
15. Opcional: si es necesario, seleccione el grupo de interconexiones lógicas que desee editar y, a continuación, seleccione **Actions→Edit** (Acciones > Editar) para efectuar cambios en la configuración de muestreo de utilización.

    Estos valores se utilizan en la recopilación de datos para los gráficos de utilización que se muestran en la pantalla **Interconnects** (Interconexiones). Para obtener más información, consulte los detalles de la pantalla Utilization Sampling (Muestreo de utilización).
16. Haga clic en **OK** (Aceptar) para aplicar los cambios.
17. Para comprobar los cambios, búsquelos en la vista **General**.

Más información

«Acerca de los grupos de interconexiones lógicas»

16.2.17 Información adicional

- «Grupos de interconexiones lógicas»
- «Interconexiones lógicas»
- «Conjuntos de enlaces ascendentes»
- «Solución de problemas de las interconexiones lógicas»

17 Gestión de receptáculos, grupos de receptáculos y receptáculos lógicos

Los receptáculos integran la infraestructura alimentación, refrigeración y E/S necesaria para los componentes modulares de hardware de servidor, interconexión y almacenamiento.

Un grupo de receptáculos especifica una configuración estándar para todos los receptáculos que forman parte de él. Los grupos de receptáculos les permiten a los administradores aprovisionar varios receptáculos de una manera coherente y predecible en cuestión de segundos.

Un receptáculo lógico representa una vista lógica de un único receptáculo con un grupo de receptáculos que actúa como plantilla. Si la configuración prevista en el receptáculo lógico no coincide con la configuración real del receptáculo, el receptáculo lógico pasa a ser incoherente.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Enclosures (Receptáculos)	`enclosures`
Enclosure Groups (Grupos de receptáculos)	`enclosure-groups`
Logical enclosures (Receptáculos lógicos)	`logical-enclosures`

17.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de servidores

17.2 Gestión de receptáculos

17.2.1 Tareas para receptáculos

La ayuda en línea de HPE OneView proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar un receptáculo c7000 para gestionar su contenido.
- Agregar un receptáculo c7000 para supervisar el hardware.
- Agregar hardware de servidor y otros componentes a receptáculos gestionados.
- Reclamar un receptáculo c7000 que actualmente gestiona otro dispositivo.
- Recopile datos de soporte remoto para los receptáculos.
- Editar un receptáculo.
- Agregar por la fuerza un receptáculo c7000 supervisado que actualmente está siendo supervisado por otro sistema de gestión.
- Eliminar por la fuerza un receptáculo c7000 si falla una acción de eliminación.
- Migrar un receptáculo c7000 que VCM está gestionado actualmente.
- Trasladar un receptáculo c7000 supervisado a un estado gestionado.
- Volver a aplicar la configuración del receptáculo.
- Actualizar el receptáculo para volver a sincronizarlo con HPE OneView.
- Quitar un receptáculo c7000 de HPE OneView.

- Quitar un servidor y otros componentes de un receptáculo existente.
- Ver actividades (alertas y tareas).

17.2.2 Acerca de los receptáculos

Un receptáculo es una estructura física con compartimentos de dispositivo que admiten elementos de cálculo, conexión de red y almacenamiento. Estos elementos constitutivos comparten la infraestructura común de gestión, refrigeración y alimentación del receptáculo.

Para obtener información sobre los receptáculos, consulte los temas siguientes.

- «Acerca de los receptáculos c7000»
- «Acerca de los receptáculos c7000 gestionados»
- «Acerca de los receptáculos c7000 supervisados»
- «Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión»
- «Acerca de los receptáculos c7000 no gestionados y no admitidos»

17.2.2.1 Acerca de los receptáculos c7000

Un receptáculo c7000 se agrega a HPE OneView como un receptáculo `Managed` (Gestionado), que puede ser `Migrated` (Migrado) o `Monitored` (Supervisado).

Gestionado	HPE OneView gestiona el receptáculo, lo que le permitirá aplicar configuraciones, implementar perfiles de servidor, supervisar el estado de funcionamiento, recopilar estadísticas y alertar a los usuarios cuando se den determinadas situaciones. Los receptáculos gestionados requieren una licencia HPE OneView Advanced o HPE OneView Advanced w/o iLO. Consulte «Tipos de licencias».
Supervisado	HPE OneView supervisa el hardware únicamente a efectos de inventario y de estado del hardware. No está permitida la gestión de perfiles de servidor dentro de HPE OneView para un receptáculo supervisado. Los receptáculos supervisados utilizan una licencia gratuita HPE OneView Standard. Consulte «Tipos de licencias».
Migrado	HPE OneView migra un receptáculo desde Virtual Connect Manager (VCM) de modo que su contenido se pueda gestionar en HPE OneView. Si se migra un receptáculo, la configuración existente se captura y se vuelve a crear en HPE OneView, siempre que la configuración sea compatible con HPE OneView.

17.2.2.2 Acerca de los receptáculos c7000 gestionados

La adición de un receptáculo para gestionarlo permitirá aplicar configuraciones, implementar perfiles de servidor, supervisar el estado de funcionamiento, recopilar estadísticas y alertar a los usuarios cuando se den determinadas situaciones. Existen distintas formas de añadir un receptáculo gestionado a HPE OneView.

- *Agregar* un receptáculo que es nuevo en el entorno (uno que no gestiona otro sistema). Los valores de configuración existentes se borran y no se incorporan en HPE OneView. Consulte «Antes de agregar un receptáculo para gestionarlo» para obtener más información.
- *Migrar* un receptáculo si está gestionado por Virtual Connect Manager (VCM), de forma que la configuración existente se captura y se vuelve a crear en HPE OneView. Consulte «Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión» para obtener más información.

NOTA: Se puede agregar por la fuerza un receptáculo desde otro sistema de gestión. Sin embargo, esto elimina *todos* los parámetros de configuración actuales de donde se esté gestionando actualmente y no los importa en HPE OneView.

La adición o migración de un receptáculo para gestionarlo requiere una licencia HPE OneView Advanced o HPE OneView Advanced w/o iLO. Consulte «Tipos de licencias».

Blades de servidor ProLiant G6 y ProLiant BL680c G7

Si se agrega un receptáculo para gestionarlo que contiene un blade de servidor ProLiant G6 o un blade de servidor ProLiant BL680c, ocurre lo siguiente:

- Estos blades de servidor se agregan a HPE OneView en un estado `Monitored` (Supervisado). Consulte «Acerca de los receptáculos c7000 supervisados».
- La licencia HPE OneView Standard se aplica automáticamente a estos servidores solamente, a pesar de que estén en un receptáculo gestionado. Consulte «Tipos de licencias».
- El firmware de estos servidores no se actualiza durante la adición del receptáculo. El firmware del servidor debe actualizarse manualmente (fuera de HPE OneView) después de agregar el receptáculo.

17.2.2.2.1 Antes de agregar un receptáculo para gestionarlo

Antes de agregar un receptáculo para gestionarlo, tenga en cuenta lo siguiente:

- ¿Desea que haya *una* o *varias* interconexiones lógicas para todas las interconexiones del receptáculo? Consulte «Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos» para obtener más información.
- ¿Desea usar un grupo de receptáculos *nuevo* o *existente*?
    - Un grupo de receptáculos existente aplica las configuraciones de ese grupo al receptáculo nuevo. Las interconexiones del receptáculo se configuran automáticamente basándose en los grupos de interconexiones lógicas asociados al grupo de receptáculos.

      Para una configuración de varios grupos de interconexiones lógicas, seleccione el grupo de receptáculos que ha creado y que contiene la configuración de varios grupos de interconexiones lógicas.
    - Un grupo de receptáculos nuevo crea una configuración basada en el receptáculo que se agrega. Esto crea automáticamente una sola interconexión lógica para todas las interconexiones del receptáculo.
- Si va a crear un grupo de receptáculos nuevo, escriba un nombre exclusivo para el grupo. ¿Desea usar un grupo de interconexiones lógicas *nuevo* o *existente*?
    - Un grupo de interconexiones lógicas existente aplica sus configuraciones a las interconexiones.
    - Un grupo de interconexiones lógicas nuevo crea una configuración basada en las interconexiones que se encuentran en el receptáculo.

17.2.2.3 Acerca de los receptáculos c7000 supervisados

Puede agregar receptáculos c7000 para hacer el inventario del hardware y supervisarlo. Esto es útil cuando se dispone de receptáculos que ya están implementados y que no se pueden migrar a HPE OneView. Los receptáculos con blades de servidor ProLiant G6 y posteriores no se pueden gestionar, pero se pueden supervisar.

La supervisión del hardware de los receptáculos c7000 puede realizarse con una licencia gratuita denominada HPE OneView Standard. Para obtener más información, consulte «Tipos de licencias».

NOTA: Si el firmware de cualquier parte del receptáculo no es de la versión mínima admitida, el receptáculo se agregará en un estado `Unmanaged` (No gestionado). Para solucionar este problema, actualice el firmware de forma manual (fuera de HPE OneView) y, a continuación, actualice el receptáculo.

Para agregar un receptáculo c7000 para supervisarlo, consulte "Add an enclosure to monitor the hardware" (Adición de un receptáculo para supervisar el hardware) en la ayuda en línea.

Cambio de un receptáculo c7000 de supervisado a gestionado

Una vez que se está supervisando un receptáculo en HPE OneView, si decide cambiarlo de `monitored` (supervisado) a `managed` (gestionado), debe quitarlo de HPE OneView y, a continuación, migrarlo o agregarlo nuevamente como un receptáculo gestionado, obteniendo la licencia adecuada. Con la migración se conservan los parámetros de configuración, mientras que con la adición no se migra la configuración.

17.2.2.4 Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión

Los receptáculos gestionados por VCM (Virtual Connect Manager) o VCEM (Virtual Connect Enterprise Manager) se pueden migrar a HPE OneView. La migración vuelve a crear la información de configuración de un receptáculo, incluyendo el hardware, el dominio de Virtual Connect, las redes y los perfiles de servidor (incluidas las direcciones MAC y los WWN de las conexiones de los perfiles).

Hasta cuatro dominios de un único receptáculo gestionados por VCM se pueden migrar simultáneamente a HPE OneView a través de la interfaz de usuario o la API de REST.

Los receptáculos gestionados por VCEM pueden prepararse para la migración a HPE OneView a través de la GUI de VCEM o de un módulo de PowerShell. Consulte «Preparación de un receptáculo de VCEM para la migración a HPE OneView» para obtener más información.

NOTA: HPE OneView no permite realizar la migración ni la gestión de blades de servidor G6. Puede remplazar los blades de servidor G6 por blades G7 o posteriores, o puede supervisar el receptáculo. Consulte «Acerca de los receptáculos c7000 supervisados».

Cuando se agrega un receptáculo para migrarlo, se puede especificar un grupo de receptáculos o crear un nuevo grupo de receptáculos. Consulte «Acerca de los receptáculos c7000 gestionados».

Más información

«Sobre la migración sin conexión y en servicio»
«Sobre la migración de dominios parcialmente apilados»
«Sobre la configuración de VCM que no se migrará»
«Antes de migrar receptáculos c7000»
«Sobre problemas de bloqueo durante la migración»
«Sobre las confirmaciones de la migración»
«Duración y tipo de migración»
«Prácticas recomendadas para migran un receptáculo de VCM a HPE OneView.»

17.2.2.4.1 Sobre la migración sin conexión y en servicio

Se pueden migrar receptáculos a HPE OneView sin conexión o en servicio.

Sin conexión Los servidores se apagan antes de la migración

Ventajas: tiempo de migración más rápido y compatibilidad con dominios parcialmente apilados

En servicio Los servidores se mantienen encendidos durante la migración

Ventaja: el tiempo de inactividad en la conectividad del servidor es mínimo

Ambos tipos de migración necesitan que:

- Se hayan resuelto todos los problemas de bloqueo, como se indica en el informe de compatibilidad.
- Todas las confirmaciones se hayan entendido y aceptado, incluidas las confirmaciones adicionales para la migración en servicio (por ejemplo, BIOS y SR-IOV)

Además, la migración en servicio necesita:

- Un receptáculo completamente apilado en un anillo dual o una configuración de enlace de apilamiento vertical izquierda/derecha. Consulte las conexiones de apilamiento recomendadas en la ***Guía de instalación y configuración de HPE Virtual Connect para c-Class BladeSystem*** .

NOTA: Los cambios realizados durante la migración en servicio no tienen efecto hasta que el servidor se reinicia por primera vez después de la migración. Programe un reinicio en caso de que una de las confirmaciones, por ejemplo una configuración de función virtual de SR-IOV, indique un cambio que afectaría al funcionamiento.

Si no se pueden cumplir las condiciones de migración en servicio adicionales, se recomienda la migración sin conexión.

Más información

«Sobre problemas de bloqueo durante la migración»
«Sobre las confirmaciones de la migración»

17.2.2.4.2 Sobre la migración de dominios parcialmente apilados

En Virtual Connect Manager, se admiten tres tipos de configuraciones de apilamiento Ethernet y se pueden migrar a HPE OneView:

Completa Todas las interconexiones de Ethernet tienen una ruta al resto de interconexiones de Ethernet. El apilamiento completo es el modo por defecto.

Esta configuración se migra a HPE OneView con todas las interconexiones de Ethernet y Fibre Channel de un grupo de interconexiones lógicas. Esta configuración se puede migrar en servicio o sin conexión. Consulte Figura 15: «Migración de apilamiento completo de Virtual Connect Manager a HPE OneView».

Principal-sección El apilamiento solo se produce entre las interconexiones de Ethernet principal y en espera dentro del dominio.

Esta configuración se migra a HPE OneView con todas las interconexiones principales y secundarias configuradas dentro de un grupo de interconexiones lógicas. El resto de interconexiones de Ethernet se configuran en su propio grupo de interconexiones lógicas con una interconexión de Ethernet por grupo de interconexiones lógicas. Las interconexiones de Fibre Channel se configuran conjuntamente en otro grupo de interconexiones lógicas independiente. Esta configuración se debe migrar sin conexión. Consulte Figura 16: «Migración de apilamiento principal-sección de Virtual Connect Manager a HPE OneView».

Horizontal El apilamiento se produce entre cada par de interconexiones de Ethernet horizontales.

Esta configuración se migra a HPE OneView con todas las interconexiones adyacentes horizontalmente configuradas dentro de un grupo de interconexiones lógicas. Si no hay ninguna interconexión adyacente horizontalmente presente, cuando se migra, el grupo de interconexiones lógicas correspondiente contiene únicamente una interconexión de Ethernet. Esta configuración se debe migrar sin conexión. Las interconexiones de Fibre Channel se configuran conjuntamente en otro grupo de interconexiones lógicas independiente. Consulte Figura 17: «Migración de apilamiento horizontal de Virtual Connect Manager a HPE OneView».

Figura 15 Migración de apilamiento completo de Virtual Connect Manager a HPE OneView

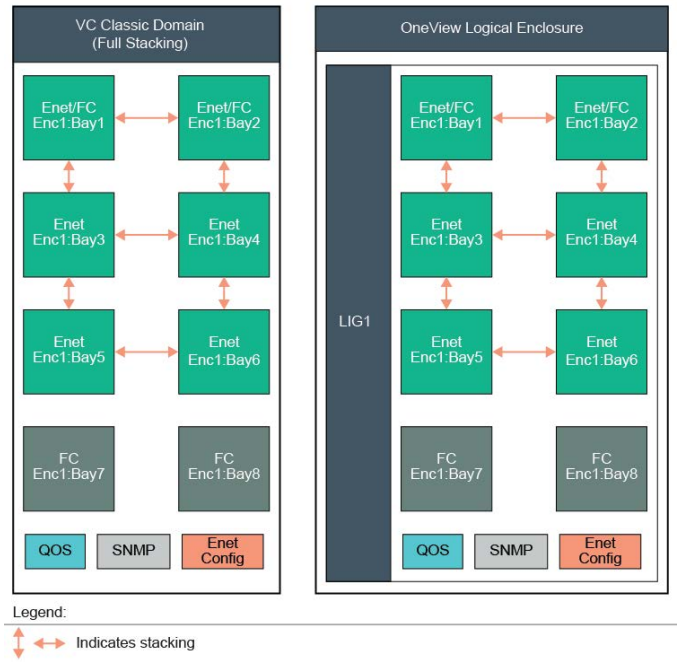


Figura 16 Migración de apilamiento principal-sección de Virtual Connect Manager a HPE OneView

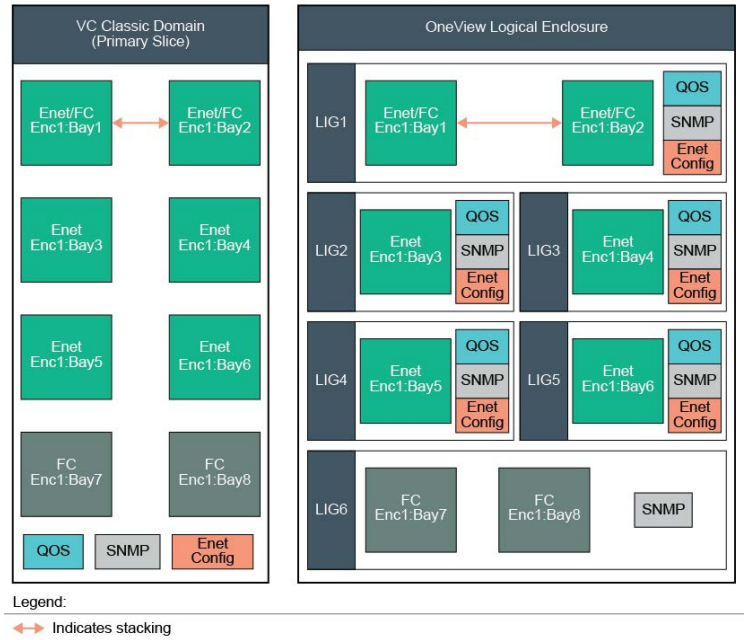
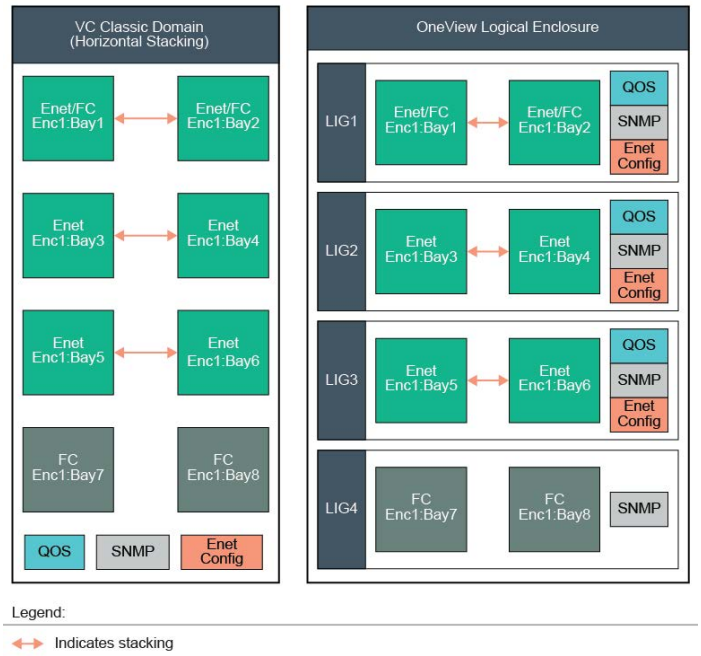


Figura 17 Migración de apilamiento horizontal de Virtual Connect Manager a HPE OneView



Usted migra un receptáculo gestionado mediante VCM a un grupo de receptáculos nuevo o existente.

- **Grupo de receptáculos nuevo** — los grupos de interconexiones lógicas se crean en función de la configuración de apilamiento de Virtual Connect. Las redes y los conjuntos de enlaces ascendentes se copian en los grupos de interconexiones lógicas creados recientemente.

  Para horizontal o principal-sección:

  - Las redes Ethernet se copian en todos los grupos de interconexiones lógicas que contienen interconexiones de Ethernet. Los conjuntos de enlaces ascendentes se copian en todos los grupos de interconexiones lógicas. Los puertos de conjuntos de enlaces ascendentes solo se copian en el conjunto de enlaces ascendentes creado dentro de los grupos de interconexiones lógicas que contienen dichos puertos.

    Todos los ajustes de Ethernet tales como QoS se migran a los grupos de interconexiones lógicas de Ethernet configurados recientemente.

  - Las redes FCoE se agregan al conjunto de enlaces ascendentes creado en el grupo de interconexiones lógicas que contiene los puertos de los conjuntos de enlaces ascendentes asociados.

  - Las estructuras de Virtual Connect se copian como conjuntos de enlaces ascendentes de Fibre Channel dentro del grupo de interconexiones lógicas que contienen los puertos de enlaces ascendentes de estructuras. También se crea una red de Fibre Channel asociada.

  - Las configuraciones de SNMP se migran a todos los grupos de interconexiones lógicas, incluido el grupo de interconexiones lógicas de Fibre Channel.

- **Grupo de receptáculos existente** — los grupos de interconexiones lógicas de HPE OneView existentes deben coincidir con el tipo de interconexión y compartimento exacto de la configuración de Virtual Connect. En caso contrario, se producirá un error de compatibilidad y la migración se bloqueará.

  Por ejemplo, si un receptáculo gestionado por VCM es principal-sección y los compartimentos 1, 2, 3 y 4 se llenan con módulos HPE Virtual Connect FlexFabric 10Gb de 24 puertos, si HPE OneView no tiene un grupo de receptáculos que coincida con los grupos de

interconexiones lógicas definidas con el mismo tipo de interconexión (módulo HPE Virtual Connect FlexFabric 10Gb de 24 puertos) para los cuatro compartimentos, se produce un error. Además, los compartimentos 1 y 2 deben configurarse conjuntamente en un grupo de interconexiones lógicas y los compartimentos 3 y 4 deben configurarse en dos grupos de interconexiones lógicas diferentes (como vimos en Figura 16: «Migración de apilamiento principal-sección de Virtual Connect Manager a HPE OneView»).

Los atributos aplicados a los grupos de interconexiones lógicas tales como conjuntos de enlaces ascendentes, configuración Ethernet y configuraciones SNMP también deben coincidir; en caso contrario, se producirán errores.

Más información

«Sobre problemas de bloqueo durante la migración»

17.2.2.4.3 Sobre la configuración de VCM que no se migrará

No se migrarán los siguientes ajustes de VCM a HPE OneView.

- Información específica de cuentas de usuario, como por ejemplo, los certificados, las cuentas de usuario, LDAP, RADIUS, TACACS +, el tiempo de espera de sesión y las configuraciones de roles de usuario
- Configuración de la supervisión de puertos. Después de la migración, la supervisión de puertos puede configurarse por separado en cada interconexión lógica. Para obtener más información, consulte Configure a port to monitor network traffic (Configuración de un puerto para supervisar el tráfico de red) en la ayuda en línea.
- Los pools de direcciones de MAC, WWN y números de serie definidos en le VCM. HPE OneView migra las MAC, WWN y números de serie que forman parte de los perfiles asignados.

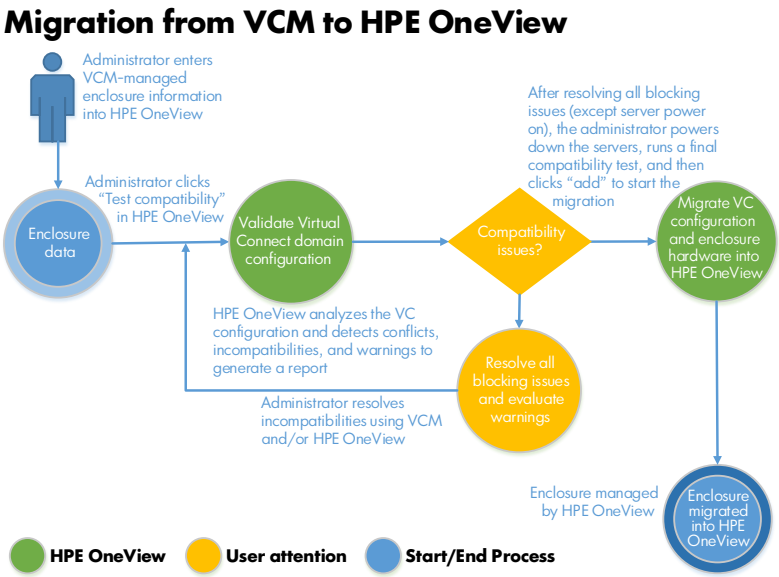
NOTA: Las direcciones nuevas ubicadas en HPE OneView tras la migración proceden de los pools de direcciones de HPE OneView. Un administrador puede definir manualmente intervalos personalizados en HPE OneView para coincidir con aquellos definidos en el VCM para seguir asignando para dicho intervalo.

17.2.2.4.4 Antes de migrar receptáculos c7000

Antes de iniciar el proceso de migración, planifíquela. Consulte “Planning for enclosure migration from VCM into HPE OneView” (Planificación de la migración de receptáculos de VCM a HPE OneView) en la ***Guía de usuario de HPE OneView*** para asegurarse de que se cumplen determinados requisitos, tales como la copia de seguridad de la configuración del VCM.

El proceso de migración se ilustra en la figura siguiente. Para obtener más información, consulte «Migración de un receptáculo c7000 actualmente gestionado por VCM».

Figura 18 Proceso de migración



Consulte Capítulo 9, «Planificación de la migración de receptáculos de VCM a HPE OneView» para obtener sugerencias sobre la preparación de la configuración para la migración.

Funciones automatizadas

Una vez que se han corregido los problemas de compatibilidad y se ha llevado a cabo la migración, HPE OneView valida la información de configuración y, a continuación, realiza automáticamente estas funciones:

- Crea redes y conjuntos de redes.
- Crea un grupo de interconexiones lógicas o utiliza un grupo existente.
- Crea un grupo de receptáculos o utiliza un grupo existente.
- Crea perfiles de servidor sin asignar a servidores pero asociados a tipos de hardware de servidor. Los perfiles de servidor recién creados por HPE OneView conservan las mismas direcciones MAC y WWN que se utilizaban en los perfiles de servidor correspondientes de VCM.
- Importa el receptáculo y agrega recursos físicos tales como interconexiones y servidores.
- Asigna los perfiles de servidor.
- Para la migración en servicio, las interconexiones se vuelven a configurar secuencialmente durante la migración, sobrescribiendo la configuración del VCM con la configuración de HPE OneView. Con una configuración redundante, HPE OneView detecta la pérdida de conectividad para una interconexión y redirige el tráfico a una ruta alternativa.

Al final de la migración, el dominio de Virtual Connect deja de estar disponible en el VCM.

Para migrar un receptáculo, consulte “Migrate an enclosure managed by VCM (Migración de un receptáculo gestionado por VCM) en la ayuda en línea.

17.2.2.4.4.1 Acerca del firmware y la migración de receptáculos c7000

Antes de migrar el receptáculo, asegúrese de que el firmware tenga la versión mínima necesaria. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener más información. Al migrar receptáculos, la línea de base de firmware se establece automáticamente en `manage manually` (gestionar manualmente). La configuración del firmware de VCM se migra a HPE OneView.

HPE OneView no permite actualizaciones de firmware durante el proceso de migración del receptáculo.

Una vez que el receptáculo se migra a HPE OneView, es posible actualizar el firmware. Para obtener más información, consulte Best practices for firmware (Prácticas recomendadas para el firmware) y Update firmware for enclosures (Actualización del firmware de los receptáculos) en la ayuda de la interfaz de usuario.

17.2.2.4.5 Sobre problemas de bloqueo durante la migración

A continuación se incluye una lista parcial de las funciones de Virtual Connect que se consideran problemas de *bloqueo* debido a que no son compatibles con HPE OneView. También se pueden producir problemas de bloqueo cuando hay conflictos de configuración entre el dominio de Virtual Connect y el grupo de interconexiones lógicas de HPE OneView al que se va a migrar el dominio. HPE OneView comprueba estas funciones y bloquea la migración cuando encuentra estos problemas. Para resolver un problema, podría ser necesario deshabilitar una función de Virtual Connect, cambiar una configuración de Virtual Connect o, en algunos casos, cambiar el grupo de interconexiones lógicas de HPE OneView.

Si se necesita una función en su entorno y el receptáculo contiene blades de servidor ProLiant G6 o posteriores, puede que le convenga supervisar el receptáculo. Consulte «Acerca de los receptáculos c7000 supervisados».

NOTA: Es posible migrar a HPE OneView receptáculos gestionados por VCEM. Consulte «Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión» para obtener más información.

Problemas de bloqueo		
• SR-IOV avanzado[1] • Autoimplementación • Receptáculos c3000, blades de servidor ProLiant G1 hasta G6, blades de Integrity y blades de servidor de almacenamiento • Tipo de velocidad de conexión Ethernet, iSCSI y FCoE deshabilitada • Estándar federal para procesamiento de la información (FIPS 140–2)	• Filtros de multidifusión y conjuntos de filtros de IGMP • Más de 1000 redes definidas en el dominio de VC • Dominios de varios receptáculos apilados • Dominios parcialmente apilados[2] • Redes VLAN de servidor asignadas a redes VLAN alternativas	• SNMP v3 • Credenciales de gestión de almacenamiento • Conexiones de red Ethernet, iSCSI o FCoE sin asignar[2] • Velocidades de Fibre Channel no admitidas[2] • Varios iniciadores de FC de VCEM

[1] Problema de bloqueo por mezclar configuración automática y no automática para la migración en servicio. Sin embargo, para la migración sin conexión, la configuración se determina por defecto (las funciones virtuales se separan equitativamente entre todas las funciones físicas).

[2] Problema de bloqueo únicamente para la migración en servicio.

NOTA: En general, para las funciones que no son necesarias en su entorno, la desactivación de la función en VCM le permite migrar el receptáculo.

17.2.2.4.5.1 Sobre las conexiones del perfil de servidor del VCM sin asignar durante la migración

Una conexión de perfil de servidor del VCM sin asignar es una conexión sin una estructura o red especificada. Dentro del VCM existen cinco tipos de conexiones.

- Ethernet — Una o más redes Ethernet asignadas a la misma conexión de perfil de servidor.
- FCoE — Una red FCoE asociada con un conjunto de enlaces ascendentes. Las redes Ethernet y FCoE pueden compartir el mismo conjunto de enlaces ascendentes.

- SAN de FCoE FC — Una conexión FCoE asignada a una estructura SAN. Estas conexiones tienen una o más conexiones Fibre Channel nativas con los puertos de enlaces ascendentes que forman parte de la estructura SAN. Utilizan la función física FlexFabric 2 del adaptador.
- Fibre Channel nativa — Una conexión de adaptador Fibre Channel nativa con una interconexión Fibre Channel.
- iSCSI — Una red iSCSI, Ethernet o red iSCSI no compartida asociada con un conjunto de enlaces ascendentes. Las redes Ethernet e iSCSI pueden compartir el mismo conjunto de enlaces ascendentes.

HPE OneView no admite conexiones de perfil de servidor sin asignar, por lo que las conexiones no se migran y no se pueden recrear para el perfil de servidor migrado. Para las conexiones Fibre Channel nativas, aparece una advertencia de problema en el informe de compatibilidad. Para el resto de conexiones, en el informe de compatibilidad para migraciones en servicio aparece un problema de bloqueo.

La solución a las conexiones de perfil de servidor sin asignar depende del motivo de la existencia de la conexión sin asignar y de las ramificaciones a la configuración del sistema operativo si la conexión no se migra.

Más información

«Sobre problemas de bloqueo durante la migración»
«Migración de un receptáculo c7000 actualmente gestionado por VCM»

17.2.2.4.6 Sobre las confirmaciones de la migración

Algunos de los problemas que no se consideran problemas de bloqueo o advertencia para la migración del VCM aparecen como confirmaciones. Algunas confirmaciones hacen referencia a advertencia en el informe de compatibilidad. Sea como sea, las confirmaciones son instrucciones importantes que se deben seguir y confirmar antes de que empiece la migración. Las confirmaciones aparecen en la interfaz de usuario cuando todos los problemas de bloqueo se solucionan y se genera un informe de compatibilidad final. En la API de REST, las confirmaciones se devuelven en el atributo `confirmaciones`.

Para confirmaciones específicas, consulte lo siguiente:

- «Confirmación de la copia de seguridad de la confirmación del VCM»
- «Confirmación de la modificación de recursos»
- «Confirmación de la configuración de software y hardware redundante para la migración en servicio»
- «Confirmación de BIOS para la migración en servicio»
- «Confirmación de SR-IOV para la migración en servicio»
- «Confirmación del perfil de servidor»

17.2.2.4.6.1 Confirmación de la copia de seguridad de la confirmación del VCM

Compruebe que se haya obtenido una copia de seguridad de la configuración del VCM (incluido el resultado de `show config - includepoolinfo`) y que esté asegurada donde estará disponible en caso de que la migración del receptáculo no se complete. Si la configuración del VCM se tiene que devolver al control del Virtual Connect Manager, se utiliza la copia de seguridad. La copia de seguridad de la configuración del VCM se puede crear a través de la interfaz de usuario web del VCM o el VCMCLI.

Más información

Virtual Connect User Guide (Guía del usuario de Virtual Connect) en **http://www.hpe.com/info/virtualconnect/docs**

«Migración de un receptáculo c7000 actualmente gestionado por VCM»
«Sobre las confirmaciones de la migración»

17.2.2.4.6.2 Confirmación de la modificación de recursos

Si bien HPE OneView es completamente funcional durante una migración, no modifique los recursos de HPE OneView hasta que se complete la migración.

IMPORTANTE: Si se modifican los recursos de HPE OneView la migración puede fallar, dejando el receptáculo sin configuración y necesitando una recuperación para que pueda ser operativa. La migración se completa cuando la tarea en la pantalla HPE OneView Activities muestra `migration complete` (migración completa).

Por ejemplo, no edite las redes, los conjuntos de redes, los receptáculos lógicos, los grupos de interconexiones lógicas ni los perfiles de servidor de los receptáculos implicados en la integración. No realice otras actividades de mantenimiento tales como la alimentación del servidor, el reinicio del dispositivo o la actualización del firmware durante el proceso de migración.

Más información

«Migración de un receptáculo c7000 actualmente gestionado por VCM»
«Sobre las confirmaciones de la migración»

17.2.2.4.6.3 Confirmación de la configuración de software y hardware redundante para la migración en servicio

Para minimizar el impacto en las aplicaciones y los servicios durante una migración en servicio de HPE OneView, se necesitan configuraciones de hardware y software redundantes. El receptáculo completamente apilado debe configurarse en un anillo dual o una configuración de enlace de apilamiento vertical izquierda/derecha. Consulte las conexiones de apilamiento recomendadas en la ***Guía de instalación y configuración de HPE Virtual Connect para c-Class BladeSystem***.

Las interconexiones se vuelven a configurar secuencialmente durante la migración, sobrescribiendo la configuración del VCM con la configuración de HPE OneView. Como máximo, el almacenamiento se ve interrumpido para una interconexión única en cualquier momento durante la migración y el tráfico de red se ve interrumpido para los compartimentos de número par o impar en cualquier momento de la migración.

Configure conexiones de almacenamiento y red redundantes y proporcione conmutación por errores tales como vinculación de interfaz de red y controladoras de MPIO para que el tráfico de almacenamiento y red continúe para pasar un módulo del par mientras el otro módulo se reconfigura. Del mismo modo que en la actualización del firmware de una interconexión lógica, el sistema operativo del servidor detecta la pérdida de conectividad para el módulo de interconexiones y redirige el tráfico a la ruta alternativa.

Más información

«Migración de un receptáculo c7000 actualmente gestionado por VCM»
«Sobre las confirmaciones de la migración»

17.2.2.4.6.4 Confirmación de BIOS para la migración en servicio

En Virtual Connect Manager, los administradores pueden configurar configuraciones de arranque concretas (tales como arranque SAN o PXE) para las conexiones de perfil al tiempo que dejan la configuración `USE-BIOS` predeterminada en otras conexiones del mismo perfil. Tras la migración en servicio, el servidor sigue arrancando en función de los ajustes de arranque configurados. Aún así, la primera vez que el servidor se reinicia después de una migración en servicio, todas las conexiones del perfil configuradas para `USE-BIOS` se convierten a `not bootable` para coincidir con las convenciones de HPE OneView.

Más información

«Migración de un receptáculo c7000 actualmente gestionado por VCM»
«Sobre las confirmaciones de la migración»

17.2.2.4.6.5 Confirmación de SR-IOV para la migración en servicio

En el VCM, los administradores pueden especificar la distribución de las funciones virtuales de SR-IOV (Virtualización E/S de raíz única) en los FlexNIC de los perfiles de servidor. HPE OneView distribuye las funciones virtuales de manera equitativa por todos los FlexNIC del perfil de servidor. Cuando la configuración de la conexión SR-IOV en el dominio de Virtual Connect es `default (por defecto)`, el VCM asigna todas las funciones virtuales de SR-IOV al tercer FlexNIC del puerto. Cuando se migra de VCM a HPE OneView, esta redistribución tiene efecto la primera vez que el servidor se reinicia después de la migración a HPE OneView. La redistribución provoca que el servidor vuelva a enumerar los dispositivos PCI, lo que puede interrumpir el tráfico de red del servidor, como resultado del nuevo orden de los dispositivos. Revise y compruebe la configuración de red de los hipervisores y las máquinas virtuales invitadas en el sistema operativo del host, en caso necesario, para no interrumpir su conectividad de red.

Más información

«Migración de un receptáculo c7000 actualmente gestionado por VCM»
«Sobre las confirmaciones de la migración»

17.2.2.4.6.6 Confirmación del perfil de servidor

Los perfiles de servidor de Virtual Connect que no se asignan a hardware de servidor no se migran a HPE OneView. Para migrar estos perfiles de servidor:

- Asígnelos al hardware de servidor, si estuviera disponible.
- Vuelva a crear manualmente los perfiles de servidor en HPE OneView tras la migración. Consulte «Realice las tareas posteriores a la migración».

Más información

«Migración de un receptáculo c7000 actualmente gestionado por VCM»
«Sobre las confirmaciones de la migración»

17.2.2.4.7 Prácticas recomendadas para migran un receptáculo de VCM a HPE OneView.

La siguiente lista engloba algunas prácticas recomendadas para guiarle durante una migración de VCM a HPE OneView.

- Planifique la migración.
- Revise las opciones de migración sin conexión o en servicio.
- Entienda los problemas de bloqueo.
- Entienda las confirmaciones.
- Obtenga las licencias de HPE OneView Advanced necesarias para los servidores migrados.
- Si se utiliza la secuencia de comandos VCMCLI, realice la transición al módulo HPE PowerShell en **http://hewlettpackard.github.io/POSH-HPOneView**.
- Para la migración en servicio, programe una ventana de mantenimiento después de la migración en la que los servidores puedan reiniciarse y se pueden realizar los ajustes necesarios para dar cabida a cualquier configuración de SR-IOV actualizada.

Más información

«Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión»

17.2.2.5 Acerca de los receptáculos c7000 no gestionados y no admitidos

Receptáculos no gestionados

Un receptáculo no gestionado es aquel que HPE OneView no gestiona ni supervisa actualmente. Consulte «Acerca de los equipos no gestionados» para obtener más información acerca de los dispositivos no gestionados.

Un firmware que no cumpla con los requisitos mínimos puede impedir la gestión de un receptáculo. Para incluir el receptáculo en la gestión, actualice el firmware.

Receptáculos no admitidos

Un receptáculo no admitido es aquel que no puede ser gestionado por HPE OneView. Sin embargo, sí pueden instalarse receptáculos no admitidos en bastidores. La adición a HPE OneView de receptáculos no admitidos le permite hacerse una idea del espacio físico que ocupa un receptáculo en un bastidor para fines de planificación o inventario. Si tiene un receptáculo con blades de servidor ProLiant G6, considere la posibilidad de añadirlo como supervisado en lugar de no admitido. Consulte «Acerca de los receptáculos c7000 supervisados». Los blades de servidor ProLiant G7 o posteriores pueden gestionarse en HPE OneView. Consulte «Acerca de los receptáculos c7000 gestionados».

HPE OneView muestra información básica acerca de los receptáculos no admitidos, como el nombre del modelo, el nombre del Onboard Administrator o el número de OA que contiene el receptáculo.

Puede especificar la alimentación máxima del receptáculo no admitido, que le permite definir su capacidad de alimentación y permite que HPE OneView genere alertas cuando se alcanza su capacidad máxima.

17.2.2.6 Conectividad y sincronización con HPE OneView

HPE OneView supervisa el estado de conectividad de los receptáculos. Si HPE OneView pierde la conectividad con un receptáculo, se muestra una notificación hasta que se restaura la conectividad. HPE OneView intenta resolver los problemas de conectividad y borra la alerta automáticamente, pero si no lo consigue, se debe resolver el problema y actualizar manualmente el receptáculo para sincronizarlo.

HPE OneView también se asegura de que los receptáculos permanecen sincronizados con los cambios que se producen en el hardware y en los parámetros de configuración. Sin embargo, algunos cambios realizados en los receptáculos desde fuera de HPE OneView (desde el OA, por ejemplo), pueden hacer que los receptáculos dejen de estar sincronizados. Puede que tenga que actualizar manualmente los receptáculos que pierdan la sincronización con HPE OneView.

Para sincronizar manualmente un receptáculo con HPE OneView, actualícelo en la pantalla **Enclosures** (Receptáculos). Si se actualiza un receptáculo, se actualizarán todos los equipos que contiene. Consulte la ayuda en línea de la pantalla **Enclosures** (Receptáculos) para obtener más información.

17.2.3 Requisitos previos para incluir un receptáculo c7000 en HPE OneView

Elemento	Requisito
Modelo de receptáculo	El receptáculo debe ser un modelo compatible según la ***Matriz de compatibilidad de HPE OneView***. El receptáculo debe estar encendido.
Hardware de servidor	El hardware de servidor instalado en un receptáculo debe cumplir los requisitos previos indicados en «Requisitos previos para incluir el hardware de servidor en un dispositivo».
Firmware	El firmware del receptáculo debe tener al menos la versión de firmware mínima compatible que se indica en la ***Matriz de compatibilidad de HPE OneView***.

Elemento	Requisito
Licencias	Es necesaria una licencia de HPE OneView para gestionar servidores. Consulte «Acerca de las licencias».
Onboard Administrator	Los OA principal y en espera deben estar configurados con un nombre de host o una dirección IP, y HPE OneView debe tener acceso a ellos. Durante la inclusión de un OA en la gestión, se agrega una cuenta de usuario local, por lo que el OA debe configurarse para que admita cuentas de usuario locales. Si el receptáculo tiene dos Onboard Administrators, ambos deben tener la misma versión de firmware.
Direcciones IP	Se requiere la configuración de IPv4 o IPv6.
Dirección IP de iLO	Los iLO del hardware de servidor deben configurarse con direcciones IP, bien de forma automática con direcciones DHCP o manualmente con direcciones especificadas mediante EBIPA (Enclosure Bay IP Addressing). HPE OneView debe ser capaz de conectarse a los iLO del hardware de servidor.
Interconexiones	Las interconexiones se deben configurar con direcciones IP, bien de forma automática con direcciones DHCP o manualmente con direcciones especificadas mediante EBIPA. • Si tiene una interconexión HPE Virtual Connect Fibre Channel, consulte la sección sobre cómo actualizar el firmware de las interconexiones lógicas en la ayuda en línea para determinar si necesita actualizar el firmware. • Si tiene una interconexión HPE Virtual Connect FlexFabric–20/40 F8, consulte en la sección «Sobre el módulo de interconexión Virtual Connect FlexFabric–20/40 F8» la cantidad máxima de los módulos recomendados por receptáculo.
Puertos abiertos	Los siguientes puertos deben estar abiertos entre HPE OneView y el receptáculo: • TCP 80, 443 • UDP 123, 161, 162

17.2.4 Lista de comprobación: Conexión de un servidor a una red del centro de datos

Los elementos de configuración siguientes son necesarios para que un blade de servidor se conecte a una red del centro de datos. El servidor debe tener una tarjeta intermedia de conexión de red en una ranura correspondiente a la ubicación de las interconexiones de Virtual Connect del receptáculo.

Requisito de configuración	¿Por qué es necesario?
Se debe haber definido un grupo de interconexiones lógicas	Un grupo de interconexiones lógicas define las configuraciones estándar que deben utilizarse para las interconexiones del receptáculo. Determine si desea definir uno o varios grupos de interconexiones lógicas para el receptáculo. Consulte «Acerca de la configuración de varios grupos de interconexiones lógicas en un grupo de receptáculos».
Se debe haber agregado al menos un conjunto de enlaces ascendentes al grupo de interconexiones lógicas, con una red y un puerto de enlace ascendente como mínimo	El conjunto de enlaces ascendentes determina las redes del centro de datos que pueden enviar tráfico por cada uno de los puertos de enlace ascendente físicos. Define las redes a las que se debe tener acceso desde esta interconexión lógica y qué puertos de enlace ascendente pueden aceptar tráfico de qué redes.
Debe haberse definido un grupo de receptáculos y debe estar asociado a uno o varios grupos de interconexiones lógicas	El grupo de receptáculos especifica una configuración estándar para todos los receptáculos que forman parte de él e identifica los grupos de interconexiones lógicas que le pertenecen. El grupo de receptáculos define las configuraciones de las interconexiones lógicas del receptáculo físico a través de los grupos de interconexiones lógicas.
El receptáculo debe pertenecer a un receptáculo lógico	El receptáculo lógico identifica el grupo de receptáculos al que pertenece el receptáculo y las interconexiones lógicas y los grupos de interconexiones lógicas asociados.

Requisito de configuración	¿Por qué es necesario?
El perfil de servidor debe asignarse al hardware de servidor	El hardware de servidor proporciona las conexiones físicas con al menos una interconexión que forma parte de la interconexión lógica.
El perfil de servidor debe tener al menos una conexión, que debe especificar una red o un conjunto de redes	No tiene que conocer la configuración de hardware, pero tiene que elegir una red o un conjunto de redes disponible para especificar las redes que va a utilizar el servidor.

17.2.5 Adición de un receptáculo c7000

Al agregar un receptáculo, se incluyen en la gestión el receptáculo, el hardware de servidor y las interconexiones.

Para agregar un receptáculo c7000, proporcione su dirección IP o nombre de host, junto con las credenciales del OA.

17.2.6 Adición de un receptáculo c7000 para supervisar el hardware

Puede añadir receptáculos al inventario y supervisar el hardware. Para obtener más información sobre los receptáculos supervisados, consulte «Acerca de los receptáculos c7000 supervisados».

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores.

Adición de un receptáculo para supervisar el hardware

1. En el menú principal, seleccione **Enclosures** (Receptáculos) y realice una de las acciones siguientes:
   - Haga clic en **+ Add enclosure** (+ Agregar receptáculo) en el panel principal.
   - Seleccione **Actions→Add** (Acciones > Agregar).
2. Seleccione **Add enclosure for monitoring** (Agregar el receptáculo para la supervisión).
3. Introduzca los datos solicitados en la pantalla.
4. Elija **Add** (Agregar) o **Add +** (Agregar +).

   Si tiene que agregar más receptáculos, puede agregar el siguiente inmediatamente; no es necesario que espere a que concluya la última acción Add Enclosure (Agregar receptáculo) antes de comenzar la siguiente.
5. Compruebe que el receptáculo se ha agregado en el panel principal.

17.2.7 Migración de un receptáculo c7000 actualmente gestionado por VCM

La siguiente información describe cómo un receptáculo gestionado por Virtual Connect Manager (VCM) se puede migrar a HPE OneView a través de la interfaz de usuario.

17.2.7.1 Requisitos previos

- Privilegios necesarios: administrador de infraestructuras de HPE OneView, administrador de Onboard Administrator y administrador del dominio de VCM.
- Credenciales de OA y de VCM, así como la dirección IP del OA del receptáculo.
- Para los receptáculos gestionados por VCEM: las credenciales de VCEM para eliminar el dominio de Virtual Connect del grupo de dominios mediante la interfaz web de VCEM o el módulo de HPE PowerShell. Consulte «Preparación de un receptáculo de VCEM para la migración a HPE OneView» para obtener más información.
- Copia de seguridad y garantía de la configuración del VCM (incluido el resultado de `show config -includepoolinfo`). Consulte «Confirmación de la copia de seguridad de la confirmación del VCM» para obtener más información.

- Consulte la ***Matriz de compatibilidad de HPE OneView*** y compruebe que el receptáculo contiene servidores, módulos de interconexión y tarjetas intermedias compatibles.
- Asigne perfiles de servidor antes de la migración o vuelva a crear los perfiles de servidor después de la migración, si corresponde. Consulte «Confirmación del perfil de servidor» para obtener más información.
- Compruebe la conectividad de red con OA y los iLO en el dominio de Virtual Connect.
- Asegúrese de que todos los módulos de interconexión se encuentran en el receptáculo y están encendidos.

17.2.7.2 Migración de un receptáculo gestionado por VCM

1. En el menú principal, seleccione **Enclosures** (Receptáculos) y realice una de las acciones siguientes:
   - Haga clic en **+ Add enclosure** (+ Agregar receptáculo) en el panel principal.
   - Seleccione **Actions→Add** (Acciones > Agregar).
2. Seleccione **Add enclosure and migrate Virtual Connect domain** (Agregar receptáculo y migrar el dominio de Virtual Connect).
3. Introduzca la siguiente información:
   - Nombre de host o dirección IP del OA del receptáculo de Virtual Connect
   - Sus credenciales del OA (nombre de usuario y contraseña)
4. Introduzca los datos solicitados en la pantalla.

   NOTA: Para migrar a un grupo de receptáculos nuevo, seleccione **Create new enclosure group** (Crear nuevo grupo de receptáculos).

   Para migrar a un grupo de receptáculos existente, seleccione uno en la lista de grupos de receptáculos.

5. Haga clic en **Test compatibility** (Probar compatibilidad).

   Se muestra un resumen de informe debajo de **Migration Details** (Detalles de la migración).
6. ¿El resumen indica errores?
   a. Sí. Haga clic en **migration report** (informe de la migración) para ver y solucionar todos los problemas de bloqueo.
   b. No. Revise todas las confirmaciones.

      Todas las confirmaciones deben leerse completamente (haciendo clic en todos los enlaces para obtener más información cuando corresponda). Cuando haya entendido las implicaciones, marque todas las confirmaciones para proceder con la migración.
7. ¿Es una migración sin conexión?
   a. Sí, apague los servidores del receptáculo que está en proceso de migración.
   b. No, continúe con el paso siguiente.
8. ¿Desea migrar otro receptáculo?
   a. Sí. Haga clic en **Add+** (Agregar+).

      La migración del receptáculo actual empieza. Cuando los recursos de HPE OneView (grupo de receptáculos, grupo de interconexiones lógicas, redes, conjuntos de redes, tipos de hardware de servidor y perfiles de servidor) se hayan creado para el receptáculo actual, la pantalla **Add Enclosure** (Agregar receptáculo) le pedirá que agregue la dirección IP del OA del siguiente receptáculo.

NOTA: Si se ha alcanzado el número máximo de cuatro migraciones simultáneas, aparecerá un error que le indicará que espera a que el número de migraciones sea menor de cuatro.

b. No. Haga clic en **Agregar**.

La migración del receptáculo actual empieza y la pantalla **Activities** (Actividades) aparece para mostrar las tareas de migración.

Si la migración tiene éxito, la tarea de migración aparece como `Completed` (Completada). Si no es así, utilice la solución propuesta. Consulte «La migración no se realiza» para obtener más información.

9. «Realice las tareas posteriores a la migración».

17.2.7.3 Migración de un receptáculo de VCM mediante las API de REST

1. Determine si ya hay una migración en curso.

   `GET /rest/migratable-vc-domains`

   Se devuelve un conjunto de informes de compatibilidad junto con el número de migraciones en curso de manera simultánea y la posibilidad de crear un informe de compatibilidad o migrar un receptáculo mientras hay otras operaciones en curso. El `migratabilityState` debe ser **MigrationValid** para continuar.

2. Valide la configuración del receptáculo.

   `POST /rest/migratable-vc-domains`

   - Para el grupo de receptáculos, realice una de las acciones siguientes:
     - Si desea migrar el receptáculo a un grupo de receptáculos existente, utilice `enclosureGroupUri`.
     - Si desea migrar el receptáculo a un grupo de receptáculos nuevo, el nombre del grupo de receptáculos se genera automáticamente a partir del número de serie.

   Se devuelve un `tasks/{id}` que identifica el informe de compatibilidad.

   NOTA: `GET /rest/tasks/{id}`

   Una vez completada la tarea, se devuelve un URI `/rest/migratable-vc-domains/{id}`.

3. Recupere un informe de compatibilidad con el URI `/rest/migratable-vc-domains/{id}` obtenido en el paso 2.

   `GET /rest/migratable-vc-domains{id}`

4. ¿El informe indica errores?
   a. Sí, solucione los errores de compatibilidad. Repita el paso 3 hasta que se resuelvan todos los problemas de bloqueo.
   b. No, continúe con el paso siguiente.
5. ¿Es una migración sin conexión?
   a. Sí, apague los servidores del receptáculo que está en proceso de migración y cree un informe de compatibilidad final.
   b. No, cree un informe de compatibilidad final.
6. Responda a las confirmaciones e importe el receptáculo de VC.

   `PUT /rest/migratable-vc-domains/{id}`

   Incluya `migrationState` configurado como **Migrated** (Migrado) y `AcknowledgementKey` para cada confirmación.

La migración del receptáculo actual empieza.

7. ¿Desea migrar otro receptáculo?
   a. Sí. Continúe con el paso 1.
   b. No, continúe con el paso siguiente.
8. Compruebe la finalización de las migraciones.

   `GET /rest/migratable-vc-domains`

   `migrationSubState` aparece como **Completed** (Completado). Si no es así, utilice la solución propuesta.
9. «Realice las tareas posteriores a la migración».

17.2.7.4 Realice las tareas posteriores a la migración

1. ¿La migración fue una migración sin conexión?
   a. Sí, encienda los servidores del receptáculo migrado.
   b. No, continúe con el paso siguiente.
2. Opcional: vuelva a crear los perfiles de servidor en HPE OneView, si los perfiles de servidor no se asignaron a un hardware de servidor antes de la migración.
   a. mediante la información de VCMCLI `show config –includepoolinfo` capturada antes de la migración.
   b. Escriba el número de serie, MAC, WWN, información de UUID como “usuario especificado” para mantener los mismos valores en HPE OneView presentes en el perfil de servidor de VCM.
3. Realice estas prácticas recomendadas:
   a. Realice una copia de seguridad de la nueva configuración en HPE OneView.
   b. Compruebe la conectividad de la red y el almacenamiento.
   c. Programe un reinicio en caso de que una de las confirmaciones, por ejemplo una configuración de función virtual de SR-IOV, indique un cambio que afectaría al funcionamiento.

   NOTA: Durante una migración en servicio, algunos cambios no tienen efecto hasta que los servidores se reinician por primera vez después de una migración.

17.2.7.5 Solución de problemas de compatibilidad

La herramienta de migración detecta si las funciones y el hardware de un receptáculo gestionado por VCM son compatibles con HPE OneView. Cada problema detectado se agrupa en una categoría, por ejemplo, hardware, dominio, grupo de interconexiones lógicas o perfil de servidor para identificar la parte del dominio de Virtual Connect o del sistema HPE OneView que se ve afectada.

Solución de problemas de compatibilidad

1. Revise cada problema y la solución recomendada.

   NOTA: Si realiza una migración sin conexión, solucione todos los problemas relacionados con la falta de alimentación antes de apagar el servidor para limitar el tiempo de inactividad de la operación.

   a. Evalúe las advertencias para determinar si es necesario realizar alguna acción.

      Si el mensaje de advertencia indica que el problema va a afectar al uso de la configuración, intervenga. En caso contrario, puede hacer caso omiso del mensaje de advertencia.

b. Resuelva todos los problemas de bloqueo de la migración modificando la configuración en VCM o en HPE OneView.

   Para resolver un problema, puede ser necesario deshabilitar una función de Virtual Connect, cambiar una configuración de Virtual Connect o, en algunos casos, cambiar el grupo de interconexiones lógicas de HPE OneView.

   Por ejemplo, si se produce un error de coincidencia con los conjuntos de enlaces ascendentes y uno ellos ya existe en HPE OneView y se van a migrar 10 receptáculos con la misma configuración al mismo grupo de receptáculos, actualice el conjunto de enlaces ascendentes en HPE OneView.

2. Vuelva a ejecutar el informe de prueba de compatibilidad hasta que estén resueltos todos los problemas de bloqueo.
3. Continúe con el proceso de migración.

Más información

«Sobre problemas de bloqueo durante la migración»
«Acerca de la migración de receptáculos c7000 gestionados por otros sistemas de gestión»

17.2.8 Preparación de un receptáculo de VCEM para la migración a HPE OneView

Es posible migrar un receptáculo gestionado por Virtual Connect Enterprise Manager (VCEM) a HPE OneView. El dominio de Virtual Connect del receptáculo debe quitarse del grupo de dominios de Virtual Connect antes de iniciar el proceso de migración. Para quitar el dominio de Virtual Connect, utilice una de las opciones siguientes:

Opción 1: Utilice la GUI de VCEM

1. En primer lugar, quite los dominios de Virtual Connect del grupo de dominios de Virtual Connect mediante la interfaz web de VCEM. VCEM marca las direcciones MAC y WWN asignadas a los perfiles del dominio como "Externas". De esta forma, VCEM se asegura de que no volverá a utilizar esas direcciones en el futuro.

   El receptáculo está gestionado por VCM.

   NOTA: Los intervalos de VCM, incluso si proceden de un grupo de dominios de VCEM, no se migrarán. Cada una de las direcciones MAC/WWN de cada conexión del perfil se utilizará como un ID definido por el usuario en HPE OneView. En el futuro, las direcciones nuevas se asignarán desde los pools de direcciones de HPE OneView.

2. Siga el proceso de migración de VCM que se explica en «Antes de migrar receptáculos c7000».

Opción 2: Utilice el módulo de HPE PowerShell

Existe un módulo de HPE PowerShell para automatizar el proceso descrito en la opción 1.

1. Descargue la biblioteca de HPE PowerShell desde **http://hewlettpackard.github.io/POSH-HPOneView/**.
2. Desde el módulo de HPE PowerShell, ejecute el comando `Invoke-HPOVVcmMigration`. Para obtener más información, consulte la documentación de HPE PowerShell.
3. Siga el proceso de migración de VCM que se explica en «Antes de migrar receptáculos c7000».

17.2.9 Efectos de la gestión de un receptáculo c7000

Cuando HPE OneView está gestionando un receptáculo, este se configura como sigue:

- Se crea una cuenta de gestión.
- Se activa SNMP y el dispositivo se añade como destino de captura SNMP.

- Se activa NTP (Network Time Protocol) y el dispositivo se convierte en la fuente de tiempo NTP.
- El intervalo de sondeo predeterminado de NTP se establece en 8 horas.
- Se instala un certificado del dispositivo para permitir las operaciones de inicio de sesión único.
- La gestión del firmware del receptáculo está desactivada (salvo para los receptáculos supervisados).
- Se desactiva Virtual Connect Manager en las interconexiones de Virtual Connect de este receptáculo.
- Cuando se agrega un receptáculo con un SPP, el firmware de la interconexión y el Onboard Administrator (OA) se actualizan para coincidir con la versión en el SPP. La línea de base también se configura en cada una de las interconexiones lógicas del receptáculo; tal y como aparece en la ***Matriz de compatibilidad de HPE OneView*** (a excepción de los receptáculos supervisados).

17.3 Gestión de grupos de receptáculos

17.3.1 Tareas para los grupos de receptáculos

La ayuda en línea de HPE OneView proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Crear un grupo de receptáculos
- Editar un grupo de receptáculos.
- Eliminar un grupo de receptáculos.

17.3.2 Acerca de los grupos de receptáculos

Un grupo de receptáculos es una plantilla que define una configuración coherente para un receptáculo lógico. La conectividad de red de un grupo de receptáculos se define mediante los grupos de interconexiones lógicas asociados al grupo de receptáculos.

17.3.2.1 Grupos de receptáculos y grupos de interconexiones lógicas

- Un grupo de interconexiones lógicas asignado a un compartimento dentro de un grupo de receptáculos debe tener ese compartimento ocupado dentro del grupo de interconexiones lógicas.
- Todos los compartimentos ocupados de un grupo de interconexiones lógicas deben estar asignado al grupo de receptáculos. Por ejemplo, un grupo de interconexiones lógicas que tenga los compartimentos 1 y 2 ocupados debe asignarse a los compartimentos 1 y 2 del grupo de receptáculos para que pueda crearse el grupo de receptáculos.

17.3.3 Creación de un grupo de receptáculos

Un grupo de receptáculos es un recurso lógico que define una configuración coherente para un receptáculo que compone un receptáculo lógico. La conectividad de red de un grupo de receptáculos se define mediante los grupos de interconexiones lógicas asociados al grupo de receptáculos.

17.3.3.1 Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores
- Como mínimo un grupo de interconexiones lógicas creado

17.3.3.2 Cómo crear un grupo de receptáculos

1. En el menú principal, seleccione **Enclosure Groups** (Grupos de receptáculos) y, a continuación:
   - Seleccione **Actions→Create** (Acciones > Crear).
   - Haga clic en **Create enclosure group** (Crear grupo de receptáculos).
2. Especifique un nombre exclusivo para un grupo de receptáculos nuevo.
3. Escriba los datos solicitados en la pantalla. Consulte la información en la pantalla **Enclosure Groups** (Grupos de receptáculos) en la ayuda en línea, si necesita ayuda con las entradas.
4. Opcional. Especifique una secuencia de comandos de configuración. Las secuencias de comandos de configuración de receptáculos simplifican la implementación de receptáculos mediante la creación de una configuración coherente y eliminan la necesidad de configurar manualmente un receptáculo a través de su OA (Onboard Administrator). Para obtener más información, consulte Configure an enclosure with an OA configuration script (Configuración de un receptáculo con una secuencia de comandos de configuración de OA) en la ayuda en línea.
5. Haga clic en **Create** (Crear) para crear el grupo de receptáculos, o haga clic en **Create +** (Crear +) para crear varios grupos de receptáculos.
6. Compruebe que el grupo de receptáculos se ha agregado; para ello, asegúrese de que se muestra en el panel principal.

Más información

«Acerca de los grupos de receptáculos»

17.4 Gestión de receptáculos lógicos

17.4.1 Tareas para los receptáculos lógicos

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Crear un receptáculo lógico
- Editar un receptáculo lógico
- Eliminar un receptáculo lógico
- Actualizar el firmware desde un receptáculo lógico
- Incluir en la gestión un receptáculo no gestionado con firmware no válido
- Actualizar el receptáculo lógico desde el grupo de receptáculos
- Volver a aplicar la configuración del receptáculo lógico
- Configurar un receptáculo con una secuencia de comandos de configuración de OA
- Crear un volcado de soporte de un receptáculo lógico

17.4.2 Acerca de los receptáculos lógicos

Un receptáculo lógico representa una vista lógica de un único receptáculo con un grupo de receptáculos que actúa como plantilla. Si la configuración prevista en el receptáculo lógico no coincide con la configuración real de los receptáculos, el receptáculo lógico pasa a ser incoherente. Utilice la pantalla **Logical Enclosures** (Receptáculos lógicos) para gestionar el firmware y las secuencias de comandos de configuración, crear un volcado de soporte y aplicar las actualizaciones realizadas desde la pantalla **Enclosure Groups** (Grupos de receptáculos) en los receptáculos del receptáculo lógico.

Cuando se agrega un receptáculo c7000, se crea automáticamente un receptáculo lógico.

17.4.2.1 Sobre receptáculos lógicos incoherentes

Un receptáculo lógico puede convertirse en incoherente en los casos siguientes:

- El grupo de receptáculos al que hace referencia el receptáculo lógico o la secuencia de comandos de configuración del receptáculo lógico se ha modificado. Por ejemplo, si se ha agregado, modificado o eliminado un grupo de interconexiones lógicas en el grupo de receptáculos.
- Las interconexiones lógicas son incoherentes con los grupos de interconexiones lógicas.
- Cualquier otro ajuste de configuración del receptáculo lógico es incoherente con el grupo de receptáculos.
- Faltan o sobran interconexiones lógicas con respecto al inventario de grupos de interconexiones lógicas del grupo de receptáculos.

Más información

“Update the logical enclosure configuration from the enclosure group” (Actualización de la configuración del receptáculo lógico desde el grupo de receptáculos) en la ayuda en línea

17.4.2.2 Sobre la actualización del firmware desde un receptáculo lógico

Puede actualizar el firmware de un receptáculo lógico en la infraestructura compartida, la infraestructura compartida y los perfiles o solo en los OA (Onboard Administrators), si los hay.

Cuando se actualiza el firmware de un receptáculo asociado con un receptáculo lógico, la selección de la línea de base de firmware configurada para el receptáculo lógico define la línea de base del receptáculo y de cada una de las interconexiones lógicas del receptáculo, así como del OA.

Las actualizaciones de firmware se pueden iniciar desde pantalla **Logical Enclosures** (Receptáculos lógicos). El firmware se actualiza en el orden siguiente:

1. Onboard Administrators
2. Interconexiones lógicas
3. Hardware de servidor y sus perfiles de servidor asociados

Más información

“Update the firmware in a logical enclosure” (Actualización del firmware en un receptáculo lógico) de la ayuda en línea

17.4.3 Creación de un receptáculo lógico

Un receptáculo lógico se crea automáticamente al agregar un receptáculo al dispositivo.

17.4.4 Actualización del firmware desde un receptáculo lógico

Puede actualizar el firmware de un receptáculo lógico en la infraestructura compartida, la infraestructura compartida y los perfiles o solo en los OA (Onboard Administrators), si los hay.

NOTA: Cuando haya una actualización del firmware del receptáculo lógico en curso, no inicie una actualización del firmware de una interconexión lógica que forme parte de dicho receptáculo lógico.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores
- Se han agregado uno o varios SPP al repositorio de firmware del dispositivo.

- Apague todos los servidores que no tengan perfiles.

Actualización del firmware desde un receptáculo lógico

1. En el menú principal, seleccione **Logical Enclosures** (Receptáculos lógicos).
2. En el panel principal, seleccione el receptáculo al que desea aplicar un lote de firmware.
3. Seleccione **Actions→Update firmware** (Acciones > Actualizar firmware).
4. Introduzca los datos solicitados en la pantalla. Consulte los detalles de la pantalla en la ayuda.
5. Haga clic en **OK** (Aceptar).

   A medida que avanza la actualización, si falla la actualización de cualquier componente, fallará la actualización del receptáculo lógico.
6. Compruebe que la nueva línea de base de firmware aparece en el panel de detalles de la pantalla **Logical Enclosures** (Receptáculos lógicos).

Más información

«Sobre la actualización del firmware desde un receptáculo lógico»

17.4.5 Creación de un archivo de volcado de soporte de un receptáculo lógico

Un archivo de volcado de soporte de receptáculo lógico incluye contenido de cada interconexión lógica miembro además del contenido del volcado de soporte del dispositivo. El lote completo de archivos se comprime y se cifra para su descarga. El volcado de soporte del receptáculo lógico consolidado se cifra como información de volcado de soporte de las interconexiones lógicas e incluye propiedad intelectual propiedad de HPE.

NOTA: Puede ver el contenido de un volcado de soporte de dispositivo sin cifrar si crea un archivo de volcado de soporte desde la pantalla **Settings: Appliance** (Configuración: dispositivo).

Si se le indica que cree un volcado de soporte a partir de más de un receptáculo lógico, vaya hasta la pantalla de cada receptáculo lógico de forma individual y cree un volcado de soporte. Para crear un volcado de soporte posterior, primero debe esperar a que cada volcado de soporte termine.

Por defecto, el volcado de soporte de receptáculo lógico incluye el volcado de soporte del dispositivo. Si se le indica que cree un volcado de soporte de receptáculo lógico que no contenga el volcado de soporte del dispositivo, deberá utilizar las API REST de receptáculo lógico. Para obtener más información, consulte la ayuda en línea sobre secuencias de comandos de la API de REST relacionada con los receptáculos lógicos.

Requisitos previos

- Un recurso de receptáculo lógico
- Cualquier rol de usuario puede crear un volcado de soporte

Creación de un volcado de soporte de un receptáculo lógico

1. En el menú principal **Logical Enclosures** (Receptáculos lógicos) y seleccione un receptáculo lógico.
2. Seleccione **Actions (Acciones)→Create logical enclosure support dump (Crear volcado de soporte de receptáculo lógico)**.
3. Haga clic en **Yes, create** (Sí, crear) para confirmar.

   Puede seguir realizando otras tareas mientras se crea el volcado de soporte en un segundo plano.

4. Cuando esta tarea acaba, el archivo comprimido de volcado de soporte se descarga en la carpeta de descarga predeterminada del navegador, o se le pide que indique dónde descargar el archivo.

   El nombre del archivo de volcado de soporte del receptáculo lógico tiene el formato *nombre_host*-LE-*nombre*-*fecha*-*hora*.sdmp.

5. Compruebe que el archivo comprimido esté en la ubicación de archivos especificada.
6. Póngase en contacto con el personal de asistencia técnica autorizado para obtener instrucciones sobre cómo proporcionar el archivo de volcado de soporte.

Más información

«Acerca del archivo de volcado de soporte»
«Acerca de los receptáculos lógicos»

17.5 Información adicional

- «Conceptos básicos sobre el modelo de recursos» (página 45)
- «Gestión de licencias» (página 193)

18 Gestión de firmware para los equipos gestionados

NOTA: En este capítulo se describe cómo gestionar el firmware de los equipos gestionados por el dispositivo. Para obtener información sobre cómo actualizar el firmware del dispositivo, consulte «Actualización del dispositivo» (página 321).

Un lote de firmware, también conocido como un HPE Service Pack para ProLiant (SPP), consta de un conjunto de lotes, un archivo ISO completo y seis ISO parciales divididas por familias de servidores HPE ProLiant y sistemas operativos. Un SPP es una colección completa de firmware y software del sistema que se han probado juntos como un único conjunto de soluciones que incluye controladores, agentes, utilidades y paquetes de firmware para servidores HPE ProLiant, controladoras, almacenamiento, blades de servidor y receptáculos. Cada paquete del SPP contiene Smart Update Manager (SUM), y componentes Smart de software y de firmware.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Firmware Bundles (Lotes de firmware)	`firmware-bundles`

18.1 Tareas para firmware

La ayuda en línea de HPE OneView proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar un lote de firmware al repositorio de firmware del dispositivo
- Crear un SPP personalizado.
- Ir a una versión anterior del firmware
- Establecer una línea de base del firmware para los dispositivos gestionados.
- Quitar un lote de firmware del repositorio de lotes de firmware.
- Actualización del firmware en dispositivos gestionados
- Ver el repositorio de firmware de los lotes de firmware para ver lo siguiente:
  - La lista de lotes de firmware disponibles en el repositorio
  - El contenido de un lote de firmware
  - El espacio de almacenamiento disponible para el repositorio

18.2 Acerca de los lotes de firmware

El dispositivo permite realizar la gestión de firmware de todo el centro de datos sin necesidad de descargar ni instalar ninguna herramienta adicional. Las funciones de gestión de firmware integradas en el dispositivo permiten definir líneas de base de firmware y llevar a cabo actualizaciones de firmware en muchos recursos. Cuando se agrega un recurso al dispositivo, este actualiza automáticamente el firmware del recurso a la versión mínima necesaria para que el dispositivo pueda gestionarlo o a la versión definida como línea de base. Consulte también «Acerca del firmware no admitido».

Un lote de firmware, también conocido como un Service Pack para ProLiant (SPP), es una colección completa de componentes de firmware y de software del sistema que se han probado conjuntamente como una única solución combinada que incluye controladores, agentes, utilidades

y paquetes de firmware. Los paquetes de firmware permiten actualizar el firmware de servidores HPE ProLiant, controladoras, almacenamiento, blades de servidor y receptáculos.

Es posible instalar por la fuerza una versión anterior de firmware del dispositivo, pero tenga en cuenta que, si lo hace, puede dar lugar a velocidades de instalación más lentas, y cabe la posibilidad de que el equipo no pueda utilizarse.

Repositorio de firmware

Un repositorio de firmware integrado permite cargar lotes de firmware del SPP y revisiones en el dispositivo e implementarlos en todo el entorno siguiendo las prácticas recomendadas. Puede ver las versiones y el contenido de los SPP del repositorio desde la pantalla **Firmware Bundles** (Lotes de firmware). Al seleccionar un lote de firmware se muestra su fecha de publicación, los idiomas y sistemas operativos que incluye, y los componentes del lote. La pantalla también muestra la cantidad de espacio de almacenamiento disponible para los lotes de firmware adicionales en el dispositivo. No se puede agregar un lote de firmware cuyo tamaño sea mayor que la cantidad de espacio disponible en el repositorio.

NOTA: Para asegurarse de que su hardware tiene el lote de firmware más reciente y más estable que aprovecha todas las funciones de gestión disponibles, descargue el lote de firmware más reciente en su dispositivo y agréguelo al repositorio de firmware.

HPE OneView admite las actualizaciones del firmware de servidor en paralelo 128 para Windows y Linux, y actualizaciones del firmware de servidor en paralelo 10 para ESXi.

Acerca de la aplicación de los SPP como líneas de base

Puede aplicar los SPP como líneas de base a receptáculos, interconexiones y perfiles de servidor, con lo que establecerá una versión deseada para el firmware y los controladores de los distintos equipos. Cuando descargue un SPP desde **http://www.hpe.com/info/spp** en el sistema local, cárguelo en el repositorio de lotes de firmware del dispositivo. Cada paquete del SPP contiene Smart Update Manager y componentes Smart de firmware. La gestión del firmware de todo el receptáculo se puede iniciar desde la pantalla **Enclosures** (Receptáculos). El firmware de las interconexiones lógicas se puede actualizar desde la pantalla **Logical Interconnects** (Interconexiones lógicas). En la pantalla **Server Profiles** (Perfiles de servidor), puede establecer la línea de base de firmware para el hardware de servidor asignado. El dispositivo identifica los problemas de compatibilidad de firmware, e indica los equipos que no están en el nivel de actualización establecido por la línea de base de firmware seleccionada.

Puede ampliar manualmente el disco virtual para aumentar el tamaño del repositorio de firmware de los 12 GB por defecto a 100 GB (se necesitan como mínimo 275 GB de espacio en disco en total). La mejor opción es ampliar el disco virtual durante la instalación del dispositivo. Para obtener más información, consulte la ***Guía de instalación de HPE OneView***.

Puede eliminar alguno o todos los SPP del repositorio de lotes de firmware. Sin embargo, Hewlett Packard Enterprise recomienda que tenga al menos un SPP disponible en todo momento debido a que es necesario un SPP cuando se agregan recursos al dispositivo que están por debajo de las versiones mínimas de firmware necesarias para supervisarlos o gestionarlos. Si desea eliminar un SPP, Hewlett Packard Enterprise recomienda que antes reasigne todos los recursos a otro SPP. Un SPP se asigna editando el perfil de servidor o el receptáculo y configurando el campo de la línea de base de firmware.

Para los receptáculos c7000, seleccione `Manage manually` (Gestionar manualmente) si desea gestionar el firmware mediante otra herramienta.

Acerca de la carga y el uso de revisiones

En ocasiones, Hewlett Packard Enterprise publica revisiones para los componentes entre las versiones principales del SPP. Hewlett Packard Enterprise le notificará que hay una revisión disponible para cargarla y le proporcionará información detallada sobre el SPP al que se aplica.

Deberá crear un SPP personalizado en HPE OneView mediante el SPP base y la revisión. Consulte “Upload a hotfix” (Carga de una revisión) en la **ayuda sobre secuencias de comandos de la API de REST** para obtener más información.

El nuevo SPP personalizado puede utilizarse para configurar la línea de base de los diversos recursos gestionados desde HPE OneView. Si una revisión está relacionada con un recurso gestionado que ya se encuentra en la línea de base, solo se aplica la revisión.

NOTA: Si el sistema objetivo de la actualización del firmware es sistema operativa Linux, la versión de ROM de HPE ProLiant System enumerada es el componente de la revisión de ROM Linux. En caso contrario, se enumera la última versión de ROM actualizada del lote SPP.

18.2.1 Acerca de la actualización del firmware

Cuando se agrega un dispositivo, el firmware se actualiza automáticamente a la línea de base de gestión de firmware especificada, con las excepciones siguientes:

- Servidores HPE ProLiant G6 y servidores HPE ProLiant G7 que deben gestionarse fuera de HPE OneView.
- El firmware de interconexión de Virtual Connect que se gestiona por separado como parte de la interconexión lógica. Consulte “Update firmware on logical interconnects for c7000 enclosures (Actualización del firmware de las interconexiones lógicas de los receptáculos c7000) en la ayuda en línea.

NOTA: Cuando se agrega un receptáculo y el firmware del OA o de iLO está por debajo de la versión mínima admitida para HPE OneView, el firmware se actualiza automáticamente mediante el SPP que contiene el firmware más reciente del OA o de iLO durante la adición del receptáculo. Sin embargo, si se han eliminado todos los SPP, dicho receptáculo no se puede importar. En este caso, antes de agregar el receptáculo debe cargar un SPP que proporcione al menos las versiones mínimas necesarias para el OA e iLO.

Todos los recursos (OA, iLO, servidores o Virtual Connect) se ponen fuera de línea cuando se actualiza su firmware. Realice siempre la actualización durante una ventana de mantenimiento. Para ayudar a reducir al mínimo el tiempo de inactividad durante la activación del firmware,

consulte «Mantenimiento de la disponibilidad durante las actualizaciones del firmware de las interconexiones de Virtual Connect».

Recurso	Al actualizar el firmware
Receptáculos	El OA (Onboard Administrator) se pone fuera de línea cuando se actualiza el firmware de un receptáculo.
Perfiles de servidor	Las actualizaciones de firmware requieren que se edite el perfil de servidor para cambiar la línea de base de firmware. Debe apagar el hardware de servidor al que asigna el perfil de servidor antes de cambiar la línea de base de firmware. La línea de base de firmware se puede cambiar mientras el servidor está encendido si se utiliza Smart Update Tools.
Interconexiones	Una interconexión se pone fuera de línea cuando: • Se actualiza o se activa el firmware de una interconexión lógica. El almacenamiento provisional de firmware no requiere poner fuera de línea las interconexiones. • Se actualiza el firmware de un receptáculo y se selecciona la opción de actualizar el receptáculo, la interconexión lógica y los perfiles de servidor. Si una interconexión tiene firmware que se ha almacenado provisionalmente pero no se ha activado, cualquier reinicio posterior de esa interconexión activa el firmware, lo que pone la interconexión fuera de línea. Puede evitar la pérdida de conectividad de red de los servidores conectados a una interconexión lógica que tiene un modo de apilamiento de receptáculo y un estado de apilamiento `Redundantly Connected` (Conexión redundante) si actualiza el firmware con el método siguiente: 1. Almacene provisionalmente el firmware en la interconexión lógica. 2. Active el firmware de las interconexiones situadas en los compartimientos del receptáculo con números pares. 3. Espere hasta que termine la actualización del firmware y las interconexiones estén en el estado `Configured` (Configurada). 4. Active el firmware de las interconexiones situadas en los compartimientos del receptáculo con números impares.

La actualización del firmware se basa en el rol asignado:

- El rol de administrador de servidores puede actualizar el firmware del OA del receptáculo y de los servidores.
- El rol de administrador de la red puede actualizar el firmware de las interconexiones.
- El rol de administrador de infraestructuras puede actualizar el firmware de todos los equipos.

18.2.1.1 Acerca de la gestión manual del firmware

Los receptáculos y los perfiles de servidor pueden configurarse para `Manage manually` (Gestionar manualmente) lo que significa que el firmware se gestiona mediante herramientas externas como SUM. HPE OneView informa de las versiones de firmware de los dispositivos, pero no intenta actualizar el firmware. A continuación, SUM puede gestionar el firmware y los controladores a través del sistema operativo.

El firmware de Virtual Connect siempre se gestiona a través de HPE OneView.

Uso de SUM para las actualizaciones

SUM puede actualizar tanto el firmware como los controladores de los dispositivos gestionados por HPE OneView, con excepción de las interconexiones de Virtual Connect.

SUM puede descargarse gratuitamente desde **http://www.hpe.com/info/SmartUpdate**.

SUM a:	Descripción
Instalar o actualizar controladores	Después de actualizar firmware mediante HPE OneView, utilice SUM para actualizar los controladores del entorno utilizando la misma línea de base del SPP que se ha aplicado mediante HPE OneView.
Actualizar el firmware	Después de actualizar firmware mediante SUM, actualice los dispositivos afectados en HPE OneView para reflejar la nueva versión del firmware. Seleccione **Actions→Refresh** (Acciones > Actualizar) en las pantallas **Enclosures** (Receptáculos) o **Server Hardware** (Hardware de servidor). **NOTA:** No se recomienda cambiar el firmware de los dispositivos a una versión anterior a la mínima admitida mientras que los dispositivos están gestionados por HPE OneView. Si necesita cambiar el firmware a una versión anterior a la mínima admitida, quite el receptáculo de HPE OneView antes de hacerlo.
Instalar revisiones	Utilice SUM para instalar revisiones. Después de realizar la actualización, actualice los dispositivos afectados en HPE OneView para reflejar la nueva versión del firmware. Seleccione **Actions→Refresh** (Acciones > Actualizar) en las pantallas **Enclosures** (Receptáculos) o **Server Hardware** (Hardware de servidor).

18.3 Acerca del firmware no admitido

Cuando se agrega un recurso para incluirlo en la gestión, el firmware del recurso se debe actualizar al nivel mínimo admitido. El dispositivo intenta actualizar automáticamente el firmware mientras el recurso se añade al dispositivo. Si la actualización falla, se genera una alerta.

NOTA: Debe cargar un SPP compatible en el repositorio de firmware del dispositivo antes de poder actualizar el firmware del componente. Consulte **http://www.hpe.com/info/hpeoneview/updates** para obtener actualizaciones de software de HPE OneView y lotes de firmware específicos para los productos.

Firmware no admitido para los lotes de firmware

Si intenta agregar un lote de firmware que contiene firmware por debajo de las versiones mínimas admitidas, se genera una alerta y el lote de firmware no se agrega al repositorio de firmware del dispositivo.

Firmware no admitido para los receptáculos

Al agregar un receptáculo, el dispositivo:

- Genera una alerta si el firmware de las interconexiones lógicas es anterior al mínimo necesario o si los niveles de firmware de las interconexiones no coinciden. Debe actualizar el firmware de las interconexiones lógicas desde la pantalla **Logical Interconnects** (Interconexiones lógicas) o mediante las API de REST.
- Actualiza el firmware del OA automáticamente, si es anterior al mínimo necesario (se debe tener un SPP compatible instalado en el dispositivo)
- Actualiza el firmware de iLO automáticamente, si es anterior al mínimo necesario (se debe tener un SPP compatible instalado en el dispositivo)

Firmware no admitido para los receptáculos lógicos

Cuando se agrega un receptáculo lógico, el dispositivo:

- Genera una alerta si las versiones de firmware reales de uno o varios componentes no coinciden con el mínimo necesario. Incluso si no se especifica un SPP de línea de base, el firmware de iLO se actualizará automáticamente, si es anterior al mínimo necesario (se

debe tener un SPP compatible instalado en el dispositivo). Seleccione la línea de base de firmware en la pantalla **Receptáculos lógicos** o en las API de REST.

Firmware no admitido para los perfiles de servidor

No está permitido aplicar perfiles de servidor si el firmware de iLO asociado está por debajo de la versión mínima admitida; en este caso, se accede a la pantalla **Server Hardware** (Hardware de servidor) para actualizar el firmware de iLO.

Firmware no admitido para las interconexiones

Si intenta agregar una interconexión cuyo firmware está por debajo de la versión mínima admitida, se genera una alerta. Debe actualizar el firmware de las interconexiones lógicas desde la pantalla **Logical Interconnects** (Interconexiones lógicas) o mediante las API de REST.

El panel **Firmware** de la pantalla **Logical Interconnects** (Interconexiones lógicas) muestra la versión instalada del firmware y la línea de base de firmware de cada interconexión.

18.4 Mantenimiento de la disponibilidad durante las actualizaciones del firmware de las interconexiones de Virtual Connect

Las interconexiones de Virtual Connect (VC) se reinician durante la etapa de activación del proceso de actualización del firmware, lo que interrumpe la conectividad de los servidores con estos módulos. Puede minimizar el impacto de la activación del firmware de los módulos si dispone de una configuración de hardware redundante, redes y conjuntos de enlaces ascendentes conectados de forma redundante, así como servidores con la formación de equipos NIC configurada correctamente. Hewlett Packard Enterprise recomienda el uso de estas metodologías de diseño de redes. Cuando actualice interconexiones de HPE FlexFabric, también debe configurar la conectividad SAN de forma redundante con objeto de evitar interrupciones de funcionamiento de las aplicaciones.

Al diseñar la conectividad de red, tenga en cuenta todas las dependencias que pueden influir en la capacidad de las aplicaciones de los servidores para seguir pasando tráfico sin interrupciones durante el proceso de actualización del firmware de las interconexiones de VC. Compruebe los siguientes aspectos del diseño redundante antes de actualizar el firmware en entornos que no admiten el tiempo de inactividad:

Configuración	Descripción
Enlaces de apilamiento	Configure los enlaces de apilamiento entre las interconexiones de VC para garantizar la accesibilidad de la red para cualquier blade de servidor a cualquier red o conjunto de enlaces ascendentes dentro de la interconexión lógica, independientemente de la ubicación del servidor. Esto desempeña un papel fundamental en relación con la capacidad de cada una de las interconexiones de VC para soportar una interrupción de funcionamiento durante la actualización del firmware.
Activación del firmware	Active manualmente el firmware o cree una secuencia de comandos para realizar la activación mediante las API de REST para reducir al mínimo la interrupción de funcionamiento de la red. En este caso, el orden de activación de los módulos desempeña un papel fundamental en el modo en que se interrumpirá o mantendrá la conectividad de red y de almacenamiento durante una actualización de firmware. Hewlett Packard Enterprise recomienda alternar la activación del firmware de interconexión de VC. • Si la conectividad de red y almacenamiento de los servidores es redundante entre interconexiones de VC adyacentes horizontalmente, alternar la activación entre los módulos de los lados izquierdo y derecho (impares y pares) puede minimizar las interrupciones de conectividad de red y almacenamiento. • Si la conectividad de red y almacenamiento de los servidores es redundante entre interconexiones de VC adyacentes verticalmente, se debe alternar el orden de activación, de modo que un servidor no pierda la conectividad con los dos puertos del adaptador al mismo tiempo para minimizar las interrupciones de conectividad de red y almacenamiento.

Configuración	Descripción
Conectividad para los lados A y B	Cree redes Ethernet y Fibre Channel con conectividad para los lados A y B con objeto de permitir que todos los enlaces ascendentes del conjunto de enlaces ascendentes estén en un estado activo en todo momento o para proporcionar una conmutación por error controlada.
Conexiones de red redundantes	Configure la formación de equipos NIC y la configuración de vSwitch para garantizar la redundancia de la conectividad de red, la detección rápida de fallos de ruta de red y la conmutación por error rápida a una ruta redundante, si está disponible. Los siguientes ajustes del sistema operativo permiten realizar con más rapidez la detección de fallos de enlace y la inicialización de la conmutación por error: • En condiciones normales de funcionamiento, la configuración de **Smart Link** (Enlace inteligente) altera el estado del puerto NIC individual en el vSwitch (conmutador virtual), vDS (vNetwork Distributed Switch) o el software de formación de equipos al desactivar el puerto NIC del servidor correspondiente. Esto hace que el sistema operativo detecte un fallo y dirija el tráfico a una ruta alternativa. Para que la funcionalidad Smart Link funcione según lo previsto, deben instalarse controladores y firmware de NIC válidos compatibles con DCC (Device Control Channel) en el blade de servidor. Sin embargo, durante el proceso de actualización del firmware, cuando las interconexiones de VC se restablecen para su activación, Smart Link y el protocolo DCC no serán capaces de enviar un mensaje a la NIC para indicar que el enlace se ha desactivado, debido a que el procesador de gestión de la interconexión se está reiniciando. Por lo tanto, durante la operación de actualización del firmware, la NIC y el sistema operativo del host son los responsables de detectar los fallos de enlace mediante la configuración de la opción de detección de la conmutación por error de red **Link Status Only** (Solo el estado de enlace) de vSwitch o vDS en la configuración de red de VMware ESXi Server. • En entornos vSphere, Hewlett Packard Enterprise recomienda desactivar el modo de alta disponibilidad (HA) o aumentar el tiempo de espera de HA de vSphere del valor predeterminado de 13 segundos a entre 30 y 60 segundos. Cuando se configuren estas opciones, todos los sistemas operativos invitados sobrevivirán a la actualización y a la interrupción esperada de la red gracias a la recuperación de la convergencia del enlace de apilamiento y a que se vuelve a calcular la ruta de red óptima. • Para los entornos donde no es posible cambiar las opciones de detección de la conmutación por error de la red o la configuración de alta disponibilidad, utilice la opción **Stage firmware for later activation** (Almacenar provisionalmente el firmware para activarlo más tarde) de la actualización del firmware. Las interconexiones de VC se actualizarán, pero no se activarán. A continuación, puede activar manualmente el firmware reiniciando los módulos VC con el OA o desplazándose a **Logical Interconnects→Actions→Update firmware** (Interconexiones lógicas > Acciones > Actualizar el firmware) en la interfaz de usuario y seleccionando **Activate firmware** (Activar el firmware). • La función Spanning Tree Edge Port de algunos conmutadores permite que un puerto del conmutador omita las fases ‘listening’ (escuchando) y ‘learning’ (aprendiendo) del árbol de expansión y pase rápidamente a la fase ‘forwarding’ (reenvío). Si se activa esta función, los dispositivos de borde comienzan la comunicación en la red inmediatamente en vez de tener que esperar a que el árbol de expansión determine si es necesario bloquear el puerto para evitar un bucle —un proceso que puede tardar más de 30 segundos con los temporizadores de árbol de expansión predeterminados—. Puesto que las interconexiones de VC son dispositivos de borde, esta función permite que las NIC de los servidores inicien la comunicación inmediata en la red en lugar de esperar los 30 segundos adicionales a que se recalcule el algoritmo del árbol de expansión.

18.5 Prácticas recomendadas para gestionar el firmware

Práctica recomendada	Descripción
Aumento del tamaño del disco virtual para el repositorio de SPP	Aumente el tamaño del disco virtual para ampliar el repositorio de firmware a 100 GB. Consulte la ***Guía de instalación de HPE OneView***.
Configure la NIC en OA.	Antes de comenzar un proceso de actualización del firmware en los dispositivos del receptáculo, siga estos pasos: **1.** En OA, seleccione **Enclosure Information→Enclosure Settings→Enclosure TCP/IP Settings** (Información de receptáculos > Configuración de receptáculos > Configuración de TCP/IP del receptáculo). **2.** Seleccione la ficha **NIC Options** (Opciones de NIC). **3.** Defina la configuración de la NIC en `Auto-negotiate` (Negociación automática).
Cargue el SPP más reciente.	Descargue el SPP más reciente desde **www.hpe.com/servers/spp/download** y, a continuación, cargue el SPP en el repositorio del dispositivo. Aplique su filtro favorito para descargar un SPP específico para su entorno. **NOTA:** Cada paquete del SPP contiene HPE Smart Update Manager y componentes Smart de firmware.
Establezca la misma línea de base de firmware para todos los dispositivos de un receptáculo.	Hewlett Packard Enterprise recomienda establecer la línea de base de firmware utilizando la opción **Update Firmware** (Actualizar el firmware) de la pantalla **Logical Enclosures** (Receptáculos lógicos). Esto actualiza inmediatamente todos los dispositivos del receptáculo al nivel del SPP especificado.
Si opta por crear SPP personalizados, utilice la descarga personalizada de SPP para crearlos.	Inicie sesión en el portal web de descarga personalizada de SPP en **http://www.hpe.com/info/spp** para crear un SPP personalizado utilizando filtros específicos para su entorno. Aplique un filtro de modelo de servidor o un filtro de sistema operativo para crear un SPP más pequeño. **SUGERENCIA:** Guarde el filtro para usarlo en el futuro.
Actualice el firmware en el orden apropiado.	Aunque Hewlett Packard Enterprise recomienda establecer la línea de base de firmware para todos los dispositivos en un receptáculo lo que provocará que todo el firmware se instale en el orden apropiado, puede actualizar el firmware de componentes concretos. Si decide actualizar el firmware de los componentes de manera independiente, actualice el firmware en el orden siguiente: OA, interconexión lógica y, a continuación, el perfil de servidor. Hewlett Packard Enterprise recomienda instalar los controladores desde el mismo SPP que contiene el firmware.
Actualice el firmware y los controladores mediante Smart Update Tools (SUT) cuando el servidor está encendido y funcionando en un sistema operativo	El firmware y los controladores pueden actualizarse mediante el perfil de servidor cuando se utiliza Smart Update Tools. Consulte la *Guía de usuario de Smart Update Tools* en **www.hpe.com/info/sut-docs** para ver las instrucciones de instalación. Establezca el modo de SUT en **Auto Stage Deploy** (Implementar con almacenamiento provisional automático). Reinicie durante la ventana de mantenimiento.
Compruebe la configuración del equipo gestionado antes de actualizar el firmware.	No actualice el firmware de un equipo gestionado usando SUM u otra herramienta externa a menos que la línea de base de firmware esté establecida en **Manage manually** (Gestionar manualmente).
Almacene los SSP en una ubicación diferente a la del dispositivo.	HPE OneView no crea una copia de seguridad del repositorio del firmware, por lo que debe almacenar los SPP en un repositorio que no esté en el dispositivo, como por ejemplo en el repositorio de SUM utilizado para crear el SPP personalizado.
Elimine los SSP más antiguos del repositorio de firmware.	Tenga al menos un SPP disponible en todo momento debido a que es necesario un SPP cuando se agregan recursos al dispositivo que están por debajo de las versiones mínimas de firmware necesarias para supervisarlos o gestionarlos. Si desea eliminar un SPP más antiguo, reasigne todos los recursos a otro SPP antes de eliminarlo.

Más información

Capítulo 18, «Gestión de firmware para los equipos gestionados»

18.6 Creación de un SPP personalizado

En ocasiones, HPE publica revisiones para los componentes entre las versiones principales del SPP. Deberá crear un SPP personalizado en HPE OneView mediante el SPP base y la revisión. Para aplicar la revisión a los recursos gestionados, cree un SPP personalizado con la revisión.

Existen distintos mecanismos para aplicar una revisión en OneView:

- Utilice la descarga personalizada de SPP para crear un nuevo SPP con la revisión (método recomendado por Hewlett Packard Enterprise).
- Utilice SUM para crear un nuevo SPP con la revisión.
- Cargue la revisión y cree un SPP personalizado utilizando HPE OneView.

NOTA: En cualquier SPP personalizado que cree, debe incluir el firmware de iLO, OA y Virtual Connect.

Para las revisiones del OA, VC e iLO, asegúrese de que carga la versión .scexe de la revisión.

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras, administrador de red o administrador de servidores
- Software que permita montar un archivo ISO (imagen)

Opción 1: Utilice la descarga personalizada de SPP para crear un SPP personalizado

Hewlett Packard Enterprise recomienda utilizar la función de descarga personalizada de SPP para cargar un SPP personalizado en HPE OneView. Para obtener instrucciones y acceso, vaya a **http://hpe.com/servers/spp**.

Opción 2: Utilice SUM para crear un archivo ISO con el SPP personalizado

1. Descargue el SUM desde **http://www.hpe.com/servers/hpsum**.
2. Descomprima el archivo de SUM en un directorio.
3. Descargue el archivo ISO del SPP desde **http://www.hpe.com/info/spp** a un directorio local.
4. Monte el archivo ISO del SPP en un sistema de archivos al que tenga acceso, siguiendo las instrucciones de su software.
5. Inicie SUM haciendo doble clic en `hpsum.bat` en el directorio `\hpsum`.
6. En el menú principal de SUM, seleccione **Baseline Library→+Add Baselines** (Biblioteca de líneas de base > + Agregar líneas de base).

   La revisión está incluida en la línea de base personalizada.
7. Para obtener los **Location Details** (Detalles de la ubicación), vaya al directorio `hpe\swpackages` del SPP que ha montado.
8. Haga clic en **Add** (Agregar). Espere a que finalice la operación de adición antes de continuar.
9. Agregue los demás componentes (actualizaciones) que haya descargado desde HPE a la biblioteca de líneas de base que desea incluir en el SPP personalizado.
10. Seleccione el SPP y los componentes de la biblioteca de líneas de base.
11. Seleccione **Actions→Create Custom** (Acciones > Crear personalizado).
12. Seleccione los filtros que desee utilizar; sin embargo, los siguientes filtros son obligatorios:
    - **Overview** (Información general): seleccione **Bootable ISO** (ISO de arranque)
    - **OS Type** (Tipo de SO): seleccione **RHEL 5** y **RHEL 6**

13. Haga clic en **Create ISO** (Crear ISO) para crear el nuevo lote de firmware.
14. Agregue un lote de firmware al repositorio de firmware del dispositivo. Consulte la ayuda en línea para obtener más información.
15. Compruebe que la carga ha finalizado consultando el contenido del lote de firmware en el panel de detalles de la pantalla **Firmware Bundles** (Lotes de Firmware).

Opción 3: Cargue la revisión y cree un SPP personalizado

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras, administrador de red o administrador de servidores
- En el repositorio debe haber como mínimo una revisión válida.

1. En el menú principal, seleccione **Firmware Bundles (Lotes de firmware)**.
2. Seleccione **Actions (Acciones)→Create Custom firmware bundle (Crear lote de firmware personalizado)**.
3. Escriba un nombre de spp personalizado y seleccione un SPP de base.
4. Haga clic en **Add Hotfix (Agregar revisión)** para agregar las revisiones disponibles.
5. Haga clic en **OK** (ACEPTAR).
6. Compruebe que la carga ha finalizado consultando el contenido del lote de firmware en el panel de detalles de la pantalla **Firmware Bundles** (Lotes de Firmware).

También puede utilizar las API de REST para cargar una revisión y crear un SPP personalizado. Para obtener más información, consulte la **ayuda sobre secuencias de comandos de la API de** REST.

NOTA: La carga de una revisión para crear un SPP personalizado debe usarse específicamente para aplicar revisiones a un *recurso gestionado*.

18.7 Actualización del firmware en dispositivos gestionados

Los lotes de firmware permiten actualizar el firmware de los servidores, los blades de servidor y la infraestructura (receptáculos e interconexiones) gestionados. Puede optar por actualizar todos los recursos de un receptáculo, solo el firmware del Onboard Administrator, el firmware de una interconexión lógica o el firmware de un servidor específico mediante un perfil de servidor. Si opta por actualizar todos los recursos de un receptáculo, se actualizan todos los servidores aun cuando no estén asociados con un perfil de servidor.

En la pantalla **Logical Enclosures** (Receptáculos lógicos), puede iniciar las actualizaciones de firmware de los Onboard Administrators. Consulte «Actualización del firmware desde un receptáculo lógico» para obtener más información.

También puede optar por actualizar el firmware de componentes individuales. Como práctica recomendada al actualizar el firmware de componentes individuales, actualice el firmware en el siguiente orden:

1. Onboard Administrator
2. Interconexiones lógicas
3. Perfiles de servidor

18.7.1 Actualización del firmware del receptáculo lógico

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores (para los receptáculos)
- Se deben haber agregado uno o varios SPP al repositorio de firmware del dispositivo.

Actualización del firmware del receptáculo c7000 en el receptáculo lógico

Al agregar un receptáculo o actualizar el firmware de un receptáculo, la selección de la línea de base de firmware en el receptáculo lógico define la línea de base del receptáculo y de cada una de sus interconexiones lógicas, así como del OA.

1. En el menú principal, seleccione **Logical Enclosures** (Receptáculos lógicos).
2. En el panel principal, seleccione el receptáculo al que desea aplicar un lote de firmware.
3. Seleccione **Actions→Update firmware** (Acciones > Actualizar firmware).
4. Para **Firmware baseline** (Línea de base de firmware), seleccione el lote de firmware que desee instalar.

   Si selecciona `Manage manually` (Gestionar manualmente), significa que está utilizando mecanismos externos al dispositivo para gestionar el firmware de los equipos.

   NOTA: Para instalar una versión de firmware más antigua que la versión incluida en el SPP, debe seleccionar la opción **Force installation** (Forzar instalación) para cambiar el firmware a una versión anterior. Es posible que desee instalar un firmware más antiguo si sabe que el firmware más reciente provoca un problema en su entorno.

   △ **ATENCIÓN:** Tenga en cuenta que cambiar a una versión anterior del firmware puede inutilizar un servidor y podría dar lugar a velocidades de instalación más lentas. Por ejemplo, si el Firmware de iLO se cambia a una versión anterior que no utiliza RIS (Rich Infrastructure Specification), se interrumpirá la comunicación entre HPE Smart Update Tools y HPE OneView.

5. En **Update firmware for** (Actualizar el firmware de), seleccione una de las opciones siguientes:

Opción	Equipo actualizado
Receptáculo	Firmware de fuentes de alimentación, ventiladores y OA **NOTA:** Si no se ha configurado una línea de base de firmware para las interconexiones lógicas, se muestra la **línea de base** como `Not set` (Sin configurar). La línea de base de la interconexión lógica se puede definir durante la adición del receptáculo o durante una actualización del firmware de la interconexión lógica.
Enclosure + logical interconnect + server profiles (Receptáculo + interconexión lógica + perfiles de servidor)	Firmware de OA, de todas las interconexiones que son miembros y del hardware de servidor (incluido iLO) para los servidores con perfiles de servidor asociados

6. Haga clic en **OK** (Aceptar).
   - Las actualizaciones de firmware se producen en el siguiente orden: OA, interconexiones lógicas y, a continuación, hardware de servidor.
   - Los componentes de hardware que ejecutan la misma versión de firmware que la actualización se omiten de la operación de actualización de firmware.
   - La operación de actualización de las interconexiones lógicas se inicia si se pueden actualizar todas las interconexiones que son miembros.
   - Si actualiza los perfiles de servidor, la operación sobrescribe cualquier línea de base del SPP que se haya asignado anteriormente a los distintos perfiles de servidor.
7. Compruebe que la nueva línea de base de firmware aparece en el panel de detalles de la pantalla **Logical Enclosures** (Receptáculos lógicos).

18.7.2 Actualización del firmware con un perfil de servidor

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores

Cómo actualizar el firmware con un perfil de servidor

Para actualizar el firmware de un servidor específico, edite el perfil de servidor existente o cree un nuevo perfil de servidor y especifique la versión del SPP.

NOTA: La línea de base de firmware del perfil de servidor no volverá a aplicarse si no ha cambiado.

1. En el menú principal, seleccione **Server Profiles** (Perfiles de servidor) y, a continuación, realice una de las acciones siguientes:
   - Haga clic en **Create profile** (Crear perfil) en el panel principal.
   - En el panel principal, seleccione un perfil de servidor y, a continuación, seleccione **Actions→Edit** (Acciones > Editar).
2. Seleccione el lote de firmware para la **Línea de base de Firmware**.

   Para instalar una versión anterior del firmware incluida en el SPP, debe seleccionar la opción **Force installation** (Forzar instalación) para cambiar el firmware a una versión anterior. Es posible que desee instalar un firmware más antiguo si sabe que el firmware más reciente que está instalado en el servidor provoca un problema en su entorno, algo que se describe en las Notas de la versión

△ **ATENCIÓN:** Tenga en cuenta que cambiar a una versión anterior del firmware puede inutilizar un dispositivo y podría dar lugar a velocidades de instalación más lentas. Por ejemplo, si el Firmware de iLO se cambia a una versión anterior que no utiliza RIS (Rich Infrastructure Specification), se interrumpirá la comunicación entre HPE Smart Update Tools y HPE OneView.

3. Para completar la actualización, realice una de las acciones siguientes:
   - Si se trata de un perfil nuevo, haga clic en **Create** (Crear) para crear el perfil de servidor.
   - Si va a modificar un perfil existente, haga clic en **OK** (Aceptar) para actualizar el perfil de servidor.
4. Encienda el servidor para activar el firmware nuevo.
   a. En el menú principal, seleccione **Server Hardware** (Hardware de servidor).
   b. Seleccione el servidor y, a continuación, seleccione **Actions→Power on** (Acciones > Encender).
5. Compruebe que la nueva línea de base de firmware se muestra en el panel de detalles de la pantalla **Server Profiles** (Perfiles de servidor).

18.7.3 Actualización del firmware con una plantilla de perfil de servidor

Requisitos previos

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores

Cómo actualizar el firmware con una plantilla de perfil de servidor

Para actualizar el firmware de un servidor específico, edite la plantilla de perfil de servidor existente o cree una nueva plantilla de perfil de servidor y especifique la versión del SPP.

NOTA: La línea de base de firmware de la plantilla de perfil de servidor no volverá a aplicarse si no ha cambiado.

1. En el menú principal, seleccione **Server Profile Templates** (Plantillas de perfiles de servidor) y, a continuación, realice una de las acciones siguientes:
   - Haga clic en **Create server profile template** (Crear plantilla de perfil de servidor) en el panel principal.
   - En el panel principal, seleccione una plantilla de perfil de servidor y, a continuación, seleccione **Actions→Edit** (Acciones > Editar).
2. Seleccione el lote de firmware para la **Firmware baseline** (Línea de base de Firmware).

   Para instalar una versión anterior del firmware incluida en el SPP, debe seleccionar la opción **Force installation** (Forzar la instalación) para cambiar el firmware a una versión anterior. Es posible que desee instalar un firmware más antiguo si sabe que el firmware más reciente que está instalado en el servidor provoca un problema en su entorno, algo que probablemente se describe en las Notas de la versión.

△ **ATENCIÓN:** Tenga en cuenta que cambiar a una versión anterior del firmware puede inutilizar un dispositivo y podría dar lugar a velocidades de instalación más lentas. Por ejemplo, si el Firmware de iLO se cambia a una versión anterior que no utiliza RIS (Rich Infrastructure Specification), se interrumpirá la comunicación entre HPE Smart Update Tools y HPE OneView.

3. Para completar la actualización, realice una de las acciones siguientes:
   - Si se trata de una plantilla nueva, haga clic en **Create** (Crear) para crear la plantilla de perfil de servidor.
   - Si está editando una plantilla existente, haga clic en **OK** (Aceptar) para actualizar la plantilla de perfil de servidor.
4. Compruebe que la nueva línea de base de firmware se muestra en el panel de detalles de la pantalla **Server Profile Templates** (Plantillas de perfiles de servidor).

18.8 Información adicional

- «Solución de problemas de los lotes de firmware» (página 425)
- «Acerca de los receptáculos»
- «Sobre el firmware asociado con una interconexión lógica»
- «Acerca de los perfiles de servidor»

19 Gestión de la energía, la temperatura y el centro de datos

Puede gestionar la energía y la temperatura de su hardware de TI mediante el dispositivo. Para gestionar y supervisar la temperatura del hardware, añada su hardware de servidor a los bastidores, colóquelos en ellos y añada los bastidores a centros de datos.

19.1 Gestión de energía

Para gestionar la energía, debe describir los equipos de suministro de energía al dispositivo mediante la pantalla **Power Delivery Devices** (Dispositivos de suministro de energía) o las API de REST. El dispositivo detecta las unidades HPE Intelligent Power Distribution Unit (iPDU) y sus conexiones de forma automática.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Power Delivery Devices (Dispositivos de suministro de alimentación)	`power-devices`
	`enclosures` (potencia)
	`server-hardware` (potencia)

19.1.1 Roles

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores

19.1.2 Tareas de gestión de energía

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario y las API de REST para:

- Agregar un equipo de suministro de energía.
- Agregar una conexión de alimentación.
- Filtrar los dispositivos de suministro de energía.
- Ver los últimos 5 minutos de consumo de energía para una iPDU.
- Ver las últimas 24 horas de consumo de energía para una iPDU.
- Editar las propiedades de un equipo de suministro de energía.
- Encender o apagar la luz de localización de un equipo de suministro de energía.
- Apagar un equipo de suministro de energía.
- Quitar un equipo de suministro de energía.
- Resolver problemas de conectividad entre una iPDU y el dispositivo.
- Agregar una iPDU que actualmente gestiona otro sistema de gestión.
- Ver las estadísticas de utilización de energía.
- Actualizar la configuración de potencia del receptáculo (solamente con la API de REST).
- Actualizar la configuración de potencia del hardware de servidor (solamente con la API de REST).

19.1.3 Acerca de los dispositivos de suministro de energía

Los dispositivos de suministro de energía proporcionan energía para el hardware de TI. Una topología de energía típica de un centro de datos incluye dispositivos de suministro de energía, tales como tomas de alimentación eléctrica, paneles de disyuntores, circuitos de derivación y unidades de distribución de energía (PDU), así como segmentos de carga, barras de salida y componentes de salida de estos dispositivos. Al agregar los equipos de suministro de energía al dispositivo, se activa la gestión de energía utilizando los límites térmicos, la potencia nominal y la potencia reducida.

La pantalla **Power Delivery Devices** (Dispositivos de suministro de energía), describe las siguientes clases de dispositivos:

- Intelligent Power Distribution Units (iPDU), que el dispositivo puede detectar y controlar de forma automática.
- Otros equipos de suministro de energía que el dispositivo no se puede detectar. Al añadir manualmente estos equipos gestionados al dispositivo, están disponibles para fines de seguimiento, inventario y gestión de energía.

Independientemente del modo en que se añaden los equipos de suministro de energía al dispositivo, este genera automáticamente los mismos tipos de análisis (capacidad, redundancia y configuración). Para las iPDU, el dispositivo recopila datos estadísticos e informa de los errores.

Conectividad y sincronización con el dispositivo

El dispositivo supervisa el estado de conectividad de las iPDU. Si el dispositivo pierde la conectividad con una iPDU, se muestra una alerta hasta que se restablece la conectividad. El dispositivo intentará resolver los problemas de conectividad y desactivar la alerta automáticamente, pero si no lo consigue, se debe resolver el problema y actualizar manualmente la iPDU para sincronizarla con el dispositivo.

El dispositivo también supervisa las iPDU para comprobar que permanecen sincronizadas con los cambios en el hardware y las conexiones de alimentación. Sin embargo, algunos cambios realizados en los equipos gestionados fuera del control del dispositivo (desde iLO o el OA, por ejemplo) pueden hacer que se pierda la sincronización con el dispositivo. Puede que tenga que actualizar manualmente los equipos gestionados que pierdan la sincronización con el dispositivo.

NOTA: Hewlett Packard Enterprise recomienda que no use iLO ni el OA para realizar cambios en un equipo gestionado. Si se realizan cambios en un equipo gestionado desde su iLO o su OA, se podría perder la sincronización con el dispositivo.

Puede actualizar manualmente la conexión entre el dispositivo y una iPDU desde la pantalla **Power Delivery Devices** (Dispositivos de suministro de energía). Consulte la ayuda en línea de la pantalla **Power Delivery Devices** (Dispositivos de suministro de energía) para obtener más información.

19.2 Gestión del centro de datos

En el dispositivo, un centro de datos representa un área físicamente contigua en la que se encuentran los bastidores que contienen los equipos informáticos, tales como servidores, receptáculos y dispositivos. Un centro de datos describe una parte de una sala de informática y proporciona una agrupación útil para resumir un entorno y sus requisitos térmicos y eléctricos.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Data Centers (Centros de datos)	`datacenters`

19.2.1 Roles

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores

19.2.2 Tareas para centros de datos

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario y las API de REST para:

- Agregar y editar un centro de datos.
- Manipular la vista de una visualización del centro de datos.
- Supervisar la temperatura del centro de datos.
- Quitar un centro de datos de la gestión.

19.2.3 Acerca de los centros de datos

Un centro de datos representa un área físicamente contigua en la que se encuentran bastidores que contienen equipos informáticos.

Por ejemplo, suponga que tiene equipos informáticos en dos salas o en pisos separados. Podría crear un centro de datos para cada una de estas áreas.

Cada servidor, receptáculo, o dispositivo de distribución de energía del centro de datos puede informar sobre sus requisitos de energía, pero puede resultar difícil entender los requisitos de energía y refrigeración del centro de datos en su conjunto. El dispositivo le permite incluir la gestión de la energía y la refrigeración de los servidores, receptáculos y dispositivos de suministro de energía en un único sistema de gestión.

La vista **Layout** (Diseño) del centro de datos utiliza un código de colores para representar la temperatura máxima registrada en las últimas 24 horas.

Centro de datos predeterminado: Datacenter 1

Cuando se inicializa el dispositivo por primera vez, se crea un centro de datos denominado `Datacenter 1`. El dispositivo proporciona este centro de datos como un lugar donde visualizar los bastidores. Puede cambiar el nombre o modificar este centro de datos para que coincida con los valores y el diseño de su centro de datos, puede utilizarlo como base para un modelo de centro de datos planificado, o puede eliminarlo sin problema.

Colocación predeterminada de los bastidores

Cuando se agrega un bastidor al dispositivo para que lo gestione, el dispositivo lo muestra en todos los centros de datos, aunque no se conozca su ubicación real. Si visualiza un centro de datos que muestra bastidores sin colocar, aparecerá una advertencia para avisarle de que se están mostrando bastidores sin colocar. Cuando asigne un bastidor a un centro de datos, dejará de mostrarse en los demás centros de datos.

19.3 Gestión de bastidores

Los bastidores le permiten gestionar la temperatura y la alimentación, y muestran la disposición de los receptáculos.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Racks (Bastidores)	`racks`

19.3.1 Roles

- Privilegios necesarios: administrador de infraestructuras o administrador de servidores

19.3.2 Tareas para bastidores

- Agregar, editar o extraer un bastidor.
- Cambiar el diseño de los dispositivos del bastidor.
- Establecer el límite de temperatura de un bastidor.

19.3.3 Acerca de los bastidores

Un bastidor es una estructura física que contiene equipos de TI, tales como receptáculos, servidores, equipos de suministro de energía y equipos no gestionados (un equipo no gestionado utiliza ranuras en el bastidor y consume energía o disipa calor, pero no está gestionado por el dispositivo). Puede gestionar los bastidores y los equipos que contienen si los incluye en la gestión del dispositivo. Si incluye los bastidores en la gestión del dispositivo, podrá utilizar el dispositivo para planificar el espacio y la energía. El dispositivo también recopila datos estadísticos y supervisa la energía y la temperatura de los bastidores que gestiona.

Cuando se agrega un receptáculo al dispositivo, este crea automáticamente un bastidor y coloca el receptáculo en el mismo. El dispositivo coloca en el bastidor todos los receptáculos conectados por cables de enlace de gestión. Cuando se agregan receptáculos, el dispositivo los coloca en el bastidor de arriba a abajo. Cuando se coloca un receptáculo en un bastidor Intelligent Series, las ranuras del receptáculo se detectan automáticamente. En otros bastidores, para disponer de una representación exacta de la disposición de los receptáculos dentro del bastidor, debe editar el bastidor para colocar los receptáculos en las ranuras correctas.

Puede utilizar el dispositivo para ver y gestionar la configuración y la topología de suministro de energía del bastidor. Puede especificar las dimensiones físicas del bastidor (anchura, altura y profundidad), el número de ranuras U y la ubicación de cada equipo en el bastidor. Puede especificar las PDU del bastidor que proporcionan energía al mismo y su posición física en el bastidor o en cualquiera de sus dos lados. También puede describir el modo en que están conectados los equipos del bastidor a las PDU.

El dispositivo detecta automáticamente la altura y el modelo del bastidor para un servidor ProLiant por medio de Location Discovery Services y actualiza las ubicaciones físicas de los equipos cuando se reubican en los bastidores para los receptáculos c7000.

NOTA: Cuando el dispositivo detecta un bastidor HPE Intelligent Series, establece automáticamente altura del bastidor por medio de Intelligent Rack Location Discovery Services para los receptáculos c7000. Para bastidores no inteligentes o bastidores vacíos, la altura de bastidor por defecto es de 42U.

Después de agregar un bastidor al dispositivo para gestionarlo, puede agregar el bastidor a un centro de datos para visualizar el diseño del centro de datos y para supervisar los datos de energía y refrigeración de los equipos.

Una vez que el bastidor esté gestionado, puede configurar la topología de suministro de energía con sistemas de alimentación ininterrumpida y fuentes de alimentación redundantes para los equipos del bastidor.

Nomenclatura de bastidor

La forma en que se denomina un bastidor y cómo cambia su nombre depende de cómo se haya agregado al dispositivo.

Tabla 11 Nomenclatura de bastidor

Método de adición	Método de nomenclatura inicial	Método de cambio de nombre
Agregado automáticamente cuando el dispositivo detecta un receptáculo del bastidor para receptáculos c7000	Definido por el OA del receptáculo	Cambie el nombre del bastidor desde el OA del receptáculo
Detectado automáticamente desde un servidor ProLiant con Location Discovery Services para receptáculos c7000	Asignado utilizando el número de serie del bastidor como nombre del bastidor	Edite el bastidor
Manualmente desde la pantalla de **Racks** (Bastidores)	Definido por el usuario	Edite el bastidor

19.4 Información adicional

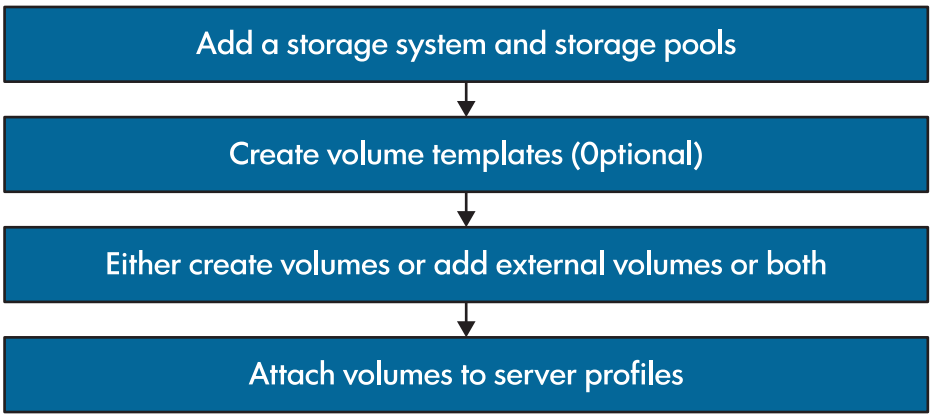
- Capítulo 27, «Supervisión de la energía y la temperatura»
- «Acerca de los gráficos y contadores de utilización»

20 Gestión del almacenamiento

Este capítulo describe los recursos de almacenamiento y las tareas asociadas con dichos recursos.

- Sistemas de almacenamiento: hardware que contiene varios discos de almacenamiento, por ejemplo, el sistema HPE 3PAR StoreServ Storage System.
- Pools de almacenamiento: grupos de discos físicos en un sistema de almacenamiento.
- Volúmenes: espacios de almacenamiento lógico aprovisionados desde los pools de almacenamiento que se pueden conectar a perfiles de servidor.
- Plantillas de volumen: puede crear varios volúmenes con la misma configuración.
- Administradores de SAN: sistemas de hardware o software que gestionan redes SAN.
- Redes SAN: las SAN pueden utilizarse para automatizar la distribución en zonas de la estructura.

Figura 19 Descripción general de la gestión de almacenamiento



Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST

SAN Managers (Administradores de SAN)	`fc-sans/device-managers`
	`fc-sans/providers`
	`fc-sans/managed-sans`

Storage Systems (Sistemas de almacenamiento)	`storage-systems`
Storage Pools (Pools de almacenamiento)	`storage-pools`
Volumes (Volúmenes)	`storage-volumes`
Volume Templates (Plantillas de volumen)	`storage-volume-templates`

20.1 Sistemas de almacenamiento

Un sistema de almacenamiento es hardware que contiene varios discos de almacenamiento, por ejemplo, el sistema HPE 3PAR StoreServ Storage System.

20.1.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de almacenamiento

20.1.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario y las API de REST para:

- Agregar, editar, editar credenciales, actualizar y quitar un sistema de almacenamiento
- Adición de un volumen

20.1.3 Acerca de los sistemas de almacenamiento

Un sistema de almacenamiento (o una matriz de almacenamiento) es un dispositivo de almacenamiento cuyos discos lógicos (volúmenes) se pueden aprovisionar y asignar o enmascarar a los servidores. Al incluir los sistemas de almacenamiento SAN en la gestión del dispositivo, podrá agregar y crear volúmenes. A continuación, puede conectar volúmenes a perfiles de servidor a través de conexiones de volúmenes. Esto le permite al hardware de servidor asignado a los perfiles de servidor acceder al sistema de almacenamiento SAN.

Al agregar un sistema de almacenamiento, debe elegir un dominio en el sistema de almacenamiento. A continuación, puede seleccionar pools de almacenamiento de ese dominio en el sistema de almacenamiento para agregarlos al dispositivo. Después de agregar pools de almacenamiento, puede asignar redes a los puertos de almacenamiento asociados con el sistema de almacenamiento.

Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener una lista de los sistemas de almacenamiento admitidos.

20.1.3.1 Acerca de los sistemas HPE 3PAR StoreServ Storage System

Puede conectar sistemas HPE 3PAR Storage StoreServ compatibles al dispositivo. Debe configurar un sistema 3PAR mediante el software 3PAR para incluirlo en la gestión del dispositivo.

Estados de los puertos asociados

Estado del puerto	Definición	Estado de 3PAR equivalente
none (ninguno)	Estado normal, sin conmutación por error.	`none`
failing over (realizando la conmutación por error)	El puerto está fuera de línea y está realizando la conmutación por error al puerto asociado.	`failover_pending`
failed over (conmutado por error)	El puerto está fuera de línea y ha conmutado por error al puerto asociado.	`failed_over`
failed (ha fallado)	El puerto está desactivado fuera de línea y no puede conmutar por error al puerto asociado.	`active_down`
recovering (recuperándose)	El puerto está en línea y en el proceso de vuelta a su estado normal.	`failback_pending`
partner port failed over (puerto asociado conmutado por error)	El puerto asociado ha conmutado por error y el puerto está gestionando el tráfico del puerto asociado.	`active`
partner failed (ha fallado el asociado)	El puerto asociado ha fallado y la operación de conmutación por error no se ha realizado correctamente.	`active_down`

20.2 Pools de almacenamiento

Los pools de almacenamiento son grupos de discos físicos de un sistema de almacenamiento que pueden dividirse en volúmenes lógicos.

20.2.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de almacenamiento

20.2.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario y las API de REST para:

- Agregar o quitar un pool de almacenamiento

20.2.3 Acerca de los pools de almacenamiento

Un pool de almacenamiento es de suma de recursos de almacenamiento físicos (discos) en un sistema de almacenamiento. Los sistemas de almacenamiento contienen información sobre los puertos de almacenamiento a través de los cuales se puede acceder a ellos. Se pueden aprovisionar espacios de almacenamiento lógico, conocidos como volúmenes, desde pools de almacenamiento.

Puede elegir uno o más pools de almacenamiento al agregar un sistema de almacenamiento al dispositivo. Los pools de almacenamiento se crean en un sistema de almacenamiento mediante el software de gestión para dicho sistema. No se pueden crear ni eliminar pools de almacenamiento del dispositivo —solo se pueden agregar o eliminar de la gestión. Después de agregar pools de almacenamiento, puede aprovisionar volúmenes en ellos.

20.3 Volúmenes

Los volúmenes son espacios de almacenamiento lógico aprovisionados en pools de almacenamiento. Pueden crearse varios volúmenes con la misma configuración utilizando una plantilla de volumen.

20.3.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras, administrador de almacenamiento o administrador de redes

20.3.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario y las API de REST para:

- Crear, agregar, editar, eliminar y aumentar la capacidad de un volumen
- Crear una instantánea de un volumen, crear un volumen a partir de una instantánea y revertir un volumen a una instantánea

20.3.3 Acerca de los volúmenes

Un volumen representa un disco lógico aprovisionado desde un pool de almacenamiento de un sistema de almacenamiento. Es posible conectar volúmenes a uno o varios servidores mediante la configuración de una conexión de volumen en el perfil de servidor. La conexión de volumen gestiona la presentación del volumen en el sistema de almacenamiento (selección de puerto de StoreServ, host y creación de vlun), así como la distribución en zonas SAN de las SAN (con la

distribución en zonas automática activada) que conecta el servidor con el sistema de almacenamiento.

Por medio de plantillas de volumen, puede crear varios volúmenes con la misma configuración.

Puede aumentar la capacidad (el tamaño) de un volumen, modificándolo. No puede reducir la capacidad de un volumen.

20.3.3.1 Acerca de las instantáneas

Una instantánea es una copia virtual de un volumen existente en un momento dado. Puede utilizar una instantánea como una copia de seguridad de un volumen y, a continuación, usarla para revertir un volumen a la copia de seguridad, o para crear volúmenes nuevos a partir de la instantánea.

Una instantánea es una copia estática de un volumen en el momento en que se crea la instantánea. Las instantáneas no se actualizan para reflejar los cambios que se han producido en el volumen desde que se tomaron.

Un nuevo volumen creado a partir de una instantánea tendrá el mismo tamaño que la instantánea y contendrá todos los datos de la instantánea. El nuevo volumen no tiene ninguna relación con el volumen que se utilizó para crear la instantánea.

Si se revierte un volumen a una instantánea, se revertirán los datos que el contenía el volumen cuando se tomó la instantánea. El tamaño del volumen será el mismo que tenía cuando se revirtió. Por ejemplo, si se toma una instantánea de un volumen de 50 GiB, se aumenta el volumen a 100 GiB y, a continuación, se revierte a la instantánea, el volumen tendrá 100 GiB y contendrá los datos de la instantánea de 50 GiB.

Si se revierte un volumen a una instantánea, se perderán todos los datos creados o modificados desde la que se tomó la instantánea. Haga una copia de seguridad de los datos para evitar su pérdida.

20.4 Plantillas de volumen

Puede utilizar plantillas de volumen para crear varios volúmenes con la misma configuración.

20.4.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de almacenamiento

20.4.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario y las API de REST para:

- Agregar, editar y eliminar una plantilla de volumen

20.4.3 Acerca de las plantillas de volumen

Una plantilla de volumen es un recurso lógico que le permite crear una configuración estándar desde la cual crear varios volúmenes.

20.5 Administradores de SAN

Un administrador de SAN es un sistema de hardware o software que administra diferentes SAN. No se necesita un administrador de SAN para conectar un volumen a un perfil de servidor, pero los administradores de SAN permiten realizar la distribución automática en zonas de la estructura.

20.5.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de almacenamiento

20.5.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar, editar y quitar un administrador de SAN

20.5.3 Acerca de los administradores de SAN

Los administradores de SAN son un recurso de HPE OneView que representa una conexión con una entidad externa a través de la cual las SAN se detectan y se gestionan. La entidad externa puede ser el software de gestión específico del proveedor o un conmutador físico.

Las SAN se crean fuera de HPE OneView en la interfaz de gestión del proveedor del administrador de SAN. Una vez creadas, las SAN pueden detectarse y gestionarse en HPE OneView utilizando el recurso del administrador de SAN.

Cuando se crean administradores de SAN, es posible que dos administradores de SAN detecten la misma SAN, lo que hará que se muestre dos veces en la vista de SAN. Cuando se asocia una red de HPE OneView a la SAN, la elección de qué SAN se asocia determina el administrador de SAN que se utilizará para gestionar la SAN, y el otro se eliminará (se ocultará), ya que HPE OneView no permite que una SAN se gestione mediante más de un administrador de SAN.

HPE OneView es compatible con administradores de SAN de distintos proveedores. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener una lista de los administradores de SAN admitidos.

20.5.3.1 Acerca de los conjuntos de zonas

Un conjunto de zonas es un grupo de zonas. Es posible configurar todas las zonas de un administrador de SAN mediante la activación de un conjunto de zonas desde el administrador de SAN. HPE OneView modifica el conjunto de zonas activo cuando se lleva a cabo la distribución en zonas o la configuración de alias. Los conjuntos de zonas no se exponen en HPE OneView.

Conjunto de zonas activo	El conjunto de zonas que actualmente está en vigor en la estructura.
Conjuntos de zonas inactivos	Los conjuntos de zonas que no están activos para la SAN. Solo puede haber un conjunto de zonas activo en cada momento.

Administrador de SAN	Denominación del conjunto de zonas inactivo
HPE	Conjunto de zonas en espera
Cisco	Conjunto de zonas local
Brocade (BNA)	Configuraciones de zonas

20.5.3.2 Configuración de administradores de SAN para que los gestione HPE OneView

Debe configurar los administradores de SAN mediante el software de gestión suministrado por el proveedor del administrador de SAN para gestionarlos correctamente en HPE OneView. Después de configurar correctamente el administrador de SAN, puede agregarlo a HPE OneView.

⚠ **ATENCIÓN:** Si se llevan a cabo operaciones de zonas desde varios conmutadores sin ejecutar una distribución completa en conjuntos de zonas, se puede provocar la pérdida de los datos de distribución en zonas.

NOTA: Los proveedores de conmutadores admiten membresías de zona de nombre World Wide de estructura (FWWN) o nombre World Wide de puerto de nodo (PWWN). HPE OneView solo utiliza PWWN para la membresía de zona.

Práctica recomendada: Administradores de SAN

- Utilice siempre un único conmutador para llevar a cabo todas las operaciones de distribución en zonas, independientemente del software de gestión que utilice para realizar la distribución en zonas.
- Utilice siempre la configuración y los comandos de distribución en conjuntos de zonas completos cuando realice cambios en las zonas. HPE OneView lo hace en el administrador de SAN y la SAN a través de los que realiza la gestión de forma predeterminada.

Configuración de administradores de SAN de HPE

- Debe disponer de un usuario válido de SNMP v3 con los permisos de `lectura` predeterminados. Consulte «Inicio rápido: Configuración de un HPE 5900 para gestionarlo con HPE OneView».
- Las SAN de HPE solo pueden ser gestionadas por un único dispositivo de HPE OneView.

Configuración del administrador de SAN de Cisco

- Debe disponer de un usuario válido de SNMP v3 con permisos de `escritura`. Consulte «Inicio rápido: Configuración de un conmutador Cisco para agregarlo como administrador de SAN para gestionarlo con HPE OneView».
- Las SAN de Cisco solo pueden ser gestionadas por un único dispositivo de HPE OneView.

Configuración de un administrador de SAN Brocade Network Advisor (BNA)

- Debe disponer de una cuenta de usuario válida con SMIS ejecutándose. Para obtener más información, consulte la documentación del administrador de SAN.
- Para permitir que HPE OneView vea los cambios en la topología de la estructura SAN automáticamente, debe deshabilitar `Track Fabric Changes` (Seguimiento de los cambios en la estructura) en el BNA. En caso contrario, debe utilizar una operación `Accept Changes` (Aceptar los cambios) en el BNA siempre que haga cambios en la topología de la estructura SAN para que HPE OneView los vea. Consulte la documentación de BNA para obtener más información sobre cómo deshabilitar `Track Fabric Changes` (Seguimiento de los cambios en la estructura).
- Las SAN basadas en BMA pueden ser gestionadas por uno o más dispositivos de HPE OneView.

20.6 Redes SAN

20.6.1 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Asociar una SAN gestionada a una red
- Activar o desactivar la distribución automática en zonas para una SAN gestionada
- Edición de una SAN
- Descarga de la tabla de los extremos de SAN
- Generación de un informe de división por zonas inesperada

20.6.2 Acerca de las SAN

Las SAN son redes de almacenamiento Fibre Channel (FC) o Fibre Channel sobre Ethernet (FCoE) que conectan los servidores a los sistemas de almacenamiento. Una SAN puede encontrarse en los estados siguientes:

Detectada — Es una SAN que no está asociada a una red. Las SAN se detectan automáticamente cuando se agrega un administrador de SAN a HPE OneView.

Gestionada — Es una SAN que está asociada a una o varias redes de HPE OneView. Solo las SAN gestionadas pueden configurarse para que HPE OneView las distribuya en zonas automáticamente.

Redes SAN Direct attach

HPE OneView crea una SAN Direct attach (Flat SAN) automáticamente cuando se configura un receptáculo con una interconexión lógica que contiene un conjunto de enlaces ascendentes Direct attach. HPE OneView asigna nombres a las SAN Direct attach utilizando el formato *<interconexión><conjunto de enlaces ascendentes>*. La SAN que crea HPE OneView es una SAN Fibre Channel (FC) Direct attach que no está distribuida en zonas y que no puede modificarse.

NOTA: HPE OneView crea una SAN para cada módulo de interconexión que está conectado a una red Fibre Channel Direct attach.

20.6.2.1 Acerca de la distribución en zonas SAN

Directiva de distribución en zonas

Una zona SAN permite la comunicación entre los dispositivos conectados a la SAN. Las directivas de distribución en zonas SAN determinan el modo en que debe configurarse la distribución en zonas en una SAN. Las directivas de distribución en zonas SAN definen si la distribución en zonas está automatizada, así como el formato de nomenclatura de las zonas y los alias. En HPE OneView, puede especificar el formato del nombre de las zonas y los alias de que se crearán cuando asocie un volumen de almacenamiento a un perfil de servidor a través de la conexión de volúmenes. Gracias a la especificación de formatos de nombres de zonas y de alias mediante cadenas de texto y los objetos de perfil de servidor, puede crear nombres que tengan sentido y que se ajusten a sus convenciones de nomenclatura.

NOTA: HPE OneView solo realiza la distribución en zonas cuando se agrega una conexión a un perfil de servidor y se le conecta un volumen de almacenamiento SAN. Cuando se haga esto, HPE OneView determinará si la distribución en zonas actual permite la conectividad. Si la distribución en zonas actual no permite la conectividad, HPE OneView creará la distribución en zonas necesaria basándose en la directiva de distribución en zonas especificada.

Automatización de la distribución en zonas

La distribución automática en zonas permite a HPE OneView crear, editar y eliminar zonas automáticamente en una SAN distribuida en zonas cuando se conectan volúmenes de almacenamiento a los servidores mediante una conexión de volúmenes de un perfil de servidor.

Sí — La distribución en zonas está automatizada. HPE OneView toma el control total de la nomenclatura y el contenido de las zonas basándose en la directiva de distribución en

zonas de la SAN. Utilice la distribución automática en zonas cuando desee que HPE OneView configure zonas nuevas para las conexiones de volúmenes a los perfiles de servidor. Las zonas existentes no se modifican a menos que cambien los atributos de almacenamiento SAN definidos en un perfil de servidor.

No HPE OneView no modifica la distribución en zonas. La distribución en zonas debe gestionarse manualmente.

20.7 Información adicional

- «Conceptos básicos sobre el modelo de recursos» (página 45)
- «Solución de problemas de almacenamiento» (página 447)

21 Gestión de conmutadores, conmutadores lógicos y grupos de conmutadores lógicos

Los conmutadores de la parte superior del bastidor permiten realizar la consolidación de redes y la gestión de blades de servidor cuando se agregan al centro de datos.

Un grupo conmutadores lógicos sirve como referencia estructural para crear un conmutador lógico. Un conmutador lógico permite agregar uno o varios conmutadores físicos que tienen una configuración común.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Switches (Conmutadores)	`switches`
Logical Switches (Conmutadores lógicos)	`logical-switches`
Logical Switch Groups (Grupos de conmutadores lógicos)	`logical-switch-groups`

21.1 Gestión de conmutadores

21.1.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de red

21.1.2 Tareas para conmutadores

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Actualizar las asociaciones de interconexiones actualizando un conmutador.

21.1.3 Acerca de los conmutadores de la parte superior del bastidor

Los conmutadores de la parte superior del bastidor proporcionan a una estructura unificada y convergente sobre Ethernet para el tráfico de LAN y SAN. Este unification permite la consolidación de la red, reduciendo el número de adaptadores y cables necesarios y eliminando conmutadores redundantes.

Una configuración de receptáculos, blades de servidor y dispositivos de otros fabricantes, como por ejemplo, conmutadores de la parte superior del bastidor, proporciona la capacidad de ampliación en la gestión de blades de servidor y un mayor demanda de ancho de banda desde cada servidor con la redundancia de capa de acceso. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener la lista completa de dispositivos admitidos.

Los centros de datos modulares, que implementan tanto blades de servidor individuales como bastidores de blades de servidor, pueden utilizar un modelo de implementación de conmutadores de la parte superior del bastidor como solución para la consolidación de redes. Puede aumentar la flexibilidad del centro de datos colocando recursos de conmutación en cada bastidor, de modo que se pueda agregar la conectividad del servidor.

La integración con los conmutadores de la parte superior del bastidor ofrece las ventajas siguientes:

- Un sistema modular distribuido que crea un entorno de acceso de servidor escalable
- Un único punto de gestión y de cumplimiento de directivas

- Reducción de los costes de operación (menos de cableado, menor consumo de energía para refrigeración y operación, utilización eficaz del ancho de banda)

Actualmente, el soporte de HPE OneView para estos recursos se centra en proporcionar una vista supervisada del entorno, con capacidad para cambios de configuración limitados en los puertos de interconexiones. No se admite la actualización del firmware. HPE OneView admite la supervisión de la configuración y el estado así como la supervisión de la conformidad de conmutadores de la parte superior del servidor Cisco Nexus cuando actúan como conmutadores de acceso y están conectados directamente a Cosco FEX (Cisco Fabric Extender para BladeSystem) en un receptáculo. Dentro de HPE OneView, los conmutadores de la parte superior del bastidor se agregan y se eliminan a través de las plantillas de grupos de conmutadores lógicos y los conmutadores lógicos asociados.

Con HPE OneView puede:

- Expresar los estados esperados y reales de los conmutadores y las interconexiones FEX con la supervisión de cumplimiento correspondiente.
- Ver información sobre los conmutadores físicos.
- Ver información sobre los puertos físicos.
- Ver información estadística.
- Ver los eventos de estado y los cambios de estado de los puertos como alertas, desde los conmutadores Cisco Nexus.
- Ir a la vista **mapa** de los conmutadores Cisco Nexus y las interconexiones FEX para ver la relación entre estos recursos.
- Detectar la disponibilidad de la red y ver las incoherencias entre las redes definidas dentro de HPE OneView y las aprovisionadas en los conmutadores Cisco Nexus.

21.2 Gestión de conmutadores lógicos

21.2.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de red

21.2.2 Tareas para los conmutadores lógicos

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Crear, editar, actualizar o eliminar un conmutador lógico.
- Mover un conmutador lógico de modo funcional gestionado a supervisado.
- Hacer que un conmutador lógico sea coherente con su grupo de conmutadores lógicos asociado.

21.2.3 Acerca de los conmutadores lógicos

Un conmutador lógico se agrega a HPE OneView como conmutador lógico gestionado o supervisado. El conmutador lógico puede estar formado por un máximo de dos conmutadores físicos de la parte superior del bastidor (externos al receptáculo c7000) configurados en un único dominio de apilamiento.

Hay una limitación de conectividad de una interconexión lógica con un conmutador lógico. Las interconexiones de una interconexión lógica no se pueden conectar a más de un conmutador lógico.

Un conmutador lógico se basa en una configuración de grupo de conmutadores lógicos. Si el conmutador lógico cambia a un estado `Inconsistent with group` (Incoherente con el grupo)

(debido a cambios en el conmutador lógico o en el grupo de conmutadores lógicos), para volver a un estado coherente.

Sobre la asignación de conmutadores Cisco Nexus a un conmutador lógico

Se puede crear un conmutador lógico con un máximo de dos conmutadores Cisco Nexus. Cuando hay dos conmutadores Cisco Nexus en un conmutador lógico, se espera que estén en un entorno de canal de puerto virtual (vPC). El vPC debe configurarse en los dos conmutadores, y ambos deben pertenecer al mismo dominio de vPC. Para obtener información sobre los conmutadores compatibles, consulte la información de compatibilidad en la **Biblioteca de información de Hewlett Packard Enterprise**.

Más información

«Conmutadores lógicos gestionados»
«Conmutadores lógicos supervisados»
«Directrices de configuración de conmutadores lógicos»
«Acerca de los grupo de conmutadores lógicos»

21.2.3.1 Conmutadores lógicos gestionados

Agregar un conmutador lógico para la gestión de HPE OneView le permite aplicar las configuraciones necesarias para que los puertos de enlaces ascendentes de interconexión se suministren en los puertos (de enlaces descendentes) internos del conmutador. El modo gestionado le permite implementar conexiones de perfil de servidor para interconexiones, supervisar el estado de la operación, recopilar estadísticas y avisar a los usuarios de condiciones concretas e incompatibilidades entre el conmutador ascendente y la interconexión.

Al agregar un conmutador lógico, cualquier configuración existente para los puertos conectados a interconexiones de HPE OneView se vuelve a configurar basándose en la configuración especificada por los enlaces ascendentes de interconexión de HPE OneView. Cualquier puerto gestionado activamente por un sistema de gestión externo permanece sin modificación y no queda bajo la gestión de HPE OneView.

Cuando se agrega un conmutador lógico en el modo operativo **Managed** (Gestionado) para la gestión de HPE OneView management, el banner *Message of the Day* (Mensaje del día) (MOTD) de cada conmutador vuelve a escribirse con "`This switch is being controlled by OneView Domain, Appliance ID: {}`" (Este conmutador está siendo controlado por OneView Domain, ID del dispositivo: {}). Este mensaje indica que el conmutador está siendo gestionado activamente por una instancia de HPE OneView concreta. Este mensaje se elimina y se sustituye por el mensaje del banner *Message of the Day* (Mensaje del día) predeterminado cuando el conmutador lógico pasa del modo operativo **Managed** (Gestionado) a **Monitor** (Supervisión) o cuando se elimina el conmutador lógico.

Antes de agregar un conmutador lógico gestionado

Antes de agregar un conmutador lógico como *gestionado*, tenga en cuenta lo siguiente para las interconexiones de Virtual Connect y Fabric Extender conectadas físicamente al conmutador lógico:

- Cuando solo hay redes Ethernet IPv4 asignadas a un conjunto de enlaces ascendentes en el momento de la creación, el conjunto de enlaces ascendentes se puede conectar físicamente a cualquier conmutador ascendente del conmutador lógico.
- Cuando se asigna una red FCoE a un conjunto de enlaces ascendentes en el momento de la creación, el conjunto de enlaces ascendentes se limita a la conectividad física única-albergada y todos los puertos de enlaces ascendentes deben conectarse con el mismo conmutador ascendente del conmutador lógico.

  Si posteriormente se agrega un puerto al conjunto de enlaces ascendentes con una red FCoE o si un puerto existente en el conjunto de enlaces ascendentes se conecta a un segundo conmutador ascendente, dicho puerto no está disponible para la configuración y

se genera una alerta. Si se conecta un nuevo puerto agregado al conjunto de enlaces ascendentes al mismo conmutador que los otros puertos, dicho puerto está disponible para soportar tráfico y no se genera ninguna alerta.

Para cambiar un conjunto de enlaces ascendentes de conectividad única-albergada o viceversa, la configuración del conjunto de enlaces ascendentes debe eliminarse y volverse a crear con las asignaciones de red y la configuración física adecuadas.

- Asegúrese de que el LLDP esté habilitado en los puertos internos (enlace descendente) de conmutador de la parte superior del bastidor donde las interconexiones de Virtual Connect bajo la gestión de HPE OneView están conectadas.

Más información

«Acerca de los conmutadores lógicos»
«Directrices de configuración de conmutadores lógicos»

21.2.3.2 Conmutadores lógicos supervisados

Agregar un conmutador lógico como *supervisado* permite que HPE OneView supervise el conmutador lógico para el estado de la operación, recopile estadísticas y avise a los usuarios sobre condiciones concretas e incompatibilidades entre el conmutador y la interconexión de Virtual Connect o Fabric Extender. En el modo supervisado, la implementación de las conexiones del perfil de servidor se admite para interconexiones de HPE Virtual Connect pero no para interconexiones de Fabric Extender (FEX).

Más información

«Acerca de los conmutadores lógicos»

21.2.3.3 Directrices de configuración de conmutadores lógicos

- Cuando las interconexiones de Virtual Connect están conectadas a un conmutador lógico, un conjunto de enlaces ascendentes no puede distribuir varias interconexiones. Esta limitación es similar a las interconexiones FEX. Sin embargo, una interconexión de Virtual Connect admite varios conjuntos de enlaces ascendentes.
- Cuando activa o desactiva un puerto interno de conmutador de la parte superior del bastidor, el puerto asociado en una interconexión FEX también muestra el estado del puerto actualizado.
- Cuando se recuperan las direcciones MAC para las interconexiones FEX, solo se muestran las entradas asociadas con las interconexiones FEX gestionadas.
- Si se asigna una red FCoE a un conjunto de enlaces ascendentes como dual-albergada (una configuración no válida) dicha red FCoE no se aprovisiona en el conmutador. La implementación de cualquier conexión de perfil de servidor con esta conexión FCoE dará error.
- Cuando se define y se configura un conmutador lógico con un único conmutador físico, el conjunto de enlaces ascendentes asociado con cualquier módulo FEX conectado a este conmutador lógico se considerará único-albergado. Por tanto, puede agregar una red FCoE al conjunto de enlaces ascendentes aún cuando el conjunto de enlaces ascendentes se creara inicialmente solo con redes Ethernet. La implementación de cualquier conexión de perfil de servidor con esta conexión FCoE se completará.
- Para los perfiles de servidor creados para los puertos de servidor conectados a interconexiones FEX, las redes Ethernet solo se admiten en la función física *a* y las redes FCoE solo se admiten en la función física *b* del puerto de servidor. Cuando ambas funciones físicas tienen conexiones definidas, el tráfico se divide equitativamente entre ambos puertos.

- Si HPE OneView no puede iniciar sesión en el conmutador, se genera una alerta crítica. Evite cualquier evento del conmutador que pueda activar la configuración del conmutador; por el contrario, el conmutador pasa al estado `ConfigError` y deberá volver a aplicar la configuración en las interconexiones lógicas asociadas para recuperarlo.
- Si HPE OneView no puede reclamar un conmutador miembro del conmutador lógico cuando el modo operativo del conmutador lógico es **Managed** (Gestionado), el estado operativo del conmutador pasa a `Added with Error` (Agregado con error). En este caso, el banner `Message of the Day` (Mensaje del día) (MOTD) del conmutador indica que el conmutador está siendo reclamado actualmente por otro dispositivo de HPE OneView y aparece el mensaje "`This switch is being controlled by OneView Domain, Appliance ID: {}`" (Este conmutador está siendo controlado por OneView Domain, ID de dispositivo: {}). Debe eliminar el conmutador lógico del dispositivo de HPE OneView y, a continuación, realizar una actualización en el conmutador lógico del dispositivo de HPE OneView actual para reiniciar la operación de reclamación.
- HPE OneView no automatiza completamente la configuración de la conectividad FCoE en el conmutador especificado en el conmutador lógico. Para cada red FCoE especificada en el conjunto de enlaces ascendentes, HPE OneView solo aprovisiona la VLAN para dicha red del conmutador. Los administradores de red deben aprovisionar configuración adicional para la conectividad FCoE de forma manual en el conmutador además de lo que aprovisiona HPE OneView.
    - Para implementar las conexiones de perfil de servidor en una interconexión FEX, HPE OneView aprovisiona la interfaz Fibre Channel virtual (VFC), vinculación de VFC con el puerto de enlace descendente FEX y la asignación de interfaz VSAN al conmutador.
    - Para implementar las conexiones de perfil de servidor para una interconexión de Virtual Connect, el administrador de red debe configurar la interfaz Fibre Channel virtual (vFC), la vinculación de VFC con el puerto de servidor y la vinculación de la asignación de la interfaz VSAN de forma manual.
- Cuando se elimina un módulo de expansión de conmutador Nexus, si el módulo no está apagado, se genera una alerta de advertencia.
- HPE OneView puede detectar cambios en la configuración que se producen en los conmutadores especificados en el conmutador lógico cuando ya no coincide con la configuración aprovisionada por HPE OneView. Se generan alertas de advertencia. Los administradores pueden corregir la configuración manualmente o volver a aplicar la configuración en las interconexiones lógicas asociadas a recuperar.

21.3 Gestión de grupos de conmutadores lógicos

21.3.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de red

21.3.2 Tareas para los grupos de conmutadores lógicos

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Crear, editar o eliminar un grupo de conmutadores lógicos.

21.3.3 Acerca de los grupo de conmutadores lógicos

Un grupo de conmutadores lógicos es una plantilla para la creación de conmutadores lógicos. Los conmutadores lógicos son una agregación de hasta dos conmutadores físicos de la parte superior del bastidor.

Una vez que se crea a partir de un grupo de conmutadores lógicos, un conmutador lógico sigue estando asociado a su grupo de conmutadores lógicos. Cualquier cambio en la coherencia entre el grupo de conmutadores lógicos y sus conmutadores lógicos asociados se supervisa y se muestra en la pantalla del conmutador lógico asociado en HPE OneView.

21.4 Información adicional

- «Conceptos básicos sobre el modelo de recursos» (página 45)
- «Solución de problemas de conmutadores lógicos» (página 436)

22 Gestión de usuarios y autenticación

El dispositivo requiere que los usuarios inicien sesión con un nombre de usuario y una contraseña válidos, y la seguridad se mantiene a través de la autenticación de usuarios y la autorización basada en roles. Las cuentas de usuario pueden ser locales, en las que las credenciales se almacenan en el dispositivo, o pueden estar en un directorio de la empresa o la organización (Microsoft Active Directory, por ejemplo) alojado en otro lugar, en cuyo caso el dispositivo se pone en contacto con el servidor de directorio definido para comprobar las credenciales de los usuarios.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Users and Groups (Usuarios y grupos)	`users`, `roles`, `authz`, `logindomains`, `logindomains/global-settings` y `logindomains/grouptorolemapping`

22.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

22.2 Tareas de gestión de usuarios y grupos

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Agregar, editar (incluida la actualización de una contraseña de usuario) o quitar un usuario con autenticación local.
- Agregar un usuario con autenticación basada en directorio.
- Agregar un grupo con autenticación basada en directorio.
- Designar los privilegios del usuario.
- Restablecer la contraseña del administrador.
- Agregar un servicio de directorio de autenticación.
- Habilitar o deshabilitar los inicios de sesión locales.
- Cambiar la configuración del servicio de directorio de autenticación.
- Establecer un servicio de directorio de autenticación como directorio predeterminado.
- Quitar un servicio de directorio de autenticación del dispositivo.

22.3 Acerca de las cuentas de usuario

Acceso basado en roles

El dispositivo proporciona roles predeterminadas para separar las responsabilidades en una organización. Un rol de usuario permite el acceso a determinados recursos gestionados desde el dispositivo.

El control de acceso basado en roles establece permisos para realizar las operaciones asignadas a cada uno de sus roles. Debe asignar roles específicos a los usuarios o los procesos del sistema, lo que les concede el permiso necesario para realizar ciertas operaciones en el sistema. Debido a que los permisos no se le asignan a un usuario directamente, sino que los adquiere a través de sus roles, los derechos de cada usuario se gestionan asignándole los roles adecuados.

Cuando se pone en marcha el dispositivo por primera vez, hay una cuenta de administrador predeterminada con privilegios de acceso completos (administrador de infraestructuras). Para obtener más información sobre las acciones que puede realizar cada rol, consulte «Privilegios de acciones para los roles de usuario».

Autenticación local

Puede agregar un usuario autorizado para tener acceso a todos los recursos gestionados por el dispositivo (usuario con acceso completo) o agregar un usuario que tiene acceso en función de su puesto de trabajo (especialista basado en roles). Para cada uno de estos usuarios, la autenticación se realiza comparando la información de inicio de sesión del usuario con un directorio de autenticación alojado localmente en el dispositivo.

El usuario administrador predeterminado del dispositivo recibe automáticamente privilegios de acceso total (administrador de infraestructuras).

Autenticación basada en directorios

Puede agregar un usuario autorizado por su pertenencia a grupos para tener acceso a todos los recursos gestionados por el dispositivo (usuario con acceso completo) o agregar un usuario autorizado por su pertenencia a grupos que tiene acceso en función de su puesto de trabajo (especialista basado en roles). Para cada uno de estos usuarios, la autenticación se realiza comparando la información de inicio de sesión del usuario con un directorio de empresa.

22.4 Acerca de los roles de usuario

Los roles de usuario permiten asignar permisos y privilegios a los usuarios dependiendo de sus responsabilidades laborales. Puede asignar privilegios completos a un usuario, o bien asignarle un subconjunto de permisos para ver, crear, editar o eliminar recursos gestionados por el dispositivo.

Tabla 12 Permisos del rol de usuario

Rol	Tipo de usuario	Permisos o privilegios
Completo	**Administrador de infraestructuras**	Ver, crear, editar o eliminar recursos gestionados o supervisados por el dispositivo, incluida la gestión del propio dispositivo a través de la interfaz de usuario o de las API de REST. Un administrador de infraestructuras también puede gestionar la información que proporciona el dispositivo en forma de actividades, notificaciones y registros. Solo un administrador de infraestructuras puede restaurar un dispositivo desde un archivo de copia de seguridad.
Solo lectura	**Solo lectura**	Ver información sobre recursos gestionados o supervisados. No se pueden agregar, crear, editar, quitar ni eliminar recursos.

Tabla 12 Permisos del rol de usuario *(continuación)*

Rol	Tipo de usuario	Permisos o privilegios
Especializado	**Administrador de copia de seguridad**	Crear y descargar archivos de copia de seguridad, ver la configuración y las actividades del dispositivo. Tiene autoridad para utilizar secuencias de comandos para iniciar sesión en el dispositivo y ejecutar secuencias de comandos para realizar copias de seguridad del dispositivo. No se puede restaurar el dispositivo desde un archivo de copia de seguridad. **NOTA:** Este rol ha sido específicamente diseñado para secuencias de comandos que utilizan las API de REST para iniciar sesión en el dispositivo para crear la copia de seguridad y descargarla, de forma que no exponga las credenciales de administrador de infraestructuras para las operaciones de copia de seguridad. Hewlett Packard Enterprise recomienda que los usuarios con este rol no inicien sesiones interactivas a través de la interfaz de usuario de HPE OneView.
	Administrador de la red	Ver, crear, editar, o eliminar redes, conjuntos de redes, conexiones, interconexiones, conjuntos de enlaces ascendentes y lotes de firmware. Ver notificaciones, registros y actividades relacionadas. No se pueden gestionar cuentas de usuario.
	Administrador de servidores	Ver, crear, editar o eliminar perfiles de servidor y plantillas, conjuntos de redes, receptáculos y lotes de firmware. Acceso al Onboard Administrator, a los servidores físicos y al registro de hipervisor. Ver conexiones, redes, bastidores, energía y las notificaciones, registros y actividades relacionadas. Agregar volúmenes, pero no se pueden agregar pools ni sistemas de almacenamiento. No se pueden gestionar cuentas de usuario.
	Administrador de almacenamiento	Ver, agregar, editar o quitar pools de almacenamiento. Ver, agregar o quitar pools de almacenamiento. Ver, crear, editar, agregar o eliminar volúmenes. Ver, crear, editar o eliminar plantillas de volumen. Ver, agregar o editar administradores de SAN. Ver o editar redes SAN.

22.5 Privilegios de acciones para los roles de usuario

En la tabla siguiente se muestran los privilegios de acciones de los usuarios asociados a cada rol de usuario.

El privilegio `Use` (Usar) es un caso especial que le permite asociar objetos a los objetos que le pertenecen, pero que no tiene permiso para cambiar. Por ejemplo, en un grupo de interconexiones lógicas, un usuario que tiene asignado rol de administrador de servidores no tiene permiso para definir grupos de interconexiones lógicas, pero puede utilizarlos al agregar un receptáculo.

Tabla 13 Privilegios de acciones para los roles de usuario

Categoría	Privilegios de acciones para los roles de usuario C=Create (Crear), R=Read (Leer), U=Update (Actualizar), D=Delete (Eliminar), Usar						
	Administrador de infraestructuras	Administrador de servidores	Administrador de la red	Administrador de copia de seguridad	Administrador de almacenamiento	Solo lectura	Configuración de hardware
actividades	CRUD	CRU	CRU	R	CRU	R	CRU
alertas	RUD	RUD	RUD	—	RUD	R	RUD
dispositivo	CRUD	R	R	R	R	R	R
registros de auditoría	CR	R	R	—	R	—	—
copias de seguridad	CRUD	R	R	CRD	R	R	R
cadena de comunidad	RU	R	CRU	—	R	—	—
conexiones	CRUD	R	CR	R	R	R	—
plantillas de conexión	CRUD, Usar	R, Usar	CRUD	R	R	R	—
usuarios de la consola	CRUD	—	—	—	—	—	—
centros de datos	CRUD	CRUD	R	R	R	R	CRUD
registros de depuración	CRUD	CRU	CRU	—	R	R	—
compartimentos de dispositivo	CRUD	CRUD	R	R	R	R	CRUD
dominios	CRUD	R	CRU	R	R	R	—
receptáculos	CRUD	CRUD	R	R	R	R	CRUD
grupos de receptáculos	CRUD, Usar	CRUD, Usar	R	R	R	R	—
redes Ethernet	CRUD	R	CRUD	R	R	R	—
eventos	CRU	CRU	CRU	—	R	R	CR
estructuras	CRUD	R	CRUD	R	R	R	—
alias de FC	CRUD	R	R	R	CRUD	R	—
gestores de dispositivos FC	CRUD	R	R	R	CRUD	R	—
extremos de FC	R	R	R	R	R	R	—
redes FC	CRUD	R	CRUD	R	R	R	—
redes FCOE	CRUD, Usar	R	CRUD, Usar	R	R	R	—
puertos FC	R	R	R	R	R	R	—

Tabla 13 Privilegios de acciones para los roles de usuario *(continuación)*

Categoría	Privilegios de acciones para los roles de usuario C=Create (Crear), R=Read (Leer), U=Update (Actualizar), D=Delete (Eliminar), Usar						
	Administrador de infraestructuras	**Administrador de servidores**	**Administrador de la red**	**Administrador de copia de seguridad**	**Administrador de almacenamiento**	**Solo lectura**	**Configuración de hardware**
proveedores FC	R	R	R	R	R	R	—
redes SAN FC	CRUD	R	R	R	CRUD	R	—
servicios SAN FC	CRUD	R	R	R	CRUD	R	—
conmutadores FC	R	R	R	R	R	R	—
tareas FC	R	R	R	R	R	R	—
zonas FC	CRUD	R	R	R	CRUD	R	—
controladores de firmware	CRUD	CRUD	CRUD	R	R	R	R
configuración global	CRUD	CRUD	CRUD	R	CRUD	R	CRUD
asignaciones de grupo a rol	CRUD	—	—	—	R	R	—
vmacs de intervalo de ID (direcciones MAC)	CRUD	R	CRU	R	R	R	—
vsns de intervalo de ID (números de serie)	CRUD	CRU	R	R	R	R	—
vwwns de intervalo de ID (Nombres World Wide)	CRUD	R	CRU	R	R	R	—
herramientas integradas	CRUD	R	R	R	R	R	—
interconexiones	CRUD	CR	CRUD	R	R	R	CRUD, Usar
tipos de interconexiones	R, Usar	R	CRUD	R	R	R	CRUD
etiquetas	CRUD	CRUD	CRUD	R	CRUD	R	R
licencias	CRUD	CR	R	R	R	R	—
enlaces descendentes lógicos	R	R	R	R	R	R	—
interconexiones lógicas	CRU, Usar	R, Usar	RU, Usar	R	R	R	—

Tabla 13 Privilegios de acciones para los roles de usuario *(continuación)*

Categoría	Privilegios de acciones para los roles de usuario C=Create (Crear), R=Read (Leer), U=Update (Actualizar), D=Delete (Eliminar), Usar						
	Administrador de infraestructuras	Administrador de servidores	Administrador de la red	Administrador de copia de seguridad	Administrador de almacenamiento	Solo lectura	Configuración de hardware
grupos de interconexiones lógicas	CRUD, Usar	R, Usar	CRUD, Usar	R	R	R	—
dominios de inicio de sesión	CRUD	—	—	—	R	R	—
sesiones de inicio de sesión	CRUD	RU	RU	RU	RU	RU	—
redes SAN gestionadas	CRUD, Usar	R	R, Usar	R	CRUD, Usar	R	—
dominios de VC migrables	CRUD, Usar	—	—	—	—	—	—
redes	CRUD, Usar	R, Usar	CRUD, Usar	R	R	R	—
conjuntos de redes	CRUD, Usar	CRUD[1]	CRUD	R	R	R	—
notificaciones	CRUD	CRD	CRD	R	R	R	—
organizaciones	CRUD	—	—	—	R	R	—
puertos	RU, Usar	—	RU, Usar	—	R	—	—
dispositivos de alimentación	CRUD	CRUD	R	R	R	R	CRUD
bastidores	CRUD	CRUD	R	R	R	R	CRUD
informes	R	R	R	R	R	R	—
restauraciones	CRUD	—	—	—	—	R	—
roles	CRUD	—	—	—	—	R	—
redes SAN	CRUD, Usar	R	R	R	CRUD, Usar	R	—
administrador de SAN	CRUD, Usar	R	R	R	CRUD, Usar	R	—
hardware de servidor	CRUD, Usar	CRUD, Usar	R	R	R	R	CRUD, Usar
tipos de hardware de servidor	CRUD, Usar	CRUD, Usar	R	R	R	R	CRUD, Usar
perfiles de servidor	CRUD	CRUD	R	R	R	R	—
pools de almacenamiento	CRD	R	R	R	CRUD	R	—

Tabla 13 Privilegios de acciones para los roles de usuario *(continuación)*

Categoría	Privilegios de acciones para los roles de usuario C=Create (Crear), R=Read (Leer), U=Update (Actualizar), D=Delete (Eliminar), Usar						
	Administrador de infraestructuras	Administrador de servidores	Administrador de la red	Administrador de copia de seguridad	Administrador de almacenamiento	Solo lectura	Configuración de hardware
sistemas de almacenamiento	CRUD	R	R	R	CRUD	R	—
puertos de destino de almacenamiento	CRUD	R	R	R	CRUD	R	—
volúmenes de almacenamiento	CRUD	CRUD	R	R	CRUD	R	—
conexiones de volumen de almacenamiento	CRUD	CRUD	R	R	CRUD	R	—
plantillas de volumen de almacenamiento	CRUD	R	R	R	CRUD	R	—
conmutadores	CRUD, Usar	RU	CRUD	R	R	R	—
tareas	R	R	R	R	R	R	R
reenvío de capturas	RU	R	R	R	R	R	—
equipos no gestionados	CRUD	CRUD	R	R	R	R	CRUD
conjuntos de enlaces ascendentes	CRUD	R	CRUD	R	R	R	—
usuarios	CRUD	—	—	—	—	R	—
preferencias de usuario	CRUD	—	—	—	—	R	—

[1] Los administradores de servidores no pueden editar anchos de banda.

22.6 Acerca de la configuración de autenticación

La seguridad se mantiene a través de la autenticación de usuarios y la autorización basada en roles. Las cuentas de usuario pueden ser locales, en las que las credenciales de los usuarios se almacenan en el dispositivo, o pueden estar en un directorio (Microsoft Active Directory, por ejemplo) alojado en otro lugar, en cuyo caso el dispositivo se pone en contacto con el servidor de directorio designado para comprobar las credenciales de los usuarios.

Cuando inicia sesión en el dispositivo, el servicio de directorio de autenticación autentica a cada usuario, es decir, confirma el nombre de usuario y la contraseña. Utilice el panel de configuración **Authentication** (Autenticación) para cambiar la configuración de autenticación en el dispositivo, que se rellena con valores predeterminados durante la configuración inicial del dispositivo.

Para ver o realizar cambios en la configuración de **Authentication** (Autenticación), inicie sesión con privilegios de administrador de infraestructuras. Ningún otro usuario está autorizado para cambiar o ver esta configuración.

Vea o acceda a la configuración de **Authentication** (Autenticación) seleccionando **Settings→Security→Authentication** (Configuración > Seguridad > Autenticación) o mediante las API de REST.

22.7 Acerca de la autenticación en servicios de directorio

Puede utilizar un servicio de directorio de autenticación externo (también denominado directorio de empresa o dominio de inicio de sesión de autenticación) para proporcionar un inicio de sesión único para grupos de usuarios en lugar de mantener cuentas de inicio de sesión locales individuales. A cada usuario de un grupo se le asigna el mismo rol (por ejemplo, administrador de infraestructuras). Un ejemplo de un servicio de directorio de autenticación es un directorio corporativo que utiliza LDAP (Lightweight Directory Access Protocol).

Después de que se haya configurado el servicio de directorio, cualquier usuario del grupo puede iniciar sesión en el dispositivo. En la ventana de inicio de sesión, el usuario:

- Introduce su nombre de usuario (normalmente, el atributo Nombre común, CN).

  El formato del nombre de usuario depende del tipo de directorio.
- Introduce la contraseña.
- Selecciona el servicio de directorio de autenticación.

En el control de la sesión ( ), el usuario se identifica por su nombre precedido por el servicio de directorio de autenticación. Por ejemplo:

```
CorpDir\pat
```

IMPORTANTE:

A diferencia de los usuarios locales, si se elimina un usuario de un directorio de autenticación, sus sesiones activas permanecerán activas hasta que dicho usuario las cierre.

Si se produce un cambio en la asignación de grupos a roles (incluida una eliminación) para un grupo del directorio de autenticación mientras un usuario de ese grupo tiene una sesión iniciada, su sesión activa actual no se ve afectada hasta que la cierra. Las sesiones de los usuarios locales se cierran cuando se efectúan modificaciones de ese tipo.

Autenticación de usuarios

Cuando se agrega un servicio de directorio de autenticación al dispositivo, se proporcionan criterios de búsqueda para que el dispositivo pueda encontrar el grupo.

Adición de un servidor de directorio

Si replica el servicio de directorio de autenticación para alta disponibilidad o tolerancia frente a desastres, agregue el servicio de directorio replicado como un servicio de directorio independiente.

Después de configurar y añadir un servidor de directorio, puede designarlo como servicio de directorio predeterminado.

Después de añadir un servicio de directorio de autenticación y servidor

Es posible:

- Agregar un grupo, que ya se había definido en el servicio de directorio, para que todos sus miembros puedan iniciar sesión en el dispositivo.
- Permitir solo los inicios de sesión locales, que es el valor predeterminado.
- Permitir tanto los inicios de sesión locales como los inicios de sesión para las cuentas de usuario autenticadas por el servicio de directorio.

- Desactivar los inicios de sesión locales de manera que solo los usuarios cuyas cuentas se autentican mediante el servicio de directorio puedan iniciar sesión. No se permitirá el inicio de sesión en las cuentas locales.

Consideraciones sobre la configuración de un servicio de directorio de Microsoft Active Directory

- A continuación se indica la correspondencia entre atributos de Active Directory y propiedades de LDAP:

Propiedad de LDAP	Atributo de Active Directory
`cn`	Common-Name
`uid`	UID
`userPrincipalName`	User-Principal-Name
`sAMAccountName`	SAM-Account-Name

  Si el *`nombre de usuario`* no contiene un carácter `@` (para denotar un UPN) ni un carácter `\` (para denotar un *`dominio\inicio de sesión`*), se intentan estos inicios de sesión en el orden siguiente:

  1. El *`nombre-de-usuario`* se trata como sAMAccountName y se le antepone el *`nombre-de-directorio`* (*`nombre-de-directorio\nombre-de-usuario`*)
  2. El *`nombre-de-usuario`* se trata como UID.
  3. El *`nombre-de-usuario`* se trata como CN.

- Si se crea un objeto de usuario en **Usuarios y equipos de Active Directory** en Microsoft Management Console, el valor predeterminado de los nombres es el siguiente.

  Especifique los componentes siguientes del nombre del usuario, que se muestran aquí con el atributo correspondiente:

Componente del nombre de usuario	Atributo
First Name (Nombre)	givenName
Intials (Iniciales)	initial
Last Name (Apellido)	sn

  De forma predeterminada, el campo con la etiqueta `Full Name` (Nombre completo) tiene este formato, y esta cadena se asigna al atributo `cn` (**Common Name** [Nombre común]).

  `givenName.initials.`*`givenName.initial.sn`*

  En el cuadro de diálogo **New Object – user** (Nuevo objeto: usuario), también debe especificar un **User logon name** (Nombre de inicio de sesión del usuario). Esto, junto con el nombre de dominio de DNS, se convierte en el `userPrincipalName`.

  El `userPrincipalName` es un nombre alternativo que el usuario puede utilizar para iniciar sesión. Tiene este formato:

  `LogonName``@`*`DNSDomain`*

  Por ejemplo:

  `JoeUser@exampledomain.example.com`

- Por último, a medida que se escribe el **User logon name** (Nombre de inicio de sesión del usuario), los primeros veinte caracteres se copian automáticamente en el campo **pre-Windows 2000 logon name** (Nombre de inicio de sesión anterior a Windows 2000), que se convierte en el atributo `sAMAccountName`.
- No se aceptan los inicios de sesión CN para las cuentas de usuario integradas de Active Directory, como `Administrador`. Se aceptan otros formatos de inicio de sesión si sus respectivos atributos (sAMAccountName, userPrincipalName y UID) se han configurado correctamente.

22.8 Gestión de las contraseñas de usuario

Un usuario con privilegios de administrador de infraestructuras puede gestionar las contraseñas de todos los usuarios locales del dispositivo utilizando la interfaz de usuario o las API de REST. Los usuarios que no tienen privilegios de administrador de infraestructuras solo pueden gestionar sus propias contraseñas.

Como administrador de infraestructuras, puede ver todos los usuarios que han iniciado sesión en el dispositivo mediante la pantalla **Users and Groups** (Usuarios y grupos) o las API de REST. Seleccione cualquier usuario y, a continuación, modifique su contraseña o el rol que tiene asignado.

El resto de los usuarios locales pueden editar sus propias contraseñas mediante el uso de la interfaz de usuario o las API de REST. En la interfaz de usuario, haga clic en el icono **Session** (Sesión) en la barra superior y, a continuación, haga clic en el icono **Edit** (Editar) para cambiar su contraseña o información de contacto actual.

22.9 Restablecimiento de la contraseña del administrador

Si pierde u olvida la contraseña de administrador, utilice la operación siguiente para restablecerla. La operación le permite establecer una contraseña de un solo uso para la cuenta local `administrator`.

NOTA: Esta operación restablece la contraseña de una cuenta de administrador local en el dispositivo. No se aplica a las cuentas de administrador autenticadas por un servicio de directorio.

Necesitará acceder a la consola de mantenimiento desde la consola del dispositivo, obtener un **código de solicitud** exclusivo y llamar por teléfono a su representante autorizado de soporte técnico, que le enviará un **código de autorización** tras verificar la información que le proporcione.

Requisitos previos

- Debe tener acceso a la consola del dispositivo.

Restablecimiento de la contraseña de administrador con la consola de mantenimiento

1. Acceda a la consola del dispositivo virtual.
2. Acceda al menú principal de la consola de mantenimiento.
3. Seleccione **Reset password** (Restablecer contraseña).

   La consola de mantenimiento muestra un **request code** (código de solicitud).

IMPORTANTE: El código de solicitud es válido únicamente desde la pantalla **Password reset** (Restablecimiento de la contraseña) de la consola de mantenimiento. Si se vuelve al menú principal o se finaliza la sesión de la consola de mantenimiento, el código de solicitud no será válido. Necesitará volver a comenzar este procedimiento para adquirir un nuevo código de solicitud.

4. Llame por teléfono su representante autorizado de soporte técnico y proporciónele la información siguiente:
   - El nombre de la persona que solicita el restablecimiento de la contraseña.
   - El nombre de la empresa propietaria del dispositivo.
   - El código de solicitud de la consola de mantenimiento.

   El representante autorizado de soporte técnico comprueba la información y, a continuación, envía un mensaje a la dirección de correo electrónico autorizada que tiene registrada. Este mensaje contiene el **código de autorización**, también conocido como código de respuesta. El mensaje incluye una imagen ISO, que también es el código de autorización.

   Para obtener información sobre cómo ponerse en contacto con Hewlett Packard Enterprise por teléfono, consulte «Acceso al soporte de Hewlett Packard Enterprise» (página 461).
5. Realice una de las acciones siguientes para introducir el **código de autorización** en el campo de respuesta.

IMPORTANTE: El **código de autorización** debe introducirse antes de que pase una hora, o dejará de ser válido.

   - Si puede pegar información en la consola de mantenimiento, copie el código de autorización del mensaje de correo electrónico y péguelo en el campo de respuesta de la consola de mantenimiento.
   - Lea el código de autorización desde la imagen ISO:
     1. Guarde la imagen ISO que se incluye en el mensaje de correo electrónico.
     2. Monte la imagen ISO como un montaje de Virtual Media (un CD-ROM virtual).
     3. Seleccione **Read from ISO** (Leer desde ISO) en la consola de mantenimiento.
     4. La consola de mantenimiento lee la imagen ISO y, pasado un momento, rellena automáticamente el campo de respuesta con el código de autorización.
   - Escriba el código de autorización en el campo de respuesta.
6. Elija una contraseña de administrador de un solo uso.
7. Cuando se le indique, escriba dos veces la contraseña nueva.
8. Seleccione **OK** (Aceptar) para definir la contraseña solo uso.
9. Inicie sesión en la interfaz de usuario con esta cuenta, utilizando la contraseña de un solo uso.
10. Establezca una contraseña nueva para esta cuenta en la pantalla que se visualiza.
11. Cierre la sesión y vuelva a iniciarla con la contraseña nueva para comprobar que funciona.

Consulte también

- «Acceso al soporte de Hewlett Packard Enterprise» (página 461).
- *Acerca de la consola de mantenimiento* en la ***Guía de usuario de HPE OneView***.«Acerca de la consola de mantenimiento»

22.10 Información adicional

- «Control del acceso de los usuarios autorizados» (página 72)

23 Copia de seguridad de un dispositivo

En este capítulo se describe cómo utilizar la interfaz de usuario, las API de REST o una secuencia de comandos de PowerShell personalizada para guardar los datos de gestión y los parámetros de configuración de los recursos del dispositivo en un archivo de copia de seguridad.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings→Actions (Configuración > Acciones)	`backups`

23.1 Roles

Los usuarios con los privilegios de administrador de infraestructuras y de copia de seguridad pueden crear y descargar archivos de copia de seguridad; sin embargo, solo el administrador de infraestructuras puede restaurar un dispositivo a partir de un archivo de copia de seguridad.

El administrador de copias de seguridad tiene autoridad para utilizar secuencias de comandos para iniciar sesión en el dispositivo y ejecutar secuencias de comandos para realizar copias de seguridad del dispositivo. Este rol está destinado específicamente a la creación y descarga de copias de seguridad mediante secuencias de comandos. Hewlett Packard Enterprise recomienda que los usuarios con este rol no inicien sesiones interactivas a través de la interfaz de usuario de HPE OneView.

23.2 Acerca de la realización de copias de seguridad del dispositivo

HPE OneView ofrece la posibilidad de guardar los parámetros de configuración y los datos de gestión en un archivo de copia de seguridad y permite utilizar esa copia de seguridad para restaurar un dispositivo dañado en el caso de un fallo catastrófico.

El proceso de copia de seguridad implica la creación de un archivo de copia de seguridad y la posterior descarga de este archivo para poder guardarlo en una ubicación segura, fuera del dispositivo, para usarlo en el futuro. Puede programar operaciones de copia de seguridad automáticas y designar una ubicación remota para el archivo de copia de seguridad.

Para obtener asesoramiento sobre la creación y archivado de un archivo de copia de seguridad, consulte «Prácticas recomendadas para realizar una copia de seguridad de un dispositivo».

Para conocer el procedimiento de creación de un archivo de copia de seguridad desde la interfaz de usuario, consulte «Copia de seguridad manual de un dispositivo». Para configurar copias de seguridad automáticas almacenadas remotamente, consulte «Configuración de las copias de seguridad remotas automáticas».

IMPORTANTE: En el caso poco probable de que necesite restaurar el dispositivo, Hewlett Packard Enterprise recomienda realizar copias de seguridad de la configuración del dispositivo de forma periódica, preferiblemente a diario y teniendo en cuenta lo siguiente:

- Después de añadir hardware
- Después de cambiar la configuración del dispositivo
- Antes y después de actualizar el firmware del dispositivo

Para evitar que sobrescriba o se borre un archivo de copia de seguridad, descárguelo y guárdelo en una ubicación fuera del dispositivo antes de ejecutar el siguiente proceso de copia de seguridad. El dispositivo almacena un solo archivo de copia de seguridad o archivo de volcado de soporte en el dispositivo en cada momento. La creación de un archivo de copia de seguridad sustituye el archivo de copia de seguridad o el archivo de volcado de soporte actual. Del mismo

modo, la creación de un archivo de volcado de soporte sustituye el volcado de soporte o el archivo de copia de seguridad anterior.

Si se inicia una copia de seguridad mientras se está realizando un volcado de soporte, la operación de copia de seguridad no continuará hasta que se complete la operación de volcado de soporte. Si un administrador de infraestructuras inicia un volcado de soporte mientras se está realizando una operación de copia de seguridad, tendrá la opción de cancelar la copia de seguridad y continuar con el volcado de soporte.

HPE OneView proporciona un rol de usuario administrador de copia de seguridad específicamente para realizar copias de seguridad del dispositivo; este rol permite acceder a otras vistas de recursos pero no realizar acciones con esos recursos, ni otras tareas. Solo el administrador de infraestructuras o el administrador de copias de seguridad puede crear un archivo de copia de seguridad, ya sea mediante la interfaz de usuario o las API de REST.

Elementos de los que se realiza la copia de seguridad	Elementos de los que no se realiza la copia de seguridad

• Base de datos de HPE OneView
• Archivos del sistema:
  ◦ Datos que no están en la base de datos
  ◦ Registro de auditoría
  ◦ Archivos de licencia
	• Archivos que no son de datos: archivos estáticos que se instalan como parte del entorno de ejecución y no son específicos del dispositivo ni de la configuración del entorno gestionado
	• Archivos de registro (excepto el archivo del registro de auditoría)
	• Configuración de red del dispositivo
	• Archivos de configuración inicial
	• Lotes de firmware
	• Cualquier configuración del servidor, como la siguiente, que HPE OneView no ha configurado:
	  ◦ Ajustes de la configuración de BIOS y arranque.
	  ◦ Configuraciones de almacenamiento local y SAN
	  ◦ Configuraciones de red
	  HPE OneView no valida ni mantiene configuraciones como estas

Utilice el archivo de copia de seguridad para realizar lo siguiente:

- Restaurar el dispositivo desde el que se creó el archivo de copia de seguridad.
- Restaurar la configuración en un dispositivo diferente. Por ejemplo, si falla un dispositivo y este no se puede reparar, puede utilizar un archivo de copia de seguridad para restaurar los valores de configuración de gestión y los datos de gestión a un dispositivo de reemplazo creado a partir de la misma versión de la imagen de la máquina virtual.

Las API de REST le permiten:

- Programar un proceso de copia de seguridad desde fuera del dispositivo.
- Recopilar archivos de copia de seguridad de acuerdo con las directivas de la organización.
- Realizar la integración con los productos de copia de seguridad y restauración de la empresa.

23.3 Prácticas recomendadas para realizar una copia de seguridad de un dispositivo

Método	Descripción
Creación	Realice siempre la copia de seguridad de su dispositivo por medio de la función de copia de seguridad de HPE OneView. **ATENCIÓN:** No utilice ninguna capacidad ni instantánea del hipervisor para hacer copias de seguridad de dispositivos HPE OneView, ya que esto podría provocar errores de sincronización y dar lugar a un comportamiento impredecible y no deseado.
Frecuencia	Hewlett Packard Enterprise recomienda hacer una copia de seguridad de la configuración del dispositivo con la función copia de seguridad remota automática con regularidad, a ser posible diaria. Hewlett Packard Enterprise también recomienda hacer manualmente la copia de seguridad del dispositivo: • Después de añadir hardware • Después de cambiar la configuración del dispositivo • Antes y después de actualizar el firmware del dispositivo Siempre debe disponer de un archivo de copia de seguridad con la misma versión del firmware que el dispositivo. En caso contrario, la operación de restauración fallará. Las copias de seguridad pueden realizarse mientras el dispositivo está en uso y se están realizando actividades normales. No es necesario esperar a que terminen las tareas para crear una copia de seguridad.
Archivado	El formato del archivo de copia de seguridad es de propiedad. Hewlett Packard Enterprise le recomienda que: 1. Cree y descargue un archivo de copia de seguridad. 2. Guarde el archivo de copia de seguridad en una ubicación segura, fuera del dispositivo para proteger los datos confidenciales. Hewlett Packard Enterprise proporciona las API de REST para la integración con productos empresariales de copia de seguridad.

23.4 Determinación de la directiva de copia de seguridad

Un archivo de copia de seguridad es una instantánea de la configuración y los datos de gestión del dispositivo en el momento en que se crea la copia de seguridad. Hewlett Packard Enterprise recomienda crear copias de seguridad regulares, preferiblemente una vez al día, y después de realizar cambios de configuración de hardware o de software en el entorno gestionado.

Como alternativa al uso de **Settings→Backup→Actions→Create backup** (Configuración > Copia de seguridad > Acciones > Crear copia de seguridad) desde la interfaz de usuario del dispositivo, puede escribir y ejecutar una secuencia de comandos para crear y descargar automáticamente un archivo de copia de seguridad del dispositivo. Puede programar la secuencia de comandos para que se ejecute automáticamente en modo interactivo o por lotes de forma periódica. Solo un usuario con privilegios de administrador de copia de seguridad o de infraestructuras puede ejecutar la secuencia de comandos de forma interactiva.

Hewlett Packard Enterprise proporciona y recomienda una instalación de copia de seguridad remota para almacenar los archivos de copia de seguridad. Tras una configuración inicial, las copias de seguridad se realizan automáticamente en el día y la hora especificados y se envían a una carpeta del usuario en un servidor SSH o SFTP.

23.5 Copia de seguridad manual de un dispositivo

Un archivo de copia de seguridad guarda los parámetros de configuración y los datos de gestión del dispositivo. Puede realizar la recuperación cuando se produzca un fallo catastrófico

restaurando el dispositivo desde el archivo de copia de seguridad. Para obtener más información, consulte «Acerca de la realización de copias de seguridad del dispositivo».

NOTA: Para reducir el tamaño del archivo de copia de seguridad y el tiempo que se necesita para crearlo, los lotes de firmware que se han cargado en el dispositivo no se incluyen en el archivo de copia de seguridad.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras o administrador de copias de seguridad
- Se han seguido todas las prácticas recomendadas para la copia de seguridad de un dispositivo.

Copia de seguridad manual de un dispositivo

1. En el menú principal, seleccione **Settings** (Configuración) y realice una de las acciones siguientes:
   - Haga clic en **Create backup** (Crear copia de seguridad) en el panel **Backup** (Copia de seguridad).
   - Haga clic en **Backup** (Copia de seguridad) en la pantalla **Settings** (Configuración) y, a continuación, seleccione **Actions→Create backup** (Acciones > Crear copia de seguridad).

   Mientras se crea el archivo de copia de seguridad, aparece una barra de progreso en el panel **Overview** (Información general).

   Espere a que finalice la creación del archivo de copia de seguridad.
2. De manera opcional, haga clic en la barra de notificación **Create Backup** (Crear copia de seguridad) para obtener más información y el nombre del archivo de copia de seguridad, que tiene el formato:

   appliance-host-name_backup_yyyy-mm-dd_hhmmss.bkp
3. Compruebe que el archivo de copia de seguridad se ha creado correctamente. El nombre del archivo de copia de seguridad debería reflejar la fecha y hora actuales.
4. Después de haber creado el archivo de copia de seguridad, haga una de estas acciones para descargar el archivo de copia de seguridad del dispositivo:
   - Haga clic en **Download backup** (Descargar copia de seguridad) en el panel **Backup** (Copia de seguridad).
   - Seleccione **Actions (Acciones)→Download backup** (Descargar copia de seguridad).
5. Seleccione la opción correspondiente en el cuadro de diálogo para guardar el archivo de copia de seguridad en un lugar seguro:
   - Seleccione **Transfer backup to remote backup location** (Transferir copia de seguridad a una ubicación de copia de seguridad remota) para almacenar el archivo de copia de seguridad en la ubicación de copia de seguridad remota indicada.

     Para obtener información sobre la configuración de la ubicación de la copia de seguridad remota y habilitar dicha función, consulte «Configuración de las copias de seguridad remotas automáticas».
   - Seleccione **Download the backup to my computer** (Descargar la copia de seguridad en mi ordenador) para almacenar el archivo de copia de seguridad en el equipo local.

   No almacene el archivo de copia de seguridad en el dispositivo.

Más información

Acerca de la realización de copias de seguridad del dispositivo
Prácticas recomendadas para realizar una copia de seguridad de un dispositivo
Configuración de las copias de seguridad remotas automáticas
Solución de problemas: la creación del archivo de copia de seguridad o su descarga falla

23.6 Uso de las API de REST para crear y descargar el archivo de copia de seguridad de un dispositivo

Una vez iniciada la copia de seguridad, se crea un URI `TaskResource` que se utiliza para hacer un seguimiento del progreso de la copia de seguridad. Cuando finaliza la copia de seguridad, puede utilizar una operación `GET` de la API de REST para descargar y modificar el nombre del archivo de copia de seguridad. La copia de seguridad más reciente se almacena en el dispositivo y se sustituye cuando se crea una nueva.

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de copia de seguridad

Creación y descarga del archivo de copia de seguridad de un dispositivo mediante las API de REST

1. Cree el archivo de copia de seguridad.

   `POST /rest/backups`

2. Descargue el archivo de copia de seguridad.

   `GET /rest/backups/archive/{URI de la copia de seguridad}`

NOTA: Cuando finaliza la operación `POST`, se devuelven un `TaskResource` y un URI de copia de seguridad Puede utilizar el URI `TaskResource` para supervisar el estado de la copia de seguridad. Utilice el URI de la copia de seguridad para hacer referencia a una copia de seguridad específica al descargar el archivo de copia de seguridad o al realizar otra operación.

23.7 Creación de una secuencia de comandos personalizada para crear y descargar el archivo de copia de seguridad de un dispositivo

Si prefiere escribir una secuencia de comandos personalizada para crear y descargar el archivo de copia de seguridad del dispositivo y programarla para que se ejecute periódicamente de acuerdo con sus directivas de TI, consulte «Secuencia de comandos de copia de seguridad de ejemplo» para obtener una secuencia de comandos de PowerShell de ejemplo.

23.8 Configuración de las copias de seguridad remotas automáticas

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras, administrador de copias de seguridad
- Cuenta de usuario en un equipo remoto y las credenciales para dicha cuenta.

Configuración de las copias de seguridad remotas automáticas

1. En el menú principal, seleccione **Settings** (Configuración).
2. Realice una de las acciones siguientes:
   - En el panel **Backup** (Copia de seguridad), haga clic en  .
   - Haga clic en **Backup** (Copia de seguridad) y, a continuación, seleccione **Actions (Acciones)→Edit backup (Editar copia de seguridad)**.

3. Proporcione los datos que se solicitan en la pantalla Edit Backup (Editar copia de seguridad).

   NOTA: Algunos campos se ocultan o se muestran en función de las selecciones.

   Cuando programe una copia de seguridad remota automática, indique la **Time** (Hora) como dos valores numéricos separados por dos puntos.

4. Haga clic en **OK** (ACEPTAR).
5. Compruebe el éxito de la configuración supervisando el progreso del archivo de copia de seguridad de prueba que se genera y transmite.

Más información

«Acerca de la realización de copias de seguridad del dispositivo»

23.9 Cómo deshabilitar las copias de seguridad remotas automáticas

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras

Cómo deshabilitar las copias de seguridad remotas automáticas

1. En el menú principal, seleccione **Settings** (Configuración).
2. Realice una de las acciones siguientes:
   - En el panel **Backup** (Copia de seguridad), haga clic en .
   - Haga clic en **Backup** (Copia de seguridad) y, a continuación, seleccione **Actions (Acciones)→Edit backup (Editar copia de seguridad)**.
3. En la pantalla Edit Backup (Editar copia de seguridad), seleccione **Enable remote backup location** (Habilitar la ubicación de copia de seguridad remota) para eliminar la marca de verificación.

   El resto de la pantalla ya no aparece.
4. Haga clic en **OK** (ACEPTAR).

   Los datos de la programación se conservan por si quisiera volver a habilitar las copias de seguridad remotas automáticas.

Más información

«Acerca de la realización de copias de seguridad del dispositivo»

23.10 Información adicional

- «Técnicas básicas de solución de problemas» (página 389)

24 Restauración de un dispositivo desde un archivo de copia de seguridad

En este capítulo se describe cómo utilizar la interfaz de usuario, las API de REST o una secuencia de comandos de PowerShell personalizada para restaurar un dispositivo dañado desde un archivo de copia de seguridad. Una operación de restauración solo es necesaria para realizar la recuperación cuando se produzcan fallos catastróficos, no para arreglar pequeños problemas que se pueden resolver de otras formas.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings→Actions (Configuración > Acciones)	`restores`

Para obtener más información acerca del modo de restaurar un dispositivo, consulte la ayuda en línea de la pantalla **Settings** (Configuración).

IMPORTANTE: No utilice ninguna función ni instantánea del hipervisor para restaurar un dispositivo HPE OneView, ya que puede provocar errores de sincronización y dar lugar a un comportamiento impredecible y no deseado.

24.1 Funciones

Los usuarios con los privilegios de administrador de infraestructuras y de copia de seguridad pueden crear y descargar archivos de copia de seguridad; sin embargo, solo el administrador de infraestructuras puede restaurar un dispositivo a partir de un archivo de copia de seguridad.

24.2 Sobre la restauración del dispositivo

Al restaurar un dispositivo desde un archivo de copia de seguridad, se reemplazarán todos los datos de gestión y la mayoría de los parámetros de configuración por los datos y valores del archivo de copia de seguridad, incluidos los nombres de usuario y contraseñas, y los registros de auditoría, pero no incluye la configuración de la dirección IP del dispositivo.

El dispositivo no estará operativo durante la operación de restauración y es un proceso que puede tardar varias horas. Cuantos más recursos y dispositivos necesite restaurar, más tiempo durará la operación de restauración. Una vez iniciada, no se puede cancelar ni deshacer una operación de restauración. El dispositivo bloqueará las solicitudes de inicio de sesión mientras la operación de restauración esté en curso.

IMPORTANTE: Las operaciones de restauración solo son necesarias para recuperar el dispositivo tras fallos catastróficos, no para corregir pequeños problemas que se pueden resolver de otras formas.

Por tanto, tras completar la operación de restauración, puede restaurar un dispositivo desde un archivo de copia de seguridad creado en el mismo dispositivo, o bien, en caso de error irreparable en el dispositivo, desde un archivo de copia de seguridad de otro dispositivo. En este caso, el

archivo de copia de seguridad debe haber sido creado a partir de un dispositivo que ejecuta la misma versión de HPE OneView.

Acciones durante la operación de restauración	Descripción
Valida el inventario de recursos	Durante una operación de restauración, el firmware del dispositivo valida el inventario de recursos (receptáculos, servidores e interconexiones) y combina los datos del archivo de copia de seguridad con el estado actual del entorno gestionado. Es probable que el estado del entorno gestionado sea diferente del que tenía en el momento en que se creó el archivo de copia de seguridad. Después del operación de restauración, el dispositivo utiliza alertas para informar sobre cualquier discrepancia que no pueda resolver de forma automática.
Cómo volver a detectar los receptáculos para validar el contenido	Durante la operación de restauración, el dispositivo vuelve a detectar cada receptáculo para validar su contenido; en especial para garantizar que el dispositivo pueda seguir reclamándolos y que la instancia correspondiente de HPE OneView sea lo que gestione el receptáculo. A continuación, el dispositivo vuelve a detectar cada servidor y borra los identificadores virtuales de los servidores agregados a un receptáculo desde la última vez que se creó el archivo de copia de seguridad. El dispositivo también actualiza todos los servidores del bastidor para asegurarse de que estos se reclaman.
Borra los ID virtuales	El dispositivo borrará los identificadores virtuales del hardware de servidor que no tengan asignado un perfil pero que tengan identificadores virtuales configurados. Es muy probable que se haya asignado un perfil a estos servidores después de hacer la última copia de seguridad. Consulte también «Tareas posteriores a la restauración».

También puede utilizar la interfaz de usuario para cargar un archivo de copia de seguridad y restaurar el dispositivo desde ella. También puede utilizar las API de REST para este fin.

24.3 Prácticas recomendadas para la restauración de un dispositivo

Tema	Práctica recomendada
Antes de empezar	**1.** Anote las contraseñas utilizadas. Haga una lista de las cuentas de usuario actuales del dispositivo. La operación de restauración restablece los nombres de usuario y las contraseñas a los que estaban en vigor cuando se creó el archivo de copia de seguridad. **2.** Cree un volcado de soporte. Utilice el volcado de soporte para diagnosticar los fallos que ocurrieron antes de la operación de restauración. **3.** Descargue los registros de auditoría existentes y guárdelos en un lugar seguro. La operación de restauración restaura los registros de auditoría desde el archivo de copia de seguridad y sobrescribe los registros existentes. **4.** Detenga todas las copias de seguridad programadas automáticamente. Si HPE OneView está configurado para las copias de seguridad automáticas, las copias de seguridad se reanudan después de restaurar el dispositivo. **5.** Facilite el acceso al archivo de copia de seguridad en el dispositivo desde el que tiene pensado hacer la solicitud de carga. Si utiliza un producto empresarial de copia de seguridad para archivar archivos de copia de seguridad, siga los pasos necesarios para preparar la operación de restauración. **¡ADVERTENCIA!** El archivo de copia de seguridad local se elimina durante el proceso de restauración. Descargue el archivo de copia de seguridad y guárdelo en una ubicación segura fuera del dispositivo para futuras restauraciones. **6.** Si ha añadido hardware al dispositivo después de crear el archivo de copia de seguridad, dicho hardware no estará en la base de datos del dispositivo cuando finalice el proceso de restauración. Por ello, si realiza una restauración a partir del archivo de copia de seguridad, deberá agregar dicho hardware al dispositivo y, a continuación, repetir cualquier otro cambio de configuración (como la asignación de perfiles de servidor) realizado entre el momento en que se creó el archivo de copia de seguridad y el momento en que finalizó el proceso de restauración.
Informe a los usuarios	• Asegúrese de que todos los usuarios cierren la sesión que hayan iniciado en el dispositivo. Los usuarios que hayan iniciado sesión cuando se inicia la operación de restauración se desconectan automáticamente, y pierden el trabajo que estaban realizando. Ningún usuario podrá iniciar sesión durante una operación de restauración.
Utilice el archivo de copia de seguridad correcto	

Tema	Práctica recomendada
	• Utilice el archivo de copia de seguridad más reciente para restaurar el dispositivo. El archivo de copia de seguridad no incluirá ningún cambio realizado después de la creación del archivo de copia de seguridad. • Asegúrese de que las direcciones IP del dispositivo sean las que desea que el dispositivo utilice después de la operación de restauración. Las direcciones IP del dispositivo no se restauran desde el archivo de copia de seguridad. • Asegúrese de que el dispositivo que se va a restaurar y el dispositivo en el que se creó el archivo de copia de seguridad tienen la misma versión de firmware, ya que, de lo contrario, se producirá un error en la operación. El tipo de plataforma, el modelo de hardware y los números principales y secundarios del firmware del dispositivo deben coincidir para poder restaurar una copia de seguridad. El formato de la versión de firmware del dispositivo es el siguiente: *`númeroprincipal.númerosecundario.númeroderevisión-númerodecompilación`* No es necesario que los números de revisión y de compilación coincidan. Si la copia de seguridad no es compatible con el firmware del dispositivo, la carga mostrará un error y la operación de restauración se detendrá. En ese caso, tendrá que actualizar el firmware o seleccionar otra una copia de seguridad. • Si es necesario restaurar una copia de seguridad en un nuevo dispositivo y el dispositivo antiguo aún sigue funcionando (el hardware no ha fallado), elimine el dispositivo antiguo. La supresión del dispositivo garantiza que este ya no gestione los equipos que gestionaba cuando se creó el archivo de copia de seguridad. Se pueden producir errores graves si varios dispositivos intentan gestionar los mismos equipos.

24.4 Restauración de un dispositivo a partir de un archivo de copia de seguridad

Al restaurar un dispositivo desde un archivo de copia de seguridad, se sustituyen todos los datos de gestión y la mayoría de los ajustes de configuración del dispositivo. Si procede, se le pedirá que vuelva a introducir los datos sin resolver. Para obtener más información, consulte «Sobre la restauración del dispositivo».

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras.
- Se han seguido todas las prácticas recomendadas para la restauración de un dispositivo.

IMPORTANTE: Si va a utilizar un archivo de copia de seguridad creado en otro dispositivo para restaurar un nuevo dispositivo o uno repuesto:

1. Instale HPE OneView en el dispositivo nuevo o de repuesto. Para obtener instrucciones, consulte la ***Guía de instalación de HPE OneView***.
2. Configure el nuevo dispositivo con la misma configuración de red que el dispositivo en el que se creó el archivo de copia de seguridad. De esta forma, puede utilizar la red para cargar el archivo de copia de seguridad en el dispositivo nuevo.

   Para obtener más información sobre los valores de configuración de red, consulte la ayuda en línea para los detalles de las pantallas de adición o edición de dispositivos.

   Si la configuración de red del nuevo dispositivo no coincide exactamente con la del archivo de copia de seguridad, la configuración de red no coincidirá con la información de los certificados de red del archivo de copia de seguridad. Como consecuencia, el explorador pierde la conexión con el dispositivo y este no se puede restaurar.
3. Cuando se configure la red del dispositivo nuevo, continúe con la operación de restauración descrita en el siguiente procedimiento.

Restauración de un dispositivo desde un archivo de copia de seguridad

Siga el procedimiento correspondiente al escenario que se aplica a su entorno y sus prácticas:

- «Escenario: Seleccionar un archivo de copia de seguridad e iniciar inmediatamente la restauración»
- «Escenario: Seleccionar un archivo de copia de seguridad e iniciar la restauración más tarde»

Escenario: Seleccionar un archivo de copia de seguridad e iniciar inmediatamente la restauración

1. En el menú principal, seleccione **Settings** (Configuración) y, a continuación, seleccione **Backup** (Copia de seguridad).
2. Seleccione **Actions→Restore from backup** (Acciones > Restaurar desde copia de seguridad).

   Se abre el cuadro de diálogo.
3. Lea la notificación de la pantalla y, a continuación, seleccione **Select a backup file** (Seleccionar un archivo de copia de seguridad).
4. Realice una de las acciones siguientes:
   - Arrastre el archivo de copia de seguridad y suéltelo en el cuadro de texto indicado.
   - Haga clic en **Browse** (Examinar) y, a continuación, seleccione el archivo de copia de seguridad que desea cargar.

   NOTA: No todos los exploradores y todas las versiones ofrecen la posibilidad de arrastrar y soltar archivos en las aplicaciones.
5. Haga clic en **Upload and restore** (Cargar y restaurar).

   Espere a que finalice el proceso de restauración. El progreso se indica mediante una página de estado.

   Una vez finalizado el proceso de restauración, volverá a la página de inicio de sesión, donde puede iniciar sesión en el dispositivo restaurado.
6. Cargue los lotes de firmware utilizados por los perfiles de servidor, receptáculos e interconexiones lógicas. Estos no se guardan como parte del archivo de copia de seguridad. Consulte el valor de `Firmware baseline` (Línea de base de firmware) de cada perfil para determinar el nombre de archivo de la línea de base que se necesita.

   Si utilizó HPE OneView para crear un SPP personalizado, utilice el `CMDLET Restore-HPOVCustomBaseline` para volver a crear el SPP personalizado después de cargar el SPP base y las revisiones en el repositorio. Para obtener más información, consulte **https://github.com/HewlettPackard/POSH-HPOneView/wiki/Restore-HPOVCustomBaseline**.
7. Compruebe que la operación de restauración se ha realizado correctamente iniciando una sesión el dispositivo y resolviendo correctamente las discrepancias que la operación de restauración no haya podido resolver automáticamente. Consulte «Tareas posteriores a la restauración».

Escenario: Seleccionar un archivo de copia de seguridad e iniciar la restauración más tarde

1. En el menú principal, seleccione **Settings** (Configuración) y, a continuación, seleccione **Backup** (Copia de seguridad).
2. Seleccione **Actions→Restore from backup** (Acciones > Restaurar desde copia de seguridad).

   Se abre el cuadro de diálogo.

3. Lea la notificación de la pantalla y, a continuación, seleccione **Select a backup file** (Seleccionar un archivo de copia de seguridad).
4. Realice una de las acciones siguientes:
   - Arrastre el archivo de copia de seguridad y suéltelo en el cuadro de texto indicado.
   - Haga clic en **Browse** (Examinar) y, a continuación, seleccione el archivo de copia de seguridad que desea cargar.

   NOTA: No todos los exploradores y todas las versiones ofrecen la posibilidad de arrastrar y soltar archivos en las aplicaciones.
5. Haga clic en **Upload only** (Cargar solo).

   Espere hasta que termine la carga.

   Aparecerá una barra de progreso. El nombre del archivo, la fecha de creación y la versión se muestran cuando finaliza la carga del archivo.
6. Cuando esté preparado para restaurar el dispositivo desde el archivo de copia de seguridad, vuelva al cuadro de diálogo y compruebe que el archivo de copia de seguridad es correcto y se ha cargado.
7. Seleccione **Restore from backup** (Restaurar desde copia de seguridad).
8. Haga clic en **Restore** (Restaurar).

   Espere a que finalice el proceso de restauración. El progreso se indica mediante una página de estado.

   Una vez finalizado el proceso de restauración, volverá a la página de inicio de sesión, donde puede iniciar sesión en el dispositivo restaurado.
9. Cargue los lotes de firmware utilizados por los perfiles de servidor, receptáculos e interconexiones lógicas. Estos no se guardan como parte del archivo de copia de seguridad. Consulte el valor de `Firmware baseline` (Línea de base de firmware) de cada perfil para determinar el nombre de archivo de la línea de base que se necesita. No es necesario cargar la línea de base predeterminada, `Service Pack for ProLiant - Base Firmware`, que se incluye en la imagen del dispositivo.

   Si utilizó HPE OneView para crear un SPP personalizado, utilice el `CMDLET Restore-HPOVCustomBaseline` para volver a crear el SPP personalizado después de cargar el SPP base y las revisiones en el repositorio. Para obtener más información, consulte **https://github.com/HewlettPackard/POSH-HPOneView/wiki/Restore-HPOVCustomBaseline**.
10. Compruebe que la operación de restauración se ha realizado correctamente iniciando una sesión el dispositivo y resolviendo correctamente las discrepancias que la operación de restauración no haya podido resolver automáticamente. Consulte «Tareas posteriores a la restauración».

24.5 Uso de las API de REST para restaurar un dispositivo desde un archivo de copia de seguridad

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de infraestructuras

- Debe haber cargado un archivo de copia de seguridad en el dispositivo.

Restauración del dispositivo desde un archivo de copia de seguridad mediante las API de REST

1. Inicie el proceso de restauración.

   `POST /rest/restores`

   Se devuelve el *{URI de restauración}*.

2. Muestre el estado del proceso de restauración.

   `GET /rest/restores`

24.6 Creación de una secuencia de comandos personalizada para restaurar un dispositivo

Si prefiere escribir una secuencia de comandos para restaurar un dispositivo desde un archivo de copia de seguridad, consulte «Secuencia de comandos de restauración de ejemplo» para obtener una secuencia de comandos de PowerShell de ejemplo que se puede personalizar para su entorno.

24.7 Tareas posteriores a la restauración

Durante una operación de restauración, el dispositivo combina los datos del archivo de copia de seguridad con el estado actual del entorno gestionado. Hay algunas discrepancias que una operación de restauración no puede resolver de forma automática, como por ejemplo, si se agregaron servidores después de crear el archivo de copia de seguridad. El dispositivo desconoce la configuración de red de estos servidores después de una restauración, y esto podría dar lugar a direcciones MAC y nombres World Wide (WWN) duplicados.

Cuando finalice una operación de restauración, debe resolver manualmente las alertas restantes y volver a agregar estos servidores al dispositivo para eliminar el riesgo de que existan identificadores duplicados. También debe realizar la limpieza manual del hardware (servidores, interconexiones y receptáculos) si se ha cancelado la asignación de los perfiles de servidor por la fuerza o si se quita hardware por la fuerza sin desconfigurarlo primero.

Prevención de identificadores duplicados en la red después de una restauración

1. Cuando finalice una operación de restauración, vuelva a agregar cualquier receptáculo o hardware de servidor que se agregó después de la copia de seguridad seleccionada.

   NOTA: Si decide *no* volver a agregar después de la restauración cualquier receptáculo añadido con posterioridad a la última copia de seguridad, evite los identificadores duplicados ejecutando el comando SSH `clear vcmode` de Onboard Administrator en estos receptáculos. Al ejecutar este comando, se garantiza que se han borrado las direcciones MAC y los WWN virtuales de los blades de servidor del receptáculo.

2. Si se produce cualquier alerta que indica que un perfil de servidor no coincide con el hardware de servidor:
   a. Identifique todos los perfiles de servidor cuyo mensaje de error indique que el tipo no coincide. Haga una lista de estos perfiles de servidor y del hardware de servidor asignado.
   b. Apague el servidor y, a continuación, cancele la asignación de cada uno de los perfiles de servidor. En la pantalla **Server Profiles** (Perfiles de servidor), seleccione **Actions→Edit** (Acciones > Editar) y seleccione **Unassign** (Cancelar la asignación) en el selector desplegable de hardware de servidor. Haga clic en **OK** (ACEPTAR).
   c. Vuelva a seleccionar **Actions→Edit** (Acciones > Editar) y, a continuación, vuelva a asignar al hardware de servidor correspondiente todos los perfiles que incluyó en la lista.

3. Para cualquier alerta sobre los intervalos de identificadores, el administrador de red debe examinar los intervalos de direcciones y de identificadores, y editarlos, si fuera necesario.
4. Vuelva a crear los perfiles para los servidores de los receptáculos que se agregaron en el paso 1.

25 Gestión del dispositivo

25.1 Actualización del dispositivo

Las actualizaciones de licencias se gestionan desde la pantalla **Settings (Configuración)** o utilizando las API de REST.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)	`appliance/firmware`

25.1.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

25.1.2 Tareas

La actualización del dispositivo requiere que haya un solo usuario accediendo al dispositivo y hace que este se reinicie. Esto no interrumpe el funcionamiento de los equipos gestionados, pero sí que provoca una interrupción del funcionamiento del dispositivo.

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Determinar si hay disponible una actualización más reciente del dispositivo. (Privilegios mínimos necesarios: solo lectura, administrador de red o administrador de infraestructuras)
- Actualizar el dispositivo. (privilegios mínimos necesarios: administrador de infraestructuras)

25.1.3 Acerca de las actualizaciones del dispositivo

En el dispositivo se ejecuta una combinación de software y firmware. El mantenimiento actualizado del software y el puede solucionar problemas, mejorar el rendimiento y añadir las nuevas funciones al dispositivo. El dispositivo no le notifica automáticamente cuando está disponible una actualización; la determinación de si se ha publicado una actualización del dispositivo correrá por su cuenta.

Para ver la versión instalada del firmware del dispositivo, utilice la vista **Settings →Appliance** (Configuración > Dispositivo).

A continuación, compruebe si existe alguna versión más reciente de un archivo de actualización descargable desde la página web **http://www.hp.com/go/oneview/updates**.

Antes de actualizar el dispositivo, consulte las ***Notas de la versión de HPE OneView*** para obtener información sobre rutas de actualización admitidas, nuevas funciones incluidas en la actualización, prácticas recomendadas, limitaciones, sugerencias y consejos de solución de problemas, y sobre si es necesario o no reiniciar el dispositivo después de actualizarlo.

NOTA: Cuando se descarga el archivo de actualización del dispositivo, se muestra un enlace a la actualización de las ***Notas de la versión de HPE OneView*** en el cuadro de diálogo de descargas. Hewlett Packard Enterprise recomienda hacer clic en ese enlace para leer la información y, a continuación, guardarla e imprimirla para futuras referencias. Una vez iniciada la descarga, no se podrá volver a acceder a ese enlace.

Las actualizaciones del dispositivo se gestionan desde el menú **Settings→Appliance→Actions→Update appliance** (Configuración > Dispositivo > Acciones > Actualizar dispositivo) o utilizando las API de REST. Una actualización del dispositivo se instala

desde un solo archivo durante el proceso de actualización. Puede descargar el archivo directamente al dispositivo o a otro ordenador y, a continuación, transferirlo al dispositivo.

Cuando se instala una actualización del dispositivo, este se reinicia y se pone fuera de línea. Si el dispositivo se pone fuera de línea, los recursos gestionados no se ven afectados, sino que siguen funcionando mientras el dispositivo se encuentra en ese estado.

25.1.4 Información adicional

Para obtener más información sobre cómo obtener actualizaciones de software, consulte «Asistencia y otros recursos» (página 461).

25.2 Gestión de la disponibilidad del dispositivo

La gestión y el mantenimiento de la disponibilidad del dispositivo comienza configurando la máquina virtual como se describe en «Planificación para alta disponibilidad» (página 125), y siguiendo las prácticas recomendadas descritas en «Prácticas recomendadas para la gestión de un dispositivo de VM» (página 322).

Si se apaga el dispositivo, los recursos gestionados continúan funcionando. Para obtener más información sobre el modo en que el dispositivo gestiona un cierre inesperado y lo que puede hacer para recuperarlo, consulte:

- «Cómo gestiona el dispositivo un apagado inesperado» (página 324)
- «Qué hay que hacer cuando se reinicia un dispositivo» (página 325)

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para apagar o reiniciar el dispositivo.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)	`appliance/shutdown`

25.2.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

25.2.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Apagar el dispositivo (privilegios mínimos necesarios: administrador de infraestructuras)
- Reiniciar el dispositivo (privilegios mínimos necesarios: administrador de infraestructuras)

25.2.3 Prácticas recomendadas para la gestión de un dispositivo de VM

Hewlett Packard Enterprise recomienda seguir las directrices siguientes para gestionar el dispositivo de VM (máquina virtual) desde la consola virtual:

Prácticas recomendadas para la gestión de la máquina virtual VMware vSphere

Haga esto

- Utilizar aprovisionamiento grueso. (Necesario)
- Utilizar los recursos compartidos y las reservas para garantizar el rendimiento adecuado de la CPU.

No haga esto

- Utilizar el aprovisionamiento escaso.
- Actualizar las herramientas de VMware. Si las herramientas de VMware muestran el estado **Out of Date** (Anticuado) o **Unmanaged** (No gestionado), significa que se están ejecutando correctamente. Estos mensajes de estado no son un problema, ya que las herramientas están disponibles y funcionando. Las herramientas de VMware se actualizan con cada actualización del software de HPE OneView.
- Revertir a una instantánea de VM (a menos que, en determinadas circunstancias, así se lo indique un representante autorizado de soporte técnico).
- Establecer la opción **Synchronize guest time with host** (Sincronizar la hora del invitado con el host) en el cliente de vSphere cuando el dispositivo HPE OneView está configurado para usar NTP. HPE OneView configura automáticamente la opción **Synchronize guest time with host** (Sincronizar la hora del invitado con el host) adecuada durante la configuración de la red. Cuando se configura HPE OneView para que utilice servidores NTP, la opción **Synchronize guest time with host** (Sincronizar la hora del invitado con el host) se desactiva. Si HPE OneView no está configurado para utilizar servidores NTP, se sincroniza con el reloj de VM del host y la opción **Synchronize guest time with host** (Sincronizar la hora del invitado con el host) se activa. En este caso, debe configurar el host de VM para que utilice NTP.
- Reducir la cantidad de memoria asignada a la VM.

Prácticas recomendadas para la gestión de la máquina virtual Microsoft Hyper-V

Haga esto

- Especificar un tamaño fijo.

No haga esto

- Actualizar los servicios de integración.
- Revertir a un punto de control de VM (a menos que, en determinadas circunstancias, así se lo indique un representante autorizado de soporte técnico).
- Reducir la cantidad de memoria asignada a la VM.
- Habilite la memoria dinámica. Consulte **https://technet.microsoft.com/en-us/library/hh831766(v=ws.11).aspx**.

25.2.4 Apagado del dispositivo desde la interfaz de usuario

Utilice este procedimiento para realizar un apagado correcto del dispositivo desde la interfaz de usuario.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras.
- Asegúrese de que todas las tareas se han completado o están detenidas y de que todos los demás usuarios han finalizado la sesión.

Cómo apagar el dispositivo desde la interfaz de usuario

1. En el menú principal, seleccione **Settings** (Configuración) y, a continuación, haga clic en **Appliance** (Dispositivo).
2. Seleccione **Actions→Shut down** (Acciones > Apagar).

   Aparece un cuadro de diálogo para informarle de que finalizará la sesión de todos los usuarios y se cancelarán las tareas en curso.
3. Seleccione **Yes, shut down** (Sí, apagar) en el cuadro de diálogo.
4. Compruebe que el dispositivo se apaga.

25.2.5 Reinicio del dispositivo desde la interfaz de usuario

Utilice este procedimiento para apagar correctamente y reiniciar el dispositivo desde la interfaz de usuario. Volverá a la pantalla de inicio de sesión.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras.
- Asegúrese de que todas las tareas se han completado o están detenidas y de que todos los demás usuarios han finalizado la sesión. En caso contrario, al reiniciar el dispositivo se desconectan los usuarios y se interrumpen las tareas en ejecución.

Cómo reiniciar el dispositivo desde la interfaz de usuario

1. En el menú principal, seleccione **Settings** (Configuración) y, a continuación, haga clic en **Appliance** (Dispositivo).
2. Seleccione **Actions→Restart** (Acciones > Reiniciar).

   Aparece un cuadro de diálogo para informarle de que finalizará la sesión de todos los usuarios y se interrumpirán las tareas en ejecución.
3. Seleccione **Yes, restart** (Sí, reiniciar) en el cuadro de diálogo.
4. Compruebe que se ha realizado la operación iniciando sesión cuando vuelva a aparecer la pantalla de inicio de sesión.

25.2.6 Cómo gestiona el dispositivo un apagado inesperado

El dispositivo tiene funciones, tales como la copia de seguridad automática y la alta disponibilidad, que le permiten recuperarse automáticamente cuando se apaga de forma inesperada, y los recursos gestionados siguen funcionando mientras el dispositivo está fuera de línea. Sin embargo, Hewlett Packard Enterprise recomienda que utilice las funciones de copia de seguridad y alta disponibilidad del dispositivo para asegurarse de que se hace una copia de seguridad del dispositivo diariamente, así como cuando se realizan cambios significativos en la configuración, como agregar o eliminar una red.

Operaciones de recuperación del dispositivo

Cuando se reinicia el dispositivo, realiza las siguientes operaciones:

- Detecta las tareas que se estaban realizando y las reanuda, si es seguro hacerlo. Si el dispositivo no puede completar una tarea, notifica que la tarea se ha interrumpido o que se encuentra en algún otro estado de error.
- Intenta detectar diferencias entre el entorno actual y el entorno en el momento en que se apagó el dispositivo, y actualiza su base de datos con los cambios detectados.

  Si se observa que los datos del dispositivo no coinciden con el entorno actual, se puede solicitar que el dispositivo actualice los datos de ciertos recursos, como los receptáculos.

Recuperación del dispositivo durante una actualización de firmware de un recurso gestionado

Si el dispositivo se apaga durante una actualización del firmware de un recurso gestionado, cuando el dispositivo se reinicia, detecta el error de actualización y marca las tareas de actualización del firmware con un estado de error. Para actualizar el firmware de este recurso, debe reiniciar la tarea de actualización del firmware.

Qué hay que hacer cuando se reinicia un dispositivo

La ayuda en línea proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Comprobar si hay alertas críticas o tareas con errores y seguir las instrucciones proporcionadas para solucionarlos
- Actualizar un recurso manualmente si la información que se muestra sobre él aparentemente es incorrecta o incoherente
- Crear un volcado de soporte (se recomienda para ayudar al personal de soporte a solucionar un problema cuando se dan bloqueos inesperados)
- Actualizar el firmware de un recurso si había una tarea de actualización del firmware en curso cuando se apagó el dispositivo.

25.3 Gestión de la configuración

En la pantalla **Settings** (Configuración), la información del dispositivo está dividida en paneles en los que, a simple vista, puede ver el estado actual de categorías tales como las configuraciones de **Scopes** (Ámbitos) y **Proxy**.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)→Scopes (Ámbitos)	`/rest/scopes`
Settings (Configuración)→Proxy	`/rest/proxy`

25.3.1 Roles

- Privilegios necesarios: administrador de infraestructuras

25.3.2 Tareas

En la ayuda en línea se ofrece información sobre las siguientes tareas:

- Crear, eliminar y editar un nuevo ámbito.
- Asignar un recurso a un ámbito.
- Configurar los ajustes del proxy HTTPS del dispositivo.

25.3.3 Restablecimiento del dispositivo a la configuración original de fábrica

Cuando se restablece la configuración de fábrica, el dispositivo recupera la configuración original de fábrica. La versión de firmware instalada no cambia.

Tiene la opción de conservar o borrar la configuración de red del dispositivo.

Es posible que deba restablecer el dispositivo para darlo de baja (y así poder migrar el hardware) o para devolverlo a un estado conocido para reutilizarlo (por ejemplo, para restaurar el dispositivo a partir de un archivo de copia de seguridad).

ATENCIÓN:

- Esta acción borra los datos del dispositivo, incluidos los archivos de registro y la configuración de los dispositivos gestionados existente en HPE OneView.

  Esta acción no afecta de ninguna manera a la configuración de los dispositivos gestionados. Por lo tanto, podría ser necesaria una limpieza manual de los dispositivos si HPE OneView ya no va a gestionarlos.

- No se permiten llamadas a las API de REST ni operaciones de la GUI durante la acción de restablecimiento.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras
- Asegúrese de que todas las tareas se han completado o están detenidas y de que todos los demás usuarios han finalizado la sesión.

Cómo restablecer el dispositivo a la configuración original de fábrica

1. Si se está dando de baja el dispositivo y su entorno gestionado, quite todo el hardware de la gestión de HPE OneView, por ejemplo:
   - Elimine o cancele la asignación de todos los perfiles de servidor.
   - Elimine todos los receptáculos lógicos.
   - Elimine los volúmenes de almacenamiento asignados en HPE OneView.
   - Restablezca la configuración predeterminada de la asignación de direcciones IP de los dispositivos gestionados (configurados a través de pools de direcciones IP).
2. En el menú principal, seleccione **Settings** (Configuración) y, a continuación, haga clic en **Appliance** (Dispositivo).
3. Seleccione **Actions→Factory Reset** (Acciones > Restablecer configuración de fábrica).
4. De manera opcional, seleccione **Preserve appliance network settings to erase the appliance data without losing network connectivity, for example, to rebuild the appliance** (Conservar la configurad de red del dispositivo para borrar los datos del dispositivo sin perder la conectividad de red, por ejemplo, para reconstruir el dispositivo).
5. Seleccione **OK**.
6. Si está dando de baja el dispositivo, asegúrese de que todo el hardware gestionado por HPE OneView se quita de la gestión.

Esta acción muestra una barra de progreso mientras se ejecuta. Los inicios de sesión se desactivan automáticamente. Cuando se completa el restablecimiento del dispositivo pasados varios minutos, puede iniciar una sesión y configurar el dispositivo como lo hizo por primera vez.

25.3.4 Sobre la configuración del proxy del dispositivo

El panel **Proxy** le permite configurar el proxy HTTPS, el número de puerto para las conexiones del cliente y si la autenticación requiere un nombre de usuario y una contraseña o no.

25.3.5 Sobre los ámbitos

Un ámbito es una agrupación de recursos que se puede utilizar para limitar el alcance de una operación o acción. Por ejemplo, puede crear ámbitos basados en:

- Organización o departamento (marketing, investigación y desarrollo, finanzas)

- Uso (producción, desarrollo, pruebas)
- Habilidades (Linux, Windows)

Cuando se definen los ámbitos y se les asignan recursos, usted:

- Limita los recursos mostrados en la interfaz de usuario (IU) a aquellos asignados al ámbito.
- Puede configurar notificaciones por correo electrónico filtradas para alertas basadas en ámbitos definidos previamente.

«Categorías de recursos habilitados para ámbitos» enumera las categorías de recursos que se pueden agregar a un ámbito. Existen categorías de recursos que no se pueden agregar a un ámbito.

Más información

Sobre la notificación de alertas

25.3.5.1 Categorías de recursos habilitados para ámbitos

Solo los siguientes tipos de recursos pueden agregarse o eliminarse de un ámbito:

- Receptáculos
- Hardware de servidor
- Redes (Ethernet, FC y FCoE)
- Conjuntos de redes
- Interconexiones, excluidos los recursos de SAS
- Interconexiones lógicas, excluidos los recursos de SAS
- Grupos de interconexiones lógicas, excluidos los recursos de SAS
- Conmutadores
- Logical Switches (Conmutadores lógicos)
- Logical Switch Groups (Grupos de conmutadores lógicos)

IMPORTANTE: Para la notificación por correo electrónico de alertas, los recursos no categorizados aquí se incluyen en cualquier ámbito. Un filtro de notificación por correo electrónico que especifica uno o más ámbitos no elimina las alertas generadas por los recursos que no están categorizados actualmente aquí y se envían.

Para inhibir las alertas de recursos sin ámbito es necesario utilizar categorías de recursos asociadas, que se describe en “Edit an email recipient and filter entry” (Editar un destinatario de correo electrónico y entrada de filtro) en la ayuda en línea.

25.4 Gestión de direcciones y pools de identificadores

Inicialmente se proporciona un conjunto predeterminado de pools de identificadores virtuales para direcciones MAC, WWN y números serie. Si necesita direcciones o identificadores adicionales, puede agregar intervalos de pools de identificadores personalizados o generados automáticamente.

Puede gestionar los pools de identificadores desde la pantalla **Settings** (Configuración) de la interfaz de usuario o utilizando las API de REST.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)	`id-pools`

25.4.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

25.4.2 Tareas para las direcciones y los identificadores

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Ver una lista de pools de identificadores activos y sus propiedades.
- Agregar un pool de identificadores generado automáticamente para direcciones MAC, WWN o números serie.
- Agregar un intervalo de pools de identificadores personalizado para direcciones MAC, WWN o números serie.

25.4.3 Sobre pools de ID

Un pool de ID es una colección de uno o más intervalos que puede especificar o generar aleatoriamente para ofrecer grandes espacios de direcciones. Por defecto, cuando inicializa el dispositivo se crea automáticamente un pool de ID virtual para cada dirección MAC contigua, WWN y número de serie. Los pools están formados por direcciones e intervalos de ID. Puede habilitar o deshabilitar individualmente un intervalo o eliminar cualquier intervalo que no se utilice. Los intervalos de pool de ID no entran en conflicto con los ID físicos, dados los intervalos virtuales que crea excluyen los intervalos de ID físicos.

Pools de ID admitidos

Pool de ID	Descripción
Direcciones MAC virtuales (vMAC)	• Cantidad de 6 bytes representada como 12 caracteres hexadecimales, bytes separados por dos puntos (`:`) • Solo intervalos de direcciones de unidifusión, no se debe configurar el bit multidifusión
Nombres World Wide virtuales (vWWN)	• Cantidad de 8 bytes representada como 16 caracteres hexadecimales, bytes separados por dos puntos (`:`)
Números de serie virtuales (vSN)	• 10 caracteres alfanuméricos, mayúscula

25.4.4 Cómo agregar una máscara de subred IPv4 e intervalo de direcciones

Se pueden agregar un intervalo de direcciones y una subred IPv4 para admitir una red iSCSI.

Requisitos previos

- Privilegios mínimos necesarios: administrador de red, administrador de infraestructuras

Cómo agregar una máscara de subred IPv4 e intervalo de direcciones

1. En el menú principal, seleccione **Settings** (Configuración) y, a continuación, realice una de las acciones siguientes:
   - Haga clic en **Addresses and Identifiers** (Direcciones e identificadores) y, a continuación, haga clic en **Actions (Acciones)→Edit (Editar)**.
   - Pase el puntero por encima del panel **Addresses and Identifiers** (Direcciones e identificadores) y, a continuación, haga clic en el icono **Edit** (Editar).
2. Haga clic en **Add IPv4 subnet and address range** (Agregar intervalo de subred IPv4 e intervalo de direcciones) y escriba la información de subred solicitada.
3. Haga clic en **Add address range** (Agregar intervalo de direcciones) y escriba la información de dirección solicitada.
4. Haga clic en **Add** (Agregar), o en **Add +** (Agregar +) para agregar intervalos de direcciones adicionales.
5. Haga clic en **Add** (Agregar), o en **Add +** (Agregar +) para agregar intervalos de direcciones y subredes adicionales.
6. Haga clic en **OK** (Aceptar) para enviar los cambios.
7. Confirme que el nuevo intervalo de direcciones aparece en el panel **IPv4 Subnets and Address Ranges** (Intervalos de direcciones y subredes IPv4).

25.5 Gestión de las funciones de seguridad del dispositivo

Para obtener más información sobre las funciones de seguridad del dispositivo, consulte «Información sobre las funciones de seguridad del dispositivo» (página 69).

25.6 Activación o desactivación del acceso de Soporte Hewlett Packard Enterprise al dispositivo

HPE OneView contiene una funcionalidad técnica que permite a un representante autorizado de soporte técnico in situ acceder a su sistema a través de la consola del sistema y evaluar los problemas de los que haya informado. El acceso se controla mediante una contraseña generada por Hewlett Packard Enterprise que solo se proporcionará al representante autorizado de soporte técnico. Puede desactivar el acceso en cualquier momento con el sistema en funcionamiento.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)	`appliance/settings`

25.6.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

25.6.2 Tareas

La ayuda en línea del dispositivo proporciona información para activar o desactivar el acceso de Soporte Hewlett Packard Enterprise de **Settings** (Configuración) desde la pantalla o desde las API de REST.

25.7 Gestión de certificados TLS

Un certificado TLS (Transport Layer Security) certifica la identidad del dispositivo. El certificado lo necesita el servidor HTTP subyacente para establecer un canal de comunicaciones seguro (cifrado) con el explorador web del cliente.

Los certificados se gestionan desde la pantalla **Settings** (Configuración) o utilizando las API de REST de configuración del dispositivo.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)	`certificates`

25.7.1 Roles

- Privilegios mínimos necesarios para todas las tareas excepto donde se indica: administrador de infraestructuras

25.7.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Crear un certificado autofirmado.
- Crear una solicitud de firma de certificado.
- Importar un certificado.
- Ver la configuración de certificados TLS (Privilegios mínimos necesarios: administrador de infraestructuras, administrador de copias de seguridad o solo lectura).

25.7.3 Información adicional

Consulte «Información sobre las funciones de seguridad del dispositivo» (página 69).

25.8 Gestión de la clave pública de Hewlett Packard Enterprise

La clave pública de Hewlett Packard Enterprise verifica que:

- Hewlett Packard Enterprise ha creado sus paquetes de software (RPM) y sus actualizaciones.
- El código no ha sido modificado después de su firma.

25.8.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

25.8.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre cómo gestionar las claves públicas desde la pantalla **Settings** (Configuración) o mediante el uso de las API de REST para:

- Adquisición e instalación de la clave pública de Hewlett Packard Enterprise.
- Visualización de la clave pública de Hewlett Packard Enterprise.

25.9 Descarga de los registros de auditoría

El registro de auditoría ayuda al administrador de seguridad a conocer las acciones relacionadas con la seguridad que se han realizado. Puede recopilar los archivos de registro y otra información que el representante autorizado de soporte técnico necesita para poder diagnosticar y solucionar problemas en un dispositivo.

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Settings (Configuración)	`audit-logs`

25.9.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras.

25.9.2 Tareas

La ayuda en línea del dispositivo proporciona información sobre cómo descargar los registros de auditoría desde la pantalla **Settings** (Configuración) o mediante el uso de las API de REST.

25.9.3 Descarga de los registros de auditoría

El registro de auditoría muestra al administrador de seguridad las acciones relacionadas con la seguridad que se han realizado.

Puede descargar los archivos de registro y otra información que pueda usar el representante autorizado de soporte técnico para poder diagnosticar y solucionar problemas en un dispositivo.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras

Cómo descargar los registros de auditoría

1. En el menú principal, seleccione **Settings** (Configuración).
2. Haga clic en **Security** (Seguridad).
3. Seleccione **Actions→Download audit logs** (Acciones > Descargar registros de auditoría).
4. El dispositivo genera un archivo comprimido de registros de auditoría y lo descarga en el sistema local.

   El nombre del archivo comprimido sigue este formato:

   `audit-logs-`*`aaaa_mm_dd-hh_mm_ss`*

   `aaaa_mm_dd` indica la fecha y *`hh_mm_ss`* indica la hora en la que se creó el archivo. El nombre del archivo de registro de auditoría aparece en la pantalla.

   El archivo de registro de auditoría se descarga en la carpeta de descarga predeterminada. Si no hay ningún carpeta de descarga predeterminada configurada en su explorador, se le solicitará que especifique un archivo de destino.
5. Compruebe que el archivo de registro se ha descargado en la carpeta correcta.

25.9.4 Información adicional

- «Conceptos básicos sobre el registro de auditoría» (página 75)
- «Elección de una directiva para el registro de auditoría» (página 77)

Parte V Supervisión

En los capítulos de esta sección se describe el uso del dispositivo para supervisar el centro de datos. La información de esta parte se utiliza después de configurar el dispositivo y de añadir los recursos del centro de datos al dispositivo.

26 Supervisión del estado y el rendimiento del centro de datos

En este capítulo se describen las prácticas recomendadas para la supervisión del estado y el rendimiento del centro de datos mediante HPE OneView.

26.1 Supervisión diaria

Como parte de la supervisión diaria del centro de datos, es importante ser capaz de examinar rápidamente los recursos gestionados por el dispositivo para evaluar el estado general del centro de datos. Puede examinar las pantallas de la interfaz de usuario para analizar rápidamente el estado y las condiciones en que se encuentra el centro de datos.

26.1.1 Comprobación inicial: el panel de control

La pantalla **Dashboard** (Panel de control) proporciona un resumen visual del estado de los recursos del dispositivo que está autorizado a ver. El **panel de control** puede mostrar un resumen del estado de:

- Perfiles de servidor
- Hardware de servidor
- Receptáculos
- Interconexiones lógicas
- Pools de almacenamiento
- Volúmenes
- Alertas del dispositivo

El estado de cada recurso se indica mediante un icono: `correcto` (), `advertencia` ( ) o `crítico` (). Puede desplazarse a las pantallas de los recursos de la interfaz de usuario para obtener más información haciendo clic en los iconos de estado que aparecen para cada recurso.

Para obtener más información sobre la pantalla **Dashboard** (Panel de control), consulte «Uso de la pantalla del panel de control».

26.1.2 Actividades

La pantalla **Activity** (Actividad) proporciona un registro de notificaciones de estado. El dispositivo comprueba la actividad actual de los recursos del entorno y muestra alertas en la pantalla **Activity** (Actividad) y en las pantallas de los recursos asociados para que pueda revisarlas.

La pantalla **Activity** (Actividad) también es una base de datos de todas las tareas que se han ejecutado, ya sea de forma síncrona o asíncrona, e iniciado por el usuario o el sistema. Es similar a un registro de auditoría, pero proporciona más detalles y resulta sencillo acceder a ella desde la interfaz de usuario.

26.1.3 Gráficos de utilización

Para ciertos recursos, el dispositivo recopila estadísticas de utilización de CPU, energía y temperatura de los procesadores de gestión (el iLO, Onboard Administrator e iPDU). Los gráficos de utilización permiten entender las estadísticas de utilización recientes relativas a la capacidad disponible, ver las tendencias de utilización a lo largo del tiempo y ver la utilización histórica a través del tiempo. Pase el ratón por encima de la zona de utilización de la interfaz de usuario para mostrar cuadros emergentes con información.

Pantalla **Enclosures** (Receptáculos)	Permite ver estadísticas históricas de consumo de energía (promedio, máximo y límite de alimentación) y de temperatura.
Pantalla **Server Hardware** (Hardware de servidor)	Permite ver estadísticas históricas de utilización o frecuencia de la CPU, consumo de energía (promedio, máximo y límite de alimentación) y de temperatura.
Pantalla **Power Delivery Devices** (Dispositivos de suministro de energía)	Permite ver estadísticas históricas de consumo de energía (promedio, máximo, y durante los últimos 5 minutos y las últimas 24 horas).
Pantalla **Racks** (Bastidores)	Permite ver estadísticas históricas de consumo de energía (promedio, máximo y límite de alimentación) y de temperatura.
Pantalla **Interconnects** (Interconexiones)	Permite ver estadísticas de las velocidades de transferencia en bits (transmitidos y recibidos) de los puertos de enlace ascendente.
Pantalla **Storage systems** (Sistemas de almacenamiento)	Permite ver la capacidad de almacenamiento en tebibytes (TiB).

Para obtener más información sobre los gráficos de utilización, consulte el Capítulo 27, «Supervisión de la energía y la temperatura».

26.1.4 Supervisión de la temperatura del centro de datos

El dispositivo de gestión proporciona datos de supervisión detallados que puede utilizar para determinar las capacidades de energía y refrigeración de los dispositivos del centro de datos. Es posible que la refrigeración global del centro de datos sea suficiente, pero podría haber áreas que no tengan suficiente refrigeración debido a situaciones como poco flujo de aire, excesiva concentración de salida de calor o flujo de aire recirculante al final de los pasillos. Para identificar fácilmente los problemas de temperatura y detectar puntos calientes en todas las áreas del centro de datos, utilice las funciones de visualización 3D disponibles en la pantalla de centros de datos de la interfaz de usuario.

Para obtener más información sobre la temperatura, consulte el Capítulo 27, «Supervisión de la energía y la temperatura».

26.2 Prácticas recomendadas para la supervisión de centros de datos

A continuación se indican las prácticas recomendadas para usar el dispositivo HPE OneView con el fin de asegurarse del estado de los componentes gestionados del entorno del centro de datos.

26.2.1 Prácticas recomendadas para la supervisión del estado con la interfaz de usuario del dispositivo

Hewlett Packard Enterprise recomienda las siguientes prácticas recomendadas para supervisar el estado de los recursos del entorno.

Pasos generales de supervisión del estado

NOTA: Puede ver el estado y las alertas de todos los servidores gestionados y de algunos servidores supervisados. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener más información sobre el hardware de servidor supervisado.

Paso de supervisión	Información relacionada
1. Vaya a la pantalla **Activity** (Actividad) y filtre las actividades utilizando las opciones de filtrado más adecuadas para su caso concreto. También puede comenzar desde la pantalla **Dashboard** (Panel de control) para ver las alertas de determinados recursos.	«Acerca de la pantalla de actividad» «Uso de la pantalla del panel de control»
2. Vaya a una pantalla específica de un recurso para ver las actividades específicas de ese recurso. En la pantalla del recurso, compruebe el estado de las instancias del recurso a través de los iconos de estado correspondientes. **3.** Investigue cada instancia de recurso que tenga un estado de advertencia o de error.	«Descripciones de los iconos»
4. Expanda las alertas críticas y de advertencia para ver sus descripciones completas y haga clic en **Event details** (Detalles del evento) para ver información adicional sobre los eventos que provocaron la alerta.	
5. Siga las instrucciones de la solución recomendada (si existe) o investigue la alerta para corregir el problema. **NOTA:** Si una alerta está `Active` (Activa) y no es necesario realizar ninguna acción, puede cerrar la alerta. Si una alerta está `Locked` (Bloqueada), no podéis cerrar la alerta si no arregláis la condición que la ha causado.	

Para supervisar el estado actual de una red, vaya a los recursos **Interconnects** (Interconexiones) y **Logical Interconnects** (Interconexiones lógicas) para ver la actividad, alertas y notificaciones recientes, y el estado actual.

26.2.2 Prácticas recomendadas para la supervisión del estado utilizando las API de REST o SCMB

Para garantiza el estado de los componentes en el entorno del centro de datos, utilice el State-Change Message Bus (SCMB) para recibir mensajes de estado de salud. SCMB utiliza la mensajería asíncrona para notificar a los suscriptores los cambios en los recursos gestionados, tanto lógicos como físicos. Por ejemplo, puede recibir notificaciones cuando el nuevo hardware de servidor se agrega al entorno gestionado o cuando el estado de salud de los recursos físicos cambia.

Para utilizar las API de REST para supervisar el estado, consulte:

- Supervisión del estado global
- Supervisión del estado del hardware de servidor
- Supervisión del estado de la red

Supervisión del estado global

NOTA: Puede ver el estado y las alertas de todos los servidores gestionados y de algunos servidores supervisados. Para ver qué servidores se pueden supervisar, consulte el hardware de servidor supervisado en la ***Matriz de compatibilidad de HPE OneView***.

Paso de supervisión
• Filtre las alertas basándose en la gravedad o en la fecha para ver los problemas de estado actuales. `GET /rest/alerts?filter="severity='{UNKNOWN, OK, WARNING, CRITICAL}'"&filter="created='{YYYY-MM-DDThh:mm:ss.sssZ}'"` **NOTA:** El nivel de gravedad `DISABLED` (DESACTIVADO) no se aplica a las alertas. Consulte la ayuda en línea acerca de secuencias de comandos para obtener más información sobre las alertas.
• Obtenga las alertas de un tipo de recurso físico específico, como el hardware de servidor. `GET /rest/alerts?filter="physicalResourceType='{physical_server}'"` Consulte la ayuda en línea acerca de secuencias de comandos para obtener más información sobre perfiles de hardware.

Revise los eventos que provocaron una alerta específica.
1. Seleccione una alerta.
`GET /rest/alerts/`
2. Obtenga una alerta específica utilizando el ID de alerta.
`GET /rest/alerts/{id}`
3. Obtenga los eventos asociados.
`GET /rest/events/{id}`

• Solucione el problema. Utilice la solución recomendada (realice una operación GET en el recurso de alerta específico y consulte el atributo `correctiveAction`) o investigue la alerta.

Supervisión del estado del hardware de servidor

Uno o varios servidores pueden pasar al estado de advertencia o al estado crítico cuando algo no es correcto dentro del dispositivo. Si se ha aplicado un perfil de servidor a un servidor que ha fallado, el perfil de servidor también estará en un estado de error.

Paso de supervisión
• Utilice los detalles de la alerta para solucionar el problema. Cuando esté disponible, intente utilizar la solución recomendada en primer lugar. En algunos casos, puede ser necesario investigar la alerta más a fondo para determinar mejor la solución. `GET /rest/alerts?filter="physicalResourceType='{physical_servers}'"&filter="severity='{WARNING, CRITICAL}'"` Consulte la ayuda en línea acerca de secuencias de comandos para obtener más información sobre las alertas.
• Asegúrese de que se han asignado correctamente los perfiles de servidor al hardware de servidor. Consulte la ayuda en línea acerca de secuencias de comandos para obtener más información sobre perfiles de servidor.

Supervisión del estado de la red

Para determinar el estado actual de una o varias redes en el dispositivo, revise las alertas de las interconexiones e interconexiones lógicas para comprobar que las conexiones son correctas. Para obtener una lista de alertas, puede realizar una operación `GET` con las alertas y filtrarlas para obtener las alertas relacionadas con las interconexiones. Para obtener una lista de estados,

puede realizar una operación `GET` con las interconexiones e interconexiones lógicas y filtrarlas para obtener el estado `OK` (Correcto).

Paso de supervisión

Revise las alertas para las interconexiones.
1. Seleccione una alerta de interconexión.
`GET /rest/alerts?filter="physicalResourceType='{interconnect}'"&filter="severity='{WARNING, CRITICAL}'"`
2. Obtenga una alerta específica utilizando el ID de alerta.
`GET /rest/alerts/{id}`
Consulte el capítulo *REST API* (API de REST) de la ayuda en línea para obtener más información sobre las interconexiones.

Aplique un filtro para obtener las interconexiones lógicas con un estado de apilamiento incorrecto.
1. Obtenga una interconexión lógica en mal estado.
`GET /rest/logical-interconnects?filter="stackingHealth='{Unknown, Disconnected}'"`
2. Revise la interconexión específica que se encuentra en mal estado utilizando el ID de interconexión.
`GET /rest/logical-interconnects/{id}`
Consulte el capítulo *REST API* (API de REST) de la ayuda en línea para obtener más información sobre las interconexiones lógicas.

• Utilice la información suministrada en la alerta para solucionar el problema. Utilice la solución recomendada, si la hay, o investigue la alerta. Consulte la ayuda en línea acerca de secuencias de comandos para obtener más información sobre las alertas.

26.3 Gestión de actividades

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

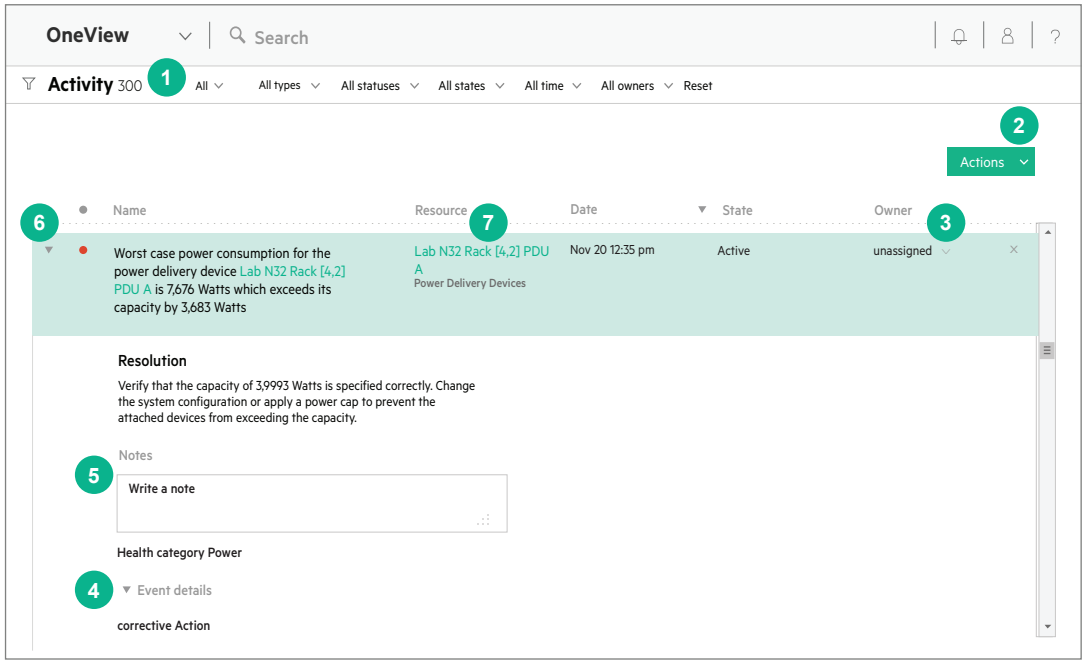
- Ver las actividades de un recurso.
- Filtrar las actividades por fecha, estado o estado.
- Asignar un propietario a una alerta.
- Agregar una nota a una alerta.
- Desactivar una alerta.
- Restaurar una actividad desactivada al estado activo.

26.3.1 Acerca de la pantalla de actividad

La pantalla **Activity** (Actividad) enumera las alertas y otras notificaciones sobre la actividad del dispositivo y los eventos que se producen en su centro de datos. Puede filtrar, ordenar y expandir las áreas de la pantalla para refinar cómo se muestra la información. Los enlaces de los detalles de actividades también le permiten ver información adicional sobre los recursos específicos, especialmente si la notificación informa sobre un evento que requiere de atención inmediata.

Componentes de la pantalla Activity (Actividad)

La imagen que se muestra a continuación ilustra las áreas más importantes de la pantalla que puede utilizar para supervisar, resolver y gestionar la actividad.



1. De manera predeterminada, la pantalla **Activity** (Actividad) muestra **todas** las alertas, tareas y eventos que se han producido. Para filtrar rápidamente la lista predeterminada de actividades para que muestre las notificaciones que requieren su atención, haga clic en el icono ⌄ pasar de **All** (Todo) a **Needs attention** (Que requieren atención).

   Utilice los filtros y los selectores de intervalo de fechas de la barra de menús **Filters** (Filtros) para que se muestre solamente el tipo de actividad que desee ver. Para ampliar las opciones para cualquier selector de filtrado de la barra superior de filtros, haga clic en el icono ⌄ que se encuentra junto a cada selector de filtrado.
2. Utilice el menú **Actions** (Acciones) para asignar, borrar o restaurar las notificaciones seleccionadas.
3. Para asignar una alerta u otra notificación a un usuario determinado, seleccione un nombre de la lista en la columna **Owner** (Propietario) de cada notificación.
4. Cuando se expande una notificación, haga clic en el enlace de **Event Details** (Detalles del evento) para ver más detalles acerca de esta notificación, donde podrá encontrar la acción correctiva necesaria específica para la actividad que requiere su atención.
5. Empiece escribiendo en el cuadro de nota para añadir instrucciones u otra información a una notificación.

SUGERENCIA: Puede hacer clic en el ángulo inferior derecho del cuadro de la nota y arrastrarlo para expandirlo y facilitar así su lectura o su edición.

6. Haga clic en el icono ▶ para expandir la vista de una notificación y ver todo su contenido.

   Haga clic en el icono ▼ para contraer la notificación en un resumen de un sola línea.
7. Si una notificación informa de un estado que no sea correcto (verde), haga clic en el vínculo que se muestra para ver los detalles del recursos que generó dicha notificación.

26.3.2 Tipos de actividades: alertas y tareas

26.3.2.1 Acerca de las alertas

El dispositivo utiliza los mensajes de alerta para informar sobre los problemas que surgen en los recursos que gestiona y supervisa. Los recursos generan alertas para notificarle que se ha producido algún evento significativo y que es posible que sea necesario realizar una acción.

Un evento describe un único problema o cambio que se produjo en un recurso. Por ejemplo, un evento puede ser una captura SNMP recibida del procesador de gestión (iLO) de un servidor.

Cada alerta incluye la siguiente información sobre el evento que notifica: gravedad, estado, descripción y urgencia. Puede borrar las alertas, asignar propietarios a las alertas y añadir notas a las alertas.

Mientras las alertas tienen un estado activo o bloqueado, contribuyen al estado general de un recurso que se muestra. Después de cambiar el estado a `Cleared` (Borrado), dejan de afectar al estado mostrado.

IMPORTANTE:
El dispositivo realiza un recuento de las alertas entrantes. En intervalos de 500 mensajes de alerta, el dispositivo determina si el número de alertas ha alcanzado los 75.000. Cuando lo hace, se produce una autolimpieza en la que se eliminan los mensajes de alerta hasta que la cantidad total es inferior a 74.200. Cuando se ejecuta la autolimpieza, primero se eliminan las alertas borradas más antiguas. A continuación, se eliminan las alertas más antiguas por gravedad, comenzando por las menos graves.

Más información

«Alertas del servicio»

26.3.2.2 Acerca de las tareas

Todas las tareas iniciadas por el usuario o por el sistema se consideran actividades:

- Las tareas iniciadas por el usuario se crean cuando un usuario agrega, crea, quita, actualiza o elimina recursos.
- Otras tareas las crean los procesos que se ejecutan en el dispositivo, tales como la recopilación de datos de utilización de un servidor.

El registro de tareas proporciona una valiosa fuente de información que puede utilizar para la solución de problemas. Puede determinar el tipo de tarea realizada, si se completó, cuándo se completó y quién la inició.

Los tipos de tareas son:

Tipo de tarea	Descripción
Usuario	Tarea iniciada por el usuario, como crear, editar o eliminar un grupo de receptáculos o un conjunto de redes
Dispositivo	Tarea iniciada por el dispositivo, como la actualización de los datos de utilización
Segundo plano	Tarea que se realiza en segundo plano. Este tipo de tarea no aparece en el registro.

IMPORTANTE: El dispositivo mantiene una base de datos de tareas que contiene información sobre las tareas de unos 6 meses o 50.000 tareas. Si la base de datos de tareas supera las 50.000 tareas, se eliminan bloques de 500 tareas hasta que el total sea inferior a 50.000. Las tareas con una antigüedad superior a los 6 meses se eliminan de la base de datos.

La base de datos de tareas y la base de datos en la que se almacenan las alertas son independientes.

26.3.3 Estados de las actividades

Actividad	Estado	Descripción
Alerta	**Active (Activa)**	La alerta no se ha borrado o resuelto. Las alertas activas de un recurso se tienen en cuenta en el estado general del recurso. Las alertas activas contribuyen al resumen de recuento de alertas.
	Locked (Bloqueada)	Una alerta `Active` (Activa) que fue bloqueada por un gestor de recursos interno. No se puede desactivar manualmente una alerta `Locked` (Bloqueada). Examine la acción correctiva asociada con una alerta para determinar cómo solucionar el problema. Una vez solucionado el problema, el gestor de recursos cambia la alerta al estado `Active` (Activa). A partir de ese momento, puede desactivar o eliminar la alerta. Las alertas bloqueadas de un recurso contribuyen a su estado general.
	Cleared (Borrada)	La alerta se ha resuelto o notificado. Borre una actividad cuando ya no sea necesario realizar un seguimiento. El dispositivo borra determinadas actividades automáticamente. Las actividades `Cleared` (Borradas) no afectan al estado del recurso y no se cuentan para los resúmenes mostrados.
Alerta del servicio	**Pending (Pendiente)**	El caso de soporte está pendiente de envío a HPE.
	Submitted (Enviado)	El caso de soporte se ha enviado a HPE.
	Received (Recibido)	HPE ha recibido el caso de soporte.
	Abra	El caso de soporte está abierto.
	Closed (Cerrado)	El caso de soporte está cerrado. **NOTA:** Un soporte de caso puede cerrarse sin ninguna acción: • Si se trata de un evento de prueba • Si el dispositivo no está habilitado para soporte remoto • Si el dispositivo no está cubierto por el contrato de soporte o en garantía
	Error	La solicitud de servicio ha encontrado un error durante el procesamiento.
	No hay	No hay ninguna alerta de servicio. Este es el valor predeterminado.

Actividad	Estado	Descripción
Tarea	**Completed (Completada)**	La tarea se inició y se ejecutó por completo.
	Running (En ejecución)	La tarea se inició y se está ejecutando, pero todavía no se ha completado.
	Pending (Pendiente)	La tarea todavía no se ha ejecutado.
	Interrupted (Interrumpida)	La tarea se ejecutó, pero se interrumpió. Por ejemplo, podría estar esperando a un recurso.
	Error	Una tarea falló o generó una alerta `Critical` (Crítica). Investigue inmediatamente los estados de `Error`.
	Terminated (Terminada)	Una tarea se ha cerrado o cancelado correctamente.
	Warning (Advertencia)	Se ha producido un evento que podría requerir su atención. Una advertencia puede implicar que hay algún error en el dispositivo. Investigue inmediatamente los estados de `Warning`.

26.3.4 Niveles de gravedad de las actividades

El estado indicado para cada recurso de HPE OneView representa el estado de ese recurso concreto y no el estado agregado de sus subcomponentes. Por ejemplo, el estado de un receptáculo no es el estado agregado de todos sus blades de servidor y servidores, sino solo el estado del receptáculo (Onboard Administrator, ventiladores y fuentes de alimentación).

Nivel de gravedad	Descripción
Critical (Crítico)	Se ha recibido un mensaje de alerta crítica, o una tarea ha fallado o se ha interrumpido. Investigue inmediatamente las actividades con un nivel de gravedad `Critical` (Crítico).
Warning (Advertencia)	Se ha producido un evento que podría requerir su atención. Una advertencia puede implicar que hay un error en el dispositivo que precisa atención. Investigue inmediatamente las actividades con un nivel de gravedad `Warning` (Advertencia).
OK (Correcto)	Para una alerta, `OK` (Correcto) indica que un recurso tiene un comportamiento normal o que envía información normal. Para una tarea, `OK` (Correcto) indica que se ha completado correctamente.
Unknown (Desconocido)	El nivel de gravedad de la alerta o tarea es desconocido. El nivel de gravedad de una tarea que está configurada para ejecutarse posteriormente es `Unknown` (Desconocido).
Disabled (Desactivado)	Se ha evitado que la tarea continúe o se complete.

26.3.5 Alertas del servicio

Un dispositivo (por ejemplo, un iLO) puede generar una alerta de servicio asociada con una alerta. Cuando aparece en la pantalla **Activity** (Actividad), la alerta de servicio proporciona información de servicio con un identificador de caso (ID de caso) incluido e información de contacto principal para facilitar una llamada de servicio. La información de contacto principal se introdujo al configurar Remote Support (soporte remoto).

Para los dispositivos en garantía o cubiertos activamente por un contrato de soporte, Remote Support cierra y elimina automáticamente las alertas de servicio cuando las condiciones son

normales; por ejemplo, después de cambiar un ventilador defectuoso. Remote Support no realiza ninguna acción con los dispositivos que no están cubiertos activamente por un contrato de soporte.

Más información

«Estados de las actividades»

26.4 Gestión de notificaciones por correo electrónico

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario para:

- Configurar el dispositivo para la notificación de alertas por correo electrónico.
- Agregar un destinatario de correo electrónico y un filtro.
- Modificar una entrada de filtro y destinatarios de correo electrónico.
- Activar o desactivar un destinatario de correo electrónico y un filtro.
- Desactivar una alerta.
- Eliminar una entrada de filtro y destinatarios de correo electrónico.

26.5 Acerca de la notificación de mensajes de alerta por correo electrónico

Esta función avisa a los destinatarios indicados cuando se produce una alerta concreta.

Cuando esta función se configura y se habilita, el dispositivo realiza estos pasos además de emitir la alerta:

- El dispositivo compara la alerta con los criterios de búsqueda configurados.
- Si la alerta coincide, crea un mensaje de correo electrónico que contiene el texto de la alerta.
- El dispositivo envía el mensaje de correo electrónico a los destinatarios indicados tanto en texto sin formato como en los tipos HTML y MIME. Al enviarlo en ambos tipos, la aplicación de correo del destinatario puede determinar la visualización.

Puede activar o desactivar esta función de notificación por correo electrónico, o puede activar o desactivar las notificaciones de determinados filtros, según le convenga.

El dispositivo admite hasta 100 combinaciones de filtros y destinatarios, y puede haber hasta 50 destinatarios en un mismo mensaje de correo electrónico. Esta flexibilidad le permite ajustar con precisión qué mensajes de alerta se envían y a quién. Por ejemplo, puede configurar el dispositivo para que envíe las alertas de tipo `Warning` (Advertencia) a un destinatario y las alertas de tipo `Critical` (Crítico) a otro.

Puede enviar mensajes de prueba para comprobar la configuración.

26.6 Configuración del dispositivo para la notificación de alertas por correo electrónico

Utilice este procedimiento para configurar el dispositivo para el envío de mensajes de correo electrónico de alerta. Posteriormente, podrá agregar, editar o eliminar entradas para los destinatarios o los filtros.

NOTA: Los filtros de notificación por correo electrónico solo pueden configurarse para los mensajes de alerta.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras

Configuración del dispositivo para la notificación de alertas por correo electrónico

1. En el menú principal, vaya a la pantalla **Settings** (Configuración).
2. Localice el panel **Notifications** (Notificaciones) y haga clic en .
3. Proporcione los datos solicitados en el panel **Email** (Correo electrónico) de la pantalla Edit Notifications (Editar notificaciones):

   NOTA: El servidor SMTP se determina automáticamente a partir del nombre de dominio de la dirección de correo electrónico del dispositivo. Si tiene que especificar la configuración de SMTP, haga clic en **SMTP options** (Opciones de SMTP) para hacerlo.

4. Continúe para agregar una o varias entradas.

26.7 Uso de la pantalla del panel de control

26.7.1 Información sobre el panel de control

Los gráficos del **panel de control** proporcionan una representación visual del estado general del dispositivo, así como de los recursos gestionados del centro de datos. En el **panel de control** puede ver inmediatamente los recursos que requieren su atención. Para acceder directamente a los recursos que necesitan su atención, haga clic en el nombre del recurso.

Cada vez que inicie sesión en el dispositivo, la primera pantalla que verá es el **panel de control**. Seleccione **Dashboard** (Panel de control) en el menú principal en cualquier momento para ver los gráficos del **panel de control**.

El **panel de control** muestra el estado de los recursos más relevantes que están asociados a los roles de usuario asignados. Si tiene asignados varios roles, por ejemplo, los roles Network (Red) y Storage (Almacenamiento), el panel de control predeterminado muestra la combinación de los recursos que vería cada rol en el panel de control. Puede personalizar la visualización del panel de control mediante la adición, eliminación y traslado de paneles de recursos.

26.7.2 Detalles de la pantalla del panel de control

IMPORTANTE: El **panel de control** está en blanco la primera vez que se inicia sesión en el dispositivo porque todavía no se ha configurado ningún recurso.

Si es la primera vez que inicia sesión en el dispositivo, consulte «Inicio rápido: Configuración inicial de HPE OneView» (página 137) para definir el entorno de su centro de datos e incluir su infraestructura en la gestión del dispositivo.

Pase el puntero por encima de un sector de un gráfico para ver el número de instancias de recursos que representa ese sector. Si pasa el puntero por otro sector del mismo gráfico, cambian el texto y el recuento mostrados en el centro del gráfico. Haga clic en un sector para ir a la página de recursos filtrada por el estado o el valor asociado al sector.

Si está viendo el **panel de control** en una pantalla estrecha, los gráficos de los recursos con varios gráficos se disponen verticalmente, por lo que deberá utilizar la barra de desplazamiento para desplazarse a cada uno de ellos.

El **panel de control** muestra los siguientes tipos de gráficos:

Tipo de gráfico	Descripción
Status (Estado)	En el gráfico **Status** (Estado) se resume el estado. El número que aparece junto al nombre del recurso indica el número total de instancias del recurso conocidas por el dispositivo. Para obtener más información, haga clic en el nombre del recurso para que se muestre su pantalla principal y ver información detallada del estado. En el gráfico **Status** (Estado), el sector en color gris oscuro indica el número de recursos que no están ofreciendo información, bien porque están desactivados o porque el dispositivo no los está gestionando. Para filtrar la vista de un recurso en función de su estado, haga clic en el icono de estado. Para obtener más información sobre los iconos de estado y nivel de gravedad, consulte «Descripciones de los iconos».
Servers with profiles (Servidores con perfiles)	El gráfico **Servers with profiles** (Servidores con perfiles) informa sobre el número de instancias de hardware de servidor con perfiles de servidor asignados. Si el gráfico no es completamente azul, pase el puntero sobre el sector de color gris claro del gráfico para ver el número de servidores que no tienen asignado un perfil de servidor.
Blade Bays (Compartimentos de blades)	El gráfico **Blade bays** (Compartimentos de blades) informa sobre el número de instancias de hardware de servidor de todos los compartimentos de receptáculos gestionados. Si el gráfico no es completamente azul, pase el puntero sobre el sector de color gris claro del gráfico para ver el número de compartimentos de receptáculos vacíos.

26.7.3 Cómo se interpretan los gráficos del panel de control

Los colores del **panel de control** le ayudan a interpretar rápidamente los datos que se muestran.

Tabla 14 Colores de los gráficos del panel de control

Color	Indicación
Verde	Estado correcto
Amarillo	Se ha producido un evento que podría requerir su atención
Rojo	Existe un estado crítico que requiere su atención inmediata
Azul	Para un gráfico de estado, las instancias de recursos que coinciden con los datos que se miden (un gráfico totalmente azul indica el 100%) Para los gráficos personalizados, puede haber distintos tonos de azul, cada uno de los cuales representa un valor diferente para un atributo.
Gris claro	Las instancias de recursos que no coinciden con los datos que se miden (utilizado en combinación con el azul para completar el 100%)
Gris oscuro	Instancias de recursos cuyo estado es distinto de `OK` (Correcto), `Warning` (Advertencia) o `Critical` (Crítico); es decir, que su estado es `Disabled` (Desactivado) o `Unknown` (Desconocido)

Iconos de estado

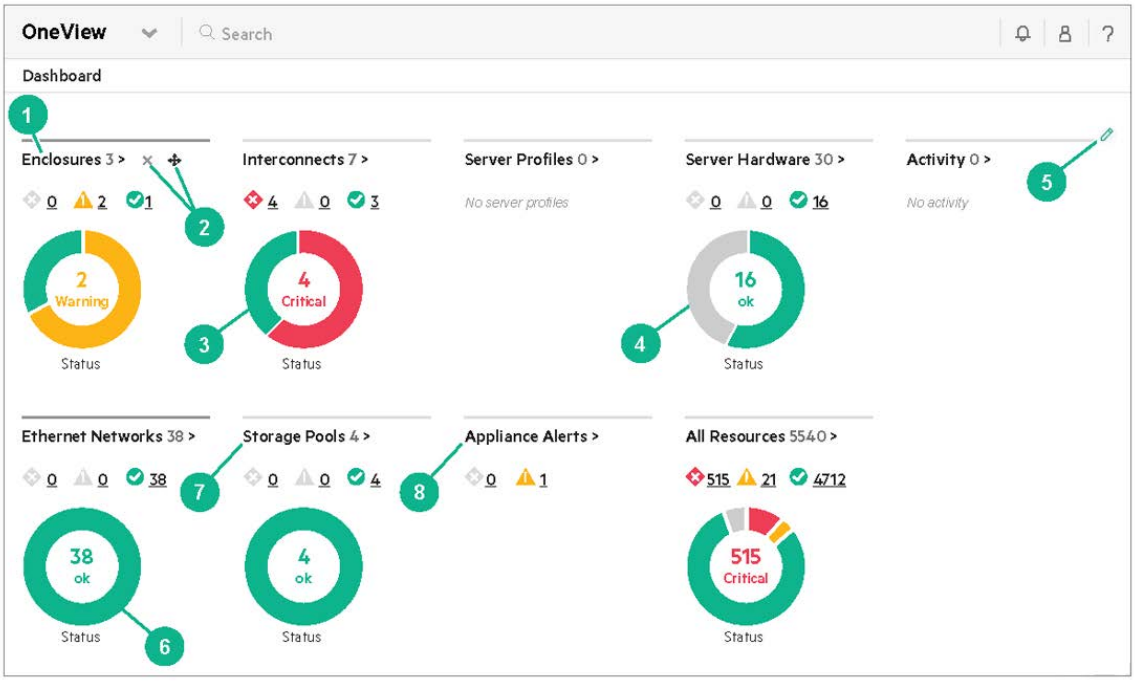
Para ayudarle a identificar los recursos que no están en un estado correcto, los iconos de estado indican el número de recursos cuyo estado es `correcto` (), `advertencia` ( ) o `crítico` ().

Puede seleccionar un icono de estado para ver la pantalla principal del recurso, con las instancias del recurso filtradas según ese estado o hacer clic en la sección del anillo del mismo color. Si no se han definido recursos o si no se han detectado instancias de recursos con un estado

determinado (lo que se indica con el número cero), el icono asociado es casi incoloro (gris muy claro).

Para saber cómo interpretar los datos que se muestran en los gráficos, consulte las descripciones numeradas que aparecen después de la figura.

Figura 20 Ejemplo de panel de control



1. Haga clic en un nombre de recurso para ver la pantalla principal del recurso y obtener más información. El número adyacente identifica cuántas instancias de ese recurso está gestionando el dispositivo. En este ejemplo, se han añadido tres receptáculos al dispositivo y uno se encuentra en un estado correcto.
2. Cuando se sitúa el puntero sobre un panel del panel de control, aparecen iconos adicionales como los que se muestran en el panel de **Enclosures** (Receptáculos).
   - El icono de quitar o eliminar (x) elimina el panel del panel de control.
   - El cursor de mover (✥) permite mover el panel a otra posición del panel de control.
   - Para los paneles personalizados, también aparece el icono de editar (✎), que permite editar un panel personalizado.
3. El gráfico de ejemplo para el recurso **Interconnects** (Interconexiones) muestra un total de siete interconexiones, cuatro de las cuales tienen un estado `Critical` (Crítico) y las otras tres un estado correcto.

   Haga clic en el icono de estado `Critical` (Crítico) para abrir la pantalla **Interconnects** (Interconexiones) y comenzar a investigar la causa.
4. En un gráfico de **estado**, un sector gris oscuro representa el número de recursos que no proporcionan información de estado debido a que el recurso está desactivado o a que su estado es desconocido.

   En el gráfico de ejemplo, el recurso **Server Hardware** (Hardware de servidor) muestra un total de 30 instancias de hardware de servidor, 14 de las cuales están desactivadas o son dispositivos desconocidos. Pase el puntero por el sector de color gris oscuro del gráfico para ver el número de instancias de hardware de servidor cuyo estado es `Disabled` (Desactivado) y `Unknown` (Desconocido).

5. El icono ✎ le permite personalizar el panel de control añadiendo paneles personalizados o predefinidos. Consulte «Personalización del panel de control» para obtener más información sobre el modo de personalizar paneles.
6. El gráfico **Ethernet Networks** (Redes Ethernet) ilustra un panel personalizado donde un usuario ha definido el número de redes Ethernet que tiene asignadas. Para ver más ejemplos, consulte «Personalización del panel de control».
7. El gráfico **Storage Pools** (Pools de almacenamiento) informa del estado de los pools de almacenamiento gestionados por el dispositivo, si los hay.

   Consulte «Acerca de los pools de almacenamiento» para obtener más información sobre los pools de almacenamiento.
8. En el área **Appliance alerts** (Alertas del dispositivo) se resumen las alertas importantes relacionadas con el dispositivo, que suelen deberse a problemas con las licencias y las copias de seguridad. Aquí no se incluyen las alertas relacionadas con los otros recursos.

   Si se detecta una alerta del dispositivo, el texto de la alerta aparece aquí. Cuando hay varias alertas, se muestra el número de alertas y se puede hacer clic en **Appliance** (Dispositivo) para ir directamente a la pantalla **Activity** (Actividad) para ver una vista filtrada de todas las alertas relacionadas con el dispositivo.

   Consulte «Acerca de la pantalla de actividad» para obtener más información sobre las alertas.

26.7.4 Personalización del panel de control

Puede personalizar el panel de control para mostrar los paneles que le interesen.

- Puede elegir entre un conjunto de paneles predefinidos, como por ejemplo, Unassigned Alerts (Alertas sin asignar) o Server Profiles (Perfiles de servidor).
- Puede crear o editar su propio panel personalizado seleccionando los datos que desea ver mediante el uso de las consultas del panel de control.
- Puede reorganizar o mover paneles en el panel de control para adaptarlo a sus necesidades.
- Puede quitar los paneles que no le interesen.

NOTA: Si desea borrar las personalizaciones del panel de control y restaurar el panel de control predeterminado, consulte la ayuda en línea para obtener información sobre cómo restablecer el panel de control.

26.8 Gestión del soporte remoto

26.8.1 Sobre el soporte remoto

Regístrese con Hewlett Packard Enterprise para permitir la creación automática de casos para fallos de hardware en los servidores y los receptáculos y para activar **Proactive Care**. Cuando se activa, todos los dispositivos aptos que se agreguen en el futuro se habilitarán automáticamente para el soporte remoto.

Los dispositivos que se pueden elegir son blades Gen8 y posteriores y receptáculos y servidores de bastidor.

NOTA: Los servidores deben estar al nivel de firmware 2.1 de iLO o superior para poderse habilitar para el soporte remoto

Hewlett Packard Enterprise se pondrá en contacto con usted para enviarle una pieza de recambio o enviarle a un ingeniero para los dispositivos en garantía o dentro de un contrato de soporte.

Remote support habilita los servicios de Proactive Care, incluidos los informes de Proactive Scan y Firmware/Software Analysis con recomendaciones basadas en los datos de configuración recopilados.

El soporte remoto es seguro. No se recopilan datos empresariales, solo datos de errores y de configuración específicos para el dispositivo. Todas las comunicaciones son únicamente salientes y utilizan el cifrado TLS estándar de la industria para garantizar la confidencialidad y la integridad de la información.

Más información

Documento de soporte remoto

26.8.2 Sobre los socios de canal

El ID de socio identifica en exclusiva un socio como HPE Authorized Partner. Hewlett Packard Enterprise es el socio de canal predeterminado si no se asigna ningún otro socio de canal.

Distribuidores autorizados de HPE

Al habilitar el soporte remoto, se permite que el distribuidor acceda a los informes de configuración y los informes de garantía del contrato en Insight Online en el HPE Support Center, así como a los detalles de la configuración y algunos detalles sobre el contrato y la garantía.

Socios de servicio autorizados de HPE

Además de la información facilitada más arriba a los distribuidores autorizados, el Service Partner (Socio de servicio) tiene acceso a los informes y estados del evento de servicio, con enlaces al portal HPE Channel Services Network.

26.8.3 Sobre la recopilación de datos

La recopilación básica envía información de configuración a Hewlett Packard Enterprise para servicios proactivos y de análisis de conformidad con sus contratos de servicio y garantía. Estos datos se transmiten cada 30 días.

Los receptáculos solo admiten la recopilación básica.

El estado Active (Activo) envía información sobre el estado, las configuraciones y la telemetría de tiempo de ejecución del servidor a Hewlett Packard Enterprise. Esta información se utiliza para la solución de problemas y para realizar análisis de calidad en circuito cerrado. Estos datos se transmiten cada 7 días.

27 Supervisión de la energía y la temperatura

HPE OneView permite supervisar la energía y la temperatura del entorno de hardware.

Información general sobre las funciones de supervisión de energía y temperatura

El dispositivo:

- Muestra una visualización en 3D de la temperatura del hardware con un código de colores (solamente en la interfaz de usuario)
- Recopila y muestra informes estadísticos sobre las mediciones de energía
- Recopila y muestra informes estadísticos sobre las mediciones de temperatura
- Muestra estadísticas de utilización con gráficos de utilización personalizables (solamente en la interfaz de usuario)

Funciones de supervisión de energía y temperatura por recurso

- **Centros de datos**
  - Visualización de las temperaturas de los bastidores y el hardware de servidor que contienen mediante un código de colores
- **Receptáculos hardware de servidor**
  - Alertas para condiciones de temperatura y energía degradadas y críticas
  - Análisis y alertas proactivas de los errores de configuración de energía
  - Gráficos de utilización para las estadísticas de energía y temperatura
- **Dispositivos de suministro de alimentación**
  - Alertas sobre los umbrales de potencia
  - Análisis y alertas proactivas de los errores de configuración de energía
  - Gráficos de utilización para las estadísticas de energía y temperatura
- **Bastidores**
  - Análisis y alertas proactivas de los errores de configuración de energía
  - Gráficos de utilización para las estadísticas de energía y temperatura

27.1 Supervisión de la energía y la temperatura por medio de la interfaz de usuario

La pantalla **Data Centers** (Centros de datos) proporciona una visualización en 3D del entorno de hardware y utiliza un sistema con un código de colores para mostrar los datos de temperatura del hardware.

El panel Utilization (Utilización) y los gráficos de utilización muestran las estadísticas de alimentación y temperatura a través de la vista **Utilization** (Utilización) de las pantallas **Enclosures** (Receptáculos), **Interconnects** (Interconexiones) (solo gráficos de utilización), **Power Delivery Devices (Dispositivos de suministro de alimentación)**, **Racks** (Bastidores), y **Server Hardware** (Hardware de servidor).

27.1.1 Supervisión de la temperatura del centro de datos

El recurso **Data Centers** (Centros de datos) proporciona una visualización de los bastidores del centro de datos y muestra su temperatura máxima mediante un sistema con un código de colores. Para activarla, primero debe especificar las posiciones físicas de los bastidores y la posición que ocupan los componentes en ellos utilizando el recurso **Data Centers** (Centros de datos).

Puede utilizar la visualización de temperaturas para identificar las áreas del centro de datos que tienen un exceso de refrigeración. Puede cerrar las baldosas de ventilación de las áreas que tienen temperaturas máximas más bajas para aumentar el flujo de aire a las áreas que tienen una refrigeración insuficiente. Si todo el centro de datos tiene un exceso de refrigeración, puede elevar la temperatura para ahorrar en costes de refrigeración.

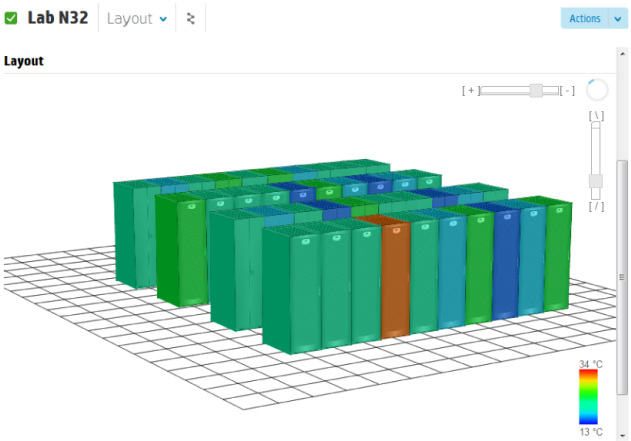
Requisitos previos

- Privilegios necesarios: administrador de servidores.
- Debe haber creado un centro de datos y colocado los bastidores en él.
- La colocación de los bastidores en el centro de datos debe representar con precisión su ubicación física.
- Debe haber especificado un límite térmico para el bastidor utilizando la pantalla **Racks** (Bastidores), si la directiva impone un límite (opcional).

Detalles de la recopilación y visualización de temperaturas

- La visualización muestra la temperatura máxima del bastidor mediante un sistema con un código de colores. El color de cada bastidor depende de la temperatura máxima más alta (en las últimas 24 horas) del dispositivo del bastidor para el que se haya registrado la temperatura máxima más alta (entre los dispositivos que son capaces de generar informes con el historial de temperatura ambiente).
- Las temperaturas se determinan utilizando los datos de utilización de temperatura recopilados de cada dispositivo.
- La recopilación de datos en segundo plano se produce al menos una vez al día, por lo que la temperatura máxima alcanzada en un bastidor se habrá producido dentro de las últimas 48 horas.
- Los bastidores para los que no se haya observado una temperatura máxima en las últimas 48 horas se representan sin codificación de color (en color gris).

Figura 21 Visualización del centro de datos en 3D



27.1.1.1 Manipulación de la vista de una visualización del centro de datos

Puede acercar o alejar la imagen y ajustar el ángulo de visión del centro de datos en las vistas **Overview** (Información general) o **Layout** (Diseño) de la pantalla **Data Centers** (Centros de datos).

Requisitos previos

- Privilegios necesarios: administrador de servidores.

NOTA: Los controles de vista del centro de datos no aparecerán en el panel **Layout** (Diseño) de la vista **Overview** (Información general) hasta que no pase el puntero por encima del panel.

Manipulación de la vista de una visualización del centro de datos

Para cambiar la vista del centro de datos, realice una o varias de las acciones siguientes:

- Mueva el control deslizante horizontal hacia la izquierda para acercar y hacia la derecha para alejar.
- Mueva el control deslizante vertical hacia arriba y hacia abajo para cambiar el ángulo de visión vertical.
- Haga clic en el dial de rotación y arrástrelo para cambiar el ángulo de visión horizontal.

27.1.2 Supervisión de la utilización de energía y temperatura

Las estadísticas de utilización de energía y temperatura se muestran en:

- El panel Utilization (Utilización)
- Los gráficos de utilización de la vista **Utilization** (Utilización)

27.1.2.1 Acerca del panel de utilización

Las pantallas **Enclosures** (Receptáculos), **Power Delivery Devices** (Dispositivos de suministro de alimentación), **Racks** (Bastidores), **Server Hardware** (Hardware de servidor) y **Storage Systems** (Sistemas de almacenamiento) muestran un panel **Utilization** (Utilización) en la pantalla **Overview** (Información general) de cada recurso.

El panel **Utilization** (Utilización) puede encontrarse en los estados siguientes:

Contenido del panel	Motivo
Los contadores de utilización muestran los datos de utilización.	El dispositivo ha recopilado datos y se están mostrando.
Se muestra un mensaje sobre las licencias.	El hardware de servidor que no tiene una licencia iLO Advanced no muestra los datos de utilización.
Se muestra `no data` (no hay datos).	El dispositivo no ha recopilado datos durante las últimas 24 horas.

Contenido del panel	Motivo
Se muestra `not set` (sin configurar) (un contador de color gris con signos de almohadilla).	Puede que el contador no esté configurado por las siguientes razones: • La página se está cargando y los datos todavía no están disponibles. • No hay datos de utilización anteriores al período de recopilación más reciente de 5 minutos. Puede que haya datos históricos en los gráficos de utilización. • Los receptáculos no muestran datos de temperatura si no hay ningún servidor encendido. • Los bastidores no mostrarán los datos si no hay ningún dispositivo montado en el bastidor y no está configurado el límite de temperatura.
Se muestra `not supported` (no compatible).	El equipo gestionado no es compatible con la recopilación de datos de utilización.

Para obtener más información, consulte la ayuda en línea sobre **Utilization** (Utilización).

27.1.2.2 Acerca de los gráficos y contadores de utilización

El dispositivo recopila y muestra datos sobre CPU, consumo de energía, temperatura y capacidad de ciertos recursos a través de los gráficos y contadores de utilización.

NOTA: El intervalo mínimo de recopilación de datos es de 5 minutos (por término medio) y el máximo es de una hora (por término medio).

Los gráficos de utilización pueden mostrar un intervalo de datos de hasta tres años como máximo.

Tabla 15 Estadísticas de utilización recopiladas por cada recurso

Recurso	Estadística de utilización				
	CPU	Alimentación	Temperatura	Personalizado	Capacidad
Receptáculos		✓	✓	✓	
Bastidores		✓	✓		
Dispositivos de suministro de alimentación		✓			
Hardware de servidor	✓	✓	✓	✓	
Sistemas de almacenamiento					✓

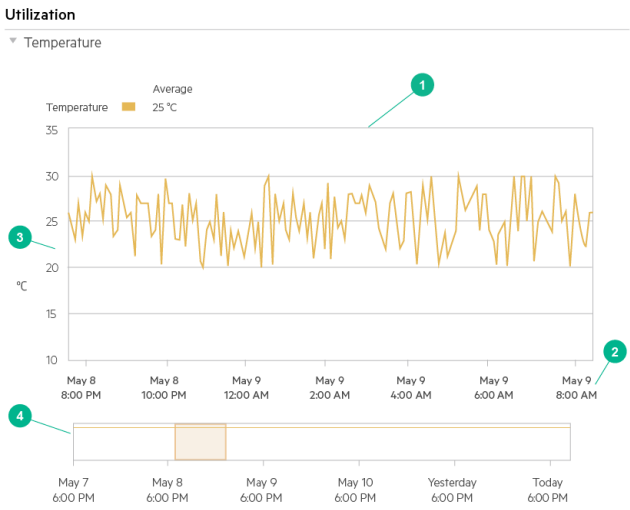
NOTA: Puede utilizar la pantalla **Interconnects** (Interconexiones) para visualizar gráficos de utilización que muestran las estadísticas de transferencia de datos para los puertos de interconexión. Consulte la ayuda en línea de la pantalla **Interconnects** (Interconexiones).

Estadísticas de utilización y las licencias

Las estadísticas y los gráficos de utilización están desactivados para el hardware de servidor que no tiene asignada una licencia de iLO. Consulte «Acerca de las licencias» para obtener más información.

Si la utilización está desactivada, el panel **Utilization** (Utilización) muestra un mensaje que indica la razón por la que está desactivada en el panel de detalles del recurso sin licencia.

Gráficos de utilización



1. **Gráfico principal**: el gráfico grande de utilización principal muestra los datos de las mediciones (eje vertical) de los dispositivos a lo largo de un intervalo de tiempo (eje horizontal) utilizando una línea para representar gráficamente los puntos de datos.
2. **Eje horizontal**: el eje horizontal del gráfico de utilización principal representa el intervalo de tiempo de los datos que se visualizan, con los datos más recientes del intervalo a la derecha. El intervalo de tiempo mínimo es de dos minutos y el máximo es de cinco días.
3. **Eje vertical**: el eje vertical del gráfico de utilización principal representa el intervalo para la estadística que se muestra en la unidad de medida correspondiente indicada en el lado izquierdo del gráfico. El intervalo de cada unidad de medida es fijo y no se puede cambiar. Los gráficos que muestran dos estadísticas con unidades de medida distintas tienen un segundo intervalo en el lado derecho del gráfico. El valor de la medición que se muestra en la parte superior del gráfico representa la capacidad máxima de utilización de una estadística determinada.
4. **Gráfico de navegación**: el gráfico de navegación situado debajo del gráfico principal muestra el intervalo de tiempo máximo de datos disponibles. Utilice el gráfico de navegación para seleccionar el intervalo de tiempo que desea mostrar en el gráfico principal, resaltando el intervalo con el dispositivo señalador.

Consulte la ayuda en línea para obtener más información sobre cómo crear un gráfico de utilización personalizado y cómo cambiar el nivel de detalle que se muestra en él.

27.2 Supervisión de energía y de temperatura mediante la API de REST

27.2.1 Actualización de la configuración de capacidad de potencia de los receptáculos

Para actualizar la configuración de capacidad del receptáculo, realice una operación `PUT` que solo incluya el atributo `calibratedMaxPower`. Para ver los atributos de configuración de capacidad del receptáculo, utilice una operación `GET`, edite el atributo `calibratedMaxPower` y, a continuación, realice una operación `PUT` que solo incluya el atributo `calibratedMaxPower` editado.

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de servidores

Actualización de la configuración de capacidad del receptáculo usando las API de REST

1. Seleccione el URI de un receptáculo.

   `GET /rest/enclosures`

2. Obtenga la capacidad del receptáculo utilizando el URI del paso 1.

   `GET {enclosure URI}/environmentalConfiguration`

3. Edite la capacidad del receptáculo. El único atributo que hay que enviar en el cuerpo de la respuesta es `calibratedMaxPower`. No envíe todos los atributos de la operación `GET`.
4. Actualice la capacidad del receptáculo.

   `PUT {enclosure URI}/environmentalConfiguration`

27.2.2 Actualización de la configuración de capacidad de potencia del hardware de servidor

Para actualizar la configuración de capacidad del hardware de servidor, realice una operación `PUT` que solo incluya el atributo `calibratedMaxPower`. Para ver los atributos de configuración de capacidad del hardware de servidor, utilice una operación `GET`, edite el atributo `calibratedMaxPower` y, a continuación, realice una operación `PUT` que solo incluya el atributo `calibratedMaxPower` editado.

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de servidores

Actualización de la configuración de capacidad del hardware de servidor usando las API de REST

1. Seleccione el URI de un hardware de servidor.

   `GET /rest/server-hardware`

2. Obtenga la capacidad del hardware de servidor actual utilizando el URI del paso 1.

   `GET {server hardware URI}/environmentalConfiguration`

3. Edite la capacidad del hardware de servidor. El único atributo que hay que enviar en el cuerpo de la respuesta es `calibratedMaxPower`. No envíe todos los atributos de la operación `GET`.
4. Actualice la capacidad del hardware de servidor.

   `PUT {server hardware URI}/environmentalConfiguration`

28 Uso de un bus de mensajes para enviar datos a los suscriptores

28.1 Acerca del acceso a los buses de mensajes de HPE OneView

HPE OneView admite la mensajería asíncrona para notificar a los suscriptores los cambios que se producen en los recursos gestionados —tanto lógicos como físicos– y los cambios en las estadísticas de los recursos gestionados. Por ejemplo, puede programar aplicaciones para recibir notificaciones cuando se añada hardware de servidor nuevo al entorno gestionado o cuando cambie el estado de los recursos físicos, y puede transmitir estadísticas de alimentación, temperatura y CPU para los recursos gestionados. Mediante las API de REST de HPE OneView, puede obtener certificados para acceder a los dos buses de mensajes que se describen en este capítulo: el bus State-Change Message Bus (SCMB) o el bus Metric Streaming Message Bus (MSMB).

El contenido del mensaje se envía con formato JSON (JavaScript Object Notation) e incluye el modelo de recursos.

Antes de configurar la suscripción a los mensajes, debe crear y descargar un certificado AMQP (Advanced Message Queuing Protocol) desde el dispositivo mediante las API de REST. A continuación, se conectará al bus de mensajes mediante el mecanismo de autenticación `EXTERNAL` especificando o no un nombre de usuario y una contraseña. Esto garantiza que utiliza la autenticación basada en certificados entre el bus de mensajes y el cliente. Después de conectarse al bus de mensajes, se configura una cola cuyo nombre está vacío, y AMQP genera un nombre exclusivo para la cola. Este nombre de cola se utiliza para enlazar el cliente con los conmutadores y recibir mensajes.

Para conectar con el mensaje y configurar una cola, debe utilizar un cliente que admita AMQP.

28.2 Uso del bus State-Change Message Bus (SCMB)

28.2.1 Conexión con el bus SCMB

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de infraestructuras

Para utilizar el bus SCMB, debe realizar las tareas siguientes:

- Utilice las API de REST para crear y descargar un certificado Advanced Message Queuing Protocol (AMQP) desde el dispositivo.
- Conéctese con el bus SCMB utilizando uno de estos dos métodos o ambos:
  - Utilice el mecanismo de autenticación “EXTERNAL”
  - Conéctese sin necesidad de enviar un nombre de usuario y contraseña

  El uso de uno de estos métodos garantiza que se emplea la autenticación basada en certificados.
- Configure una cola con un nombre de cola vacío.

  AMQP genera un nombre de cola exclusivo. Este nombre de cola se utiliza para enlazar con los conmutadores y recibir mensajes.

Creación y descarga del certificado de cliente, la clave privada y la certificado raíz de CA

1. Cree el certificado.

   `POST /rest/certificates/client/rabbitmq`

   Cuerpo de la solicitud: `{"type":"RabbitMqClientCertV2","commonName":"default"}`

2. Descargue el certificado y la clave privada.

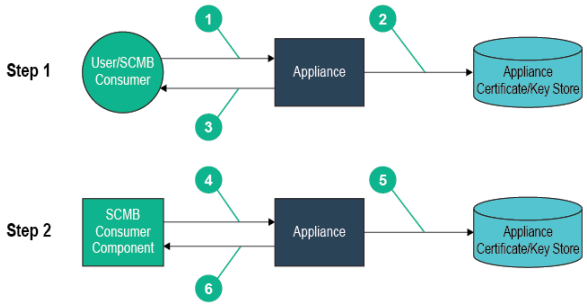
   `GET /rest/certificates/client/rabbitmq/keypair/default`

3. Descargue el certificado raíz de CA.

   `GET /rest/certificates/ca`

4. Después de conectar el cliente al SCMB, puede llevar a cabo la «Configuración de una cola para conectarse al conmutador SCMB de HPE OneView»

Figura 22 Conexión del cliente al bus SCMB



1. El consumidor SCMB solicita un certificado de cliente durante el proceso de registro.
2. El dispositivo gestiona los certificados de cliente en un archivo JVK (Java KeyStore).
3. El dispositivo emite un certificado de cliente para el consumidor SCMB.
4. El cliente SCMB proporciona un certificado de cliente SSL para crear una conexión con el dispositivo.
5. El dispositivo puede revocar el certificado del cliente SCMB para denegar el acceso al cliente SCMB. El cliente se gestiona en un archivo CRL (Lista de revocaciones de certificados).
6. El dispositivo autentica el cliente SCMB utilizando el certificado de cliente.

28.2.2 Configuración de una cola para conectarse al conmutador SCMB de HPE OneView

Los mensajes de cambio de estado se publican en el nombre del conmutador SCMB de HPE OneView. Para suscribirse a los mensajes, debe crear una cola o conectarse a una cola existente que reciba mensajes del conmutador SCMB basándose en una clave de enrutamiento.

Cuando se crea una cola, se define la clave de enrutamiento asociada a la cola para recibir determinados mensajes.

NOTA: La clave de enrutamiento distingue entre mayúsculas y minúsculas. El *`tipo-de-cambio`* requiere una letra inicial en mayúsculas. La *`categoría-del-recurso`* y el *`uri-del-recurso`* se indican en minúsculas.

Por ejemplo, si se establece el *`tipo-de-cambio`* de la clave de enrutamiento en `created` en lugar de `Created`, no recibirá ningún mensaje.

La sintaxis de la clave de enrutamiento es la siguiente:

`scmb.`*`categoría-del-recurso`*`.`*`tipo-de-cambio`*`.`*`uri-del-recurso`* donde:

`scmb`	Nombre del conmutador HPE OneView.
`categoría-del-recurso`	Es la categoría del recurso. Para obtener una lista completa de recursos, consulte el capítulo *HPE OneView REST API Reference* (Referencia de la API de REST de HPE OneView) de la ayuda en línea.
`tipo-de-cambio`	Es el tipo de cambio sobre el que se informa. Los valores válidos son `Created` (Creado), `Updated` (Actualizado) y `Deleted` (Eliminado).
`uri-del-recurso`	Es el URI del recurso específico asociado con el mensaje de cambio de estado.

NOTA: La sintaxis de la clave de enrutamiento para los recursos de tipo *task* es `scmb.`*`categoría-del-recurso`* y no utiliza *`tipo-de-cambio`* ni *`uri-del-recurso`*. Para recibir mensajes de todos los recursos de tipo *task*:

- `scmb.#`
- `scmb.tasks`

Colas de ejemplo

Suscripción	Ejemplo
Recibir todos los mensajes SCMB de los servidores físicos	`scmb.server-hardware.#` **NOTA:** Para que coincida todo a partir de un punto específico de la clave de enrutamiento, utilice el carácter almohadilla (`#`). En este ejemplo se utiliza `#` en lugar del *`uri-del-recurso`*. La cola de mensajes recibe todos los URI de los recursos de `server-hardware`.
Recibir todos los mensajes de las conexiones creadas	`scmb.connections.Created.#`
Recibir todos los mensajes del receptáculo cuyo URI es /rest/enclosures/Enc1234	`scmb.enclosures.*./rest/enclosures/Enc1234` **NOTA:** Para que coincida cualquier cosa con un campo específico de la clave de enrutamiento, utilice el asterisco (`*`). En este ejemplo se utiliza `*` en lugar del *`tipo-de-cambio`*. La cola de mensajes recibe todos los tipos de cambios: `Created`, `Updated` y `Deleted`.
Recibir todos los mensajes de creación (para todas las categorías y tipos de recursos)	`scmb.*.Created.#`

28.2.3 Estructura JSON del mensaje recibido desde el SCMB

En la tabla siguiente se muestran los atributos incluidos en la carga JSON de cada mensaje del bus SCMB. El modelo de recursos para el recurso de HPE OneView se incluye en el atributo `resource`. Para ver todos los modelos de recursos, consulte el capítulo *HPE OneView REST API Reference* (Referencia de la API de REST de HPE OneView) de la ayuda en línea.

Atributo	Tipo de dato	Descripción
`resourceUri`	Cadena	URI del recurso.
`changeType`	Cadena	El tipo de cambio de estado: `Created`, `Updated` o `Deleted`. Para obtener más información, consulte «Valores de ChangeType» (página 360).

Atributo	Tipo de dato	Descripción
`newState`	Cadena	El nuevo estado del recurso.
`eTag`	Cadena	La ETag del recurso cuando se produjo el cambio de estado.
`timestamp`	Cadena	La fecha y hora en que se envió el mensaje.
`newSubState`	Cadena	Si se requieren mensajes de subestado (para las máquinas de subestado asociadas con un estado primario), este es el subestado específico del recurso.
`resource`	Objeto	El modelo de recurso.
`associatedTask`	Cadena	Si no hay una tarea asociada a este mensaje, el valor es `null`.
`userInitiatedTask`	Cadena	El valor del atributo `userInitiated` incluido en el atributo `associatedTask`.
`changedAttributes`	Array	Lista de atributos de nivel superior que han cambiado debido a la llamada `POST` o `PUT` que provocó el envío del mensaje de cambio de estado.
`data`	Objeto	Información adicional sobre el cambio de estado del recurso.

Valores de ChangeType

Valor de `ChangeType`	Descripción
`Created`	El recurso se ha creado o agregado a HPE OneView.
`Updated`	Se han actualizado el estado, los atributos o ambos en el recurso.
`Deleted`	El recurso se ha eliminado definitivamente de HPE OneView.

Ejemplo 2 Ejemplo de JSON

```
{
    "resourceUri" : "/rest/enclosures/123xyz",
    "changeType" : "Created",
    "newState" : "Managed",
    "eTag" : "123456",
    "timestamp" : "2013-07-10T18:30:44Z",
    "newSubState" : "null",
    "resource" : {
        "category" : "enclosures",
        "created" : "2013-07-10T18:30:00Z",
        ...
    },
    "associatedTask" : "/rest/tasks/4321",
    "userInitiatedTask" : "true",
    "changedAttributes" : [],
    "data" : {},
}
```

28.2.4 Ejemplo de conexión y suscripción al bus SCMB utilizando .NET C#

Requisitos previos

Además de completar los requisitos previos, antes de utilizar los ejemplos de .NET C# debe completar los requisitos previos específicos del ejemplo.

Para utilizar los ejemplos de .NET C#, agregue lo siguiente al almacén de certificados de Windows:

- Certificado de raíz de la CA

- Certificado de cliente
- Clave privada

Para probar los ejemplos de .NET C#, haga lo siguiente:

1. Descargue el certificado raíz de la CA.

   ```
   GET /rest/certificates/ca
   ```

2. Guarde el contenido en el cuerpo de la respuesta en un archivo de texto denominado `rootCA.crt`. Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas.
3. Importe el archivo `rootCA.crt` en el almacén de certificados de Windows bajo `Entidades de certificación raíz de confianza`.
4. Descargue el certificado de cliente y la clave privada.

   ```
   GET /rest/certificates/client/rabbitmq/keypair/default
   ```

5. Guarde el contenido del certificado de cliente y la clave privada en el cuerpo de la respuesta en un archivo de texto denominado `scmb.crt`.

   Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----` para el certificado de cliente. A continuación, copie y pegue todo, desde `-----BEGIN RSA PRIVATE KEY-----` hasta `-----END RSA PRIVATE KEY-----` para la clave privada. Debe incluir los guiones, pero no incluya las comillas.

Ejemplo 3 Uso de .NET C# para hacer referencia directamente a un certificado de cliente

Convierta el certificado de cliente y la clave privada al formato PKCS para .Net.

```
openssl.exe pkcs12 -passout pass:default -export -in scmb.crt -out scmb.p12
```

Ejemplo

```
 public void Connect()
       {
           string exchangeName = "scmb";
           string hostName = "OneView.domain";
           string queueName = "";
           string routingKey = "scmb.#";


            ConnectionFactory factory = new ConnectionFactory();
          factory.AuthMechanisms = new RabbitMQ.Client.AuthMechanismFactory[] { new ExternalMechanismFactory()
};
            factory.HostName = hostname;
            factory.Port = 5671;
            factory.Ssl.CertPath = @".\scmb.p12";
            factory.Ssl.CertPassphrase = "default";
            factory.Ssl.ServerName = hostname;
            factory.Ssl.Enabled = true;


            IConnection connection = factory.CreateConnection();
            IModel model = connection.CreateModel();


            queueName = model.QueueDeclare(queueName, false, false, false, null);
            model.QueueBind(queueName, exchangeName, routingKey, null);


            using (Subscription sub = new Subscription(model, queueName))
            {
                foreach (BasicDeliverEventArgs ev in sub)
                {
                    DoSomethingWithMessage(ev);
                    sub.Ack();
                }
            }
       }
```

Ejemplo 4 Uso de .NET C# para importar el certificado en el almacén de certificados de Microsoft Windows

Importe el archivo `scmb.crt` en su almacén de certificados de Windows preferido.

Ejemplo

```
public void Connect()
        {
            string exchangeName = "scmb";
            string hostName = "OneView.domain";
            string queueName = "";
            string routingKey = "scmb.#";
            string userName = "rabbitmq_readonly";


            X509Store store = new X509Store(StoreName.Root, StoreLocation.LocalMachine);
            store.Open(OpenFlags.ReadWrite);


            X509Certificate cert = store.Certificates
                 .Find(X509FindType.FindBySubjectName, userName, false)
                 .OfType<X509Certificate>()
                 .First();


            ConnectionFactory factory = new ConnectionFactory();
           factory.AuthMechanisms = new RabbitMQ.Client.AuthMechanismFactory[] { new ExternalMechanismFactory()
 };
            factory.HostName = hostname;
            factory.Port = 5671;
            factory.Ssl.Certs = new X509CertificateCollection(new X509Certificate[] { cert });
            factory.Ssl.ServerName = hostname;
            factory.Ssl.Enabled = true;


            IConnection connection = factory.CreateConnection();
            IModel model = connection.CreateModel();


            queueName = model.QueueDeclare(queueName, false, false, false, null);
            model.QueueBind(queueName, exchangeName, routingKey, null);


            using (Subscription sub = new Subscription(model, queueName))
            {
                foreach (BasicDeliverEventArgs ev in sub)
                {
                    DoSomethingWithMessage(ev);
                    sub.Ack();
                }
            }
        }
```

NOTA: El ejemplo 2 de código .Net C# (almacén de certificados de Microsoft Windows) hace referencia al almacén `Entidades de certificación raíz de confianza`, situado debajo de `Equipo local`.

- `StoreName.Root` = `Entidades de certificación raíz de confianza`
- `StortLocation.LocalMachine` = `Equipo local`

28.2.5 Ejemplo de conexión y suscripción al bus SCMB utilizando Java

1. Descargue el certificado de cliente y la clave privada.

   `GET /rest/certificates/client/rabbitmq/keypair/default`

2. Guarde el contenido del certificado de cliente del cuerpo de la respuesta en un archivo de texto denominado `default-client.crt`.

   Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas.

3. Guarde el contenido de la clave privada del cuerpo de la respuesta en un archivo de texto denominado `default-client.key`.

   Debe copiar y pegar todo, desde `-----BEGIN RSA PRIVATE KEY-----` hasta `-----END RSA PRIVATE KEY-----`, incluyendo los guiones, pero sin incluir las comillas.

4. Cree un almacén de claves PKCS12 a partir de la clave privada y el certificado público.

```
openssl pkcs12 -export -name myclientcert -in default-client.crt -inkey default-client.key -out myclient.p12
```

5. Convierta el almacén de claves PKCS12 en un almacén de claves JKS.

```
keytool -importkeystore -destkeystore c:\\MyKeyStore -srckeystore myclient.p12 -srcstoretype pkcs12 -alias
 myclient
```

Ejemplo 5 Ejemplo de conexión y suscripción al bus SCMB utilizando Java

```
//c://MyKeyStore contains client certificate and private key. Load it into Java Keystore
final char[] keyPassphrase = "MyKeyStorePassword".toCharArray();
final KeyStore ks = KeyStore.getInstance("jks");
ks.load(new FileInputStream("c://MyKeyStore"), keyPassphrase);
final KeyManagerFactory kmf = KeyManagerFactory.getInstance("SunX509");
kmf.init(ks, keyPassphrase);

//c://MyTrustStore contains CA certificate. Load it into Java Trust Store
final char[] trustPassphrase = "MyTrustStorePassword".toCharArray();
final KeyStore ks = KeyStore.getInstance("jks");
tks.load(new FileInputStream("c:\\MyTrustStore"), trustPassphrase);
final TrustManagerFactory tmf = TrustManagerFactory.getInstance("SunX509");
tmf.init(tks);


//load SSLContext with keystore and truststore.
final SSLContext c = SSLContext.getInstance("SSL");
c.init(kmf.getKeyManagers(), tmf.getTrustManagers(), new SecureRandom());

final ConnectionFactory factory = new ConnectionFactory();
factory.setHost("192.168.2.144");

//Set Auth mechanism to "EXTERNAL" so that commonName of the client certificate is mapped to AMQP user name.
Hence, No need to set userId/Password here.
factory.setSaslConfig(DefaultSaslConfig.EXTERNAL);
factory.setPort(5671);
factory.useSslProtocol(c);

final Connection conn = factory.newConnection();
final Channel channel = conn.createChannel();


//do not specify queue name. AMQP will create a queue with random name starting with amq.gen* e.g.
amq.gen-32sfQz95QJ85K_lMBhU6HA
final DeclareOk queue = channel.queueDeclare("", true, false, true, null);

//Now get the queue name from above call and bind it to required Exchange with required routing key.
channel.queueBind(queue.getQueue(), "scmb", "scmb.#");

//Now you should be able to receive messages from queue
final GetResponse chResponse = channel.basicGet(queue.getQueue(), false);
if (chResponse == null)
{
    System.out.println("No message retrieved");
}
else
{
    final byte[] body = chResponse.getBody();
    System.out.println("Received: " + new String(body));
}

channel.close();
conn.close();
```

28.2.6 Ejemplos de conexión y suscripción al bus SCMB utilizando Python

Los ejemplos de código Python muestran cómo conectar y suscribirse al bus SCMB. Para obtener más información sobre Python (bibliotecas de cliente Pika AMQP y AMQP), consulte **http://pika.readthedocs.org/**, **http://www.python.org/** y **https://pypi.python.org/pypi/amqplib/**.

28.2.6.1 Instalación

1. Instale las bibliotecas pika y amqp.
   a. Descargue e instale setuptools (instalación setup.py de Python) de **https://pypi.python.org/pypi/setuptools#downloads**.
   b. Instale las herramientas pika.

      Al instalar las bibliotecas pika o amqp, ejecute el comando `python setup.py install` desde el directorio de descarga de pika o amqp.

2. Cree el certificado.

   `POST /rest/certificates/client/rabbitmq`

   Cuerpo de la solicitud:
   `{"type":"RabbitMqClientCertV2","commonName":"default"}`

3. Descargue el certificado de cliente y la clave privada.

   `GET /rest/certificates/client/rabbitmq/keypair/default`

4. Guarde el contenido del certificado de cliente del cuerpo de la respuesta en un archivo de texto denominado `client.pem`.

   Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas. Debe sustituir todas las instancias de `\n` por CR/LF (retorno de carro / salto de línea).

5. Guarde el contenido del certificado de cliente del cuerpo de la respuesta en un archivo de texto denominado `key.pem`.

   Debe copiar y pegar todo, desde `-----BEGIN RSA PRIVATE KEY-----` hasta `-----END RSA PRIVATE KEY-----`, incluyendo los guiones, pero sin incluir las comillas. Debe sustituir todas las instancias de `\n` por CR/LF (retorno de carro / salto de línea).

6. Descargue el certificado raíz de CA.

   `GET /rest/certificates/ca`

7. Guarde el contenido en el cuerpo de la respuesta en un archivo de texto denominado `carrot.crt`. Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas. Debe sustituir todas las instancias de `\n` por CR/LF (retorno de carro / salto de línea).

28.2.6.2 Pika

Ejemplo 6 Ejemplo de pika

Al llamar a la secuencia de comandos, debe pasar `-host:`*`{IP o nombre del host}`*. Consulte los ejemplos siguientes:

- `--host:192.168.1.1`
- `-host:mi-dispositivo.ejemplo.com`

IMPORTANTE: Si la conexión da error en el primer intento de ejecución de esta secuencia de comandos después de reiniciar un dispositivo, pruebe a volver a ejecutarla.

```
import pika, ssl
from optparse import OptionParser
from pika.credentials import ExternalCredentials
import json
import logging


logging.basicConfig()


############################################
# Callback function that handles messages
def callback(ch, method, properties, body):
    msg = json.loads(body)
    timestamp = msg['timestamp']
    resourceUri = msg['resourceUri']
    resource = msg['resource']
    changeType = msg['changeType']


    print
    print ("%s: Message received:" %(timestamp))
    print ("Routing Key: %s" %(method.routing_key))
    print ("Change Type: %s" %(changeType))
    print ("Resource URI: %s" %(resourceUri))
```

```
    print ("Resource: %s" %(resource))


#   Pem Files needed, be sure to replace the \n returned from the APIs with CR/LF
#   caroot.pem - the CA Root certificate   - GET /rest/certificates/ca
#   client.pem, first POST /rest/certificates/client/rabbitmq Request body:
{"type":"RabbitMqClientCert","commonName":"default"}
#   GET /rest/certificates/client/rabbitmq/keypair/default
#   client.pem is the key with  -----BEGIN CERTIFICATE-----
#   key.pem is the key with -----BEGIN RSA PRIVATE KEY-----
# Setup our ssl options
ssl_options = ({"ca_certs": "caroot.pem",
                "certfile": "client.pem",
                "keyfile": "key.pem",
                "cert_reqs": ssl.CERT_REQUIRED,
                "server_side": False})


parser = OptionParser()
parser.add_option('--host', dest='host',
        help='Pika server to connect to (default: %default)',
        default='localhost',
)


options, args = parser.parse_args()


# Connect to RabbitMQ
host = options.host
print ("Connecting to %s:5671, to change use --host hostName " %(host))
connection = pika.BlockingConnection(
               pika.ConnectionParameters(
                       host, 5671, credentials=ExternalCredentials(),
                       ssl=True, ssl_options=ssl_options))

# Create and bind to queue
EXCHANGE_NAME = "scmb"
ROUTING_KEY = "scmb.#"


channel = connection.channel()
result = channel.queue_declare()
queue_name = result.method.queue


channel.queue_bind(exchange=EXCHANGE_NAME, queue=queue_name, routing_key=ROUTING_KEY)


channel.basic_consume(callback,
                      queue=queue_name,
                      no_ack=True)


# Start listening for messages
channel.start_consuming()
```

28.2.6.3 AMQP

Ejemplo 7 Ejemplo de AMQP

Al llamar a la secuencia de comandos, debe pasar `–host:`*`{IP o nombre del host}`*. Consulte los ejemplos siguientes:

- `--host:192.168.1.1`
- `–host:mi-dispositivo.ejemplo.com`

IMPORTANTE: Si la conexión da error en el primer intento de ejecución de esta secuencia de comandos después de reiniciar un dispositivo, pruebe a volver a ejecutarla.

```
#!/usr/bin/env python


from optparse import OptionParser
from functools import partial


import amqplib.client_0_8 as amqp



def callback(channel, msg):
    for key, val in msg.properties.items():
```

```
        print ('%s: %s' % (key, str(val)))
    for key, val in msg.delivery_info.items():
        print ('> %s: %s' % (key, str(val)))


    print ('')
    print (msg.body)
    print ('-------')
    print msg.delivery_tag
    channel.basic_ack(msg.delivery_tag)


    #
    # Cancel this callback
    #
    if msg.body == 'quit':
        channel.basic_cancel(msg.consumer_tag)



def main():
    parser = OptionParser()
    parser.add_option('--host', dest='host',
        help='AMQP server to connect to (default: %default)',
        default='localhost',
    )


    options, args = parser.parse_args()
    host = options.host+":5671"
#   Pem Files needed, be sure to replace the \n returned from the APIs with CR/LF
#   caroot.pem - the CA Root certificate   - GET /rest/certificates/ca
#   client.pem, first POST /rest/certificates/client/rabbitmq Request body:
{"type":"RabbitMqClientCert","commonName":"default"}
#   GET /rest/certificates/client/rabbitmq/keypair/default
#   client.pem is the key with -----BEGIN CERTIFICATE-----
#   key.pem is the key with -----BEGIN RSA PRIVATE KEY-----


    ssl_options = ({"ca_certs": "caroot.pem",
                "certfile": "client.pem",
                "keyfile": "key.pem",
#                "cert_reqs": CERT_REQUIRED,
                "server_side": False})


    print ('Connecting to host %s, to change use --host hostName ' %host)


    conn = amqp.Connection(host, login_method='EXTERNAL',
                           ssl=ssl_options)


    print ('Successfully connected, creating and binding to queue')


    ch = conn.channel()


    qname, _, _ = ch.queue_declare()
    ch.queue_bind(qname, 'scmb', 'scmb.#')
    ch.basic_consume(qname, callback=partial(callback, ch))


    print ('Successfully bound to queue, waiting for messages')


    #pyamqp://


    #
    # Loop as long as the channel has callbacks registered
    #
    while ch.callbacks:
        ch.wait()


    ch.close()
    conn.close()


if __name__ == '__main__':
    main()
```

28.2.7 Recreación del certificado de cliente AMQP

Si cambia el nombre del dispositivo, debe volver a crear el certificado de cliente AMQP.

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de infraestructuras

Volver a crear y descargar el certificado de cliente, la clave privada y el certificado raíz de CA

1. Revoque el certificado.

   ```
   DELETE /rest/certificates/ca/rabbitmq_readonly
   ```

   No se requiere el cuerpo de la solicitud.

   NOTA: Cuando se revoca el certificado de cliente predeterminado, el dispositivo vuelve a generar el certificado de CA, el certificado de servidor AMQP y el certificado de cliente predeterminado.
2. Descargue el certificado y la clave privada.

   ```
   GET /rest/certificates/client/rabbitmq/keypair/default
   ```
3. Descargue el certificado raíz de CA.

   ```
   GET /rest/certificates/ca
   ```

28.3 Uso del bus Metric Streaming Message Bus (MSMB)

El bus Metric Streaming Message Bus (MSMB) es una interfaz que utiliza la mensajería asíncrona para notificar a los suscriptores las estadísticas más recientes de los recursos gestionados. Puede configurar el intervalo y las estadísticas que desea recibir mediante las API de REST.

28.3.1 Conexión con el bus MSMB

Requisitos previos

Para utilizar el bus MSMB, debe realizar las tareas siguientes:

- Utilice las API de REST para crear y descargar un certificado Advanced Message Queuing Protocol (AMQP) desde el dispositivo.
- Conéctese con el bus MSMB utilizando uno de estos dos métodos o ambos:
  - Utilice el mecanismo de autenticación “EXTERNAL”
  - Conéctese sin necesidad de enviar un nombre de usuario y contraseña

  El uso de uno de estos métodos garantiza que se emplea la autenticación basada en certificados.
- Configure una cola con un nombre de cola vacío.

  AMQP genera un nombre de cola exclusivo. Este nombre de cola se utiliza para enlazar con los conmutadores y recibir mensajes.

Creación y descarga del certificado de cliente AMQP

Creación y descarga del certificado de cliente, la clave privada y la certificado raíz de CA

1. Cree el certificado.

   `POST /rest/certificates/client/rabbitmq`

   Cuerpo de la solicitud: `{"type":"RabbitMqClientCertV2","commonName":"default"}`

2. Descargue el certificado y la clave privada.

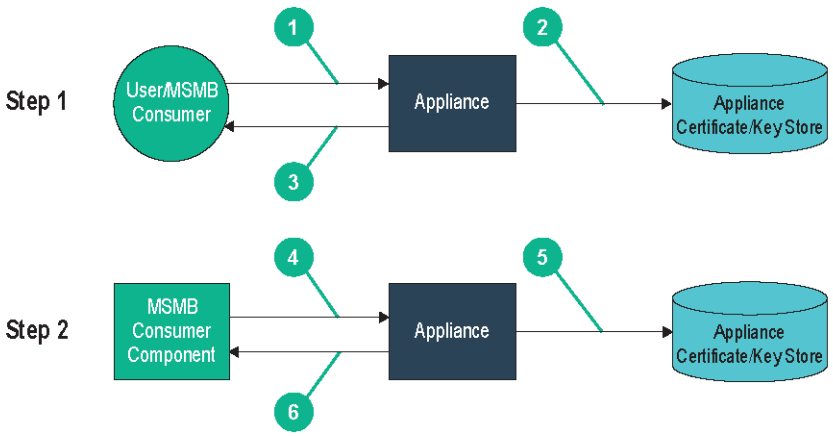
   `GET /rest/certificates/client/rabbitmq/keypair/default`

3. Descargue el certificado raíz de la CA.

   `GET /rest/certificates/ca`

4. Después de conectar el cliente al bus MSMB, puede «Configuración de una cola para conectarse al conmutador MSMB de HPE OneView».

Figura 23 Conexión del cliente al bus MSMB



1. El consumidor MSMB solicita un certificado de cliente durante el proceso de registro.
2. El dispositivo gestiona los certificados de cliente en un archivo JVK (Java KeyStore).
3. El dispositivo emite un certificado de cliente para el consumidor MSMB.
4. El cliente MSMB proporciona un certificado de cliente SSL para crear una conexión con el dispositivo.
5. El dispositivo puede revocar el certificado del cliente MSMB para denegar el acceso al cliente MSMB. El cliente se gestiona en un archivo CRL (Lista de revocaciones de certificados).
6. El dispositivo autentica el cliente MSMB utilizando el certificado de cliente.

28.3.2 Configuración de una cola para conectarse al conmutador MSMB de HPE OneView

Los mensajes de transmisión de estadísticas se publican en el nombre del conmutador MSMB de HPE OneView. Para suscribirse a los mensajes, debe crear una cola o conectarse a una cola existente que reciba mensajes del conmutador MSMB basándose en una clave de enrutamiento.

Cuando se crea una cola, se define la clave de enrutamiento asociada a la cola para recibir determinados mensajes.

Nombre del conmutador: `msmb`

Clave de enrutamiento: `msmb.#`

donde:

`msmb` es el nombre del conmutador de HPE OneView para la transmisión de estadísticas.

Colas de ejemplo

Suscripción	Ejemplo
Recibir todos los mensajes MSMB para los servidores físicos, receptáculos y dispositivos de alimentación	El conmutador es `msmb` La clave de enrutamiento es `msmb.#` Configure la retransmisión de las estadísticas mediante la API de configuración de transmisión de estadísticas.

28.3.3 Estructura JSON del mensaje recibido desde el MSMB

En la tabla siguiente se muestran los atributos incluidos en la carga JSON de cada mensaje del bus MSMB. El modelo de recursos para el recurso de HPE OneView se incluye en el atributo `resource`. Para ver todos los modelos de recursos, consulte el capítulo *HPE OneView REST API Reference* (Referencia de la API de REST de HPE OneView) de la ayuda en línea.

Atributo	Tipo de dato	Descripción
`resourceUri`	Cadena	URI del recurso.
`changeType`	Cadena	El tipo de cambio de estado: `Created`, `Updated` o `Deleted`.
`newState`	Cadena	El nuevo estado del recurso.
`eTag`	Cadena	La ETag del recurso cuando se produjo el cambio de estado.
`timestamp`	Cadena	La fecha y hora en que se envió el mensaje.
`newSubState`	Cadena	Si se requieren mensajes de subestado (para las máquinas de subestado asociadas con un estado primario), este es el subestado específico del recurso.
`resource`	MetricData	El modelo de recurso.
`associatedTask`	Cadena	Si no hay una tarea asociada a este mensaje, el valor es `null`.
`userInitiatedTask`	Cadena	El valor del atributo `userInitiated` incluido en el atributo `associatedTask`.
`changedAttributes`	Array	Lista de atributos de nivel superior que han cambiado debido a la llamada `POST` o `PUT` que provocó el envío del mensaje de cambio de estado.
`data`	Objeto	Información adicional sobre el cambio de estado del recurso.

MetricData

Atributo	Tipo de dato	Descripción
`startTime`	Cadena	La hora de inicio de la recopilación de la estadística.
`sampleIntervalInSeconds`	Integer	Intervalo entre muestras.
`numberOfSamples`	Integer	Número de muestras de la lista para cada tipo de estadística.
`resourceType`	Cadena	Identifica la categoría del recurso. Los dispositivos admitidos son server-hardware, enclosures y power-devices.
`resourceDataList`	Lista	Lista de ejemplo de estadísticas.
`uri`	Cadena	URI canónico del recurso.

Atributo	Tipo de dato	Descripción
`category`	Cadena	Identifica la categoría del recurso. Los dispositivos admitidos son server-hardware, enclosures y power-devices.
`created`	Timestamp	Fecha y hora de creación del recurso.
`modified`	Timestamp	Fecha y hora en que se modificó el recurso por última vez.
`eTag`	Cadena	Etiqueta de entidad/ID de versión del recurso, el mismo valor que se devuelve en el encabezado ETag al aplicar GET al recurso.
`type`	Cadena	Identifica el tipo de objeto JSON de forma exclusiva.

Ejemplo 8 Estructura del mensaje recibido desde el bus SCMB


```
{
    "eTag": null,
    "resourceUri": "/rest/enclosures/09SGH100X6J1",
    "changeType": "Updated",
    "newState": null,
    "newSubState": null,
    "associatedTask": null,
    "userInitiatedTask": false,
    "changedAttributes": null,
    "data": null,
    "resource": {
        "type": "MetricData",
        "resourceType": "enclosures",
        "resourceDataList": [
            {
                "metricSampleList": [
                    {
                        "valueArray": [
                            null
                        ],
                        "name": "RatedCapacity"
                    },
                    {
                        "valueArray": [
                            523
                        ],
                        "name": "AveragePower"
                    },
                    {
                        "valueArray": [
                            573
                        ],
                        "name": "PeakPower"
                    },
                    {
                        "valueArray": [
                            null
                        ],
                        "name": "PowerCap"
                    },
                    {
                        "valueArray": [
                            23
                        ],
                        "name": "AmbientTemperature"
                    },
                    {
                        "valueArray": [
                            null
                        ],
                        "name": "DeratedCapacity"
                    }
                ],
                "resourceId": "09SGH100X6J1"
            }
        ],
        "numberOfSamples": 1,
        "sampleIntervalInSeconds": 300,
        "startTime": "2014-09-17T08:43:36.294Z",
        "eTag": null,
        "modified": null,
        "created": null,
        "category": "enclosures",
```

```
        "uri": "/rest/enclosures/09SGH100X6J1"
    },
    "timestamp": "2014-09-17T08:48:36.819Z"
}
```

28.3.4 Ejemplo de conexión y suscripción al bus MSMB utilizando .NET C#

Requisitos previos

Además de completar los requisitos previos, antes de utilizar los ejemplos de .NET C# debe completar los requisitos previos específicos del ejemplo.

Para utilizar los ejemplos de .NET C#, agregue lo siguiente al almacén de certificados de Windows:

- Certificado de raíz de la CA
- Certificado de cliente
- Clave privada

Para probar los ejemplos de .NET C#, haga lo siguiente:

1. Descargue el certificado raíz de la CA.

   `GET /rest/certificates/ca`

2. Guarde el contenido en el cuerpo de la respuesta en un archivo de texto denominado `rootCA.crt`. Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas.
3. Importe el archivo `rootCA.crt` en el almacén de certificados de Windows bajo `Entidades de certificación raíz de confianza`.
4. Descargue el certificado de cliente y la clave privada.

   `GET /rest/certificates/client/rabbitmq/keypair/default`

5. Guarde el contenido del certificado de cliente y la clave privada del cuerpo de la respuesta en un archivo de texto denominado `msmb.crt`.

   Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----` para el certificado de cliente. A continuación, copie y pegue todo, desde `-----BEGIN RSA PRIVATE KEY-----` hasta `-----END RSA PRIVATE KEY-----` para la clave privada. Debe incluir los guiones, pero no incluya las comillas.

Ejemplo 9 Uso de .NET C# para hacer referencia directamente a un certificado de cliente

Convierta el certificado de cliente y la clave privada al formato PKCS para .Net.

```
openssl.exe pkcs12 -passout pass:default -export -in msmb.crt -out msmb.p12
```

Ejemplo

```
 public void Connect()
       {
           string exchangeName = "msmb";
           string hostName = "OneView.domain";
           string queueName = "";
           string routingKey = "msmb.#";


            ConnectionFactory factory = new ConnectionFactory();
          factory.AuthMechanisms = new RabbitMQ.Client.AuthMechanismFactory[] { new ExternalMechanismFactory()
};
            factory.HostName = hostname;
            factory.Port = 5671;
            factory.Ssl.CertPath = @".\msmb.p12";
            factory.Ssl.CertPassphrase = "default";
            factory.Ssl.ServerName = hostname;
            factory.Ssl.Enabled = true;


            IConnection connection = factory.CreateConnection();
            IModel model = connection.CreateModel();


            queueName = model.QueueDeclare(queueName, false, false, false, null);
            model.QueueBind(queueName, exchangeName, routingKey, null);


            using (Subscription sub = new Subscription(model, queueName))
            {
                foreach (BasicDeliverEventArgs ev in sub)
                {
                    DoSomethingWithMessage(ev);
                    sub.Ack();
                }
            }
       }
```

Ejemplo 10 Uso de .NET C# para importar el certificado en el almacén de certificados de Microsoft Windows

Importe el archivo `msmb.crt` en su almacén de certificados de Windows preferido.

Ejemplo

```
public void Connect()
        {
            string exchangeName = "msmb";
            string hostName = "OneView.domain";
            string queueName = "";
            string routingKey = "msmb.#";
            string userName = "rabbitmq_readonly";


            X509Store store = new X509Store(StoreName.Root, StoreLocation.LocalMachine);
            store.Open(OpenFlags.ReadWrite);


            X509Certificate cert = store.Certificates
                 .Find(X509FindType.FindBySubjectName, userName, false)
                 .OfType<X509Certificate>()
                 .First();


            ConnectionFactory factory = new ConnectionFactory();
           factory.AuthMechanisms = new RabbitMQ.Client.AuthMechanismFactory[] { new ExternalMechanismFactory()
 };
            factory.HostName = hostname;
            factory.Port = 5671;
            factory.Ssl.Certs = new X509CertificateCollection(new X509Certificate[] { cert });
            factory.Ssl.ServerName = hostname;
            factory.Ssl.Enabled = true;


            IConnection connection = factory.CreateConnection();
            IModel model = connection.CreateModel();


            queueName = model.QueueDeclare(queueName, false, false, false, null);
            model.QueueBind(queueName, exchangeName, routingKey, null);


            using (Subscription sub = new Subscription(model, queueName))
            {
                foreach (BasicDeliverEventArgs ev in sub)
                {
                    DoSomethingWithMessage(ev);
                    sub.Ack();
                }
            }
        }
```

NOTA: Cuando se usa .Net C# para importar el certificado en el almacén de certificados de Microsoft Windows se hace referencia al almacén `Entidades de certificación raíz de confianza`, situado en `Equipo local`.

- `StoreName.Root` = `Entidades de certificación raíz de confianza`
- `StortLocation.LocalMachine` = `Equipo local`

28.3.5 Ejemplo de conexión y suscripción al bus MSMB utilizando Java

1. Descargue el certificado de cliente y la clave privada.

   `GET /rest/certificates/client/rabbitmq/keypair/default`

2. Guarde el contenido del certificado de cliente del cuerpo de la respuesta en un archivo de texto denominado `default-client.crt`.

   Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas.

3. Guarde el contenido de la clave privada del cuerpo de la respuesta en un archivo de texto denominado `default-client.key`.

   Debe copiar y pegar todo, desde `-----BEGIN RSA PRIVATE KEY-----` hasta `-----END RSA PRIVATE KEY-----`, incluyendo los guiones, pero sin incluir las comillas.

4. Cree un almacén de claves PKCS12 a partir de la clave privada y el certificado público.

```
openssl pkcs12 -export -name myclientcert -in default-client.crt -inkey default-client.key -out myclient.p12
```

5. Convierta el almacén de claves PKCS12 en un almacén de claves JKS.

```
keytool -importkeystore -destkeystore c:\\MyKeyStore -srckeystore myclient.p12 -srcstoretype pkcs12 -alias
 myclient
```

Ejemplo 11 Ejemplo de conexión y suscripción al bus MSMB utilizando Java

```
//c://MyKeyStore contains client certificate and private key. Load it into Java Keystore
final char[] keyPassphrase = "MyKeyStorePassword".toCharArray();
final KeyStore ks = KeyStore.getInstance("jks");
ks.load(new FileInputStream("c://MyKeyStore"), keyPassphrase);
final KeyManagerFactory kmf = KeyManagerFactory.getInstance("SunX509");
kmf.init(ks, keyPassphrase);

//c://MyTrustStore contains CA certificate. Load it into Java Trust Store
final char[] trustPassphrase = "MyTrustStorePassword".toCharArray();
final KeyStore ks = KeyStore.getInstance("jks");
tks.load(new FileInputStream("c:\\MyTrustStore"), trustPassphrase);
final TrustManagerFactory tmf = TrustManagerFactory.getInstance("SunX509");
tmf.init(tks);


//load SSLContext with keystore and truststore.
final SSLContext c = SSLContext.getInstance("SSL");
c.init(kmf.getKeyManagers(), tmf.getTrustManagers(), new SecureRandom());

final ConnectionFactory factory = new ConnectionFactory();
factory.setHost("192.168.2.144");

//Set Auth mechanism to "EXTERNAL" so that commonName of the client certificate is mapped to AMQP user name.
Hence, No need to set userId/Password here.
factory.setSaslConfig(DefaultSaslConfig.EXTERNAL);
factory.setPort(5671);
factory.useSslProtocol(c);

final Connection conn = factory.newConnection();
final Channel channel = conn.createChannel();


//do not specify queue name. AMQP will create a queue with random name starting with amq.gen* e.g.
amq.gen-32sfQz95QJ85K_lMBhU6HA
final DeclareOk queue = channel.queueDeclare("", true, false, true, null);

//Now get the queue name from above call and bind it to required Exchange with required routing key.
channel.queueBind(queue.getQueue(), "msmb", "msmb.#");

//Now you should be able to receive messages from queue
final GetResponse chResponse = channel.basicGet(queue.getQueue(), false);
if (chResponse == null)
{
    System.out.println("No message retrieved");
}
else
{
    final byte[] body = chResponse.getBody();
    System.out.println("Received: " + new String(body));
}

channel.close();
conn.close();
```

28.3.6 Ejemplos de conexión y suscripción al bus MSMB utilizando Python

Los ejemplos de Python muestran cómo conectar y suscribirse al bus MSMB. Para obtener más información sobre Python (bibliotecas de cliente Pika AMQP y AMQP), consulte *Introduction to Pika* (Introducción a Pika) (**http://pika.readthedocs.org/**, **http://www.python.org/**) y *AMQP Client Library* (Biblioteca de cliente AMQP) (**https://pypi.python.org/pypi/amqplib/**).

28.3.6.1 Instalación

1. Instale las bibliotecas pika y amqp.
   a. Descargue e instale las herramientas de instalación (`Python setup.py install`) de **https://pypi.python.org/pypi/setuptools#downloads**.
   b. Instale las herramientas pika.

      Al instalar las bibliotecas pika o amqp, ejecute el comando `python setup.py install` desde el directorio de descarga de pika o amqp.

2. Cree el certificado.

   `POST /rest/certificates/client/rabbitmq`

   Cuerpo de la solicitud:
   `{"type":"RabbitMqClientCertV2","commonName":"default"}`

3. Descargue el certificado de cliente y la clave privada.

   `GET /rest/certificates/client/rabbitmq/keypair/default`

4. Guarde el contenido del certificado de cliente del cuerpo de la respuesta en un archivo de texto denominado `client.pem`.

   Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas. Debe sustituir todas las instancias de `\n` por CR/LF (retorno de carro / salto de línea).

5. Guarde el contenido del certificado de cliente del cuerpo de la respuesta en un archivo de texto denominado `key.pem`.

   Debe copiar y pegar todo, desde `-----BEGIN RSA PRIVATE KEY-----` hasta `-----END RSA PRIVATE KEY-----`, incluyendo los guiones, pero sin incluir las comillas. Debe sustituir todas las instancias de `\n` por CR/LF (retorno de carro / salto de línea).

6. Descargue el certificado raíz de la CA.

   `GET /rest/certificates/ca`

7. Guarde el contenido en el cuerpo de la respuesta en un archivo de texto denominado `carrot.crt`. Debe copiar y pegar todo, desde `-----BEGIN CERTIFICATE-----` hasta `-----END CERTIFICATE-----`, incluyendo los guiones, pero sin incluir las comillas. Debe sustituir todas las instancias de `\n` por CR/LF (retorno de carro / salto de línea).

28.3.6.2 Pika

Ejemplo 12 Ejemplo de pika

Al llamar a la secuencia de comandos, debe pasar `-host:`*`{IP o nombre del host}`*. Consulte los ejemplos siguientes:

- `--host:192.168.1.1`
- `-host:mi-dispositivo.ejemplo.com`

IMPORTANTE: Si la conexión da error en el primer intento de ejecución de esta secuencia de comandos después de reiniciar un dispositivo, pruebe a volver a ejecutarla.

```
import pika, ssl
from optparse import OptionParser
from pika.credentials import ExternalCredentials
import json
import logging


logging.basicConfig()


############################################
# Callback function that handles messages
def callback(ch, method, properties, body):
    msg = json.loads(body)
    timestamp = msg['timestamp']
    resourceUri = msg['resourceUri']
    resource = msg['resource']
    changeType = msg['changeType']


    print
    print ("%s: Message received:" %(timestamp))
    print ("Routing Key: %s" %(method.routing_key))
    print ("Change Type: %s" %(changeType))
    print ("Resource URI: %s" %(resourceUri))
```

```
    print ("Resource: %s" %(resource))


#   Pem Files needed, be sure to replace the \n returned from the APIs with CR/LF
#   caroot.pem - the CA Root certificate   - GET /rest/certificates/ca
#   client.pem, first POST /rest/certificates/client/rabbitmq Request body:
{"type":"RabbitMqClientCert","commonName":"default"}
#   GET /rest/certificates/client/rabbitmq/keypair/default
#   client.pem is the key with  -----BEGIN CERTIFICATE-----
#   key.pem is the key with -----BEGIN RSA PRIVATE KEY-----
# Setup our ssl options
ssl_options = ({"ca_certs": "caroot.pem",
                "certfile": "client.pem",
                "keyfile": "key.pem",
                "cert_reqs": ssl.CERT_REQUIRED,
                "server_side": False})


parser = OptionParser()
parser.add_option('--host', dest='host',
        help='Pika server to connect to (default: %default)',
        default='localhost',
)


options, args = parser.parse_args()


# Connect to RabbitMQ
host = options.host
print ("Connecting to %s:5671, to change use --host hostName " %(host))
connection = pika.BlockingConnection(
               pika.ConnectionParameters(
                       host, 5671, credentials=ExternalCredentials(),
                       ssl=True, ssl_options=ssl_options))

# Create and bind to queue
EXCHANGE_NAME = "msmb"
ROUTING_KEY = "msmb.#"


channel = connection.channel()
result = channel.queue_declare()
queue_name = result.method.queue


channel.queue_bind(exchange=EXCHANGE_NAME, queue=queue_name, routing_key=ROUTING_KEY)


channel.basic_consume(callback,
                      queue=queue_name,
                      no_ack=True)


# Start listening for messages
channel.start_consuming()
```

28.3.6.3 AMQP

Ejemplo 13 Ejemplo de AMQP

Al llamar a la secuencia de comandos, debe pasar `–host:`*`{IP o nombre del host}`*. Consulte los ejemplos siguientes:

- `--host:192.168.1.1`
- `–host:mi-dispositivo.ejemplo.com`

IMPORTANTE: Si la conexión da error en el primer intento de ejecución de esta secuencia de comandos después de reiniciar un dispositivo, pruebe a volver a ejecutarla.

```
#!/usr/bin/env python


from optparse import OptionParser
from functools import partial


import amqplib.client_0_8 as amqp



def callback(channel, msg):
    for key, val in msg.properties.items():
```

```
        print ('%s: %s' % (key, str(val)))
    for key, val in msg.delivery_info.items():
        print ('> %s: %s' % (key, str(val)))


    print ('')
    print (msg.body)
    print ('-------')
    print msg.delivery_tag
    channel.basic_ack(msg.delivery_tag)


    #
    # Cancel this callback
    #
    if msg.body == 'quit':
        channel.basic_cancel(msg.consumer_tag)



def main():
    parser = OptionParser()
    parser.add_option('--host', dest='host',
        help='AMQP server to connect to (default: %default)',
        default='localhost',
    )


    options, args = parser.parse_args()
    host = options.host+":5671"
#   Pem Files needed, be sure to replace the \n returned from the APIs with CR/LF
#   caroot.pem - the CA Root certificate   - GET /rest/certificates/ca
#   client.pem, first POST /rest/certificates/client/rabbitmq Request body:
{"type":"RabbitMqClientCert","commonName":"default"}
#   GET /rest/certificates/client/rabbitmq/keypair/default
#   client.pem is the key with -----BEGIN CERTIFICATE-----
#   key.pem is the key with -----BEGIN RSA PRIVATE KEY-----


    ssl_options = ({"ca_certs": "caroot.pem",
                "certfile": "client.pem",
                "keyfile": "key.pem",
#                "cert_reqs": CERT_REQUIRED,
                "server_side": False})


    print ('Connecting to host %s, to change use --host hostName ' %host)


    conn = amqp.Connection(host, login_method='EXTERNAL',
                           ssl=ssl_options)


    print ('Successfully connected, creating and binding to queue')


    ch = conn.channel()


    qname, _, _ = ch.queue_declare()
    ch.queue_bind(qname, 'msmb', 'msmb.#')
    ch.basic_consume(qname, callback=partial(callback, ch))


    print ('Successfully bound to queue, waiting for messages')


    #pyamqp://


    #
    # Loop as long as the channel has callbacks registered
    #
    while ch.callbacks:
        ch.wait()


    ch.close()
    conn.close()


if __name__ == '__main__':
    main()
```

28.3.7 Recreación del certificado de cliente AMQP

Si cambia el nombre del dispositivo, debe volver a crear el certificado de cliente AMQP.

NOTA: Si ya se han creado los certificados, puede omitir este paso.

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de infraestructuras

Volver a crear y descargar el certificado de cliente, la clave privada y el certificado raíz de CA

1. Revoque el certificado.

   ```
   DELETE /rest/certificates/ca/rabbitmq_readonly
   ```

   No se requiere el cuerpo de la solicitud.

   NOTA: Cuando se revoca el certificado de cliente predeterminado, el dispositivo vuelve a generar el certificado de CA, el certificado de servidor AMQP y el certificado de cliente predeterminado.
2. Descargue el certificado y la clave privada.

   ```
   GET /rest/certificates/client/rabbitmq/keypair/default
   ```
3. Descargue el certificado raíz de la CA.

   ```
   GET /rest/certificates/ca
   ```

29 Generación de informes

HPE OneView ofrece informes predefinidos para ayudarle a gestionar el dispositivo y su entorno. Puede ver los informes en la interfaz de usuario o generarlos mediante la API de REST. También puede guardar los informes como un libro de Microsoft Excel (*.xlsx) o CSV MS-DOS (*.csv).

Pantallas de la interfaz de usuario y recursos de la API de REST

Pantalla de la interfaz de usuario	Recurso de la API de REST
Reports (Informes)	`reports`

29.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras (para el informe local de los usuarios)

29.2 Tareas para los informes

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar la interfaz de usuario o las API de REST para:

- Ver un informe.
- Guardar un informe.

30 Uso de los servicios de datos

Usando las API de REST, puede recopilar estadísticas de los equipos gestionados por HPE OneView y guardar esos datos fuera del dispositivo HPE OneView para verlos en otras herramientas de software. Esto le proporciona la flexibilidad de analizar los datos más a fondo y de formas significativas.

30.1 Acerca de los servicios de datos

Los servicios de datos permiten disponer de los datos para el análisis y la solución de problemas fuera de línea. Para obtener información sobre los tipos de datos compatibles, consulte las secciones siguientes sobre transmisión de estadísticas y reenvío de registros.

30.1.1 Acerca de la transmisión de estadísticas

Las API de REST de HPE OneView permiten configurar la retransmisión por MSMB de estadísticas de rendimiento de receptáculos, hardware de servidor y dispositivos de alimentación. A continuación se incluye la lista de estadísticas admitidas.

- Receptáculos:
  - Potencia nominal: el límite de consumo de energía máximo del receptáculo, en vatios.
  - Potencia reducida: el límite de consumo de energía medio del receptáculo, en vatios.
  - Temperatura ambiente: la temperatura del receptáculo en el período de tiempo, en grados Celsius o Fahrenheit.
  - Potencia media: el consumo de energía medio del dispositivo en el período de tiempo, en vatios.
  - Límite de alimentación: el límite de alimentación configurado para el receptáculo, en vatios.
  - Potencia máxima: el consumo de energía máximo del receptáculo en el período de tiempo, en vatios.
- Dispositivos de alimentación:
  - Potencia media: el consumo de energía medio del dispositivo en el período de tiempo, en vatios.
  - Potencia máxima: el consumo de energía máximo del dispositivo en el período de tiempo, en vatios.
- Hardware de servidor:
  - Utilización de CPU: el porcentaje de CPU utilizado por el dispositivo en el período de tiempo.
  - Frecuencia media de CPU: la velocidad de la CPU del dispositivo en el período de tiempo, en GHz.
  - Temperatura ambiente: la temperatura del receptáculo en el período de tiempo, en grados Celsius o Fahrenheit.
  - Potencia media: el consumo de energía medio del dispositivo en el período de tiempo, en vatios.
  - Límite de alimentación: el límite de alimentación definido por el usuario, configurado para el hardware de servidor.

- Potencia máxima: el consumo de energía máximo del dispositivo en el período de tiempo, en vatios.

30.1.2 Acerca del reenvío de entradas de registro a un servidor de registro del sistema remoto

Las API de REST pueden utilizarse para configurar el destino de registro del sistema remoto. Una vez configurado, los registros se transmiten directamente desde el dispositivo con `rsyslog`.

30.2 API de REST para habilitar la transmisión de estadísticas

Las estadísticas de los recursos gestionados pueden transmitirse con un intervalo especificado.

- `/rest/metrics/capability`
- `/rest/metrics/configuration`

Tabla 16 Frecuencia recomendada de retransmisión de estadísticas para un número máximo de dispositivos por tipo de dispositivo

Tipo de dispositivo	Dispos. máx.	Frecuencia (seg.)	Dispos. máx.	Frecuencia (seg.)	Dispos. máx.	Frecuencia (seg.)	Dispos. máx.	Frecuencia (seg.)	Dispos. máx.	Frecuencia (seg.)
Receptáculo	5	300	5	300	10	600	20	900	40	1800
Dispositivos de alimentación	10	300	10	300	20	900	40	1800	80	3600
Hardware de servidor	40	300	80	600	160	900	320	1800	640	3600

Por ejemplo, la configuración recomendada para 640 servidores, 80 dispositivos de alimentación y 40 receptáculos es la siguiente:

```
{
"sourceTypeList": [
{
"frequencyOfRelayInSeconds": 3600,
"sampleIntervalInSeconds": 300,
"sourceType": "/rest/server-hardware"
},
{
"frequencyOfRelayInSeconds": 3600,
"sampleIntervalInSeconds": 300,
"sourceType": "/rest/power-devices"
},
{
"frequencyOfRelayInSeconds": 1800,
"sampleIntervalInSeconds": 300,
"sourceType": "/rest/enclosures"
}
]
}
```

30.2.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras

30.2.2 Tareas para la API de REST de estadísticas

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar las API de REST para:

- Obtener la capacidad de transmisión de estadísticas
- Obtener la configuración de transmisión de estadísticas
- Actualizar la configuración de transmisión de estadísticas

NOTA: Cuando se configuran, las estadísticas solo se transmiten para los servidores con la licencia HPE OneView Advanced.

30.3 API de REST para usar registros de un sistema remoto

La API de REST remoteSyslog le permite implementar un servidor de registro del sistema remoto para recibir y conservar datos de registro del sistema remotos y para configurar la retransmisión de datos.

Esta API de REST le permite configurar un servidor y un puerto de destino de registro del sistema remoto. Una vez configurados, todos los servidores con la licencia HPE OneView Advanced y los receptáculos reenviarán los registros a este servidor de registro del sistema remoto.

- `/rest/logs/remoteSyslog`

30.3.1 Roles

- Privilegios mínimos necesarios: administrador de infraestructuras

30.3.2 Tareas para la API de REST remoteSyslog

La ayuda en línea del dispositivo proporciona información sobre el modo de utilizar las API de REST para:

- Obtener la configuración de remoteSyslog
- Actualizar la configuración de remoteSyslog

Parte VI Solución de problemas

En los capítulos de esta parte se incluye información que puede utilizar para solucionar problemas en el centro de datos, así como información acerca de cómo restaurar el dispositivo partiendo de un archivo de copia de seguridad en caso de un fallo catastrófico.

31 Solución de problemas

HPE OneView tiene diversas herramientas de solución de problemas que puede utilizar para resolver los que se le presenten. Siguiendo un método combinado de análisis de las pantallas y los registros, puede obtener un historial de la actividad y de los errores que se produjeron durante el proceso. Para obtener instrucciones específicas de solución de problemas, seleccione un tema de la lista siguiente.

Categoría

- Actividad
- Dispositivo
- Configuración de red del dispositivo
- Receptáculos y grupos de receptáculos
- Lotes de firmware
- Interconexiones
- Licencias
- Interconexiones lógicas
- Logical switches (Conmutadores lógicos)
- Redes
- Hardware de servidor
- Perfiles de servidor
- Storage (Almacenamiento)
- Cuentas de usuario y grupos

Más información

- «Técnicas básicas de solución de problemas»
- «Creación de un archivo de volcado de soporte»
- «Creación de un volcado de soporte para el soporte técnico autorizado utilizando las secuencias de comandos de la API de REST»
- «Uso de la consola del dispositivo virtual»
- «Solución de problemas de configuraciones regionales»

31.1 Técnicas básicas de solución de problemas

HPE OneView tiene diversas herramientas de solución de problemas que puede utilizar para resolver los que se le presenten. Siguiendo un método combinado de análisis de las pantallas y los registros, puede obtener un historial de la actividad y de los errores generados.

- La pantalla Activity (Actividad) muestra un registro de todos los cambios realizados en el dispositivo, tanto los iniciados por el usuario como por el dispositivo. Es similar a un registro de auditoría, pero proporciona más detalles y resulta sencillo acceder a ella desde la interfaz de usuario.

  La pantalla **Activity** (Actividad) también proporciona un registro de alertas y notificaciones de estado.

- Descargue un registro de auditoría para ayudar a un administrador a comprender qué acciones relativas a la seguridad se llevaron a cabo en el sistema.
- Cree un archivo de volcado de soporte para recopilar los registros y demás información necesaria para la depuración en un archivo comprimido y cifrado que puede enviar a su representante autorizado de soporte técnico para que lo analice.
- Examine los informes para conocer el estado de las interconexiones, los servidores y los receptáculos. Los informes también pueden proporcionar información de inventario y ayudarle a ver los tipos de modelos de servidor y procesadores existentes en su centro de datos. También pueden mostrarle el firmware que necesita actualizarse.

NOTA: Si la interfaz de usuario no está disponible, puede utilizar la consola de mantenimiento para la solución de problemas.

Recomendación	Detalles
Busque un mensaje	**Acerca de los errores de sintaxis:** • La interfaz de usuario comprueba la sintaxis cuando se introduce un valor. Si comete un error de sintaxis, aparece un mensaje con instrucciones junto a la entrada. La interfaz de usuario o la línea de comandos continúa mostrando mensajes hasta que introduzca el valor correcto. **Acerca de los errores de configuración de red:** • Antes de aplicarlos, el dispositivo comprueba los parámetros clave de la red, como la dirección IP y el nombre de dominio completo (FQDN), para asegurarse de que tengan el formato adecuado. • Después de aplicar la configuración de red, el dispositivo realiza pruebas de validación adicionales, tales como comprobaciones de accesibilidad y consultas de la IP del nombre de host. Si un parámetro no es correcto, el dispositivo genera una alerta que describe los errores de validación de la tarjeta de interfaz de red (NIC) y la conexión entre el explorador y el dispositivo puede perderse. **Acerca de los errores graves:** • Compruebe la conectividad con el receptáculo desde el dispositivo. • Cree un volcado de soporte y póngase en contacto con su representante autorizado de soporte técnico.
Examine la pantalla Activity (Actividad)	**Para buscar un mensaje correspondiente a una actividad:** **NOTA:** Puede que tenga que realizar estos pasos desde la consola virtual. 1. Localice las actividades recientes cuyo estado sea **Critical** (Crítico) o **Warning** (Advertencia). 2. Expanda la actividad para ver recomendaciones sobre cómo resolver el error. 3. Siga las instrucciones.
Compruebe la máquina virtual del dispositivo	**Cuando el host de VM está fuera de servicio o no responde:** 1. Desde el equipo local, utilice el comando `ping` para determinar si tiene acceso al dispositivo. • Si el comando `ping` funciona correctamente, determine si la configuración del explorador, especialmente el servidor proxy, es correcta. Considere la posibilidad de omitir el servidor proxy. • Si el comando `ping` no alcanza el dispositivo, asegúrese de que el dispositivo esté conectado a la red. 2. Inicie sesión en el hipervisor para comprobar que el hipervisor se está ejecutando. 3. Compruebe que el invitado virtual para el dispositivo está operativo. 4. Asegúrese de que la configuración del host de VM es válida. Compruebe la exactitud de la dirección IP y otros parámetros de red del host de VM. 5. Examine los datos de rendimiento del hipervisor. Si el dispositivo está funcionando al 100 % de utilización, reinicie el hipervisor.

31.2 Acerca del archivo de volcado de soporte

En algunos mensajes de error se recomienda crear un volcado de soporte del dispositivo y enviarlo a un representante autorizado de soporte técnico para realizar un análisis. El proceso de volcado de soporte realiza las siguientes funciones:

- Elimina el archivo de volcado de soporte existente
- Recopila los registros y otra información necesaria para la depuración

- Crea un archivo comprimido con un nombre con el siguiente formato:

  nombre de host-identificador—marca de tiempo.sdmp

  Donde, para los archivos de volcado de soporte creados desde la interfaz de usuario, *identificador* es CI (que indica un volcado de soporte del dispositivo), o bien LE (que indica un volcado de soporte de un receptáculo lógico).

A menos que especifique lo contrario, todos los datos del archivo de volcado de soporte se cifran de modo que solo pueda tener acceso a ellos un representante autorizado de soporte técnico.

Puede optar por no cifrar el archivo de volcado de soporte si usted es un administrador de infraestructuras. Esto puede ser útil si tiene un representante autorizado de soporte técnico in situ o si en su entorno están prohibidas las conexiones externas. También puede validar el contenido del archivo de volcado de soporte y comprobar que no contiene datos que se consideran confidenciales en su entorno.

IMPORTANTE: Si el dispositivo está en un estado de error, aparecerá una pantalla especial Oops (¡Vaya!). Cualquier persona puede crear un archivo de volcado de soporte cifrado desde dicha pantalla sin necesidad de iniciar sesión ni de ninguna otra autenticación.

El archivo de volcado de soporte contiene lo siguiente:

- Registros del sistema operativo
- Registros del producto
- Los resultados de algunos comandos relacionados con el producto y el sistema operativo

Los elementos del archivo de volcado de soporte se registran según la Hora UTC.

Acerca los volcados de soporte de receptáculos lógicos

Puede crear un volcado de soporte de receptáculo lógico, que, de manera predeterminada, incluye el volcado de soporte del dispositivo. El archivo de volcado de soporte de receptáculo lógico incluye contenido de cada una de sus interconexiones lógicas. Una vez creado el archivo de volcado de soporte de receptáculo lógico, se incorpora al archivo de volcado de soporte del dispositivo, y el lote completo de archivos se comprime en un archivo zip y, opcionalmente, se cifra para su descarga.

NOTA: Para crear un volcado de soporte de receptáculo lógico que no contenga el volcado de soporte del dispositivo, deberá utilizar las API REST de receptáculo lógico. Para obtener más información, consulte la ayuda en línea sobre secuencias de comandos de la API de REST relacionada con los receptáculos lógicos.

Consulte también

- «Creación de un archivo de volcado de soporte»

31.3 Creación de un archivo de volcado de soporte

Utilice este procedimiento para crear un archivo de volcado de soporte solo para el dispositivo o para el receptáculo lógico y el dispositivo.

Requisitos previos

- Privilegios mínimos necesarios: administrador de red, administrador de servidores, administrador de infraestructuras, administrador de copia de seguridad, solo lectura

  NOTA: Solo el administrador de infraestructuras tiene la opción de no cifrar un archivo de volcado de soporte. Cuando un usuario con otro rol crea un archivo de volcado de soporte, se cifra automáticamente.

Cómo crear un archivo de volcado de soporte

1. Para obtener un archivo de volcado de soporte del dispositivo, realice una de las acciones siguientes:
   - En el menú principal, haga clic en **Settings** (Configuración) y, a continuación, en el panel **Appliance** (Dispositivo), haga clic en **Create support dump** (Crear volcado de soporte).
   - En el menú principal, haga clic en **Settings** (Configuración), haga clic en **Appliance** (Dispositivo) y, a continuación, seleccione **Actions→Create support dump** (Acciones > Crear volcado de soporte).
2. Si usted es administrador de infraestructuras, elija si desea cifrar el archivo de volcado de soporte o no:
   a. Para cifrar el archivo de volcado de soporte, confirme que está activada la casilla de verificación **Enable support dump encryption** (Habilitar cifrado de volcado de soporte).
   b. Para desactivar el cifrado, desactive la casilla de verificación **Enable support dump encryption** (Habilitar cifrado de volcado de soporte).
3. Haga clic en **Yes, create** (Sí, crear).

   Puede seguir realizando otras tareas mientras se crea el archivo de volcado de soporte.
4. El archivo de volcado de soporte se descarga cuando finaliza esta tarea. Si en la configuración del explorador se encuentra especificada una carpeta de descarga predeterminada, esa será la ubicación donde se colocará el archivo de volcado de soporte. De lo contrario, se le pedirá que indique dónde desea descargar el archivo.
5. Compruebe que el archivo de volcado de soporte se ha guardado en la carpeta correcta.
6. Póngase en contacto con un representante autorizado de soporte técnico para obtener instrucciones sobre cómo transferir el archivo de volcado de soporte a Hewlett Packard Enterprise.

   Para obtener información sobre cómo ponerse en contacto con Hewlett Packard Enterprise por teléfono, consulte «Acceso al soporte de Hewlett Packard Enterprise» (página 461).

IMPORTANTE: A menos que especifique lo contrario, el archivo de volcado de soporte se cifra de modo que solo el representante autorizado de soporte técnico pueda ver su contenido.

La política de retención de datos de Hewlett Packard Enterprise requiere que todos los archivos de volcado de soporte se eliminen después de usarlos.

Consulte también

- «Acerca del archivo de volcado de soporte»
- Solución de problemas: No se puede crear un archivo de volcado de soporte

31.4 Creación de un volcado de soporte para el soporte técnico autorizado utilizando las secuencias de comandos de la API de REST

En algunos mensajes de error se recomienda la creación de un volcado de soporte del dispositivo para enviarlo a un representante autorizado de soporte técnico para realizar un análisis. El proceso de volcado de soporte:

- Elimina el archivo de volcado de soporte existente
- Recopila los registros y otra información necesaria para la depuración
- Crea un archivo comprimido

A menos que especifique lo contrario, todos los datos del archivo de volcado de soporte se cifran de modo que solamente pueda tener acceso a ellos un representante autorizado de soporte

técnico. Puede optar por no cifrar el archivo de volcado de soporte si tiene un representante autorizado de soporte técnico in situ o si en su entorno están prohibidas las conexiones externas. También puede validar el contenido del archivo de volcado de soporte y comprobar que no contiene datos confidenciales, como contraseñas.

IMPORTANTE: Si el dispositivo está en un estado de error, también puede crear un archivo de volcado de soporte cifrado sin necesidad de iniciar sesión ni de autenticarse.

El archivo de volcado de soporte contiene lo siguiente:

- Registros del sistema operativo (de `/var/log`)
- Registros del producto (de `/ci/logs`)
- Los resultados de algunos comandos relacionados con el producto y el sistema operativo

Los elementos se registran en el archivo de volcado de soporte en UTC (Tiempo Universal Coordinado).

Requisitos previos

- Privilegios de ID de sesión mínimos necesarios: administrador de infraestructuras

Creación de un volcado de soporte utilizando las API de REST

1. Cree un volcado de soporte.

   ```
   POST /rest/appliance/support-dumps
   ```

2. Utilice el valor del elemento `uri` del cuerpo de la respuesta de la operación POST del paso 1 para descargar el volcado de soporte.

   ```
   GET /rest/appliance/support-dumps/{file name}
   ```

IMPORTANTE: A menos que especifique lo contrario, el archivo de volcado de soporte se cifra de modo que únicamente el personal de soporte autorizado pueda ver su contenido.

Según la política de retención de datos de Hewlett Packard Enterprise, los archivos de volcado de soporte que se envían a Hewlett Packard Enterprise se eliminan después de usarlos.

31.5 Solución de problemas de actividad

Utilice la siguiente información para solucionar alertas que se muestren en la pantalla **Activity** (Actividad).

31.5.1 No se generan alertas.

Síntoma

Causa

El dispositivo está fuera de las especificaciones de cumplimiento.

El hardware de servidor supera la cantidad de licencias permitidas.

Action (Acción)

1. Aplique una licencia para el hardware de servidor.
2. Aplique las licencias al hardware de servidor que carece de licencia.

31.5.2 La alerta está bloqueada.

Síntoma

Una alerta está bloqueada y no puede desactivarse.

Causa

Un recurso ha creado la alerta bloqueada.

Action (Acción)

1. Expanda la alerta y siga la acción recomendada descrita en **Resolution** (Resolución).
2. Si necesita más información, expanda **Event details (Información de eventos)** y vea la información para **correctiveAction**.
3. Cuando los recursos detectan un cambio, modifican automáticamente el estado de la alerta a `Cleared` (Borrada).

31.5.3 Las alertas no aparecen en la interfaz de usuario.

Síntoma

No se puede acceder a la pantalla Alerts (Alertas) o las alertas no se publican aquí.

Causa

Permiso no apropiado

Action (Acción)

1. Si es posible, inicie sesión como usuario con privilegios. De lo contrario, solicite que el administrador de infraestructuras cambie su rol para poder ver las alertas para el tipo de recurso físico.
2. Vuelva a iniciar sesión.
3. Consulte la pantalla **Activity** (Actividad).

31.5.4 El estado de la alerta se devuelve como en blanco o inesperado

Síntoma

El estado de la alerta es diferente a:

- Critical (Crítico)
- Warning (Advertencia)
- OK (Correcto)
- Unknown (Desconocido)

Action (Acción)

1. Desactive la alerta.
2. Restaure la alerta.

31.5.5 El estado de la alerta es inesperado

Síntoma

El estado de la alerta es diferente a

- Active (Activo)
- Locked (Bloqueada)

- Cleared (Borrada)

Causa

Un recurso informó de un estado de alerta inesperado para el problema subyacente.

Action (Acción)

1. Expanda la alerta y siga la acción recomendada descrita en **Resolution** (Resolución).
2. Si necesita más información, expanda **Event details (Información de eventos)** y vea la información para **correctiveAction**.
3. Cuando el recurso detecta un cambio, cambia automáticamente el estado de alerta a `Cleared` (Borrado).

31.6 Solución de problemas del dispositivo

Registro de auditoría:

- «El registro de auditoría está ausente.»
- «No se puede descargar el registro de auditoría»
- «No se han registrado las entradas de la auditoría»

Copia de seguridad/Restauración:

- «No se puede crear ni descargar un archivo de copia de seguridad»
- «La acción de restauración no se ha realizado correctamente»

Reinicio/Apagado:

- «El dispositivo no se apagó.»
- «No se puede reiniciar el dispositivo después de apagarlo»
- «Apagado inesperado del dispositivo»

Seguridad/Autenticación:

- «No se puede importar un certificado»
- «Se ha revocado el certificado»
- «Una cadena de certificado no válida impide las operaciones»
- «Contenido del certificado no válido impide las operaciones»
- «No se puede iniciar la sesión»
- «No se puede iniciar sesión después de una acción de restauración de fábrica»

Volcado de soporte:

- «El archivo de volcado de soporte no se creó»
- «El archivo de volcado de soporte no se guarda»
- «No se puede crear un archivo de volcado de soporte sin cifrar»

Actualización:

- «No se puede actualizar el dispositivo»
- «El archivo de actualización del dispositivo se descarga, pero falla la actualización»
- «La actualización del dispositivo no es correcta»

Otros:

- «El rendimiento del dispositivo es lento»

- «El explorador no muestra la interfaz de usuario de HPE OneView»
- «Los iconos no son visibles en el panel de control del dispositivo»
- «No se puede recuperar la sesión del explorador»
- «Reinstalación de la consola remota»

31.6.1 El rendimiento del dispositivo es lento

Síntoma

El dispositivo funciona, pero su rendimiento es lento.

Causa

La configuración del dispositivo no está configurada para un rendimiento óptimo.

Action (Acción)

1. Asegúrese de que los componentes físicos cumplen con los requisitos descritos en la ***Matriz de compatibilidad de HPE OneView***.
   - Host de VM con CPU ProLiant G7 o posterior
   - VM con dos CPU virtuales de 2 GHz o más
2. Compruebe que la conexión de red entre el dispositivo y los dispositivos gestionados sea la correcta.
3. Asegúrese de que no está activada la gestión de energía.
4. Asegúrese de que el hipervisor no está sobrecargado.
5. Asegúrese de que el almacenamiento disponible es aceptable.
6. Asegúrese de que el host no está sobrecargado.

   Examine los datos de rendimiento de la máquina virtual (contadores de rendimiento). Compruebe si el host del hipervisor está funcionando al 100 % de utilización. Considere:
   - Reiniciar el host de VM
   - Mover el dispositivo a un host de VM con más recursos, en concreto, a uno que no esté tan ocupado
   - Usar reservas o recursos compartidos en el host del hipervisor
7. Desde el equipo local, utilice el comando `ping` para determinar si el tiempo de ida y vuelta del ping es aceptable. Si el tiempo es largo, puede que haya problemas con el explorador.
8. Compruebe que la configuración del explorador sea correcta.
9. Considere la posibilidad de omitir el servidor proxy.
10. Asegúrese de que no se superan los límites de escala. Consulte la ***Matriz de compatibilidad de HPE OneView***.
11. Cree un volcado de soporte y póngase en contacto con su representante autorizado de soporte técnico.

31.6.2 Apagado inesperado del dispositivo

Síntoma

Bloqueo del dispositivo

Causa

Cierres inesperados

Acciones que se deben realizar después de un bloqueo

- Es poco común que el dispositivo se apague de forma inesperada. Compruebe si hay alertas críticas o tareas que han fallado. Siga las instrucciones de resolución, si se proporcionan.
- Actualice un recurso manualmente (**Actions→Refresh**) (Acciones > Actualizar) si la información que se muestra sobre él aparentemente es incorrecta o incoherente.
- Cree un volcado de soporte (**Settings→Actions→Create support dump** [Configuración > Acciones > Crear volcado de soporte]) para ayudar al representante autorizado de soporte técnico a solucionar el problema cuando el dispositivo se apague de forma inesperada.

31.6.3 No se puede actualizar el dispositivo

Síntoma

La operación de actualización del dispositivo falla.

Solución 1

Causa

El dispositivo no puede acceder a la red.

Action (Acción)

1. Inicie sesión en el dispositivo como administrador de infraestructuras.
2. Realice de nuevo la operación de actualización.

Solución 2

Causa

El certificado del dispositivo no es válido, ha caducado o se ha cambiado.

Action (Acción)

Consulte «El dispositivo no puede acceder a la red»

Solución 3

Causa

Action (Acción)

1. Examine la configuración del certificado en el panel Security (Seguridad) de la pantalla Settings (Configuración).
2. Obtenga un nuevo certificado para el dispositivo, si no es válido o ha caducado.

   En función del tipo de certificado, consulte «Creación de un certificado autofirmado» o «Creación de una solicitud de firma de certificado».
3. Actualice la página del explorador.
4. Acepte el certificado nuevo.
5. Vuelva a intentar la operación de actualización.

31.6.4 El archivo de actualización del dispositivo se descarga, pero falla la actualización

Síntoma

El archivo de actualización se ha bajado correctamente pero la operación de actualización no actualiza el dispositivo.

Solución 1

Causa

El archivo de descarga es demasiado grande para el explorador.

Action (Acción)

1. Compruebe que el tamaño de la descarga esté dentro de la capacidad del explorador.
2. Utilice otro explorador.

Solución 2

Causa

El archivo se ha eliminado del dispositivo.

Action (Acción)

1. Descargue el archivo de actualización.
2. Vuelva a intentar la operación de actualización.

   Consulte la ayuda en línea para obtener más detalles.

Solución 3

Causa

La versión del dispositivo está fuera del intervalo de versiones que corresponden a la actualización.

Action (Acción)

1. Descargue una versión admitida (en función de la versión del dispositivo) del archivo de actualización.
2. Vuelva a intentar la operación de actualización. Si desea información, consulte la ayuda en línea.

31.6.5 La actualización del dispositivo no es correcta

Cualquier condición de bloqueo o advertencia que afecte a la actualización del dispositivo se muestra antes de realizar la operación de actualización.

Síntoma

La actualización falla

Causa

Action (Acción)

1. Confirme que no está actualizando a la misma versión ya instalada.
2. Compruebe que todos los indicadores de estado para la LAN, CPU y memoria del panel **Appliance** (Dispositivo) de la pantalla **Settings** (Configuración) están iluminados en verde antes de volver a intentar la actualización.
3. Cree un volcado de soporte y póngase en contacto con su representante de soporte técnico de HPE.

31.6.6 El explorador no muestra la interfaz de usuario de HPE OneView

Síntoma

El explorador no muestra la interfaz de usuario de HPE OneView.

Solución 1

Causa

No se admite el explorador.

Action (Acción)

Use otro explorador compatible.

Solución 2

Causa

La caché del explorador está llena.

Action (Acción)

1. Borre la caché del explorador y vuelva a intentarlo.
2. Actualice o vuelva a cargar el explorador.

Solución 3

Causa

Javascript no está activado.

Action (Acción)

Active Javascript en el explorador.

Solución 4

Causa

Hay un problema de conectividad con el dispositivo.

Action (Acción)

1. Compruebe que la configuración del proxy del explorador sea correcta.
2. Actualice o vuelva a cargar el explorador.
3. Compruebe que el dispositivo puede acceder a la red.

   «El dispositivo no puede acceder a la red».

31.6.7 Los iconos no son visibles en el panel de control del dispositivo

Síntoma

El panel de control aparece sin iconos.

Causa

Se ha superado el tiempo de espera antes de que el explorador pudiera cargar los iconos

Action (Acción)

1. Actualice o vuelva a cargar el explorador.

2. Compruebe que el dispositivo puede acceder a la red.
   «El dispositivo no puede acceder a la red».

31.6.8 No se puede recuperar la sesión del explorador

Síntoma

El explorador no muestra la sesión o la sesión aparece congelada.

Solución 1

Causa

Tiempo de espera de la sesión

Action (Acción)

1. Finalice la sesión.
2. Vuelva a identificarse para iniciar una nueva sesión.

Solución 2

Causa

Desconectado de la sesión

Action (Acción)

Identifíquese para iniciar una nueva sesión.

31.6.9 No se puede crear ni descargar un archivo de copia de seguridad

Síntoma

No se ha podido crear o descargar un archivo de copia de seguridad.

Solución 1

Causa

Hay otras operaciones relacionadas en curso. Solo se puede crear un archivo de copia de seguridad en cada momento. No se puede crear un archivo de copia de seguridad durante la operación de restauración o mientras se está cargando o descargando un archivo de copia de seguridad anterior.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Compruebe si se está ejecutando otra operación de copia de seguridad o restauración. Busque una barra de progreso en la pantalla **Settings** (Configuración) o una indicación de finalización en la barra lateral **Activity** (Actividad).
3. Espere hasta que se complete la operación.
4. Si aparece una alerta, siga su resolución y
   a. Vuelva a intentar la operación de copia de seguridad.
   b. Si falla la operación de copia de seguridad, reinicie el dispositivo.
   c. Ejecute la operación de copia de seguridad nuevamente después de reiniciar el dispositivo.

Solución 3

Causa

Los problemas de conectividad impiden la descarga.

Action (Acción)

Asegúrese de que la red está configurada correctamente y funciona como se esperaba.

El archivo de copia de seguridad no puede descargarse porque hay una operación relacionada en curso

Causa

No se puede cargar ni descargar un archivo de copia de seguridad mientras se está realizando una operación de creación o restauración del archivo de copia de seguridad.

Action (Acción)

Compruebe si se está ejecutando otra operación de copia de seguridad o restauración. Si es así, hay una barra de progreso en la pantalla **Settings** (Configuración).

Parece que el archivo de copia de seguridad no se está descargando.

Causa

La descarga de un archivo de copia de seguridad de gran tamaño puede tardar varios minutos, o incluso más, dependiendo de la complejidad de la configuración del dispositivo.

Action (Acción)

Espere hasta que finalice la operación. Supervise la operación observando la barra de progreso en la pantalla **Settings** (Configuración).

Solución 4

Causa

Durante la operación de copia de seguridad había una operación de perfil en curso que ha provocado:

- GUID duplicados en la red
- Servidor con la configuración de un perfil anterior
- Mensaje de error: se ha interrumpido la operación
- Mensaje de error: la configuración es incoherente

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Identifique el servidor afectado.
3. Cancele la asignación del perfil al servidor.
4. Vuelva a asignar el perfil al servidor.
5. Si se informa de cualquiera de los mensajes de error, determine los factores (no relacionados con HPE OneView) que contribuyeron a esta condición, tales como:
   - ¿Se trasladó el servidor?
   - ¿Se apagó la alimentación del servidor?
6. Cree un archivo de volcado de soporte.

7. Informe sobre este problema a su representante autorizado de soporte técnico.

31.6.10 El archivo de volcado de soporte no se creó

Síntoma

No se encuentra el volcado de soporte esperado

Causa

Tiempo transcurrido insuficiente

Action (Acción)

1. Espere. La creación de un archivo de volcado de soporte puede tardar varios minutos. Si los archivos de registro son grandes o si el sistema es muy grande, la creación de un archivo de volcado de soporte puede tardar incluso más.
2. Vuelva a intentar la operación de creación del archivo de volcado de soporte.

No se puede crear el volcado de soporte esperado

Síntoma

No se puede crear el volcado de soporte desde la pantalla Oops (Vaya)

Causa

El administrador de infraestructuras es el único que puede crear un archivo de volcado de soporte desde la pantalla Oops (Vaya).

Action (Acción)

Indique las credenciales para el administrador de infraestructuras y vuelva a intentarlo.

31.6.11 El archivo de volcado de soporte no se guarda

Síntoma

El archivo de volcado de soporte no está presente en el dispositivo.

Solución 1

Causa

La descarga no se ha completado debido a una configuración incorrecta del explorador.

Action (Acción)

1. Compruebe que la descarga se ha completado.
2. Compruebe la configuración del explorador.
3. Vuelva a intentar la acción para crear el volcado de soporte y examine la barra de progreso de la descarga en la barra lateral de Activity (Actividad).

Solución 2

Causa

Espacio en disco insuficiente para el archivo de volcado de soporte por parte del cliente.

Action (Acción)

1. Asegúrese de que el equipo local tiene espacio en disco suficiente para albergar el archivo de volcado de soporte.

2. Vuelva a intentar la operación de creación del archivo de volcado de soporte.

31.6.12 No se puede crear un archivo de volcado de soporte sin cifrar

Síntoma

Se puede crear un archivo de volcado de soporte cifrado, pero no uno sin cifrar.

Causa

No tiene la autorización necesaria para crear un archivo de volcado de soporte sin cifrar. Esto solo puede hacerlo el administrador de infraestructuras.

Action (Acción)

1. Inicie sesión en el dispositivo como administrador de infraestructuras.
2. Vuelva a intentar la operación de creación del archivo de volcado de soporte.
3. Especifique la opción de **volcado de soporte sin cifrar**.
4. Cree el volcado de soporte.
5. Compruebe que la operación se realiza examinando la barra de progreso.

31.6.13 No se puede importar un certificado

Síntoma

El dispositivo no permitió o no aceptó la acción de importación de un certificado.

Solución 1

Causa

Su cuenta de inicio de sesión no le da permiso para importar un certificado.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Vuelva a intentar la acción.

Solución 2

Causa

El dispositivo ha perdido la conexión con el explorador

Action (Acción)

Privilegios necesarios: administrador de infraestructuras

1. Compruebe que la red funciona correctamente.

   Consulte «El dispositivo no puede acceder a la red»
2. Espere a que el servidor web se reinicie y repita la operación.

31.6.14 Se ha revocado el certificado

Síntoma

La entidad emisora de certificados ya no reconoce el certificado.

Causa

El certificado ya no es válido.

Action (Acción)

1. Como administrador de infraestructuras, cree u obtenga un nuevo certificado para el dispositivo.
2. Genere una solicitud de firma nueva.

31.6.15 Una cadena de certificado no válida impide las operaciones

Síntoma

Se ha dañado la cadena de certificado del dispositivo remoto.

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras.

1. Como administrador de infraestructuras, cree u obtenga un nuevo certificado para el dispositivo. Para obtener más información, consulte «Creación de una solicitud de firma de certificado».
2. Genere una solicitud de firma nueva.

31.6.16 Contenido del certificado no válido impide las operaciones

Síntoma

Causa

El formato del certificado no es válido.

Action (Acción)

Privilegios necesarios: administrador de infraestructuras

1. Como administrador de infraestructuras, cree u obtenga un nuevo dispositivo con un formato válido. Para obtener más información, consulte «Creación de una solicitud de firma de certificado» o «Creación de un certificado autofirmado».
2. Importe el nuevo certificado.

31.6.17 No se puede descargar el registro de auditoría

Síntoma

No hay visible ningún elemento del menú de acciones para descargar el registro de auditoría.

Causa

La autorización no es correcta.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Descargue el registro de auditoría.

31.6.18 No se han registrado las entradas de la auditoría

Síntoma

Faltan las entradas en el registro de auditoría.

Causa

Se editó el registro de auditoría.

Action (Acción)

Reinicie el dispositivo para crear un nuevo registro de auditoría y reanudar el registro.

31.6.19 El registro de auditoría está ausente.

Síntoma

Se eliminó el registro de auditoría.

Action (Acción)

Reinicie el dispositivo para crear un nuevo registro de auditoría y reanudar el registro.

31.6.20 La acción de restauración no se ha realizado correctamente

Solución 1

Causa

El archivo de copia de seguridad es incompatible.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Vuelva a intentar la acción de restauración con un archivo de copia de seguridad reciente que cumpla estos criterios:

   El dispositivo que se está restaurando tiene los mismos números mayor y menor de HPE OneView que el dispositivo en el que se creó el archivo de copia de seguridad.

   La pantalla **Settings** (Configuración) muestra el número de versión en este formato:

   `Versión principal.menor.nn-nnnnnnmes—día—año`
3. Solucione las discrepancias que la operación de restauración no pudo resolver automáticamente.

Las operaciones de restauración y restablecimiento de la configuración predeterminada de fábrica han fallado, y el dispositivo no se ha podido reiniciar.

Causa

Se ha producido un error grave

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Cree un archivo de volcado de soporte, por si necesita ponerse en contacto con un representante autorizado de soporte técnico.
3. Si es posible, restablezca la configuración original de fábrica en el dispositivo.

   En caso contrario, cree un dispositivo de máquina virtual nuevo partiendo del archivo de imagen proporcionado (plantilla de archivo OVF).
4. Vuelva a intentar la operación de restauración.

Se ha producido un error irrecuperable durante la operación de restauración

Action (Acción)

Si se produce un error irrecuperable durante la operación de restauración, tendrá que volver a crear la máquina virtual del dispositivo desde la imagen de la máquina virtual suministrada por Hewlett Packard Enterprise.

La operación de restauración ha fallado

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Cree un archivo de volcado de soporte, por si necesita ponerse en contacto con un representante autorizado de soporte técnico.
3. Cree un dispositivo de máquina virtual nuevo partiendo del archivo de imagen proporcionado (plantilla de archivo OVF). Para obtener más información, consulte la ***Guía de instalación de HPE OneView***.
4. Realice una o las dos acciones siguientes:
   - Vuelva a intentar la operación de restauración especificando el archivo de copia de seguridad más reciente.
   - Intente realizar la operación de restauración con otro archivo de copia de seguridad que sea compatible con el dispositivo.
5. Si el problema continúa, póngase en contacto con su representante autorizado de soporte técnico.

Causa

El estado de la operación de restauración es `IN PROGRESS` (En curso), pero el porcentaje de cambio no cambia durante 2 horas y media o más.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Reinicie el dispositivo.
3. Realice una o las dos acciones siguientes:
   - Vuelva a intentar la operación de restauración especificando el archivo de copia de seguridad más reciente.
   - Intente realizar la operación de restauración con otro archivo de copia de seguridad que sea compatible con el dispositivo.

El hardware de servidor arranca desde un dispositivo incorrecto o con una configuración del BIOS incorrecta

Causa

La configuración de arranque, del BIOS o del firmware se cambió después de la copia de seguridad y antes de la operación de restauración.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Compruebe el firmware del BIOS y la configuración de arranque.
3. Cancele la asignación de los perfiles.
4. Vuelva a asignar cada perfil a su servidor correspondiente.

La operación de restauración no restaura el perfil de servidor

Causa

La operación de restauración ha superado el tiempo de espera o ha fallado.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.

2. Cree un archivo de volcado de soporte.
3. Realice una de las acciones siguientes:
   a. Vuelva a intentar la operación de restauración especificando el archivo de copia de seguridad más reciente.
   b. Intente realizar la operación de restauración con otro archivo de copia de seguridad que sea compatible con el dispositivo.
4. Compruebe que se realizaron todas las acciones necesarias para poner los perfiles de nuevo en línea con el entorno. Si todavía hay un perfil en un estado incoherente, puede haber un comportamiento incorrecto en el centro de datos.

31.6.21 El dispositivo no se apagó.

Síntoma

El dispositivo se quedó activo a pesar de una operación de apagado.

Causa

Podría haber ocurrido un error interno.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Vuelva a intentar la acción de apagado.
3. Utilice el hipervisor para llevar a cabo un cierre correcto.
4. Si el problema persiste, cree un volcado de soporte.
5. Póngase en contacto con un representante autorizado de soporte técnico y envíele el volcado de soporte.

   Para obtener información sobre cómo ponerse en contacto con Hewlett Packard Enterprise por teléfono, consulte «Acceso al soporte de Hewlett Packard Enterprise» (página 461).

31.6.22 No se puede reiniciar el dispositivo después de apagarlo

Síntoma

La acción de reinicio ha causado el apagado, pero no el reinicio.

Causa

Podría haber ocurrido un error interno.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Vuelva a intentar la acción de reinicio.
3. Vuelva a intentar la acción de reinicio desde el hipervisor.
4. Si el problema persiste, cree un volcado de soporte.
5. Póngase en contacto con un representante autorizado de soporte técnico y envíele el volcado de soporte.

   Para obtener información sobre cómo ponerse en contacto con Hewlett Packard Enterprise por teléfono, consulte «Acceso al soporte de Hewlett Packard Enterprise» (página 461).

31.6.23 No se puede iniciar la sesión

Síntoma	Posible causa y recomendación
No hay ninguna pantalla de inicio de sesión.	**El dispositivo todavía no se ha iniciado o el explorador no funciona correctamente** 1. Espere a que el dispositivo se inicie al completo. 2. Actualice el explorador e inténtelo de nuevo. 3. Abra una nueva sesión del explorador e inténtelo de nuevo. 4. Como administrador de infraestructuras, utilice las API de REST para reiniciar el dispositivo.
Aparece una pantalla de inicio de sesión, pero el dispositivo rechaza el inicio de sesión.	**La autenticación para la cuenta de usuario local no es válida** 1. Escriba su nombre de inicio de sesión y su contraseña de nuevo por si ha cometido un error. 2. Compruebe la configuración de la función y el nombre de inicio de sesión con el administrador de infraestructuras. Si el dispositivo se restableció a la configuración original de fábrica, es posible que el administrador de infraestructuras deba restablecer su usuario. 3. Como administrador de infraestructuras, haga lo siguiente: a. Compruebe el nombre de cuenta y asegúrese de que el usuario tenga asignado un rol. b. Reinicie el dispositivo y vuelva a intentarlo. **La autenticación para el servicio del directorio Authentication (Autenticación) no es válido** 1. Escriba su nombre de inicio de sesión y elija el directorio de autenticación correcto por si ha cometido un error. 2. Compruebe la configuración de la función y del grupo, y el nombre de inicio de sesión con el administrador de infraestructuras. Si el dispositivo se restableció a la configuración original de fábrica, es posible que el administrador de infraestructuras deba restablecer su usuario. 3. Como administrador de infraestructuras, haga lo siguiente: a. Compruebe el nombre de cuenta y asegúrese de que el usuario es miembro del grupo del servicio de directorio. b. Compruebe que el servicio de directorio de autenticación está configurado correctamente. c. Compruebe que el servidor del servicio de directorio esté operativo. Consulte «Servicio de directorio no disponible» d. Compruebe que el certificado de host del servicio de directorio es válido. De no serlo, vuelva a obtener un certificado e instálelo. e. Póngase en contacto con el proveedor del servicio de directorio para asegurarse de que las credenciales son correctas. f. Reinicie el dispositivo y vuelva a intentarlo.

31.6.24 No se puede iniciar sesión después de una acción de restauración de fábrica

Síntoma

El inicio de sesión no se ha aceptado después de una operación de restauración de fábrica.

Causa

La restauración de fábrica ha eliminado la autenticación.

Action (Acción)

Inicie sesión en el dispositivo con las credenciales por defecto que utilizó al iniciar sesión por primera vez.

31.6.25 Reinstalación de la consola remota

Cuando se usa Firefox o Chrome en un cliente Windows, la instalación por primera vez de la consola remota de iLO impide que el cuadro de diálogo de instalación se muestre de nuevo. Si tiene que volver a instalar el software de la consola, debe restablecer el cuadro de diálogo de instalación.

Síntoma	Posible causa y recomendación
El cuadro de diálogo de instalación no se muestra	Si ha instalado el software de la consola remota de iLO usando un explorador (Firefox o Chrome), pero está utilizando otro explorador, se muestra el cuadro de diálogo que le pide que instale el software, incluso si el software ya está instalado. Para volver a instalar la consola, pulse la tecla **Mayús** y seleccione **Actions→Launch console** (Acciones > Iniciar consola). **Reinstalación del software** 1. Haga clic en **Install software** (Instalar el software) y cierre todos los cuadros de diálogo para instalar la aplicación. 2. Haga clic en **My installation is complete (Mi instalación se ha completado)** para iniciar la consola después de su instalación.

31.6.26 El dispositivo está desconectado, se requiere acción manual.

Síntoma

La consola de mantenimiento indica que el dispositivo está desconectado y que se requiere acción manual.

Ningún dispositivo del clúster de dispositivos está activo. Las limitaciones de la integridad de datos impiden la activación automática del dispositivo.

Solución 1

Causa

Los problemas de red o las desconexiones múltiples podrían ser la causa de la interrupción.

Action (Acción)

Para restaurar con seguridad es necesaria la acción manual.

1. Restaure la alta disponibilidad solucionando la causa de la interrupción, si fuera posible. Compruebe que todos los cables están conectados correctamente.
2. Ponga el receptáculo de nuevo en línea.

   Utilice el comando **View details** (Ver detalles) de la consola de mantenimiento para identificar el dispositivo para el que no se puede confirmar el estado. El dispositivo se identifica en cuanto a su receptáculo y número de compartimento del dispositivo.

   Si el receptáculo correspondiente está desconectado, encenderlo podría solucionar el problema.
3. Si el receptáculo no se puede volver a conectar, cambie el dispositivo a un receptáculo operativo.

   Siempre que sea posible, instale los dispositivos en clúster en diferentes receptáculos para mejorar la protección contra errores.

Solución 2

Causa

Un dispositivo no funciona y la alta disponibilidad no se puede restaurar.

Action (Acción)

IMPORTANTE: Para este procedimiento es necesario que sobrescriba la protección de la integridad de los datos.

Tenga mucho cuidado cuando siga este procedimiento

1. Determine la ubicación de ambos dispositivos en el clúster de dispositivos. La ubicación se da en cuanto al receptáculo y compartimento del dispositivo. La acción **View details** (Ver detalles) de la consola de mantenimiento, desde cualquier dispositivo, puede ofrecer esta información para el otro dispositivo.

   ATENCIÓN: La identificación errónea del dispositivo puede causar una **pérdida de datos irrecuperable**.

2. Determine si cada uno de los dispositivos:
   - Está presente en el receptáculo.
   - Está encendido.
   - Muestra un mensaje de advertencia en el banner de notificaciones de la consola de mantenimiento sobre los cambios que no se han sincronizado entre dispositivos.
3. Seleccione el dispositivo a activar. Utilice los siguientes criterios:
   - Si un dispositivo muestra una advertencia de cambios sin sincronizar, selecciónelo.
   - Seleccione el otro dispositivo:
     - Si un dispositivo se ha perdido de forma irrecuperable.
     - Si un dispositivo no se puede conectar.

     Si el dispositivo perdido contenía cambios sin sincronizar, podría producirse una **pérdida de datos irrecuperable**.
4. Asegúrese de que el dispositivo no seleccionado:
   - Está apagado.
   - Se extrae del receptáculo.
   - Se acaba de reiniciar.

   Este paso es fundamental para garantizar que ambos dispositivos no se activen a la vez. En caso contrario, no podrá volver a sincronizarlos y se producirá una **pérdida de datos irrecuperable**.
5. En la consola de mantenimiento del dispositivo seleccionado, seleccione **Activate** (Activar) y confirme la acción.

   Consulte el estado del dispositivo para supervisar el progreso.

31.6.27 El dispositivo está desconectado e inservible

Síntoma

La consola de mantenimiento indica que hay un dispositivo desconectado e inservible debido a unos datos incompletos.

Ningún dispositivo del clúster de dispositivos está activo. Las limitaciones de la integridad de datos impiden la activación automática del dispositivo.

Causa

Un dispositivo en un estado `Offline / Unusable (incomplete data)` (Desconectado / Inservible (datos incompletos) ha sufrido una interrupción mientras se sincronizaban los datos o ha detectado un error de escritura en disco. **El dispositivo no puede activarse en este estado.**

Action (Acción)

1. Vuelva a conectar el dispositivo desconectado/inservible con el otro dispositivo del clúster.

   Es probable que el otro dispositivo tenga los datos más actualizados.

   Si vuelve a establecer una conexión entre los dispositivos, la sincronización de los datos podrá completarse.
2. Ponga el receptáculo del dispositivo actualizado de nuevo en línea.

   Utilice el comando **View details** (Ver detalles) en la consola de mantenimiento del dispositivo actualizado para localizar su ubicación (receptáculo y compartimento de dispositivo).

   Si el receptáculo está desconectado, encenderlo podría solucionar el problema.
3. Si el receptáculo no se puede volver a conectar, cambie el dispositivo actualizado a un receptáculo operativo.

   Siempre que sea posible, instale los dispositivos en clúster en diferentes receptáculos para mejorar la protección contra errores.
4. Asegúrese de que los cables están conectados correctamente.
5. Restore from backup (Restaurar desde copia de seguridad)

   Si el dispositivo actualizado está en un estado irrecuperable, utilice una copia de seguridad de los datos del dispositivo para la operación de restauración:

   a. Restauración de fábrica o creación de imagen de ambos dispositivos.
   b. Restaure un dispositivo desde un archivo de copia de seguridad compatible reciente.
   c. Permita que el otro (u otro) dispositivo se una en un clúster de alta disponibilidad con el dispositivo restaurado.

   Si se necesita un dispositivo de sustitución, puede agregarlo más adelante para restaurar la alta disponibilidad.

31.7 Solución de problemas de configuración de red del dispositivo

31.7.1 El dispositivo no puede acceder a la red

Síntoma

Las operaciones que requieren acceso de red no funcionan.

Causa

La red del dispositivo no se configuró correctamente.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Asegúrese de que la asignación de la dirección IP es correcta.
3. Asegúrese de que la dirección IP del DNS es correcta.
4. Asegúrese de que un cortafuegos no esté impidiendo el acceso al servidor DNS.

   Si es así, modifique la configuración del cortafuegos.
5. Compruebe que el servidor DNS está operativo.

6. Compruebe que la dirección de la puerta de enlace para la red es correcta.
7. Inicie sesión en la consola del dispositivo como administrador de infraestructuras y corrija la configuración de red.

31.7.2 El dispositivo no puede recuperar la información de DNS del servidor DHCP

Síntoma

El servidor DHCP no ofrece acceso a las direcciones IP.

Causa

El servidor DNS o DHCP no se ha configurado correctamente

Action (Acción)

1. Compruebe que la dirección IP de cada DNS es correcta.
2. Asegúrese de que un cortafuegos no esté impidiendo el acceso al servidor DNS.
   Si lo es, tal vez tenga que modificar la configuración del cortafuegos.
3. Compruebe que el servidor DNS está operativo.
4. Utilice la consola del dispositivo virtual para determinar que el servidor DHCP está configurado correctamente.
5. Si es necesario, utilice la asignación de direcciones estáticas en lugar de DHCP.

31.7.3 No es posible acceder al servidor DNS

Síntoma

Un mensaje de alerta informa de que una *`dirección IP`* no está respondiendo como servidor DNS.

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Compruebe que la dirección IP de cada DNS es correcta.
2. Compruebe que el servidor DNS está operativo.
3. Asegúrese de que un cortafuegos no esté impidiendo el acceso al servidor DNS.
   Si lo es, tal vez tenga que modificar la configuración del cortafuegos.
4. Cambie la configuración de red según corresponda.

31.7.4 No es posible acceder al servidor de la puerta de enlace

Síntoma

Un mensaje de alerta informa de que una *`dirección IP`* no es una puerta de enlace válida.

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Compruebe la dirección de la puerta de enlace para la red.
2. Compruebe que el servidor de la puerta de enlace está operativo.
3. Cambie la configuración de red según corresponda.

31.7.5 No se puede cambiar la configuración de red

Síntoma

No se puede modificar la configuración de red.

Permiso no apropiado

Action (Acción)

1. Si es posible, inicie sesión como usuario con privilegios. En caso contrario, pídale al administrador de infraestructuras que cambie su rol para que pueda modificar la configuración de red.
2. Vuelva a iniciar sesión.
3. Cambie la configuración de red.

31.7.6 La sincronización de NTP falla

Síntoma

La configuración de fecha y hora del dispositivo no coincide con la del servidor NTP

El dispositivo no está bien configurado para NTP

Causa

La configuración del dispositivo contiene un error.

Action (Acción)

1. Como administrador de infraestructuras, compruebe el nombre de host o la dirección IP especificada está en un servidor NTP.
2. Examine el panel **Appliance** (Dispositivo) de la pantalla **Settings** (Configuración) para confirmar que la dirección IP del servidor NTP es correcta.
3. Asegúrese de que un cortafuegos no esté impidiendo el acceso al servidor NTP.

   Si lo es, tal vez tenga que modificar la configuración del cortafuegos.
4. Compruebe que el servidor NTP está operativo y establece comunicación.
5. Sincronice el reloj del dispositivo con el servidor NTP. Si desea más información, consulte la ayuda en línea.

   Deje el tiempo suficiente para que el dispositivo y el servidor NTP se sincronicen. Esto podría tardar hasta una hora en caso de un servidor NTP global.

La hora del dispositivo es diferente a la del servidor NTP en más de 1000 segundos

Causa

El dispositivo no se puede sincronizar con el servidor NTP

Action (Acción)

1. Edite la configuración regional y de hora del dispositivo.

   Para un dispositivo virtual, sincronice el dispositivo con el host de VM para sincronizar la hora del dispositivo con la hora actual según el host VM.

   Para un dispositivo físico, seleccione manualmente la hora del dispositivo.
2. Compruebe que la hora según el dispositivo coincide con la hora del servidor NTP.
3. Sincronice el dispositivo con el servidor NTP. Si desea más información, consulte la ayuda en línea.

   NOTA: HPE recomienda utilizar cuatro servidores NTP durante la sincronización del dispositivo.

   Deje el tiempo suficiente para que el dispositivo y el servidor NTP se sincronicen. Esto podría durar hasta 10 minutos.

31.8 Solución de problemas de notificaciones por correo electrónico

Utilice la información siguiente para solucionar las alertas que se muestren en el panel **Notifications** (Notificaciones) de la pantalla **Settings** (Configuración).

31.8.1 No se puede configurar la notificación de alertas por correo electrónico

Síntoma

No se puede configurar la función de notificación de alertas por correo electrónico.

Causa

No tiene los permisos necesarios para utilizar esta función.

Action (Acción)

1. Inicie sesión en el dispositivo como administrador de infraestructuras.
2. Agregue o edite una entrada de filtro y un destinatario de correo electrónico.
3. Compruebe que ha agregado o editado la entrada de filtro y el destinatario de correo electrónico correctamente. El destinatario aparecerá en el panel.

31.8.2 No se puede conectar con el <nombre de host de la dirección de correo electrónico del remitente>

Síntoma

El dispositivo no puede conectar con el nombre de host de la dirección de correo electrónico del remitente. El dispositivo no puede enviar mensajes de alerta con la dirección de correo electrónico configurada.

Solución 1

Causa

Uno o más parámetros de la configuración de las notificaciones por correo electrónico no son válidas, lo que impide que el dispositivo llegue al host utilizado para enviar mensajes de correo electrónico.

Action (Acción)

1. Como administrador de infraestructuras, consulte los parámetros de configuración. Consulte la ayuda en línea para obtener más información.
2. Corrija cualquier parámetro de configuración no válido.
3. Guarde la configuración.
4. Compruebe la configuración, ya sea haciendo un ping al host o enviando o un mensaje de prueba.

Solución 2

Causa

El dispositivo tiene problemas de red, lo que le impide enviar mensajes de correo electrónico.

Action (Acción)

1. Como administrador de infraestructuras, compruebe que el nombre de host para la dirección de correo electrónico de envío esté en la red haciendo ping al host.
2. Consulte Appliance cannot access the network (El dispositivo no puede acceder a la red) para solucionar los problemas de conexión con la red.

31.8.3 El host no responde como servidor SMTP

Síntoma

El nombre de host, que debería enviar los mensajes de correo electrónico, no responde como servidor SMTP.

Solución 1

Causa

El nombre de host no se configuró correctamente.

Action (Acción)

1. Como administrador de infraestructuras, compruebe que el nombre de host para la dirección de correo electrónico de envío esté en la red haciendo ping al host.
2. Compruebe que el número de puerto utilizado es correcto.
3. Consulte los parámetros para configurar la notificación por correo electrónico de las alertas. Si desea información, consulte la ayuda en línea.
4. Actualice los parámetros de **correo electrónico** según sea necesario.
5. Guarde la configuración.
6. Compruebe la configuración con el comando `telnet`. Por ejemplo:

   ```
   telnet mail.example.com 25
   ```

7. Haga la comprobación también mediante la supervisión de notificaciones por correo electrónico.

Solución 2

Causa

El servidor SMTP que se utiliza para mandar notificaciones por correo electrónico tiene protocolos de seguridad TLS/SSL.

Action (Acción)

1. Compruebe la conexión con el servidor SMTP utilizando el puerto correcto con el comando `telnet`. Por ejemplo:

   ```
   telnet mail.example.com 587
   ```

2. Consulte los parámetros para configurar la notificación por correo electrónico de las alertas. Si desea información, consulte la ayuda en línea.
3. Compruebe que el servidor SMTP no sea compatible con TLS/SSL.

   Actualice los parámetros de **correo electrónico** según sea necesario.
4. Guarde la configuración.
5. Compruebe la configuración con el comando `telnet`. Por ejemplo:

   ```
   telnet mail.example.com 25
   ```

6. Haga la comprobación también mediante la supervisión de notificaciones por correo electrónico.

Solución 3

Causa

La configuración de notificaciones por correo electrónico tiene una contraseña que no es válida para el servidor SMTP. El mensaje de correo electrónico no se puede enviar porque no suministra la autenticación correcta.

Action (Acción)

1. Utilice el comando `telnet` para conectar con el servidor SMTP y verificar la contraseña. Por ejemplo:

   ```
   telnet mail.ejemplo.com
   ```

2. Consulte los parámetros para configurar la notificación por correo electrónico de las alertas. Si desea información, consulte la ayuda en línea.
3. Compruebe que la contraseña del servidor SMTP es correcta.

   Actualice los parámetros de **correo electrónico** según sea necesario.
4. Guarde la configuración.
5. Haga la comprobación supervisando notificaciones por correo electrónico.

31.8.4 No se puede enviar mensajes de correo electrónico a algunos ID de correo electrónico

Síntoma

Algunos usuarios reciben mensajes de correo electrónico sobre alertas pero otros no reciben los mismos mensajes.

Solución 1

Causa

El destinatario no está configurado o no está configurado correctamente.

Action (Acción)

1. Como administrador de infraestructuras, siga el procedimiento para modificar un destinatario de correo electrónico en la ayuda en línea para ver las entradas de filtro y los destinatarios.
2. Compruebe que se ha especificado el destinatario.

   Corrija la entrada según sea necesario.
3. Compruebe que la dirección de correo electrónico de cada destinatario es válida.

   Corrija la entrada según sea necesario.
4. Haga la comprobación supervisando notificaciones por correo electrónico.

Solución 2

Causa

El mensaje de correo electrónico se filtra y, por tanto, no se entrega porque se considera correo basura o spam.

Action (Acción)

1. Si el host que envía el mensaje de correo electrónico y el destinatario se encuentran en el mismo dominio, examine la aplicación de correo electrónico del destinatario.
2. Asegúrese de que la aplicación de correo electrónico no bloquea el mensaje y de que no lo considera como correo no deseado ni lo coloca en una carpeta de correo no deseado.
3. Haga la comprobación supervisando notificaciones por correo electrónico.

31.8.5 Los destinatarios indicados no reciben notificaciones de eventos por correo electrónico

Síntoma

Ninguno de los destinatarios configurados recibe notificaciones de alertas por correo electrónico.

Solución 1

Causa

La notificación por correo electrónico está desactivada actualmente.

Action (Acción)

1. Como administrador de infraestructuras, consulte los parámetros de configuración.
2. Asegúrese de que la función de notificación por correo electrónico está activada.
3. Asegúrese de que cada entrada de filtro y destinatarios de correo electrónico está activada o desactivada según corresponda.
4. Haga la comprobación supervisando notificaciones por correo electrónico.

Solución 2

Causa

Los destinatarios no pueden recibir mensajes de correo electrónico porque sus parámetros no están bien configurados.

Action (Acción)

1. Como administrador de infraestructuras, consulte los parámetros de configuración.
2. Compruebe que se ha especificado el destinatario y que su dirección de correo electrónico es válida.
3. Si no se ha especificado el destinatario, realice una de las acciones siguientes, según corresponda:
   - Incluya al destinatario en la lista de direcciones de correo electrónico para un filtro existente editando la entrada de filtro y destinatarios.
   - Agregue el destinatario a un filtro nuevo.

   Para obtener información sobre estos procedimientos, consulte la ayuda en línea.
4. Haga la comprobación supervisando notificaciones por correo electrónico.

Solución 3

Causa

La configuración para el destinatario del correo electrónico contiene una especificación de filtro no válida que no captura ninguna alerta para la notificación.

Action (Acción)

1. Como administrador de infraestructuras, siga el procedimiento para modificar un destinatario de correo electrónico en la ayuda en línea para ver las entradas de filtro.
2. Examine las alertas notificadas en la pantalla Activity (Actividad) y tome nota de las alertas que considera que deberían haber sido capturadas por el filtro.
3. Revise las entradas de filtro.

   Asegúrese de que el filtro se ha definido con precisión.
4. Guarde la entrada de filtro y destinatarios de correo electrónico.

5. Compruebe la configuración mediante la supervisión de notificaciones por correo electrónico.

31.8.6 Mensajes de correo electrónico frecuentes e irrelevantes

Síntoma

Se envían mensajes de correo electrónico a destinatarios a los que no les pertenecen.

Causa

La configuración del destinatario de correo electrónico contiene una especificación de filtro que permite las alertas no deseadas e irrelevantes.

Action (Acción)

Privilegios mínimos requeridos:

1. Como administrador de infraestructuras, siga el procedimiento para modificar un destinatario de correo electrónico en la ayuda en línea para ver las entradas de filtro.
2. Revise las entradas de filtro:
   - Asegúrese de que no haya ninguna entrada de filtro vacía. Cuando hay una entrada de filtro vacía, se genera un mensaje de correo electrónico para cualquier alerta.
   - Asegúrese de que las entradas de filtro son únicas. En caso contrario, se enviarán al menos el doble de mensajes.
   - Especifique los criterios de los filtros con precisión. Modifique la entrada de filtro de modo que solo actúe sobre las alertas para las que desea recibir notificaciones.
3. Guarde la entrada de filtro y destinatarios de correo electrónico.
4. Compruebe la configuración mediante la supervisión de notificaciones por correo electrónico.

31.8.7 No se puede enviar el mensaje de prueba

Síntoma

Se envió un mensaje de prueba, pero no lo recibió ninguno de los destinatarios.

Solución 1

Causa

Uno o más parámetros de la configuración de las notificaciones por correo electrónico no son válidas, lo que impide que el dispositivo llegue al host utilizado para enviar mensajes de correo electrónico.

Action (Acción)

1. Como administrador de infraestructuras, consulte los parámetros para configurar la notificación por correo electrónico de las alertas. Si desea más información, consulte la ayuda en línea.
2. Corrija cualquier parámetro de configuración no válido.
3. Guarde la configuración.
4. Compruebe la configuración, ya sea haciendo un ping al host o volviendo a enviar o un mensaje de prueba.

Solución 2

Causa

El dispositivo tiene problemas de red, lo que le impide enviar mensajes de correo electrónico.

Action (Acción)

1. Como administrador de infraestructuras, compruebe que el nombre de host para la dirección de correo electrónico de envío esté en la red haciendo ping al host.
2. Consulte Appliance cannot access the network (El dispositivo no puede acceder a la red) para solucionar los problemas de conexión con la red.

31.8.8 No se han recibido algunos mensajes de prueba

Síntoma

Algunos destinatarios reciben el mensaje de prueba pero otros no reciben el mismo mensaje.

Solución 1

Causa

El destinatario no está configurado o no está configurado correctamente.

Action (Acción)

1. Como administrador de infraestructuras, siga el procedimiento para modificar un destinatario de correo electrónico en la ayuda en línea para ver las entradas de filtro y los destinatarios.
2. Compruebe que se ha especificado el destinatario.

   Corrija la entrada según sea necesario.
3. Compruebe que la dirección de correo electrónico de cada destinatario es válida.

   Corrija la entrada según sea necesario.
4. Envíe otro mensaje de prueba para comprobarlo.

Solución 2

Causa

El mensaje de prueba se filtró y, por tanto, no se entregó porque se consideró correo basura o spam.

Action (Acción)

1. Si el host que envía el mensaje de correo electrónico y el destinatario se encuentran en el mismo dominio, examine la aplicación de correo electrónico del destinatario.
2. Asegúrese de que la aplicación de correo electrónico no bloquea el mensaje y de que no lo considera como correo no deseado ni lo coloca en una carpeta de correo no deseado.
3. Envíe otro mensaje de prueba para comprobarlo.

31.9 Solución de problemas de receptáculos y grupos de receptáculos

- «No es posible agregar o quitar un receptáculo»
- «La migración no se realiza»
- «Certificado de OA no válido»

31.9.1 No es posible agregar o quitar un receptáculo

<table>
<tr><th>Síntoma</th><th>Posible causa y recomendación</th></tr>
<tr><td>No se puede agregar un receptáculo c7000</td><td>Si la adición de un receptáculo c7000 no se realiza correctamente, se muestra un panel de notificación con la razón por la cual falló la acción y una solución al problema. A menudo, la solución consiste en hacer clic en el enlace Add (Agregar) incluido en el mensaje; la acción de adición vuelve a detectar todos los componentes y actualiza su conocimiento del receptáculo.
Otro software de gestión está gestionando el receptáculo y lo reclama
1. Si la primera vez que se añade un receptáculo no se añade correctamente, asegúrese de que se cumplen los requisitos previos de receptáculos aparecen en la ayuda en línea. Compruebe que los datos introducidos en la pantalla son correctos e intente realizar de nuevo la acción.
2. Siga las instrucciones del panel de notificaciones para conocer la acción correctiva que debe realizar para agregar correctamente el receptáculo.
Pueden producirse fallos durante la acción de adición si no se puede adquirir toda la información acerca de un receptáculo, sus servidores o sus módulos de interconexión. Cuando esto sucede, se proporciona en un panel de notificaciones una explicación del problema y el componente que lo provocó (el receptáculo, un servidor o una interconexión).
3. Para volver a agregar un receptáculo, haga clic en el enlace Add (Agregar) del panel de mensajes de notificación (si lo hay), o inicie la acción de adición de nuevo desde la pantalla Add Enclosure (Agregar receptáculo), proporcionando la dirección y las credenciales del Onboard Administrator del receptáculo.
Para agregar el receptáculo al dispositivo a la fuerza, consulte la ayuda para los receptáculos.</td></tr>
<tr><td>No se puede agregar por la fuerza un receptáculo c7000</td><td>Se ha agregado por la fuerza un receptáculo c7000, pero aparece un mensaje de error. Esto ocurre solo en los casos en los que se ha establecido un VCMode y Virtual Connect (VC) se encarga de gestionar el receptáculo.
1. Es necesario limpiar manualmente la configuración e investigar lo siguiente:
• Es posible que la URL de gestión siga haciendo referencia al dispositivo. Si es así, debe reiniciarlo para que haga referencia a la primera interconexión del receptáculo. Para solucionar este problema, utilice los comandos ssh siguientes para entrar en el Onboard Administrator (con credenciales de administrador) y cambiar la URL de gestión para que haga referencia a la dirección IP de la primera interconexión de VC activa:
<table><tr><td><code>clear vcmode</code></td><td>Cancela la asociación de los receptáculos del dispositivo.</td></tr><tr><td><code>restart interconnect N</code></td><td>(donde N es el número de compartimiento de una interconexión de VC). Si realiza este paso para cada interconexión de VC del receptáculo, la interconexión recuperará la configuración predeterminada.</td></tr><tr><td><code>restart oa N</code></td><td>(donde N es el número de compartimiento del Onboard Administrator activo). Esto hace que el OA obtenga la URL de gestión de la primera interconexión de VC.</td></tr></table>
2. Una vez finalizada la configuración manual, consulte la ayuda en línea para la adición de receptáculos.</td></tr>
<tr><td>Un receptáculo existente se detecta como si fuera nuevo después de cambiar un plano medio</td><td>Ha cambiado el plano medio del receptáculo, pero no ha seguido el procedimiento recomendado en la documentación del hardware.
Recomendación: vuelva a agregar el receptáculo</td></tr>
</table>

<table>
<tr><th>Síntoma</th><th>Posible causa y recomendación</th></tr>
<tr><td>No se puede quitar un receptáculo c7000</td><td>Es posible que no pueda quitar un receptáculo c7000 por las siguientes razones:
La falta de comunicación con el hardware durante la acción de eliminación puede impedir que el dispositivo sea capaz de gestionar adecuadamente la configuración de la interconexión, el hardware de servidor y el receptáculo.
Para quitar por la fuerza un receptáculo del dispositivo debido a la falta de comunicación, consulte la ayuda en línea para los receptáculos.
El receptáculo no se quita del dispositivo. Este suele ser un problema en el propio dispositivo, y la mejor solución consiste en seguir las instrucciones de los paneles de notificación.
El receptáculo se quita, pero debido a un error de comunicación, es necesario corregir manualmente la configuración.
Si es necesario limpiar manualmente la configuración, investigue lo siguiente:
Es posible que la URL de gestión siga haciendo referencia al dispositivo. Si es así, debe reiniciarlo para que haga referencia a la primera interconexión del receptáculo. Para solucionar este problema, utilice los comandos ssh siguientes para entrar en el Onboard Administrator (con credenciales de administrador) y cambiar la URL de gestión para que haga referencia a la dirección IP de la primera interconexión de VC activa:<table><tr><td><code>clear vcmode</code></td><td>Cancela la asociación de los receptáculos del dispositivo.</td></tr><tr><td><code>restart interconnect N</code></td><td>(donde N es el número de compartimiento de una interconexión de VC). Si realiza este paso para cada interconexión de VC del receptáculo, la interconexión recuperará la configuración predeterminada.</td></tr><tr><td><code>restart oa N</code></td><td>(donde N es el número de compartimiento del Onboard Administrator activo). Esto hace que el OA obtenga la URL de gestión de la primera interconexión de VC.</td></tr></table>
Puede que el dispositivo siga reclamando las interconexiones. En este caso, tiene que quitar las interconexiones manualmente.</td></tr>
<tr><td>No es posible anular la configuración del inicio de sesión único (SSO) en el Onboard Administrator al agregar o quitar un receptáculo</td><td>Solución: quite todos los certificados y reinicie el OA (Onboard Administrator).
En la interfaz de usuario del OA, seleccione Users/Authentication (Usuarios/Autenticación).
Seleccione HPE SSO integration (Integración con HPE SSO) en el panel derecho.
Compruebe que Settings (Configuración), Trust mode (Modo de confianza) está establecido en Trust by Certificate (Confiar según certificado).
Seleccione la ficha Certification Information (Información de certificación) y elimine todos los certificados de HPE SSO.
Reinicie el OA.
Vuelva a agregar el receptáculo.</td></tr>
</table>

31.9.2 Las conexiones de perfil de servidor sin asignar no se pueden migrar

Síntoma

El informe de compatibilidad de migración de HPE OneView muestra un problema de bloqueo o una advertencia como consecuencia de una conexión de perfil de servidor sin asignar. La solución a una conexión de perfil de servidor sin asignar depende del motivo de la existencia de la conexión sin asignar y de las ramificaciones a la configuración del sistema operativo si la conexión no se migra. Consulte las soluciones siguientes para determinar la causa del problema y cómo solucionarlo.

Resuelva las conexiones de perfil de servidor asociadas con un puerto de adaptador concreto

Causa

Una conexión de perfil de servidor sin asignar no se puede migrar. La conexión se creó en VCM para asociarse con un puerto de adaptador concreto.

VCM asocia conexiones de Ethernet con puertos de adaptador de servidor con un algoritmo round-robin. Si se necesita una conexión para asignarse a un puerto intermedio en lugar de un puerto LOM, se crea una conexión sin asignar en VCM para forzar la asignación. Las dos primeras conexiones no están asignadas y las dos conexiones siguientes se asignan a los puertos intermedios.

HPE OneView permite que una conexión de perfil de servidor se asocie directamente con un puerto de adaptador concreto. Durante la migración, HPE OneView asigna las conexiones específicas asociadas con el servidor en VCM a los puertos de adaptador concretos en HPE OneView. Dado que la conexión sin asignar no se migra, la eliminación de la interfaz correspondiente dentro del sistema operativo podría provocar problemas.

Action (Acción)

En VCM, realice una de estas acciones en función del tipo de conexión.

- Fibre Channel — si no se espera impacto en el sistema operativo, continúe con la migración sin la conexión. Si se prevé un impacto en el sistema operativo, solucione el problema tras la migración.
- FCoE — asigne una red con un conjunto de enlaces ascendentes que contenga un puerto de enlaces ascendentes.
- SAN de FCoE FC y Fibre Channel nativo — asigne una estructura SAN con un puerto de enlace ascendente o continúe con la migración sin la conexión.
- iSCSI — asigne una red a la conexión de perfil de servidor o continúe con la migración sin la conexión.
- Ethernet — realice al menos una de las acciones siguientes:
    - Si el estado del puerto de enlace descendente es irrelevante, asigne una red privada sin utilizar para eliminar el tráfico servidor-a-servidor.
    - Si hay que deshabilitar el puerto de enlace descendente, asocie una red privada con un conjunto de enlaces ascendentes con un puerto sin utilizar. Habilite **Smart link** en la red.
    - Si la conexión no es necesaria, elimínela.

Asignación de una red para MAC/WWN virtuales asignadas previamente

Causa

Una conexión de perfil de servidor sin asignar no se puede migrar. La conexión se creó en VCM como marcador para la asignación previa. La asignación previa de MAC/WWN virtuales requiere una red de asociación de estructuras con una conexión de perfil.

Action (Acción)

En VCM, realice una de estas acciones en función del tipo de conexión.

- FCoE — asigne una red con un conjunto de enlaces ascendentes que contenga un puerto de enlaces ascendentes.
- SAN de FCoE FC y Fibre Channel nativo — asigne una estructura SAN con un puerto de enlace ascendente o continúe con la migración sin la conexión.

- iSCSI — asigne una red a la conexión de perfil de servidor o continúe con la migración sin la conexión.
- Ethernet — realice al menos una de las acciones siguientes:
  - Si el estado del puerto de enlace descendente es irrelevante, asigne una red privada sin utilizar para eliminar el tráfico servidor-a-servidor.
  - Si hay que deshabilitar el puerto de enlace descendente, asocie una red privada con un conjunto de enlaces ascendentes con un puerto sin utilizar. Habilite **Smart link** en la red.
  - Si la conexión no es necesaria, elimínela.

Plan para la mitigación de marcadores creados para una interconexión ausente

Causa

Una conexión de perfil de servidor sin asignar no se puede migrar. La conexión se creó en VCM como conexión FC o FCoE redundante entre interconexiones verticales.

Si se crean conexiones FC o FCoE redundantes entre interconexiones verticales (por ejemplo, al utilizar dos adaptadores para redundancia) en lugar de interconexiones adyacentes horizontalmente, VCM necesita un marcador de conexión para el adaptador aún cuando el puerto del adaptador no esté asociado con una interconexión. HPE OneView no necesita un marcador porque las conexiones pueden asociarse directamente con un puerto de adaptador concreto.

Para las conexiones FC, la detección de una conexión de marcador con una interconexión ausente es un problema de alerta en el informe de compatibilidad de HPE OneView, independientemente del estado de alimentación del servidor porque la interfaz asociada con la conexión de marcador está presente para el puerto de adaptador, incluso después del reinicio del servidor. Para las conexiones FCoE, si el servidor está encendido, la detección es un problema de bloqueo en el informe de compatibilidad porque la eliminación de la conexión puede causar la eliminación de la interfaz del sistema operativo cuando se reinicie el servidor.

Action (Acción)

- FC SAN — continúe con la migración.
- Migración sin conexión y FCoE — determine si habrá un impacto en el sistema operativo y planifique la mitigación después de la migración.
- Migración en servicio y FCoE — apague el servidor y determine si habrá un impacto en el sistema operativo y planifique la mitigación después de la migración.

Elimine las conexiones FCoE, iSCSI y FC que se crean automáticamente por defecto

Causa

Una conexión de perfil de servidor sin asignar no se puede migrar. La conexión se creó en VCM porque la GUI de VCM asocia automáticamente las conexiones con interconexiones FCoE, iSCSI y FC.

Action (Acción)

Si no son necesarias, elimine las conexiones FC, iSCSI y FCoE del perfil de servidor.

Más información

«Sobre las conexiones del perfil de servidor del VCM sin asignar durante la migración»
«Sobre problemas de bloqueo durante la migración»
«Migración de un receptáculo c7000 actualmente gestionado por VCM»

31.9.3 La migración no se realiza

Síntoma	Posible causa y recomendación
Aparece un mensaje que indica que HPE OneView no puede migrar el receptáculo de VCM	**Pueden producirse fallos durante la acción de adición si no se puede adquirir toda la información acerca de un receptáculo, sus servidores o sus módulos de interconexión.** Cuando esto sucede, se proporciona en el informe de compatibilidad una explicación del problema y el componente que lo provocó (el receptáculo, un servidor o una interconexión). 1. Examine cada problema que aparece en el informe de compatibilidad y realice la acción correctiva. 2. Repita la migración. 3. Si no se puede realizar la migración, vuelva a Virtual Connect Manager realizando estos pasos: a. Quite todos los perfiles de servidor que se crearon durante la migración. b. Quite el receptáculo del dispositivo c. Desde la UI de OA, restablezca la interconexión de Virtual Connect del compartimiento que tenga el número más bajo. d. Desde el módulo VC, inicie sesión con las credenciales predeterminadas de fábrica y, a continuación, recupere la configuración de VC desde el archivo de copia de seguridad.
Verá un mensaje indicando que la migración del receptáculo no se ha completado	**La migración se ha realizado pero la tarea de migración en HPE OneView no aparece como completada. Este error puede aparecer si se produce un reinicio del dispositivo durante la migración.** 1. Consulte las tareas de migración en la vista Activity (Actividad) y siga cualquiera de las soluciones propuestas. 2. Si el problema continúa, actualice el receptáculo. 3. Si el problema continúa, reinicie el `migrationsubstate` realizando estos pasos: a. Obtenga el “auth:{token}”. `GET` **`/rest/login-sessions`** b. Escriba el siguiente comando utilizando el token {AUTH} obtenido en el paso 1: `curl -ik -X PATCH -H "Content-Type:application/json" -H "X-API-Version:300" -H "auth:${AUTH}" -d '{"op":"replace","path":"/migrationState","value":"NotApplicable"}`

31.9.4 Certificado de OA no válido

Síntoma

Se muestra un mensaje de certificado no válido

Causa

El certificado de inicio de sesión único del OA puede dañarse cuando se cambia el firmware de OA a una versión anterior y, a continuación, se actualiza a una versión posterior.

Action (Acción)

Restablezca el OA:

1. En la interfaz de usuario del OA, seleccione **Security**+**HPESIM SSO** (Seguridad > SSO de HPESIM).
2. Elimine el certificado dañado, que se muestra en amarillo.
3. Para volver a instalar el certificado original, actualice el receptáculo.

31.10 Solución de problemas de los lotes de firmware

31.10.1 Credenciales incorrectas

Síntoma	Posible causa y recomendación
El nombre de usuario o la contraseña de iLO no son válidos	**Credenciales incorrectas para un servidor** Al intentar actualizar el firmware del servidor, el nombre de usuario o la contraseña suministrados no son válidos para un procesador de gestión de iLO. Para solucionar este problema, vuelva a escribir las credenciales correctas y a agregar el receptáculo.
No es posible obtener las credenciales de Onboard Administrator (OA)	**Las credenciales del OA no están disponibles** Al intentar actualizar el firmware, el dispositivo no pudo obtener las credenciales de Onboard Administrator (OA) para el receptáculo. Para solucionar este problema, vuelva a escribir las credenciales correctas y a agregar el receptáculo.

31.10.2 Conectividad con iLO perdida

Síntoma

Error de conexión

Causa

Action (Acción)

Recomendación

1. Restablezca el servidor para restaurar la conectividad de red al procesador de gestión del servidor
2. Vuelva a actualizar el firmware.

31.10.3 Errores de SUM

Síntoma

No se pueden eliminar los archivos de registro de actualización del firmware

Causa

Action (Acción)

Recomendación

1. Reinicie el dispositivo.
2. Vuelva a actualizar el firmware.

Síntoma

No se ha podido iniciar la solicitud de actualización del firmware

Causa

Action (Acción)

Vuelva a actualizar el firmware.

31.10.4 Fallo de la actualización del firmware al agregar el receptáculo

NOTA: Al agregar un receptáculo, el firmware de OA o de iLO puede no actualizarse a la versión mínima debido a fallos de funcionamiento de la red o a cortes en el suministro eléctrico u otros problemas. El dispositivo aparece en un estado `Unmanaged` (No gestionado).

Síntoma

Fallo al actualizar el firmware de OA

Causa

Action (Acción)

Recomendación

1. En el menú principal, seleccione **Enclosures** (Receptáculos).
2. En el panel principal, seleccione el receptáculo no gestionado.
3. Seleccione **Actions→Update firmware** (Acciones > Actualizar firmware).
4. Seleccione un SPP para la **línea de base de firmware**.
5. Seleccione **Enclosure** (Receptáculo) en **Update firmware for** (Actualizar el firmware de).
6. Haga clic en **OK** (Aceptar).
7. Para comprobar que la actividad es correcta, compruebe que tiene un estado de color verde en el área de notificaciones.

   En caso contrario, utilice la solución propuesta indicada en la sección de detalles del área de notificaciones.

Síntoma

Fallo al actualizar el firmware de iLO

Causa

Action (Acción)

Recomendación

1. En el menú principal, seleccione **Server Hardware** (Hardware de servidor).
2. En el panel principal, seleccione el hardware de servidor no gestionado.
3. Seleccione **Actions→Update iLO firmware** (Acciones > Actualizar el firmware de iLO).

   NOTA: Solo verá "Update iLO firmware" (Actualizar el firmware de iLO) si el firmware de iLO es anterior al mínimo necesario y el hardware de servidor se encuentra en un estado `Unmanaged/Unsupported Firmware` (No gestionado/firmware no compatible).
4. Haga clic en **OK** (Aceptar).
5. Para comprobar que la actividad es correcta, compruebe que tiene un estado de color verde en el área de notificaciones.

   Si la actividad no se realiza correctamente, siga las instrucciones en la resolución propuesta.

31.10.5 No se pudo actualizar el firmware de todos los dispositivos de un receptáculo

Al intentar actualizar el firmware de todos los dispositivos de un receptáculo, el proceso de actualización puede fallar en algunos servidores.

Síntoma	Posible causa y recomendación
No es posible recibir resultados desde HP SUM	**La configuración de TCP/IP del OA no se ha establecido en `Auto-negotiate` (Negociación automática)** 1. En OA, seleccione **Enclosure Information→Enclosure Settings→Enclosure TCP/IP Settings** (Información de receptáculos > Configuración de receptáculos > Configuración de TCP/IP del receptáculo). 2. Seleccione la ficha **NIC Options** (Opciones de NIC). 3. Defina la configuración de la NIC en `Auto-negotiate` (Negociación automática). 4. En HPE OneView, vuelva a iniciar el proceso de actualización del firmware. a. En el menú principal, seleccione **Enclosures** (Receptáculos). b. En el panel principal, seleccione el receptáculo. c. Seleccione **Actions→Update firmware** (Acciones > Actualizar firmware). d. Seleccione un SPP para la **línea de base de firmware**. e. Seleccione **Enclosure + logical interconnect + server profiles** (Receptáculo + interconexión lógica + perfiles de servidor) en **Update firmware for** (Actualizar el firmware de). f. Haga clic en **OK** (Aceptar). g. Para comprobar que la actividad es correcta, compruebe que tiene un estado de color verde en el área de notificaciones. En caso contrario, utilice la solución propuesta indicada en la sección de detalles del área de notificaciones.

31.11 Solución de problemas de las interconexiones

31.11.1 La modificación de interconexiones no se realiza

Síntoma

Una notificación muestra que la modificación de una interconexión concluyó sin éxito.

Causa

La modificación de interconexiones no se realiza.

Action (Acción)

1. Compruebe que se cumplen los **requisitos previos** indicados en la ayuda en línea.
2. Siga las instrucciones proporcionadas en los mensajes de notificación.

NOTA: Cuando la interconexión se modifique correctamente, aparecerá una notificación en la barra de la parte superior de la pantalla y se mostrarán la configuración del puerto y el estado del puerto deseados.

31.11.2 Los módulos de interconexión se encuentran en un estado incorrecto

Síntoma	Posible causa y recomendación
El módulo de interconexión está en estado de inventario	El módulo de interconexión no forma parte de una interconexión lógica. **Para poner el módulo de interconexión en un estado gestionado o supervisado:** 1. Localice o cree el grupo de interconexiones lógicas para el receptáculo con la pantalla **Logical Interconnect Groups** (Grupos de interconexiones lógicas). 2. En el menú principal, seleccione **Enclosure Groups** (Grupos de receptáculos). Edite el grupo de receptáculos y agregue el grupo de interconexiones lógicas del paso 1. 3. En el menú principal, seleccione **Logical Enclosures** (Receptáculos lógicos) y actualice la configuración del receptáculo lógico desde el grupo de receptáculos.
Los módulos de interconexión se encuentran en un estado de mantenimiento	Hay un problema de almacenamiento en caché de credenciales de OA si los módulos de interconexión indican que su estado es `Maintenance` (Mantenimiento). **Si los módulos de interconexión se encuentran en un estado de mantenimiento:** Tiene que volver a agregar el receptáculo. 1. En el menú principal, seleccione **Enclosures→Add** (Receptáculos > Agregar). 2. Proporcione la información del receptáculo (IP/FQDN, cuenta y contraseña de administrador) y haga clic en el botón **Add** (Agregar). Esto iniciará una nueva detección del receptáculo y sus componentes.
Los módulos de interconexión se encuentran en un estado no gestionado	**Los compartimentos de interconexión no coinciden con el tipo de esperado** El grupo de interconexiones lógicas espera una interconexión diferente de la que se encuentra en el receptáculo. 1. Quite la interconexión inesperada del receptáculo. 2. Introduzca la interconexión esperada en el receptáculo. 3. Utilice la interconexión actualizando el grupo de interconexiones lógicas.
	El firmware de la interconexión es inferior a la versión mínima soportada • Para una interconexión de Virtual Connect Fibre Channel: ◦ El receptáculo contiene una interconexión Virtual Connect Fibre Channel con las direcciones IPv6 y la versión del firmware de interconexión es inferior a la 4.10 (versión de la línea de base mínima compatible). ◦ El receptáculo contiene solo una interconexión Virtual Connect Fibre Channel o consigo misma o con otras interconexiones Virtual Connect Fibre Channel y la versión de firmware de interconexión es inferior a la 4.10 (versión de la línea de base mínima admitida). **Recomendación** Si la versión de firmware de la interconexión es igual o superior al mínimo necesario para la importación (v3.15), puede actualizar a la versión admitida después de agregar la interconexión. Si el firmware de la interconexión es anterior a la versión 3.15, siga estos pasos: 1. Extraiga el receptáculo desde la pantalla **Enclosures** (Receptáculos). 2. Actualice el firmware de interconexión de las interconexiones Virtual Connect Fibre Channel según se describe en la ayuda en línea. 3. Añada el receptáculo en la pantalla **Enclosures** (Receptáculos). • Para una interconexión que no sea Virtual Connect Fibre Channel, actualice el firmware de interconexión para la interconexión lógica tal como se describe en la ayuda en línea. Consulte la ***Matriz de compatibilidad de HPE OneView*** para obtener la lista completa de versiones de firmware admitidas.

31.11.3 Sustitución de una interconexión de Virtual Connect en un receptáculo gestionado

Síntoma	Posible causa y recomendación
El estado de la interconexión es `Missing` (No se encuentra) o `Incompatible` (No compatible)	**El módulo de interconexión estaba en uso cuando se extrajo de un receptáculo.** Si un módulo Virtual Connect Fibre Channel estaba en uso y configurado en el momento en que se extrajo físicamente, debe reemplazarse por un módulo del mismo tipo y modelo. Un módulo Virtual Connect Fibre Channel está en uso si se cumple cualquiera de las condiciones siguientes: • El módulo de interconexión está en un compartimento de interconexión que utiliza una versión de Virtual Connect anterior a la versión mínima admitida • Un perfil de servidor está utilizando las redes asociadas a los puertos de enlace ascendente del módulo de interconexión
Fallo de interconexión	**La interconexión ha fallado y debe sustituirse** **1.** Desconecte todos los cables de la interconexión y extraiga la interconexión del receptáculo. **2.** Inserte la interconexión de recambio y vuelva a conectar todos los cables de la interconexión. **3.** Inicie sesión en el dispositivo. **4.** En el menú principal, seleccione **Logical Interconnects** (Interconexiones lógicas) y, a continuación, seleccione la interconexión lógica que contiene la interconexión sustituida. **5.** En el menú principal, seleccione **Activity** (Actividad). En la lista de actividades se muestra una actividad para la interconexión añadida. • Si la versión del firmware de la interconexión es igual o superior a la versión mínima admitida, el dispositivo aplica automáticamente el grupo de interconexiones lógicas a la interconexión sustituida. Desde ese momento, la interconexión estará lista para utilizarse. • Si la versión del firmware de interconexión es inferior a la mínima admitida, se genera una alerta y debe actualizar el firmware, tal como se muestra en el paso 6. **NOTA:** Para ver el firmware instalado, seleccione **Firmware** en el selector de vista. **6.** Actualice el firmware de las interconexiones. Para las interconexiones Fibre Channel, consulte más adelante. Para las interconexiones FlexFabric, vaya al paso 7. **NOTA:** HPE OneView no puede gestionar las interconexiones Fibre Channel cuya versión de firmware es inferior a la versión mínima admitida por HPE OneView. Debe quitar el receptáculo para actualizarlo o eliminar el firmware fuera de HPE OneView. Si las interconexiones Fibre Channel están por debajo de la versión mínima, quite el receptáculo de HPE OneView y actualícelas a la versión mínima. Como alternativa, quite las interconexiones del receptáculo gestionado por HPE OneView e introdúzcalas en un receptáculo que no esté gestionado por HPE OneView y actualice el firmware a la versión mínima. Los requisitos relacionados con las versiones mínimas se indican en la ***Matriz de compatibilidad de HPE OneView***. **a.** Quite el receptáculo de HPE OneView o extraiga físicamente las interconexiones Fibre Channel y colóquelas en un receptáculo que no sea gestionado por HPE OneView. **b.** Utilice el Onboard Administrator o el servidor DHCP externo para asignar una dirección IPv4 a la interconexión. **c.** Utilice HP SUM o Virtual Connect Support Utility (VCSU) para actualizar el firmware de la interconexión. **d.** Agregue el receptáculo a HPE OneView o reinstale las interconexiones Fibre Channel en un receptáculo gestionado por HPE OneView. **e.** Opcional: si piensa usar las interconexiones Fibre Channel con una dirección IPv6, utilice el Onboard Administrator o un servidor DHCP externo para asignar una dirección IPv6 a la interconexión. **7.** Consulte “Update a firmware bundle on managed devices“ (Actualización de un lote de firmware en los equipos gestionados) en la ayuda en línea para obtener información sobre la actualización del firmware. En la parte superior de la pantalla **Logical Interconnects** (Interconexiones lógicas) se muestra el progreso de actualización del firmware. Cuando haya finalizado la actualización, el dispositivo aplica automáticamente el grupo de interconexiones lógicas. En ese momento, la interconexión estará lista para ser utilizada.

31.12 Solución de problemas de licencias

31.12.1 Restauración de una clave de licencia que se ha borrado del OA de un receptáculo

Si se realiza un restablecimiento de los valores de fábrica de un receptáculo, se borra cualquier licencia integrada en el OA y es necesario recuperar y volver a agregar manualmente la clave de licencia.

NOTA: Se necesita el certificado de concesión de licencia (documento físico o electrónico) para restaurar la clave de licencia.

Síntoma	Posible causa y recomendación
La clave de licencia integrada en el OA no se detecta cuando se agrega el receptáculo	**La clave de licencia integrada en el OA se ha borrado** 1. Vaya a Hewlett Packard Enterprise Licensing for Software Portal en **http://www.hpe.com/software/licensing-support** para activar, registrar y descargar las claves de licencia. 2. Agregue las claves al dispositivo desde la pantalla **Settings** (Configuración).

31.12.2 La licencia asignada no coincide con el tipo especificado

Síntoma

El hardware de servidor tiene asignada una licencia que es distinta de la que se especificó cuando se añadió al dispositivo.

Solución 1

Causa

El hardware de servidor tiene una licencia integrada.

Action (Acción)

Las licencias integradas anulan la directiva o el tipo de licencia que se especificó cuando se agregó el receptáculo o el servidor de montaje en bastidor. Al hardware de servidor que ya disponga de una licencia iLO Advanced permanente se le asignará una licencia `HPE OneView Advanced w/o iLO`.

Solución 2

Causa

Se ha agregado de nuevo un servidor que el dispositivo gestionaba anteriormente.

Action (Acción)

Si el dispositivo gestionaba anteriormente un servidor que tenía aplicada una licencia `HPE OneView Advanced`, al agregarlo de nuevo se le asignará la misma licencia, independientemente del tipo de licencia especificado.

31.12.3 El número de licencias parece ser inexacto

Síntoma	Posible causa y recomendación
Las licencias agregadas o asignadas recientemente no aparecen en los gráficos de licencias	**Los gráficos de licencias no están actualizados** Tal vez deba actualizar la pantalla **Settings** (Configuración) para que los gráficos de licencias muestren los cambios recientes.
No se puede encontrar el número de licencias para la licencia HPE OneView Standard	**El dispositivo no muestra el número de licencias HPE OneView Standard** Sin embargo, puede obtener el número de unidades de hardware de servidor que tienen asignada una licencia HPE OneView Standard: 1. En la pantalla **Server Hardware** (Hardware de servidor), haga clic en el cuadro Smart Search (Búsqueda inteligente) y, en **Scope** (Ámbito), seleccione **Server Hardware** (Hardware de servidor). 2. En el cuadro Smart Search (Búsqueda inteligente), escriba **`state:Monitored`** y pulse la tecla **Intro**. En el panel principal se mostrará todo el hardware de servidor supervisado. A todo el hardware de servidor supervisado se le asigna una licencia HPE OneView Standard.

31.12.4 No puede ver información de la licencia

Síntoma

No hay información sobre la licencia disponible para el dispositivo.

No se ha asignado ninguna licencia al dispositivo

Action (Acción)

Privilegios mínimos requeridos:

1. Como administrador de infraestructuras, asigne la licencia.
2. Vuelva a ver los detalles de la licencia.

La entrada de filtro está en blanco o es incorrecta

Causa

Los criterios de filtro no fueron precisos y no pudieron devolver ningún resultado.

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Corrija los criterios del filtro.
2. Vuelva a ver los detalles de la licencia.

31.12.5 No se ha podido añadir una licencia

Síntoma

No se ha podido agregar una licencia para el dispositivo.

La clave de licencia está en blanco, es incorrecta o no es válida

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Compruebe la clave de licencia que ha introducido.

   No intente agregar una clave de licencia para un producto que es compatible con iLO a otro que no lo es. De igual modo, no aplique una clave de licencia para un producto que no es compatible con iLO a uno que lo es.
2. Proporcione los valores adecuados y asegúrese de que el formato de la clave de licencia es válido.
3. Inténtelo de nuevo.
4. Si el problema continúa, póngase en contacto con su representante autorizado de soporte técnico.

La clave de licencia ya ha caducado

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Adquiera una clave de licencia válida actual.
2. Vuelva a intentarlo con la nueva clave de licencia.

Configuración de fecha y hora no válida para el dispositivo

Causa

La licencia aún no se ha activado. Es demasiado pronto para agregar la licencia.

Action (Acción)

1. Compruebe la configuración de fecha y hora del dispositivo.
2. Busque la fecha y hora en que la licencia se activa.

   Asegúrese de que no sea demasiado pronto para agregar la licencia.
3. Si el problema continúa, póngase en contacto con su representante autorizado de soporte técnico.

31.12.6 No se ha podido añadir una clave de licencia.

Síntoma

No se ha podido agregar una clave de licencia para el dispositivo.

La clave de licencia está en blanco, es incorrecta o no es válida

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Compruebe la clave de licencia que ha introducido.

   No intente agregar una clave de licencia para un producto que es compatible con iLO a otro que no lo es. De igual modo, no aplique una clave de licencia para un producto que no es compatible con iLO a uno que lo es.
2. Proporcione los valores adecuados y asegúrese de que el formato de la clave de licencia es válido.
3. Inténtelo de nuevo.
4. Si el problema continúa, póngase en contacto con su representante autorizado de soporte técnico.

La clave de licencia ya ha caducado

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Adquiera una clave de licencia válida actual.
2. Vuelva a intentarlo con la nueva clave de licencia.

Configuración de fecha y hora no válida para el dispositivo

Causa

La licencia aún no se ha activado. Es demasiado pronto para agregar la licencia.

Action (Acción)

1. Compruebe la configuración de fecha y hora del dispositivo.
2. Busque la fecha y hora en que la licencia se activa.

   Asegúrese de que no sea demasiado pronto para agregar la licencia.
3. Si el problema continúa, póngase en contacto con su representante autorizado de soporte técnico.

31.12.7 No se ha podido aplicar la licencia

Síntoma

No se ha podido aplicar una licencia o una clave de licencia a una instancia.

Se ha superado la capacidad de la clave de licencia

Causa

Todas las licencias de la clave de licencia están en uso. La instancia a la que ha intentado asignar una licencia se ha marcado como sin licencia.

Action (Acción)

Privilegios mínimos necesarios: administrador de infraestructuras

1. Adquiera una clave de licencia nueva.
2. Vuelva a intentarlo con la nueva clave de licencia.

La licencia ya está activa

Causa

La licencia que intenta aplicar ya está en uso.

Action (Acción)

1. Si quedan licencias sin utilizar, vuelva a intentarlo con otra licencia.
2. En caso contrario, adquiera una clave de licencias con licencias sin utilizar y vuelva a intentarlo con una licencia de la nueva clave de licencias.

La instancia o el producto ya dispone de licencia

Causa

La licencia se ha aplicado a una instancia a un producto que ya dispone de licencia.

Action (Acción)

1. Compruebe la instancia o el producto al que intenta asignar la licencia.
2. Si es necesario, vuelva a intentarlo con el nombre del producto o la instancia correcto.

31.13 Solución de problemas de configuraciones regionales

Síntoma	Posible causa y recomendación
Mensajes devueltos por las llamadas de la API de REST en las que se especifique chino (zh) o japonés (ja) en el encabezado Accept-Language no se muestran correctamente	Al utilizar una ventana de comandos de Microsoft Windows para llamar a las interfaces API de REST (ya sea directamente o a través de la ejecución de secuencias de comandos en la ventana de línea de comandos), los mensajes devueltos desde las llamadas de la API de REST en la que se especifique el chino (zh) o japonés (ja) como idioma del encabezado Accept-Language no se muestran correctamente. **HPE OneView devuelve los mensajes en la codificación UTF-8. Esto no es compatible con las versiones actuales de la ventana de línea de comandos** 1. Al utilizar una ventana de línea de comandos, ajuste el encabezado accept-language de la API de REST en una configuración regional que admita la línea de comandos, como en-us. 2. Redirija la salida de la llamada de REST a un archivo de texto y visualice dicho archivo por medio de una herramienta de Windows que admita UTF-8, como el Bloc de notas. 3. Utilice otras herramientas de terceros disponibles para Windows que sean compatibles con UTF-8. Por ejemplo, los usuarios han informado de que el entorno Cygwin de Windows admite UTF-8.

31.14 Solución de problemas de las interconexiones lógicas

31.14.1 Errores de ocupación de compartimentos de E/S

Síntoma

Causa

Cambio en el estado de la interconexión

Action (Acción)

Los errores de estado de los errores de interconexión pueden deberse a:

- Falta la interconexión en un compartimento de E/S (el estado de la interconexión es `Absent` [Ausente])
- Se ha encontrado un modelo de interconexión no compatible en un compartimento de E/S (el estado de la interconexión es `Unsupported` [No compatible])
- No es posible gestionar la interconexión del compartimento de E/S debido a la presencia de firmware no compatible (el estado de la interconexión es `Unmanaged` [No gestionado])
- Discrepancia entre el tipo de interconexión y el tipo especificado por el grupo de interconexiones lógicas
- Discrepancia entre módulos de interconexión adyacentes horizontalmente

31.14.2 Advertencias o errores de los conjuntos de enlaces ascendentes

Síntoma	Posible causa y recomendación
El conjunto de enlaces ascendentes no está operativo	**El conjunto de enlaces ascendentes no está operativo debido a que:** • Uno o varios enlaces ascendentes no funcionan debido a un cable defectuoso, a la ausencia del cable o del transceptor, o a que el transceptor no es válido • No hay redes asignadas • Falta la información de DCBX para una red FCoE **1.** Compruebe que se cumplen los siguientes requisitos previos: • Hay al menos una red definida • Dispone de privilegios de administrador de redes o equivalente para gestionar redes. • La información de DCBX es necesaria para las redes FCoE **2.** Compruebe que los datos que ha introducido en la pantalla **Add Uplink Set** (Agregar conjunto de enlaces ascendentes) son correctos y que el nombre del conjunto de enlaces ascendentes es único. **3.** Vuelva a intentar la operación.

31.14.3 Advertencias o errores de las interconexiones físicas

Síntoma	Posible causa y recomendación
Advertencias o errores en el ámbito de la interconexión	**Los errores o advertencias de las interconexiones pueden deberse a:** • Un enlace descendente con una conexión implementada no está operativo • Versión del firmware incorrecta (distinta de la versión de línea de base de firmware) • Error de configuración • Fallo de hardware • Pérdida de comunicación • Puertos desactivados por el administrador

31.14.4 Errores de actualización del firmware

Síntoma	Posible causa y recomendación
Se muestran entradas de fallos de actualización del firmware en el registro de actividades	**Los errores de firmware de las interconexiones pueden deberse a:** • Reinicio de los módulos de interconexión mientras hay una actualización de firmware en curso. • Iniciar una actualización del firmware mientras hay otra actualización del firmware en curso. • Una interconexión de la interconexión lógica no está en un estado `Configured` (Configurada) antes de iniciar la actualización. • HPE OneView no puede comunicarse con el Onboard Administrator del receptáculo. **Recomendaciones** • No reinicie los módulos de interconexión mientras haya una actualización de firmware en curso. • Compruebe el registro de actividades para obtener más información sobre la causa principal. 1. Si ha fallado el almacenamiento provisional del firmware, compruebe el registro de actividades, corrija el problema y vuelva a iniciar la actualización. 2. Si ha fallado la activación del firmware, compruebe el registro de actividades y, a continuación, active el firmware manualmente. A continuación, confirme que las versiones de firmware de las interconexiones de VC en HPE OneView son las mismas que se muestran en OA. • Asegúrese de que todas las interconexiones de la interconexión lógica estén en el estado `Configured` (Configurada) antes de iniciar la actualización. • Si una actualización del firmware no deja de producir fallos, consulte la ayuda en línea para crear un archivo de volcado de soporte de la interconexión lógica y póngase en contacto con su representante de soporte técnico de Hewlett Packard Enterprise.

31.14.5 Condición de desbordamiento de pausa detectada en un puerto físico Flex-10

Síntoma	Posible causa y recomendación
Todos puertos lógicos Flex-10 asociados a los puertos físicos están desactivados	Cuando la protección contra desbordamiento de pausa está activada, esta función detecta condiciones de desbordamiento de pausa en los puertos de enlace descendente del servidor y desactiva el puerto. El puerto permanecerá desactivado hasta que se realice una acción administrativa. La acción administrativa conlleva los pasos siguientes: 1. Resolver el problema con la NIC en el servidor que causa la generación de pausas continuas. Esto puede incluir la actualización del firmware de NIC y los controladores de dispositivo. El reinicio del servidor puede que no elimine la condición de desbordamiento de pausa si la causa está en el firmware de NIC. En este caso, el servidor se debe desconectar completamente de la fuente de alimentación para restablecer el firmware de NIC. 2. Vuelva a activar los puertos desactivados restableciendo la protección contra desbordamiento de pausa. Puede restablecer la protección contra desbordamientos de pausa en el menú **Actions** (Acciones) en la pantalla **Interconnects** (Interconexiones).

31.15 Solución de problemas de conmutadores lógicos

31.15.1 Comunicaciones con conmutadores

Síntoma

No se puede comunicar con el conmutador

Causa

El tipo de conmutador no es correcto o las credenciales no son válidas

Action (Acción)

Tipo de conmutador incorrecto

- Edite el grupo de conmutadores lógicos para especificar el tipo correcto de conmutador de la parte superior del bastidor y el número de conmutadores.

Credenciales no válidas

El nombre de usuario o la contraseña no son válidos para el conmutador.

- Edite el conmutador lógico e introduzca las credenciales correctas

31.16 Solución de problemas de redes

31.16.1 La operación de creación de red no se realiza

Síntoma	Posible causa y recomendación
La creación de la red no se realiza	**La configuración de red no es correcta** **1.** Compruebe lo siguiente: • El nombre de la red es único. El ID de VLAN se añade al nombre de la red al crear varias redes con etiquetas mediante una operación masiva. • El número de redes no debe superar el máximo indicado en la ***Matriz de compatibilidad de HPE OneView***. • El número de redes privadas no debe superar el máximo indicado en la ***Matriz de compatibilidad de HPE OneView***. **2.** Vuelva a intentar la operación de creación de la red.

31.17 Informes de solución de problemas

31.17.1 No se pueden ver los informes

Síntoma

No puede acceder a ningún informe.

Causa

Autorización incorrecta

Action (Acción)

Cierre la sesión y, a continuación, vuelva a iniciarla con un rol de usuario que le permita consultar los informes. Por ejemplo:

- Administrador de infraestructuras
- Administrador de la red
- Administrador del servidor
- Administrador de almacenamiento
- Solo lectura

31.18 Ámbitos de la solución de problemas

31.18.1 No se puede agregar un ámbito

Síntoma

Al hacer clic en **Create** (Crear) o **Create+** (Crear+) no se genera ningún ámbito.

Solución 1

Causa

El nombre del ámbito se escribió con caracteres no válidos.

Action (Acción)

Vuelva a escribir el nombre del ámbito utilizando únicamente caracteres alfanuméricos, el signo más (+) y caracteres de espacio para el nombre del ámbito.

Solución 2

Causa

El nombre indicado para el ámbito ya está en uso.

Action (Acción)

Indique un nombre exclusivo para el ámbito.

31.18.2 No se puede editar ni eliminar un ámbito

Síntoma

La llamada de la API de REST ha fallado con el Error 412, “Precondition Failed” (Error de condición previa).

Causa

La eTag transmitida en el encabezado de la solicitud “If-Match” no coincide con la eTag actual del ámbito que se está editando o eliminando.

Action (Acción)

Vuelva a realizar la operación con una eTag actual o con la eTag configurada como “*”.

31.19 Solución de problemas de hardware de servidor

Para obtener información sobre problemas específicos de hardware de servidor, consulte las ***Notas de la versión de HPE OneView***.

31.19.1 La adición o eliminación de un servidor no se realiza

Si la adición del servidor no se realiza, se muestra un panel de notificación con la razón por la que falló la acción y con una solución al problema. A menudo, la solución consiste en hacer clic

en el enlace **add** (agregar) incluido en el mensaje; la acción de adición vuelve a detectar todos los componentes y actualiza su conocimiento del servidor.

Síntoma	Posible causa y recomendación
No se puede eliminar un servidor	**La falta de conectividad con el hardware de servidor puede impedir que se realice correctamente la acción de eliminación** El servidor no se quita del dispositivo. La causa probable es un problema interno en el dispositivo y la mejor solución es seguir las instrucciones que aparecen en el panel de notificaciones. El servidor se quita, pero debido a un error de comunicación, es necesario corregir manualmente la configuración. En el caso de que se necesite una configuración manual, investigue lo siguiente: • Es posible que la URL de gestión siga haciendo referencia al dispositivo; déjela como está. Para hacer una limpieza manual después de la eliminación, utilice la opción **Force** (Forzar) para agregar el servidor de nuevo bajo un nuevo gestor de dispositivos. • Elimine el usuario con derechos administrativos `_HPEOneViewAdmin` de la lista de usuarios de iLO a través del iLO. • Elimine el destino de captura SNMP, que es la dirección IP del dispositivo, de la lista de destinos de captura. • Vaya a la página HPE OneView de la interfaz web de iLO y, a continuación, haga clic en el botón **Delete** (Eliminar) en el cuadro de diálogo **Delete this remote manager configuration from this iLO** (Eliminar esta configuración de gestor remoto de este iLO).

31.19.2 No se puede controlar el encendido del servidor

El control de encendido del hardware de servidor depende del HPE Integrated Lights-Out (iLO) del hardware de servidor de destino y, en el caso de los servidores ProLiant, del módulo Onboard Administrador del receptáculo en que se encuentran.

Si tiene dificultades con el control de encendido del servidor, examine los cambios de configuración y seguridad recientes que podrían afectar a esta función. A menudo, el registro de eventos de iLO puede ser un punto de partida útil para ver estos cambios.

Otra área que conviene examinar para servidores ProLiant son las directivas de gestión de energía del receptáculo. Compruebe el Onboard Administrator para asegurarse de que recibe la alimentación suficiente y de que la política de funcionamiento de energía sea apropiada.

También podría haber fallado el hardware. Utilice el registro de gestión integrado (IML) del iLO para ver los errores de la POST (Power On Self Test) y determinar si se ha producido un fallo de hardware.

Si falla una acción de encendido o apagado, siga las instrucciones del mensaje de notificación.

31.19.3 Se pierde la conectividad con el hardware de servidor después de reiniciar el dispositivo

Cuando se reinicia el dispositivo después de un bloqueo, el inventario del servidor se evalúa para detectar cualquier actividad de larga duración que haya fallado, como la aplicación de la configuración del perfil de servidor, que podría haber estado realizándose cuando se produjo el bloqueo. Puede hacer la recuperación realizando la misma acción de nuevo, como volver a aplicar la configuración del perfil de servidor.

El dispositivo vuelve a sincronizar los servidores. Durante la resincronización, cada hardware de servidor entra en el estado `resyncPending`. Una resincronización completa de un elemento de hardware de servidor incluye volver a detectar el hardware de servidor, comprobar el estado de alimentación del hardware de servidor y actualizar el estado de los recursos en consecuencia, así como actualizar el estado de funcionamiento. El dispositivo crea una cola de tarea para cada tarea durante una operación de resincronización.

31.19.4 Sustitución de un servidor que tiene asignado un perfil de servidor

Síntoma	Posible causa y recomendación
Fallo de hardware de servidor	**El hardware de servidor ha fallado y se debe sustituir** **1.** Apague ordenadamente el hardware de servidor. **2.** Extraiga el servidor original e instale el servidor de sustitución. **3.** Si el tipo de hardware de servidor del servidor de sustitución coincide con el tipo de hardware de servidor del servidor original: **a.** Si la afinidad definida en el perfil es **Device Bay** (Compartimento de dispositivo), el perfil de servidor se vuelve a asignar automáticamente al nuevo servidor. Siga con el paso 5. **b.** Si la afinidad definida es **Device bay + server hardware** (Compartimento de dispositivo + hardware de servidor), debe cambiarse el perfil de servidor y volver a guardarse para permitir que el dispositivo vuelva a configurar el perfil para el nuevo servidor. No es necesario realizar cambios en el perfil de servidor. Siga con el paso 5. **4.** Si el tipo de hardware del servidor de sustitución no coincide con el tipo de hardware del servidor original, debe crearse un nuevo perfil de servidor que coincida con el tipo de hardware del servidor de sustitución. Debe revocarse o eliminarse la asignación del perfil original y asignarse el nuevo perfil al servidor de repuesto. O bien, el tipo de hardware de servidor debe actualizarse para que coincida con el hardware insertado. **5.** Si la versión de firmware de iLO es mayor o igual que la versión de firmware mínima necesaria, continúe con el paso 6. La versión mínima del firmware de iLO se indica en la ***Matriz de compatibilidad de HPE OneView***. Si el servidor de repuesto tiene una versión de firmware de iLO inferior a la versión de firmware mínima necesaria, se muestra una alerta en la pantalla **Server Hardware** (Hardware de servidor) y el estado del servidor es **Unmanaged/Unsupported Firmware** (No gestionado/firmware no compatible). **a.** Seleccione **Actions→Update iLO firmware** (Acciones > Actualizar el firmware de iLO). **b.** Haga clic en **OK** (Aceptar). **6.** Si la versión del firmware de iLO es diferente de la línea de base y el perfil de servidor está asignado a un servidor Gen8 o posterior, puede actualizarse automáticamente el firmware de iLO del servidor mediante la reasignación del perfil de servidor. **a.** En el menú principal, seleccione **Server Profiles** (Perfiles de servidor) y, a continuación, seleccione el perfil de servidor que desee editar. **b.** Seleccione **Actions→Edit** (Acciones > Editar). Si es necesario, seleccione el hardware de servidor correspondiente. **c.** Para gestionar manualmente la actualización del firmware, en la lista **Firmware baseline** (Línea de base de firmware), seleccione **managed manually** (Gestionado manualmente). **d.** Para actualizar automáticamente el firmware, seleccione la línea de base de firmware apropiada. Para forzar la instalación del firmware, seleccione **Force installation** (Forzar instalación). **e.** Haga clic en **OK** (Aceptar). Si la versión del firmware es diferente de la línea de base y el perfil de servidor está asignado a un servidor G7, debe actualizarse el firmware fuera del dispositivo.

31.19.5 Cambio de un adaptador de servidor en el hardware de servidor por un perfil de servidor asignado

IMPORTANTE: El adaptador de recambio debe coincidir con el adaptador antiguo. Si el adaptador de recambio no coincide con el adaptador antiguo, el tipo de hardware de servidor se cambiará. Si se ha asignado un perfil de servidor a dicho hardware de servidor, debe crearse un nuevo perfil de servidor para admitir el tipo de hardware de servidor modificado.

Síntoma	Posible causa y recomendación
Fallo de adaptador del servidor	**El adaptador del servidor ha producido un error y se debe sustituir** **1.** Apague ordenadamente el servidor. **2.** Sustituya el adaptador en el servidor. **3.** Si el perfil de servidor correspondiente está configurado con identificadores virtuales (direcciones MAC y WWN), continúe con el paso 4. Si el perfil está configurado con los identificadores físicos (MAC y WWN), tenga en cuenta lo siguiente: **a.** Debido a un cambio en los identificadores, las configuraciones de red Ethernet pueden perderse en el sistema operativo y puede necesitarse una reconfiguración. **b.** Puede ser necesario actualizar el WWN del host del servidor en su zona de red de almacenamiento y en el array de almacenamientos. **4.** Compruebe la versión de firmware del nuevo adaptador. **a.** En el menú principal, seleccione el **Server Hardware** (Hardware de servidor) o **Server Profiles** (Perfiles de servidor) y, a continuación, seleccione el hardware o perfil de servidor que contiene el adaptador sustituido. **b.** En la pantalla de **Server Hardware** (Hardware de servidor) o **Server Profile** (Perfil de servidor), seleccione **Actions→Launch console** (Acciones > Iniciar consola). Se inicia la consola remota de iLO. **c.** Encienda el servidor y compruebe la versión del firmware del nuevo adaptador durante el arranque. **NOTA:** Para comprobar que la versión de firmware coincide con la línea de base de su firmware, en el menú principal, seleccione **Firmware Bundles** (Lotes de firmware) y, a continuación, seleccione la línea de base de su firmware. Desplácese a través de la lista de firmware para encontrar la información que desea sobre la línea de base y compárela con su firmware del adaptador. **5.** Si la versión del firmware es diferente de la línea de base y el perfil de servidor está asignado a un servidor Gen8 o posterior, puede actualizarse automáticamente el firmware del servidor mediante la reasignación del perfil de servidor. **a.** En el menú principal, seleccione **Server Profiles** (Perfiles de servidor) y, a continuación, seleccione el perfil de servidor que desee editar. **b.** Seleccione **Actions→Edit** (Acciones > Editar). Si es necesario, seleccione el hardware de servidor correspondiente. **c.** Para gestionar manualmente la actualización del firmware, en la lista **Firmware baseline** (Línea de base de firmware), seleccione **managed manually** (Gestionado manualmente). **d.** Para actualizar automáticamente el firmware, seleccione la línea de base de firmware apropiada. Para forzar la instalación del firmware, incluso si es el mismo o una versión más reciente, seleccione **Force Installation** (Forzar instalación). **e.** Haga clic en **OK** (Aceptar). **NOTA:** Si la versión del firmware es diferente de la línea de base y el perfil de servidor está asignado a un servidor G7, debe actualizarse el firmware fuera del dispositivo.

31.20 Solución de problemas de perfiles de servidor

31.20.1 El perfil de servidor no se crea o actualiza correctamente

Cuando no se crea o se actualiza correctamente un perfil de servidor, aparece una notificación en la parte superior de la pantalla que indica que la operación de perfil no se ha realizado

correctamente; haga clic en el área de notificación para mostrar más detalles. Además, el icono de estado junto al nombre del perfil de servidor indica que está en una condición de `Error` (). El perfil permanece en el dispositivo, pero debe editar el perfil para corregirlo. Al corregir el perfil de servidor, su estado cambia a `OK` (Correcto) ().

Síntoma	Posible causa y recomendación
El perfil de servidor no se crea o actualiza correctamente	**Compruebe las condiciones siguientes:** 1. Compruebe que se han cumplido los requisitos previos indicados en la ayuda en línea. 2. Compruebe que las condiciones siguientes son **verdaderas**: • Se ha instalado y aplicado el SPP más reciente • Se ha introducido un nombre de perfil y es exclusivo • El hardware de servidor seleccionado está apagado • El hardware de servidor se encuentra en el estado `No Profile Applied` (No se ha aplicado perfil), tiene el firmware correcto, los puertos están asignados a la interconexión correcta y el compartimento de dispositivo no tiene asignado ningún perfil • El hardware de servidor es capaz de apagar y encender, y el usuario no cerró el hardware de servidor mientras se aplicaba la configuración del perfil • Se han aplicado los niveles correctos de firmware de iLO y de la ROM del sistema • Está utilizando hardware de servidor compatible • El iLO tiene una dirección IP y conectividad de red • Existe comunicación con el iLO del hardware de servidor, lo que incluye, entre otras cosas, que el iLO esté funcionando, el cableado de red esté conectado y funcione, y no haya problemas con los conmutadores o las interconexiones en la red de gestión • El dispositivo y los recursos gestionados no están separados por un cortafuegos • Se han añadido correctamente receptáculos • El OA tiene conectividad de red • Se ha añadido correctamente el hardware de servidor • La red o el conjunto de redes especificado está disponible en el puerto del hardware de servidor • Las interconexiones están en el estado `Configured` (Configurada) y tienen el firmware correcto • La configuración de la interconexión lógica coincide con su grupo de interconexiones lógicas • No hay redes duplicadas en un puerto físico • Si hay varios adaptadores instalados, todos los adaptadores deben tener la misma versión de firmware • Las direcciones especificadas por el usuario son exclusivas y tienen el formato correcto 3. Cuando se hayan solucionado los problemas, edite el perfil o elimine el perfil y cree otro perfil. **El perfil de servidor tiene redes duplicadas en el mismo puerto físico** • Cambie la conexión a otro puerto • Cambie la conexión para que utilice otra VLAN
No se puede encontrar una red al agregar una conexión	**Compruebe que la condición siguiente es verdadera:** • Las redes del grupo de interconexiones lógicas están configuradas en conjuntos de enlaces ascendentes

Síntoma	Posible causa y recomendación
No se puede agregar una conexión del perfil	**Compruebe que las condiciones siguientes son verdaderas:** • Las interconexiones del grupo de interconexiones lógicas están en el estado `Configured` (Configurada) y tienen el firmware correcto • Los servidores se encuentran en el estado `No Profile Applied` (No se ha aplicado perfil), tienen el firmware correcto y los puertos están asignados a la interconexión correcta
Se agota el tiempo de espera de una operación de perfil al aplicar la configuración del BIOS	**El hardware de servidor o su iLO están apagados o reiniciándose** • En la mayoría de los casos, el problema se resuelve volviendo a intentar la operación **El dispositivo no puede recopilar información sobre progreso del iLO** • En la mayoría de los casos, el problema se resuelve volviendo a intentar la operación
La asignación automática de la FlexNIC falla durante la asignación/ implementación de conexiones	**Configuración no válida** • La asignación automática de las conexiones de la FlexNIC no valida lo siguiente: ◦ Exceso de suscripciones de ancho de banda en el puerto físico ◦ Número máximo de redes (VLAN) en el puerto físico ◦ Redes (VLAN) duplicadas en el puerto físico • Se requiere una asignación manual

31.20.2 No se puede aplicar el perfil de servidor

Síntoma

No se puede aplicar el perfil de servidor

Causa

Action (Acción)

Si ha recibido un error que indica que Intelligent Provisioning no se ha podido arrancar en el período de tiempo requerido, siga estos pasos:

1. Intente arrancar en Intelligent Provisioning manualmente en el sistema afectado pulsando **F10** durante la POST.
2. Si funciona el arranque manual en Intelligent Provisioning, vuelva a intentar la operación desde HPE OneView.

   Si el arranque manual sigue fallando, reinicie el iLO y, a continuación, vuelva a intentar el paso 1.
3. Si fallan los pasos anteriores y el servidor es un BL465c con una controladora Smart Array activa, desactive temporalmente la IOMMU en el servidor mediante la RBSU.
   a. Durante el arranque del sistema, pulse **F9** para entrar en la RBSU.
   b. Seleccione **System Options** (Opciones del Sistema).
   c. Seleccione **Processor Options** (Opciones del procesador).
   d. Seleccione **AMD-Vi (IOMMU)**.
   e. Seleccione **Disabled** (Desactivada).
   f. Guarde la configuración y salga de la RBSU.
4. Si el arranque sigue fallando, instale la versión más reciente de Intelligent Provisioning vque se encuentra en **http://hpe.com/info/intelligentprovisioning**..

Síntoma

No se puede comprobar el estado del hardware de servidor

Causa

Action (Acción)

Compruebe el estado de funcionamiento del hardware de servidor:

1. Haga clic en **Cancel** (Cancelar) para salir de la pantalla **Create Server Profile** (Crear perfil de servidor).
2. En el menú principal, vaya a la pantalla **Server Hardware** (Hardware de servidor).
3. Busque y, a continuación, seleccione el hardware de servidor.

31.20.3 Las operaciones de perfil no son correctas

Síntoma

Un mensaje indica que otro sistema de gestión está gestionando el servidor

Causa

HPE OneView ya no gestiona el receptáculo.

Action (Acción)

Para evitar la pérdida de todos los identificadores virtuales asignados, realice los pasos siguientes antes de eliminar por la fuerza el perfil de servidor.

1. Utilice las API de REST o **Powershell** para obtener el perfil de servidor.

   `GET /rest/server-profiles`

2. Borre el perfil por la fuerza utilizando la interfaz de usuario o las API de REST.
3. Vuelva a crear los ID utilizando la opción **User Specified** (Especificado por el usuario) de la interfaz de usuario, o utilice las API de REST para crear el perfil de servidor:
   a. Obtenga el perfil de servidor.

      `GET /rest/server-profiles`

   b. Edite el perfil de servidor.
      1) Quite los valores `uri`, `serverHardwareTypeUri`, `enclosureGroupUri`, `enclosureUri` y `enclosureBay`.
      2) Cambie el valor de `serverHardwareUri` al servidor con el que va a estar asociado el perfil.
      3) Cambie `serialNumberType` de `Virtual` a `UserDefined`.
      4) En la propiedad `connections`, cambie `macType` de `Virtual` a `UserDefined`.
      5) En la propiedad `connections`, cambie `wwpnType` de `Virtual` a `UserDefined`.
      6) En la propiedad `connections`, si es aplicable, cambie `networkUri` por las redes correctas.
   c. Cree el perfil de servidor.

      `POST /rest/server-profiles`

31.20.4 No se puede actualizar o borrar el perfil

Síntoma

No se puede actualizar el perfil: MyProfile o realizar cambios de firmware adicionales

Causa

Hay una actualización del firmware en curso

Action (Acción)

- Espere hasta que finalice la instalación del firmware.

Síntoma

No se puede eliminar el perfil: MyProfile o realizar cambios de firmware adicionales

Causa

Hay una actualización del firmware en curso

Action (Acción)

Realice una de las acciones siguientes:

1. Espere hasta que finalice la instalación del firmware. Se recomienda encarecidamente que no cancele la operación antes de que finalice la instalación.
2. Seleccione la opción `Force delete` (Eliminar por la fuerza).

Causa

El servidor no está apagado.

Action (Acción)

Para eliminar un perfil:

- Apague el servidor.

NOTA: La operación Momentary press (Pulsar momentáneamente) está permitida en todo momento, pero Press and Hold (Mantener pulsado) está restringida, ya que puede poner el servidor en un estado incoherente.

Síntoma

No se ha podido apagar el perfil de servidor

Causa

La operación Press and Hold (Mantener pulsado) se ha rechazado.

Action (Acción)

Realice una de las acciones siguientes:

- Utilice la operación de encendido **Momentarily press** (Pulsar momentáneamente) y SUT se asegurará de que ningún hardware pase a un estado incoherente.
- Intente la operación de encendido **Press and hold** (Mantener pulsado) después de que SUT haya pasado al estado de terminal.

NOTA:

- No se admite la operación de encendido **Press and hold** (Mantener pulsado) mientras HPE Smart Update Tools actualiza el firmware o los controladores.
- Se recomienda encarecidamente que espere hasta que finalice la instalación del firmware y que no cancele el proceso.

Síntoma

No se puede completar la instalación del firmware

Causa

El firmware de {servidor} no coincide con la línea de base de firmware.

Action (Acción)

- Si ha optado por actualizar el firmware mediante HPE SUT, tendrá que instalar HPE SUT para completar la actualización del firmware y los controladores.

31.20.5 Versiones de firmware incoherentes

Síntoma	Posible causa y recomendación
La instalación del firmware no se ha completado o no coincide con la línea de base	**El firmware no coincide con la línea de base de firmware** Realice una de las acciones siguientes: • Instale y ejecute Smart Update Tools. • Edite el perfil de servidor para utilizar la opción “Firmware only” (Solo firmware) para la instalación de la línea de base de firmware.
No es posible actualizar el firmware	**La línea de base no es compatible con Smart Update Tools** Realice una de las acciones siguientes: • Seleccione una línea de base que tenga HP SUM 7.4 o posterior y el firmware de iLO versión 2.30 o posterior. Para obtener información sobre HP SUM, consulte la *Guía de prácticas recomendadas de HP SUM* en: **www.hpe.com/info/hpsum/documentation**. • Edite los perfiles de servidor afectados para que utilicen **Firmware only** (Solo firmware).
	El servidor no tiene la licencia necesaria para Virtual Media Aplique una licencia iLO Advanced en el servidor o aplique una revisión de iLO para la versión 2.30.
Los servidores están encendidos, pero no están configurados para SUT	**Los servidores están encendidos, pero sus perfiles de servidor no están configurados para utilizar Smart Update Tools** Edite los perfiles de servidor afectados y seleccione una opción de actualización de firmware que utilice Smart Update Tools. **NOTA:** Este síntoma también puede aparecer cuando se intenta realizar la actualización del firmware de la infraestructura compartida del receptáculo lógico y del perfil de servidor.
Cualquier fallo al actualizar el firmware y los controladores del sistema operativo	**Algunos componentes no se han implementado** Si falla la implementación de algunos componentes, inicie una sesión en el sistema operativo del servidor de destino y ejecute `gatherlogs.bat o gatherlogs.sh` (utilice el archivo *bat* o *sh*, en función de si el sistema operativo es Windows o Linux, respectivamente). gatherlogs se encuentra en el directorio de almacenamiento provisional del servidor de destino. Para identificar el directorio de almacenamiento provisional, utilice el comando `hpsut—status` desde el directorio de almacenamiento provisional y envíe el informe a HPE para la solución de problemas. Consulte la *Smart Update Tools User Guide* (Guía de usuario de Smart Update Tools) en: **http://www.hpe.com/info/hpsut/docs**.

31.21 Solución de problemas de almacenamiento

31.21.1 El administrador de SAN Brocade Network Advisor (BNA) no puede añadirse

Síntoma	Posible causa y recomendación
Al añadirse el administrador de SAN se produce el error "No SAN manager can be found en the specified location (No se ha encontrado ningún administrador de SAN en la ubicación especificada)."	**BNA o el agente SMI independiente no está instalado en el servidor** • Consulte la documentación del software BNA.
	No se ha configurado una cuenta de administrador de BNA con acceso completo que esté disponible para ser usada por el dispositivo • Consulte la documentación del software BNA.
	No se ha instalado y configurado en el servidor el Common Information Model Object Manager (CIMOM) • Consulte la documentación del software BNA.
	La configuración de SSL de BNA y la configuración de SSL para BNA en el dispositivo no coinciden 1. Utilice el software BNA para comprobar si está activado SSL. Consulte la documentación del software BNA para obtener más información. 2. En la pantalla **SAN Managers** (Administradores de SAN), asegúrese de que la configuración de **Use SSL** (Usar SSL) del dispositivo de BNA coincida con la configuración de SSL del software BNA. Si la configuración de SSL no coincide: a. En el menú principal, seleccione **SAN Managers** (Administradores de SAN) y lleve a cabo una de las siguientes acciones: • En el panel principal, seleccione el BNA y, a continuación, **Actions→Edit** (Acciones > Editar). • Pase el puntero sobre el panel de detalles y haga clic en el **icono de edición**. 3. En **Use SLL** (Usar SSL), cambie el valor para que coincida con la configuración de SSL del software BNA. 4. Haga clic en **OK** (Aceptar) para guardar los cambios.

31.21.2 No se puede establecer conexión con el administrador de SAN Brocade Network Advisor (BNA)

Síntoma	Posible causa y recomendación
No se ha podido establecer una conexión con el administrador de SAN	**El CIMOM no está enlazado con la NIC que se encuentra en la misma subred que el dispositivo** Es necesario enlazar el CIMOM con una NIC en la misma subred que el dispositivo para que el dispositivo se conecte y se comunique con el software de gestión de red de BNA. • Consulte la documentación del software BNA.

31.21.3 Volumen no disponible para el hardware de servidor

Síntoma	Posible causa y recomendación
No se puede acceder al volumen en el servidor	Una posible causa que impide que se pueda acceder a un volumen en el servidor es que no se haya configurado la zona de la SAN o que la configuración no sea correcta. Se recomiendan las soluciones siguientes: **Vuelva a realizar la conexión (en el caso de SAN gestionadas)** 1. En el menú principal, seleccione **Server Profiles** (Perfiles de servidor). 2. En el panel principal, seleccione un perfil de servidor y, a continuación, **Actions→Edit** (Acciones > Editar). 3. En **SAN Storage** (Almacenamiento SAN) localice la conexión de volumen y seleccione **Enable** (Activar). 4. Haga clic en **OK** (Aceptar). **Cree o configure la zona mediante el software de gestión de SAN (si no hay SAN gestionadas)** • Consulte la documentación del administrador de SAN. **Utilizando SAN gestionadas** 1. Asegúrese de que el administrador de SAN y la SAN estén asociados con la red. 2. Asegúrese de que esté activada la distribución automática en zonas. **La distribución automática en zonas no está activada en la SAN** Asegúrese de que la zona se haya configurado manualmente. 1. Consulte la documentación del administrador de SAN.
	Una causa posible de que no se pueda acceder a un volumen del servidor es que los iniciadores del servidor no hayan iniciado sesión en la estructura porque el puerto de interconexión está desactivado. Se recomiendan las soluciones siguientes: **Active el puerto de interconexión en el dispositivo** 1. En el menú principal, seleccione **Interconnects** (Interconexiones). 2. En el panel principal, seleccione una interconexión y **Actions→Edit** (Acciones > Editar). 3. Localice el puerto que desea habilitar y seleccionar **Enable** (Habilitar). 4. Haga clic en **OK** (Aceptar). También puede utilizar la API de REST para realizar esta tarea. **API de REST:** `/rest/interconnects/{id}/ports` Consulte la *Referencia de la API de REST de HPE OneView* para obtener más información. **Vuelva a configurar el grupo de interconexiones lógicas** 1. En el menú principal, seleccione **Logical Interconnects Groups** (Grupos de interconexiones lógicas). 2. En el panel principal, seleccione un grupo de interconexiones lógicas y **Actions→Edit** (Acciones > Editar). 3. Edite los conjuntos de enlaces ascendentes para conectar las redes con los puertos de interconexión deseados. 4. Haga clic en **OK** (Aceptar). 5. Compruebe que el enlace del grupo de interconexiones lógicas se ponga en línea. 6. En el menú principal, seleccione **Logical Interconnects** (Interconexiones lógicas). 7. En el panel principal, seleccione una interconexión lógica y **Actions→Update from group** (Acciones > Actualizar desde el grupo). También puede utilizar la API de REST para realizar esta tarea. **API de REST:** `/rest/logical-interconnect-groups/{id}` y `/rest/logical-interconnects/{id}/compliance` Consulte la *Referencia de la API de REST de HPE OneView* para obtener más información. **Compruebe el cableado** 1. Asegúrese de que el cableado físico está correctamente configurado.

Síntoma	Posible causa y recomendación
	Una posible causa que impide que no se pueda acceder a un volumen del servidor es que no se haya definido la conexión en el perfil de servidor. **Agregue una conexión a una red en el perfil de servidor** 1. En el menú principal, seleccione **Server Profiles** (Perfiles de servidor). 2. En el panel principal, seleccione un perfil de servidor y, a continuación, **Actions→Edit** (Acciones > Editar). 3. En **Connections** (Conexiones), haga clic en **Add Connection** (Agregar conexión). 4. En **Device Type** (Tipo de dispositivo), seleccione **Fibre Channel over Ethernet** (Fibre Channel sobre Ethernet). 5. En **Network** (Red), seleccione una red que esté conectada al sistema de almacenamiento y haga clic en **Add** (Agregar). 6. Haga clic en **OK** (Aceptar).

31.21.4 El volumen es visible desde el sistema de almacenamiento, pero no en el dispositivo

Síntoma	Posible causa y recomendación
El volumen no está en un estado normal	Una causa posible de que un volumen no esté visible en el dispositivo es que el volumen se haya trasladado a un pool de almacenamiento no gestionado por el dispositivo. **Mueva el volumen a un pool gestionado por el dispositivo y actualice el volumen por medio del software del sistema de almacenamiento** • Consulte la documentación del sistema de almacenamiento. **Incluir en la gestión del dispositivo el pool de almacenamiento en el que reside el volumen** **NOTA:** Si Adaptive Optimization movió el volumen, Hewlett Packard Enterprise recomienda incluir todos los pools que podría utilizar Adaptive Optimization en la gestión del dispositivo. Esto garantizará que el volumen siga estando disponible en el dispositivo en caso de que lo mueva la optimización adaptable. 1. En el menú principal, seleccione **Storage Pools** (Pools de almacenamiento) y lleve a cabo una de las siguientes acciones: • Haga clic en **+ Add storage pool** (+ Agregar pool de almacenamiento) en el panel principal. • Seleccione **Actions→Add** (Acciones > Agregar). 2. En **Storage System** (Sistema de almacenamiento), seleccione el sistema de almacenamiento que contiene los pools de almacenamiento que desea agregar. 3. En **Storage Pool** (Pool de almacenamiento), seleccione el pool de almacenamiento que desea agregar. 4. Haga clic en **Add** (Agregar) para agregar el pool de almacenamiento, o haga clic en **Add +** (Agregar +) para agregar otro. También puede utilizar la API de REST para realizar esta tarea. **API de REST:** `/rest/storage-pools` Consulte la *Referencia de la API de REST de HPE OneView* para obtener más información.

31.21.5 Fallo del puerto de destino

Síntoma	Posible causa y recomendación
El puerto de destino está en estado de fallo	Una posible causa de error del puerto de destino es que la red real y la esperada no coincidan. Algunas de las posibles causas son las siguientes: **Debe actualizarse la red esperada en el dispositivo** 1. En el menú principal, seleccione **Storage Systems** (Sistemas de almacenamiento). 2. En el panel principal, seleccione un sistema de almacenamiento y, a continuación, **Actions→Edit** (Acciones > Editar). 3. Para el puerto cambie la **Expected Network** (Red esperada) de forma que coincide con la **Actual Network** (Red real). 4. Haga clic en **OK** (Aceptar). También puede utilizar la API de REST para realizar esta tarea. **API de REST:** `/rest/storage-systems/{id}` Consulte la *Referencia de la API de REST de HPE OneView* para obtener más información. **El receptáculo que se ha conectado físicamente al sistema de almacenamiento no se ha agregado al dispositivo (Direct attach)** • Utilice la pantalla **Enclosures** (Receptáculos) para agregar el receptáculo al dispositivo. También puede utilizar la API de REST para realizar esta tarea. **REST API:** `/rest/enclosures` Consulte la *Referencia de la API de REST de HPE OneView* para obtener más información. **El cableado físico no se ha configurado correctamente (Fabric attach)** • Compruebe que el cableado entre el sistema de almacenamiento y el conmutador SAN esté correctamente configurado. **El cableado físico no se ha configurado correctamente (Direct attach)** • Compruebe que el cableado entre el sistema de almacenamiento y las interconexiones del receptáculo estén correctamente configuradas.
	Ha fallado el puerto en el dispositivo • Examine el hardware del sistema de almacenamiento. Lleve a cabo las reparaciones necesarias.

31.21.6 La operaciones de zona fallan en el administrador de SAN Cisco

Síntoma	Posible causa y recomendación
Las operaciones de zona fallan en el administrador de SAN Cisco	**El servicio `snmpd` se ha bloqueado** • Consulte el registro del administrador de SAN desde el software del administrador de SAN para comprobar si el servicio `snmpd` se ha bloqueado. El servicio `snmpd` puede bloquearse debido a que el firmware del administrador de SAN se ha quedado obsoleto. **Actualice el firmware del administrador de SAN a la versión más reciente** 1. Siga las instrucciones del fabricante para actualizar el firmware del administrador de SAN. 2. Vuelva a intentar la operación de zona en el dispositivo.

31.21.7 El estado del puerto del sistema de almacenamiento no es el deseado

El estado del puerto del sistema de almacenamiento está en un estado **failing over** (por error)

Causa

El puerto está fuera de línea y está realizando la conmutación por error al puerto asociado.

Action (Acción)

Espere a que cambie el estado.

El estado del puerto del sistema de almacenamiento está en un estado **failed over** (erróneo)

Causa

El puerto está fuera de línea y ha conmutado por error al puerto asociado.

Action (Acción)

Resuelva el problema del puerto en el sistema de almacenamiento.

Compruebe la conectividad con la infraestructura.

El estado del puerto del sistema de almacenamiento está en un estado **failed** (error)

Causa

El puerto está desactivado fuera de línea y no puede conmutar por error al puerto asociado.

Action (Acción)

Compruebe el estado y la configuración de los dos puertos de almacenamiento.

Compruebe el cableado u otros problemas de infraestructura.

El estado del puerto del sistema de almacenamiento está en un estado **recovering** (en recuperación)

Causa

El puerto está en línea y en el proceso de vuelta a su estado normal.

Action (Acción)

Espere a que cambie el estado.

El estado del puerto del sistema de almacenamiento está en un estado **partner port failed over** (puerto de socio erróneo)

Causa

El puerto asociado ha conmutado por error y el puerto está gestionando el tráfico del puerto asociado.

Action (Acción)

Resuelva el problema del puerto asociado en el sistema de almacenamiento.

Compruebe la conectividad del puerto con la infraestructura.

El estado del puerto del sistema de almacenamiento está en un estado **partner failed** (error de socio)

Causa

El puerto asociado ha fallado y la operación de conmutación por error no se ha realizado correctamente.

Action (Acción)

Compruebe el estado y la configuración de los dos puertos de almacenamiento.

Compruebe si hay algún problema con la infraestructura o el cableado.

31.22 Solución de problemas de cuentas de usuario

31.22.1 Privilegios incorrectos

Los usuarios deben tener privilegios de visualización (como mínimo) para un objeto gestionado para ver dicho objeto en la interfaz de usuario.

Síntoma

No se puede ver información específica de recursos o realizar una tarea de recursos

Causa

El rol que tiene asignado no tiene los privilegios correctos.

Action (Acción)

Solicite un rol distinto o un rol adicional al administrador de infraestructuras para llevar a cabo su trabajo.

31.22.2 No se puede modificar la cuenta de usuario local

Síntoma

No puede crear, editar o eliminar una cuenta de usuario local.

Autorización incorrecta

Causa

No tiene la autorización apropiada o ha introducido parámetros no válidos.

Action (Acción)

1. Inicie sesión en el dispositivo como administrador de infraestructuras.
2. Intente agregar, editar o eliminar la cuenta de usuario de nuevo.

Problemas en la red

Action (Acción)

1. Inicie sesión en el dispositivo como administrador de infraestructuras.
2. Consulte «El dispositivo no puede acceder a la red»
3. Intente agregar, editar o eliminar la cuenta de usuario de nuevo.

Hay que actualizar el certificado del dispositivo

Causa

El certificado del dispositivo no es válido o ha caducado.

Action (Acción)

1. Inicie sesión en el dispositivo como administrador de infraestructuras.
2. Adquiera un nuevo certificado de dispositivo.
3. Actualice la página del explorador.
4. Acepte el certificado nuevo.
5. Agregue la cuenta de usuario.
6. Intente agregar, editar o eliminar la cuenta de usuario de nuevo.

31.22.3 No se puede eliminar la cuenta de usuario local

Síntoma

La instalación falla con el código de error 500.

Action (Acción)

1. Lleve a cabo la siguiente llamada de la API de REST para modificar la cuenta de usuario a eliminar:

   `Escriba https://{appl}/rest/users`
2. Intente eliminar la cuenta de usuario de nuevo.

31.22.4 Usuario o grupo no autenticado

Al iniciar sesión en el dispositivo, cada usuario se autentica mediante el servicio de autenticación, que confirma el nombre de usuario y la contraseña. La pantalla **Edit Authentication** (Editar autenticación) le permite configurar las opciones de autenticación del dispositivo; los valores predeterminados se rellenan inicialmente durante la configuración inicial del dispositivo.

Síntoma

No se puede configurar un usuario o grupo del directorio

Causa

Las opciones de autenticación no son correctas

Action (Acción)

Para configurar las opciones de autenticación:

1. En la pantalla **Users** (Usuarios), haga clic en **Add Directory User or Group** (Agregar usuario o grupo de directorios).
2. Haga clic en **Add a directory** (Agregar un directorio).
3. En la pantalla **Edit Authentication** (Editar autenticación), haga clic en **Add directory** (Agregar directorio).
4. Proporcione la información solicitada.
5. Haga clic en **OK** (Aceptar).

31.22.5 No se acepta la clave pública del usuario

Síntoma	Posible causa y recomendación
La clave pública del usuario no funciona o no se acepta	**Los caracteres ocultos introducidas durante una operación de copiar y pegar cambian el código de la clave** • Introduzca la clave de nuevo, teniendo cuidado de evitar que se añadan caracteres especiales en la clave al pegarla en el campo de clave pública. • Solo se admiten claves RSA.

31.22.6 Servicio de directorio no disponible

Síntoma

El dispositivo no puede acceder al servicio de directorio.

Solución 1

No se puede acceder al servidor del servicio de directorio.

Causa

El servidor de servicio de directorio o la red están caídos.

Action (Acción)

1. en la dirección IP o el nombre de host del servidor de directorio para determinar si está en línea.
2. Compruebe que la red del dispositivo funciona correctamente.
3. Póngase en contacto con el administrador del servicio de directorio para determinar si el servidor está fuera de servicio.

Solución 2

Causa

Errores de configuración no permiten conectar con el servicio de directorio

Action (Acción)

1. Compruebe que el nombre del servicio de directorio sea exclusivo y que se haya introducido correctamente. No se aceptan nombres duplicados.
2. Compruebe que el **tipo de directorio** sea correcto.
3. Asegúrese de que los campos **Base DN** (DN base) para OpenLDAP, **User naming attribute** (Atributo de nomenclatura de usuario) y **Organizational unit** (Unidad organizacional) sean correctos.
4. Compruebe que las credenciales del administrador de servicios de directorio de autenticación sean correctas.
5. Compruebe que el grupo esté configurado en el servicio de directorio.
6. Asegúrese de que el rol asignado al grupo sea correcta.

31.22.7 No se puede agregar el servicio de directorio

Síntoma

No puede agregar un servicio de directorio al dispositivo.

Solución 1

Causa

Un problema externo desconectó el anfitrión del servidor de directorio.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Compruebe que la configuración del host del servicio de directorio es correcta.
3. Ejecute el comando `ping` localmente sobre la dirección IP o el nombre de host del servidor de directorio para determinar si está en línea.

4. Compruebe que el puerto para las comunicaciones LDAP con el servicio de directorio es el puerto 636.
5. Compruebe que el puerto que está utilizando para las comunicaciones (el predeterminado es el 636) no está bloqueado por ningún cortafuegos.

   Consulte «Puertos necesarios para HPE OneView».
6. Compruebe que la red del dispositivo funciona correctamente.
7. Compruebe que el dispositivo está funcionando correctamente y que hay suficientes recursos.

Solución 2

Causa

El anfitrión del servidor de directorio rechaza la autenticación del dispositivo porque el certificado ha caducado.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Compruebe que el nombre de usuario y la contraseña son correctos.

   Póngase en contacto con el proveedor del servicio de directorio para asegurarse de que las credenciales son correctas.
3. Vuelva a adquirir e instalar el certificado del host del servicio de directorio.

Solución 3

Causa

El certificado no tiene el formato x509 válido.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Corrija la configuración y vuelva a intentarlo.
3. Si es necesario, vuelva a adquirir e instalar el certificado del host del servicio de directorio.
4. Póngase en contacto con el proveedor del servicio de directorio para asegurarse de que las credenciales son correctas.

Solución 4

Causa

El certificado no contiene la extensión de uso de claves x509v3.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Asegúrese de que el certificado contiene la extensión de uso de claves.
3. Si es necesario, vuelva a adquirir e instalar el certificado del host del servicio de directorio.

Solución 5

Causa

El anfitrión del servidor de directorio no puede autenticar el dispositivo porque las credenciales no son válidas.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras

2. Compruebe que el nombre de usuario y la contraseña son correctos.
3. Compruebe que la información de contexto de búsqueda es exacta; es posible que esté intentando acceder a otra cuenta u otro grupo.
4. Vuelva a adquirir e instalar el certificado del host del servicio de directorio.
5. Póngase en contacto con el proveedor del servicio de directorio para asegurarse de que las credenciales son correctas.

31.22.8 No se puede agregar un servidor para un servicio de directorio

Síntoma

No puede configurar un servidor para el servicio de directorio.

Solución 1

Causa

El dispositivo ha perdido la conexión con el servicio de directo, pero esa conexión se ha perdido.

Action (Acción)

1. Compruebe que la configuración del host del servicio de directorio es correcta.
2. Compruebe que se utiliza el puerto correcto para el servicio de directorio.
3. Compruebe que el puerto que está utilizando para las comunicaciones (el predeterminado es el 636) no está bloqueado por ningún cortafuegos.

   Consulte «Puertos necesarios para HPE OneView».
4. Ejecute el comando `ping` localmente sobre la dirección IP o el nombre de hos't del servicio de directorio para determinar si está en línea.
5. Compruebe que la red del dispositivo funciona correctamente.
6. [Conditionalized for TBunsupported] Si el dispositivo está alojado en una máquina virtual, determine que funciona correctamente y que hay suficientes recursos.

Solución 2

Causa

Al iniciar sesión en el servidor para el servicio de directorio se produce un error de autenticación.

1. Compruebe que el nombre de usuario y la contraseña son correctos.
2. Vuelva a adquirir e instalar el certificado del host del servicio de directorio.
3. Póngase en contacto con el proveedor del servicio de directorio para asegurarse de que las credenciales son correctas.

Solución 3

Causa

Hay parámetros incorrectos cuando se configuró el servicio de directorio.

Action (Acción)

1. Compruebe que el nombre del servicio de directorio sea exclusivo y que se haya introducido correctamente. No se aceptan nombres duplicados.
2. Compruebe que el **tipo de directorio** sea correcto.
3. Asegúrese de que los campos **Base DN** (DN base) para OpenLDAP, **User naming attribute** (Atributo de nomenclatura de usuario) y **Organizational unit** (Unidad organizacional) sean correctos.

4. Compruebe que las credenciales del administrador de servicios de directorio de autenticación sean correctas.
5. Compruebe que el grupo esté configurado en el servicio de directorio.

31.22.9 No se puede agregar un grupo de directorios

Síntoma

El grupo de directorios no se ha podido agregar como grupo en el dispositivo.

Solución 1

Causa

El directorio de autenticación y el grupo especificados ya existen. Los grupos deben ser únicos.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Vuelva a asignar el grupo actual a otro rol o haga que el grupo sea único.

Solución 2

Causa

Un problema externo desconectó el anfitrión del servidor de directorio.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Compruebe que la configuración del host del servicio de directorio es correcta.
3. Compruebe que se utiliza el puerto correcto para el servicio de directorio.
4. Compruebe que el puerto que está utilizando para las comunicaciones (el predeterminado es el 636) no está bloqueado por ningún cortafuegos.

   Consulte «Puertos necesarios para HPE OneView».
5. Ejecute el comando `ping` localmente en la dirección IP o el nombre de host del servicio de directorio para determinar si está en línea.
6. Compruebe que la red del dispositivo funciona correctamente.
7. Si el dispositivo está alojado en una máquina virtual, compruebe que la máquina virtual está funcionando correctamente y que existen recursos suficientes asignados a ella.

Solución 3

Causa

Problemas con la autenticación no han permitido que el dispositivo inicie sesión en el servicio de directorios.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras.
2. Compruebe que el nombre de usuario y la contraseña son correctos.
3. Vuelva a adquirir e instalar el certificado del host del servicio de directorio.
4. Póngase en contacto con el proveedor del servicio de directorio para asegurarse de que las credenciales son correctas.

31.22.10 No se encuentra el grupo de directorios

Síntoma

No se puede hallar un grupo especificado en el servicio de directorios de autenticación.

Solución 1

Causa

O bien el grupo no está configurado en el servicio de directorios de autenticación o los parámetros de búsqueda contenían un error.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Compruebe las credenciales del servicio de directorio de autenticación.
3. Compruebe que el servicio de directorio esté operativo.
4. Compruebe el nombre del grupo.
5. Póngase en contacto con el administrador del servicio de directorio para comprobar que la cuenta del grupo está configurada en el servicio de directorio.
6. Intente volver a buscar el grupo.

   Para obtener más información, consulte «Acerca de la autenticación en servicios de directorio».

Solución 2

Causa

El tipo de directorio no se ha especificado correctamente. Por ejemplo, puede especificarse un servicio de Active Directory como `OpenLDAP`.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Compruebe que la configuración del servicio de directorio es correcta.

Solución 3

Causa

La búsqueda indicada del servicio de directorios de autenticación no contiene ningún grupo.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Compruebe la configuración del servidor de directorio.
3. Para OpenLDAP, asegúrese de que el usuario del servidor de directorio tiene privilegios de lectura (`rscdx`) para que HPE OneView pueda leer los resultados de la búsqueda.
4. Para OpenLDAP, agregue todos los contextos de búsqueda para recuperar el grupo o los grupos que desea. Utilice el botón **Add** (Agregar) para generar varias unidades organizacionales, con las que especificar `UID` o `CN`.

Solución 4

Causa

Error al acceder a los grupos de directorios. No se ha podido contactar con los servidores de servicio de directorio.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Compruebe la configuración del servidor de directorio.
3. Compruebe la conexión con el host del servidor de directorio.
4. Para OpenLDAP, agregue todos los contextos de búsqueda para recuperar el grupo o los grupos que desea. Utilice el botón **Add** (Agregar) para generar varias unidades organizacionales, con las que especificar `UID` o `CN`.

Solución 5

Causa

Un problema externo ha evitado que el dispositivo llegue al servidor configurado para el servicio de directorios.

Action (Acción)

1. Inicie sesión como administrador de infraestructuras
2. Compruebe la conexión con el host del servidor de directorio. Consulte «No se puede agregar un servidor para un servicio de directorio».
3. Compruebe la configuración del servidor de directorio.

32 Asistencia y otros recursos

32.1 Acceso al soporte de Hewlett Packard Enterprise

- Para obtener asistencia en tiempo real, vaya a la página web Contact Hewlett Packard Enterprise Worldwide (Póngase en contacto con Hewlett Packard Enterprise en todo el mundo):

  www.hpe.com/assistance

- Para acceder a la documentación y los servicios de soporte técnico, vaya a la página web del centro de soporte de Hewlett Packard Enterprise:

  www.hpe.com/support/hpesc

Información para recopilar

- Número de registro de soporte técnico (si corresponde)
- Nombre del producto, modelo o versión y número de serie
- Nombre y versión del sistema operativo
- Versión de firmware
- Mensajes de error
- Informes y registros específicos del producto
- Productos o componentes adicionales
- Productos o componentes de otros fabricantes

32.2 Acceso a las actualizaciones

- Algunos productos de software proporcionan un mecanismo para acceder a las actualizaciones de software a través de la interfaz del producto. Revise la documentación del producto para identificar el método recomendado de actualización del software.
- Para descargar actualizaciones del producto, vaya a cualquiera de las páginas web siguientes:
  - Página **Get connected with updates from HPE (Conéctese con las actualizaciones de HPE)** del centro de soporte de Hewlett Packard Enterprise:

    www.hpe.com/support/e-updates

  - Página web de Software Depot:

    www.hpe.com/support/softwaredepot

- Para ver y actualizar sus concesiones, así como para vincular sus contratos y garantías con su perfil, vaya a la página **More Information on Access to Support Materials** (Más

información sobre cómo acceder a los materiales de soporte) del centro de soporte de Hewlett Packard Enterprise:

www.hpe.com/support/AccessToSupportMaterials

IMPORTANTE: El acceso a algunas actualizaciones podría requerir la concesión de producto cuando se accede a través del centro de soporte de Hewlett Packard Enterprise. Debe disponer de una cuenta HP Passport configurada con las concesiones correspondientes.

32.3 Páginas web

Página web	Link
Biblioteca de información de Hewlett Packard Enterprise	**www.hpe.com/info/enterprise/docs**
Centro de soporte de Hewlett Packard Enterprise	**www.hpe.com/support/hpesc**
Contacto con Hewlett Packard Enterprise en todo el mundo	**www.hpe.com/assistance**
OneView Docs	**www.hpe.com/info/oneview/docs**
Servicio de suscripción/alertas de soporte	**www.hpe.com/support/e-updates**
Software Depot	**www.hpe.com/support/softwaredepot**
Reparaciones del propio cliente	**www.hpe.com/support/selfrepair**
Documento de preguntas frecuentes de soporte remoto para HPE OneView	**Documento de soporte remoto**
Matriz de compatibilidad de dispositivos de almacenamiento de Single Point of Connectivity Knowledge (SPOCK)	**www.hpe.com/storage/spock**
Guías de usuario de HPE Virtual Connect Guías de referencia de la línea de comandos de HPE Virtual Connect	**http://www.hpe.com/info/virtualconnect**
Almacenamiento HPE 3PAR StoreServ	**http://www.hpe.com/info/storage**
HPE Integrated Lights-Out	**http://www.hpe.com/info/ilo**
Cajas de protección HPE BladeSystem	**http://www.hpe.com/servers/bladesystem**
Páginas web de hardware de servidor HPE ProLiant	• Información general: **www.hpe.com/info/servers** • Blades de servidor de la serie BL: **http://www.hpe.com/info/blades** • Servidores de montaje en bastidor de la serie DL: **http://www.hpe.com/servers/dl**
Documentos técnicos e informes analíticos de almacenamiento	**www.hpe.com/storage/whitepapers**

32.4 Reparaciones del propio cliente

El programa de reparaciones del propio cliente (CSR) de Hewlett Packard Enterprise le permite reparar su producto. Si es necesario reemplazar una pieza incluida en el programa CSR, se le enviará directamente para que pueda instalarla cuando le resulte más cómodo. Algunas piezas no entran en el programa CSR. El servicio técnico autorizado de Hewlett Packard Enterprise determinará si una reparación entra en el programa CSR.

Para obtener más información sobre el programa CSR, póngase en contacto con el proveedor de servicios local o vaya a la página web del CSR:

www.hpe.com/support/selfrepair

32.5 Comentarios sobre la documentación

Hewlett Packard Enterprise se compromete a proporcionar documentación que se adapte a sus necesidades. Para ayudarnos a mejorar la documentación, envíe cualquier error, sugerencia o comentario a Comentarios sobre la documentación (**docsfeedback@hpe.com**). Cuando envíe sus comentarios, incluya el título del documento, el número de referencia, la edición y la fecha de publicación, que se encuentran en la portada del documento. Para el contenido de ayuda en línea, incluya el nombre y la versión del producto, la edición y la fecha de publicación de la ayuda, que se encuentran en la página de avisos legales.

A Uso de la consola del dispositivo virtual

A.1 Uso de la consola del dispositivo virtual

La consola del dispositivo virtual tiene una interfaz de explorador restringida que admite lo siguiente:

- Configuración de la red del dispositivo en entornos sin DHCP
- Solicitudes de restablecimiento de contraseña para la cuenta del administrador
- Diagnóstico avanzado para representantes autorizados de soporte técnico

Utilice la consola del dispositivo virtual para acceder a él y configurar su red por primera vez. La consola del dispositivo virtual permite realizar el arranque de un dispositivo en la red en entornos sin DHCP. La consola del dispositivo virtual no está pensada para sustituir por completo al explorador.

La consola del dispositivo virtual inicia una sesión del explorador; este se muestra en pantalla completa y no permite agregar fichas. No se puede realizar ninguna operación que requiera seleccionar un archivo en un cuadro de diálogo, como cargar actualizaciones de software y lotes de firmware (SPP). Solo está habilitada la navegación básica, como las operaciones de avanzar y retroceder.

Tabla 17 Combinaciones de teclas de la consola del dispositivo virtual

Combinación de teclas		Función
Alt-←	(**Alt** y flecha izquierda)	Navegar hacia atrás
Alt-→	(**Alt** y flecha derecha)	Navegar hacia adelante
Ctrl-+	(**Ctrl** y signo más)	Acercar
Ctrl--	(**Ctrl** y guion)	Alejar
Ctrl-0	(**Ctrl** y cero)	Restablecer zoom
Ctrl-F		Buscar
Ctrl-R o **F5**		Recargar/Actualizar
Ctrl-Alt-Retroceso		Reiniciar la interfaz del explorador

B Ejemplos de secuencias de comandos de copia de seguridad y restauración

B.1 Secuencia de comandos de copia de seguridad de ejemplo

Como alternativa al uso de **Settings→Actions→Create backup** (Configuración > Acciones > Crear copia de seguridad) desde la interfaz de usuario del dispositivo, puede escribir y ejecutar una secuencia de comandos para crear y descargar automáticamente un archivo de copia de seguridad del dispositivo.

El Ejemplo 14, «Secuencia de comandos backup.ps1 de ejemplo» proporciona una secuencia de comandos de PowerShell de ejemplo que utiliza llamadas REST para crear y descargar un archivo de copia de seguridad del dispositivo. Copie y pegue esta secuencia de comandos de ejemplo en un archivo en un sistema Windows que ejecute PowerShell versión 3.0, y edite la secuencia de comandos para personalizarla para su entorno. Consulte la ayuda en línea de la API de REST para obtener más información sobre las API de REST.

Puede programar la secuencia de comandos para que se ejecute automáticamente en modo interactivo o por lotes de forma periódica (Hewlett Packard Enterprise recomienda copias de seguridad diarias). Solo un usuario con privilegios de administrador de copia de seguridad o de infraestructuras puede ejecutar la secuencia de comandos de forma interactiva.

- Para ejecutar la secuencia de comandos de manera interactiva, no incluya ningún parámetro. La secuencia de comandos le pide que introduzca el nombre de host del dispositivo, el nombre de usuario y la contraseña del dispositivo, y el nombre de un archivo para almacenar estos parámetros para las ejecuciones por lotes. Introduzca el nombre y la contraseña de un usuario con el rol administrador de copias de seguridad o administrador de infraestructuras. El nombre de usuario y la contraseña se almacenan cifrados.

  Hewlett Packard Enterprise recomienda ejecutar la secuencia de comandos de manera interactiva la primera vez. Después, puede programar la secuencia de comandos para que se ejecute automáticamente en segundo plano mediante el archivo de parámetros creado en la primera ejecución.

- Para ejecutar la secuencia de comandos por lotes, especifique el nombre del archivo que contiene los parámetros de la línea de comandos.

Hewlett Packard Enterprise recomienda instalar cURL con la opción SSL para mejorar el rendimiento. La secuencia de comandos de ejemplo funciona sin cURL, pero puede tardar varias horas en descargar un archivo de copia de seguridad grande. Para descargar cURL, consulte:

http://curl.haxx.se/download.html

NOTA: También podría ser necesario instalar Microsoft Visual C++ Redistributable, el archivo `MSVCR100.dll`, disponible aquí:

- 64 bits: **http://www.microsoft.com/download/en/details.aspx?id=14632**
- 32 bits: **http://www.microsoft.com/download/en/details.aspx?id=5555**

Asegúrese de que la variable de entorno PATH incluya la ruta de cURL.

Secuencia de comandos de ejemplo

La secuencia de comandos de ejemplo hace lo siguiente para crear y descargar un archivo de copia de seguridad:

1. Llama a `queryfor-credentials()` para obtener el nombre de host, el nombre de usuario y la contraseña del dispositivo, pidiéndoselos al usuario u obteniendo los valores de un archivo.
2. Llama a `login-appliance()` para emitir una solicitud REST para obtener un ID de sesión utilizado para autorizar llamadas REST de copia de seguridad.

3. Llama a `backup-appliance()` para emitir una solicitud REST para iniciar una copia de seguridad.
4. Llama a `waitFor-completion()` para emitir solicitudes REST para preguntar sobre el estado de la copia de seguridad hasta que se complete la copia de seguridad.
5. Llama a `get-backupResource()` para emitir una solicitud REST para obtener el URI de descarga.
6. Llama a `download-backup()` para emitir una solicitud REST para descargar la copia de seguridad.

Ejemplo 14 Secuencia de comandos backup.ps1 de ejemplo

```
# (C) Copyright 2012-2014 Hewlett Packard Enterprise Development LP
##################################################################################################################################
# Name:     backup.ps1
# Usage:    {directory}\backup.ps1 or {directory}\backup.ps1 filepath
# Parameter: $filepath: optional, uses the file in that path as the login credentials. ie: host address, username,
#           password, and, optionally, the Active Directory domain name
# Purpose:  Runs the backup function on the appliance and downloads it onto your machine's drive
#           in current user's home directory
# Notes:    To improve performance, this script uses the curl command if it is installed.  The curl command
must
#           be installed with the SSL option.
#           Windows PowerShell 3.0 must be installed to run the script
##################################################################################################################################


#tells the computer that this is a trusted source that we are connecting to (brute force, could be refined)
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }


$global:interactiveMode = 0


# The scriptApiVersion is the default Api version (if the appliance supports this level
# or higher).  This variable may be changed if the appliance is at a lower Api level.
$global:scriptApiVersion = 3
# Using this Api version or greater requires a different interaction when creating a backup.
Set-Variable taskResourceV2ApiVersion -option Constant -value 3


try {
  #this log must be added if not already on your computer
  New-EventLog -LogName Application -Source backup.ps1 -ErrorAction stop
}
catch [System.Exception]
{
  #this is just to keep the error "already a script" from showing up on the screen if it is already created
}


##### Querying user for login info #####
function queryfor-credentials ()
{
  <#
        .DESCRIPTION
            Gathers information from User if in manual entry mode (script ran with zero arguments) or
            runs silently and gathers info from specified path (script ran with 1 argument)

        .INPUTS
            None, this function does not take inputs.

        .OUTPUTS
            Returns an object that contains the login name, password, hostname and
            ActiveDirectory domain to connect to.

        .EXAMPLE
            $variable = queryfor-credentials #runs function, saves json object to variable.
    #>


  if ($args[0] -eq $null)
  {


    Write-Host "Enter appliance name (https://ipaddress)"
    $appliance = Read-Host


    # Correct some common errors
    $appliance = $appliance.Trim().ToLower()
    if (!$appliance.StartsWith("https://"))
    {
       if ($appliance.StartsWith("http://"))
       {
          $appliance = $appliance.Replace("http","https")
       } else {
          $appliance = "https://" + $appliance
       }
    }


    Write-Host "Enter username"
    $username = Read-Host -AsSecureString | ConvertFrom-SecureString


    Write-Host "Enter password"
    $SecurePassword = Read-Host -AsSecureString | ConvertFrom-SecureString


    Write-Host "If using Active Directory, enter the Active Directory domain"
    Write-Host "  (Leave this field blank if not using Active Directory.)"
```

```
    $ADName = Read-Host


    Write-Host "Would you like to save these credentials to a file? (username and password encrypted)"
    $saveQuery = Read-Host


    $loginVals = [pscustomobject]@{ userName = $username; password = $SecurePassword;
                 hostname = $appliance; authLoginDomain = $ADName }
    $loginJson = $loginVals | convertTo-json


    $global:interactiveMode = 1


    if ($saveQuery[0] -eq "y") #enters into the mode to save the credentials
    {
      Write-Host "Enter file path and file name to save credentials  (example: C:\users\bob\machine1.txt)"
      $storagepath = Read-Host


      try
      {
        $loginJson | Out-File $storagepath -NoClobber -ErrorAction stop
      }
      catch [System.Exception]
      {
        Write-Host $_.Exception.message
        if ($_.Exception.getType() -eq [System.IO.IOException]) # file already exists throws an IO exception
        {
          do
          {
            Write-Host "Overwrite existing credentials for this machine?"
            [string]$overwriteQuery = Read-Host
            if ($overwriteQuery[0] -eq 'y')
            {
              $loginJson | Out-File $storagepath -ErrorAction stop
              $exitquery = 1
            }
            elseif ($overwriteQuery[0] -eq 'n')
            {
              $exitquery = 1
            }
            else
            {
              Write-Host "Please respond with a y or n"
              $exitquery = 0
            }


          } while ($exitquery -eq 0)
        }
        else
        {
          Write-Host "Improper filepath or no permission to write to given directory"
          Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Improper filepath,
$storagepath " $_.Exception.message
          return
        }
      }


      $savedLoginJson = Get-Content $storagepath


      Write-Host "Run backup?"


      $continue = 0
      do
      {
        $earlyExit = Read-Host
        if ($earlyExit[0] -eq 'n')
        {
          return
        }
        elseif ($earlyExit[0] -ne 'y')
        {
          Write-Host "Please respond with a y or n"
        }
        else
        {
          $continue = 1
        }


      } while ($continue -eq 0)


    }
    else
    {
      return $loginJson
```

```
    }
  }
  elseif ($args.count -ne 1)
  {
    Write-Host "Incorrect number of arguments, use either filepath parameter or no parameters."
    return


  }
  else
  {
    foreach ($arg in $args)
    {
      $storagepath = $arg
    }
    try
    {
      $savedLoginJson = Get-Content $storagepath -ErrorAction stop
    }
    catch [System.Exception]
    {
      Write-Host "Login credential file not found. Please run script without arguments to access manual entry
mode."
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Login credential file not
found. Please run script without arguments to access manual entry mode."
      return


    }
  }
  return $savedloginJson
}


##### getApiVersion: Get X_API_Version #####
function getApiVersion ([int32] $currentApiVersion,[string]$hostname)
{
  <#
        .DESCRIPTION
            Sends a web request to the appliance to obtain the current Api version.
     Returns the lower of: Api version supported by the script and Api version
     supported by the appliance.

        .PARAMETER currentApiVersion
     Api version that the script is currently using

        .PARAMETER hostname
            The appliance address to send the request to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the new active Api version


        .EXAMPLE
            $global:scriptApiVersion = getApiVersion()
    #>


  # the particular Uri on the Appliance to reqest the Api Version
  $versionUri = "/rest/version"


  # append the Uri to the end of the IP address to obtain a full Uri
  $fullVersionUri = $hostname + $versionUri


  # use setup-request to issue the REST request api version and get the response
  try
  {
    $applianceVersionJson = setup-request -Uri $fullVersionUri -method "GET" -accept "application/json"
-contentType "application/json"
    if ($applianceVersionJson -ne $null)
    {
      $applianceVersion = $applianceVersionJson | convertFrom-Json
      $currentApplianceVersion = $applianceVersion.currentVersion
      if ($currentApplianceVersion -lt $currentApiVersion)
      {
        return $currentApplianceVersion
      }
      return $currentApiVersion
    }
  }
  catch [System.Exception]
  {
    if ($global:interactiveMode -eq 1)
    {
      Write-Host $error[0].Exception.Message
    }
    else
    {
```

```
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message

    }
  }
}


##### Sending login info #####
function login-appliance ([string]$username,[string]$password,[string]$hostname,[string]$ADName)
{
  <#
        .DESCRIPTION
            Attempts to send a web request to the appliance and obtain an authorized sessionID.

        .PARAMETER username
            The username to log into the remote appliance

        .PARAMETER password
            The correct password associated with username

        .PARAMETER hostname
            The appliance address to send the request to (in https://{ipaddress} format)

        .PARAMETER ADName
            The Active Directory name (optional)


        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the response body containing the needed session ID.


        .EXAMPLE
            $authtoken = login-appliance $username $password $hostname $ADName
    #>


  # the particular Uri on the Appliance to reqest an "auth token"
  $loginUri = "/rest/login-sessions"


  # append the Uri to the end of the IP address to obtain a full Uri
  $fullLoginUri = $hostname + $loginUri
  # create the request body as a hash table, then convert it to json format
  if ($ADName)
  {
    $body = @{ userName = $username; password = $password; authLoginDomain = $ADName } | convertTo-json
  }
  else  # null or empty
  {
    $body = @{ userName = $username; password = $password } | convertTo-json
  }


  # use setup-request to issue the REST request to login and get the response
  try
  {
    $loginResponse = setup-request -Uri $fullLoginUri -method "POST" -accept "application/json" -contentType
"application/json" -Body $body
    if ($loginResponse -ne $null)
    {
      $loginResponse | convertFrom-Json
    }
  }
  catch [System.Exception]
  {
    if ($global:interactiveMode -eq 1)
    {
      Write-Host $error[0].Exception.Message
    }
    else
    {
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message

    }
  }
}


##### Executing backup ######
function backup-Appliance ([string]$authValue,[string]$hostname)
{
  <#
        .DESCRIPTION
            Gives the appliance the command to start creating a backup

        .PARAMETER authValue
            The authorized sessionID given by login-appliance

        .PARAMETER hostname
            The location of the appliance to connect to (in https://{ipaddress} format)
```

```
        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The task Resource returned by the appliance, converted to a hashtable object

        .EXAMPLE
            $taskResource = backup-Appliance $sessionID $hostname
    #>

  # append the REST Uri for backup to the IP address of the Appliance
  $bkupUri = "/rest/backups/"
  $fullBackupUri = $hostname + $bkupUri


  # create a new webrequest and add the proper headers (new header, auth, is needed for authorization
  # in all functions from this point on)
  try
  {
    if ($global:scriptApiVersion -lt $taskResourceV2ApiVersion)
    {
     $taskResourceJson = setup-request -Uri $fullBackupUri -method "POST" -accept "application/json" -contentType
 "application/json" -authValue $authValue
    }
    else
    {
      $taskUri = setup-request -Uri $fullBackupUri -method "POST" -accept "application/json" -contentType
"application/json" -authValue $authValue -returnLocation $true
      if ($taskUri -ne $null)
      {
        $taskResourceJson = setup-request -Uri $taskUri -method "GET" -accept "application/json" -contentType
"application/json" -authValue $authValue
      }
    }
    if ($taskResourceJson -ne $null)
    {
      return $taskResourceJson | ConvertFrom-Json
    }
  }
  catch [System.Exception]
  {
    if ($global:interactiveMode -eq 1)
    {
      Write-Host $error[0].Exception.Message
    }
    else
    {
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message

    }
  }
}


##### Polling to see if backup is finished ######
function waitFor-completion ([object]$taskResource,[string]$authValue,[string]$hostname)
{
  <#
        .DESCRIPTION
            Checks the status of the backup every twenty seconds, stops when status changes from running to a
different status

        .PARAMETER taskResource
            The response object from the backup-appliance method

        .PARAMETER authValue
            The authorized session ID

        .PARAMETER hostname
            The appliance to connect to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
           The new task resource object, which contains the Uri to get the backup resource in the next function


        .EXAMPLE
            $taskResource = waitFor-Completion $taskResource $sessionID $hostname
    #>


  # extracts the Uri of the task Resource from itself, to poll repeatedly
  $taskResourceUri = $taskResource.uri
  if ($taskResourceUri -eq $null)
  {
    # Caller will provide the error message
    return
  }
```

```
  # appends the Uri to the hostname to create a fully-qualified Uri
  $fullTaskUri = $hostname + $taskResourceUri


  # retries if unable to get backup progress information
  $errorCount = 0
  $errorMessage = ""


  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Backup initiated."
    Write-Host "Checking for backup completion, this may take a while."
  }

  # a while loop to determine when the backup process is finished
  do
  {


    try
    {
      # creates a new webrequest with appropriate headers
      $taskResourceJson = setup-request -Uri $fullTaskUri -method "GET" -accept "application/json" -authValue
$authValue -isSilent $true
      # converts the response from the Appliance into a hash table
      $taskResource = $taskResourceJson | convertFrom-Json
      # checks the status of the task manager
      $status = $taskResource.taskState
    }
    catch
    {
      $errorMessage = $error[0].Exception.Message
      $errorCount = $errorCount + 1
      $status = "RequestFailed"
      Start-Sleep -s 15
      continue
    }

    # Update progress bar
    if ($global:interactiveMode -eq 1)
    {
      $trimmedPercent = ($taskResource.completedSteps) / 5
      $progressBar = "[" + "=" * $trimmedPercent + " " * (20 - $trimmedPercent) + "]"
      Write-Host "`r Backup progress: $progressBar " $taskResource.completedSteps "%" -NoNewline
    }


    # Reset the error count since progress information was successfully retrieved
    $errorCount = 0

    # If the backup is still running, wait a bit, and then check again
    if ($status -eq "Running")
    {
      Start-Sleep -s 20
    }


  } while (($status -eq "Running" -or $status -eq "RequestFailed") -and $errorCount -lt 20);

  # if the backup reported an abnormal state, report the state and exit function
  if ($status -ne "Completed")
  {
    if ($global:interactiveMode -eq 1)
    {
      Write-Host "`n"
      Write-Host "Backup stopped abnormally"
      Write-Host $errorMessage
    }
    else
    {
      #log error message
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Backup stopped abnormally"

      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $errorMessage
    }
    return $null
  }


  # upon successful completion of task, outputs a hash table which contains task resource
  else
  {
    Write-Host "`n"
    $taskResource
    return
  }
}


##### Gets the backup resource #####
function get-backupResource ([object]$taskResource,[string]$authValue,[string]$hostname)
{
```

```
  <#
        .DESCRIPTION
            Gets the Uri for the backup resource from the task resource and gets the backup resource

        .PARAMETER taskResource
            The task resource object that we use to get the Uri for the backup resource

        .PARAMETER authValue
            The authorized sessionID

        .PARAMETER hostname
            the appliance to connect to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The backup resource object

        .EXAMPLE
            $backupResource = get-BackupResource $taskResource $sessionID $applianceName
    #>


  # the backup Resource Uri is extracted from the task resource
  if ($global:scriptApiVersion -lt $taskResourceV2ApiVersion)
  {
    $backupUri = $taskResource.associatedResourceUri
  }
  else
  {
    $backupUri = $taskResource.associatedResource.resourceUri
  }
  if ($backupUri -eq $null)
  {
    # Caller will provide the error message
    return
  }
  # construct the full backup Resource Uri from the hostname and the backup resource uri
  $fullBackupUri = $hostname + $backupUri

  # get the backup resource that contains the Uri for downloading
  try
  {
    # creates a new webrequest with appropriate headers
    $backupResourceJson = setup-request -Uri $fullBackupUri -method "GET" -accept "application/json" -auth
$authValue
    if ($backupResourceJson -ne $null)
    {
       $resource = $backupResourceJson | convertFrom-Json
       if ($global:interactiveMode -eq 1)
       {
         Write-Host "Obtained backup resource.  Now downloading.  This may take a while ..."
       }
       $resource
       return
    }
  }
  catch [System.Exception]
  {
    if ($global:interactiveMode -eq 1)
    {
      Write-Host $error[0].Exception.Message
    }
    else
    {
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message

    }
  }
}


##### Function to download the backup file #####
function download-Backup ([PSCustomObject]$backupResource,[string]$authValue,[string]$hostname)
{
  <#
        .DESCRIPTION
            Downloads the backup file from the appliance to the local system.  Tries to use the
            curl command.  The curl command has significantly better performance especially for
            large backups.  If curl isn't installed, invokes download-Backup-without-curl to
            download the backup.

        .PARAMETER backupResource
            Backup resource containing Uri for downloading

        .PARAMETER authValue
            The authorized sessionID

        .PARAMETER hostname
            The IP address of the appliance

        .INPUTS
```

```
            None, does not accept piping

        .OUTPUTS
            The absolute path of the download file

        .EXAMPLE
            download-backup $backupResource $sessionID https://11.111.11.111
    #>

  $downloadUri = $hostname + $backupResource.downloadUri
  $fileDir = [environment]::GetFolderPath("Personal")
  $filePath = $fileDir + "\" + $backupResource.id + ".bkp"
  $curlDownloadCommand = "curl -o " + $filePath + " -s -f -L -k -X GET " +
    "-H 'accept: application/octet-stream' " +
    "-H 'auth: " + $authValue + "' " +
    "-H 'X-API-Version: $global:scriptApiVersion' " +
    $downloadUri
  $curlGetDownloadErrorCommand = "curl -s -k -X GET " +
    "-H 'accept: application/json' " +
    "-H 'auth: " + $authValue + "' " +
    "-H 'X-API-Version: $global:scriptApiVersion' " +
    $downloadUri


  try
  {
    $testCurlSslOption = curl -V
    if ($testCurlSslOption -match "SSL")
    {
        invoke-expression $curlDownloadCommand
    }
    else
    {
        if ($global:interactiveMode -eq 1)
        {
          Write-Host "Version of curl must support SSL to get improved download performance."
        }
        else
        {
          Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Version of curl must
support SSL to get improved download performance"
        }

        return download-Backup-without-curl $backupResource $authValue $hostname
    }

    if ($LASTEXITCODE -ne 0)
    {
        $errorResponse = invoke-expression $curlGetDownloadErrorCommand
        if ($global:interactiveMode -eq 1)
        {
          Write-Host "Download using curl error: $errorResponse"
        }
        else
        {
          Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Download error:
$errorResponse"
        }

        if (Test-Path $filePath)
        {
           Remove-Item $filePath
        }
        return
    }

    if ($global:interactiveMode -eq 1)
    {
      Write-Host "Backup download complete!"
    }
  }
  catch [System.Management.Automation.CommandNotFoundException]
  {
    return download-Backup-without-curl $backupResource $authValue $hostname
  }
  catch [System.Exception]
  {
    Write-Host "Not able to download backup"
    Write-Host $error[0].Exception
    return
  }

  return $filePath
}


##### Function to download the Backup file without using the curl command #####
function download-Backup-without-curl ([PSCustomObject]$backupResource,[string]$authValue,[string]$hostname)
{
  <#
        .DESCRIPTION
            Downloads the backup file from the appliance to the local system (without using curl)
```

```
        .PARAMETER backupResource
            Backup resource containing Uri for downloading

        .PARAMETER authValue
            The authorized sessionID

        .PARAMETER hostname
            The IP address of the appliance

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The absolute path of the download file

        .EXAMPLE
            download-backup-without-curl $backupResource $sessionID https://11.111.11.111
    #>

  # appends Uri ( obtained from previous function) to IP address
  $downloadUri = $hostname + $backupResource.downloadUri
  $downloadTimeout = 43200000 # 12 hours
  $bufferSize = 65536 # bytes


  # creates a new webrequest with appropriate headers
  [net.httpsWebRequest]$downloadRequest = [net.webRequest]::create($downloadUri)
  $downloadRequest.method = "GET"
  $downloadRequest.AllowAutoRedirect = $TRUE
  $downloadRequest.Timeout = $downloadTimeout
  $downloadRequest.ReadWriteTimeout = $downloadTimeout
  $downloadRequest.Headers.Add("auth", $authValue)
  $downloadRequest.Headers.Add("X-API-Version", $global:scriptApiVersion)
  # accept either octet-stream or json to allow the response body to contain either the backup or an exception

  $downloadRequest.accept = "application/octet-stream;q=0.8,application/json"


  # creates a variable that stores the path to the file location. Note: users may change this to other file
paths.
  $fileDir = [environment]::GetFolderPath("Personal")


  try
  {
    # connects to the Appliance, creates a new file with the content of the response
    [net.httpsWebResponse]$response = $downloadRequest.getResponse()
    $responseStream = $response.getResponseStream()
    $responseStream.ReadTimeout = $downloadTimeout


    #saves file as the name given by the backup ID
    $filePath = $fileDir + "\" + $backupResource.id + ".bkp"
    $sr = New-Object System.IO.FileStream ($filePath,[System.IO.FileMode]::create)
    $responseStream.CopyTo($sr,$bufferSize)
    $response.close()
    $sr.close()
    if ($global:interactiveMode -eq 1)
    {
      Write-Host "Backup download complete!"
    }
  }
  catch [Net.WebException]
  {
    $errorMessage = $error[0].Exception.message

    #Try to get more information about the error
    try {
      $errorResponse = $error[0].Exception.InnerException.Response.getResponseStream()
      $sr = New-Object IO.StreamReader ($errorResponse)
      $rawErrorStream = $sr.readtoend()
      $error[0].Exception.InnerException.Response.close()
      $errorObject = $rawErrorStream | convertFrom-Json
      if (($errorObject.message.length -gt 0) -and
          ($errorObject.recommendedActions.length -gt 0))
      {
        $errorMessage = $errorObject.message + " " + $errorObject.recommendedActions
      }
    }
    catch [System.Exception]
    {
      #Use exception message
    }

    if ($global:interactiveMode -eq 1)
    {
      Write-Host $errorMessage
    }
    else
    {
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $errorMessage
    }
    return
```

```
  }

  return $filePath
}


function setup-request ([string]$uri,[string]$method,[string]$accept,[string]$contentType = "",[string]$authValue
 = "",[object]$body = $null,[bool]$isSilent=$false, [bool]$returnLocation=$false)
{
  try
  {
    [net.httpsWebRequest]$request = [net.webRequest]::create($uri)
    $request.method = $method
    $request.accept = $accept


    $request.Headers.Add("Accept-Language: en-US")
    if ($contentType -ne "")
    {
      $request.ContentType = $contentType
    }
    if ($authValue -ne "")
    {
      $request.Headers.Item("auth") = $authValue
    }
    $request.Headers.Item("X-API-Version") = $global:scriptApiVersion
    if ($body -ne $null)
    {
      $requestBodyStream = New-Object IO.StreamWriter $request.getRequestStream()
      $requestBodyStream.WriteLine($body)
      $requestBodyStream.flush()
      $requestBodyStream.close()
    }

    # attempt to connect to the Appliance and get a response
    [net.httpsWebResponse]$response = $request.getResponse()


    if ($returnLocation)
    {
        $taskUri = $response.getResponseHeader("Location")


        $response.close()
        return $taskUri
    }
    else
    {
        # response stored in a stream
        $responseStream = $response.getResponseStream()
        $sr = New-Object IO.StreamReader ($responseStream)


        #the stream, which contains a json object, is read into the storage variable
        $rawResponseContent = $sr.readtoend()
        $response.close()
        return $rawResponseContent
    }
  }
  catch [Net.WebException]
  {
    $errorMessage = $error[0].Exception.message

    #Try to get more information about the error
    try {
      $errorResponse = $error[0].Exception.InnerException.Response.getResponseStream()
      $sr = New-Object IO.StreamReader ($errorResponse)
      $rawErrorStream = $sr.readtoend()
      $error[0].Exception.InnerException.Response.close()
      $errorObject = $rawErrorStream | convertFrom-Json
      if (($errorObject.message.length -gt 0) -and
          ($errorObject.recommendedActions.length -gt 0))
      {
        $errorMessage = $errorObject.message + " " + $errorObject.recommendedActions
      }
    }
    catch [System.Exception]
    {
      #Use exception message
    }

    if ($isSilent) {
        throw $errorMessage
    }
    elseif ($global:interactiveMode -eq 1)
    {
      Write-Host $errorMessage
    }
    else
    {
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $errorMessage
    }
```

```
    #No need to rethrow since already recorded error
    return
  }
}



##### Start of function calls #####


#gets the credentials from user, either manual entry or from file
$savedLoginJson = queryfor-credentials $args[0]
if ($savedLoginJson -eq $null)
{
  #if an error occurs, it has already been logged in the queryfor-credentials function
  return
}


#extracts needed information from the credential json
try
{
  $savedLoginJson = "[" + $savedLoginJson + "]"
  $savedloginVals = $savedLoginJson | convertFrom-Json
  $SecStrLoginname = $savedloginVals.userName | ConvertTo-SecureString -ErrorAction stop
  $loginname =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecStrLoginName))

  $hostname = $savedloginVals.hostname
  $SecStrPassword = $savedloginVals.password | ConvertTo-SecureString -ErrorAction stop
  $password =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecStrpassword))

  $adname = $savedloginVals.authLoginDomain
}
catch [System.Exception]
{
  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Failed to get credentials: " + $error[0].Exception.Message
  }
  else
  {
    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Failed to get credentials: "
 + $error[0].Exception.Message
  }
}


#determines the active Api version
$global:scriptApiVersion = getApiVersion $global:scriptApiVersion $hostname
if ($global:scriptApiVersion -eq $null)
{
  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Could not determine appliance Api version"
  }


  Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not determine appliance
Api version"
  return
}


#sends the login request to the machine, gets an authorized session ID if successful
$authValue = login-appliance $loginname $password $hostname $adname
if ($authValue -eq $null)
{
  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Failed to receive login session ID."
  }
  Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Failed to receive login session
 ID."
  return
}


#sends the request to start the backup process, returns the taskResource object
$taskResource = backup-Appliance $authValue.sessionID $hostname
if ($taskResource -eq $null)
{
  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Could not initialize backup"
  }


  Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not initialize backup"
```

```
  return
}


#loops to keep checking how far the backup has gone
$taskResource = waitFor-completion $taskResource $authValue.sessionID $hostname
if ($taskResource -eq $null)
{
  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Could not fetch backup status"
  }


  Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not fetch backup status"

  return
}


#gets the backup resource
$backupResource = get-backupResource $taskResource $authValue.sessionID $hostname
if ($backupResource -eq $null)
{
  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Could not get the Backup Resource"
  }
 Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not get the Backup Resource"

  return
}


#downloads the backup file to the local drive
$filePath = download-Backup $backupResource $authValue.sessionID $hostname
if ($filePath -eq $null)
{
  if ($global:interactiveMode -eq 1)
  {
    Write-Host "Could not download the backup"
  }
  Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not download the backup"

  return
}


if ($global:interactiveMode -eq 1)
{
  Write-Host "Backup can be found at $filePath"
  Write-Host "If you wish to automate this script in the future and re-use login settings currently entered,"
  Write-Host "then provide the file path to the saved credentials file when running the script."
  Write-Host "ie: " $MyInvocation.MyCommand.Definition " filepath"
}
else
{
  Write-Host "Backup completed successfully."
  Write-Host "The backup can be found at $filePath."
}
Write-EventLog -EventId 0 -LogName Application -Source backup.ps1 -Message "script completed successfully"
```

B.2 Secuencia de comandos de restauración de ejemplo

Como alternativa al uso de **Settings→Actions→Restore from backup** (Configuración > Acciones > Restaurar desde copia de seguridad) desde la interfaz de usuario del dispositivo, puede escribir y ejecutar una secuencia de comandos para restaurar automáticamente el dispositivo desde un archivo de copia de seguridad.

NOTA: Solo un usuario con privilegios de administrador de infraestructuras puede restaurar un dispositivo.

El Ejemplo 15, «Secuencia de comandos restore.ps1 de ejemplo» proporciona una secuencia de comandos de ejemplo que restaura el dispositivo desde un archivo de copia de seguridad u obtiene el progreso de un proceso de restauración en curso.

Secuencia de comandos de ejemplo

Si no pasa parámetros a la secuencia de comandos, la secuencia de comandos carga y restaura un archivo de copia de seguridad.

1. Llama a `query-user()` para obtener el nombre de host del dispositivo, el nombre de usuario y la contraseña, y la ruta del archivo de copia de seguridad.
2. Llama a `login-appliance()` para emitir una solicitud REST para obtener un ID de sesión utilizado para autorizar llamadas REST de restauración.
3. Llama a `uploadTo-appliance()` para cargar una copia de seguridad en el dispositivo.
4. Llama a `start-restore()` para iniciar la restauración.
5. Llama a `restore-status()` para comprobar periódicamente el estado de la restauración hasta que esta termine.

Si pasa la opción `-status` a la secuencia de comandos, esta comprobará el estado de la última restauración o de la restauración en curso e informará del mismo hasta que se complete el proceso de restauración:

1. Llama a `recover-restoreID()` para obtener el URI para comprobar el estado de la última restauración o de una restauración en curso.
2. Llama a `restore-status()` para comprobar periódicamente el estado de la restauración hasta que esta termine.

Ejemplo 15 Secuencia de comandos restore.ps1 de ejemplo

```
#(C) Copyright 2012-2014 Hewlett Packard Enterprise Development LP
##################################################################################################################################
# Name:     restore.ps1
# Usage:    {directory}\restore.ps1 or {directory}\restore.ps1 -status https://{ipaddress}
# Purpose:  Uploads a backup file to the appliance and then restores the appliance using the backup data
# Notes:    To improve performance, this script uses the curl command if it is installed.  The curl command
#           must be installed with the SSL option.
#           Windows PowerShell 3.0 must be installed to run the script
##################################################################################################################################


# tells the computer that this is a trusted source we are connecting to (brute force, could be refined)
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }


# The scriptApiVersion is the default Api version (if the appliance supports this level
# or higher).  This variable may be changed if the appliance is at a lower Api level.
$global:scriptApiVersion = 3


##### Obtain information from user #####
function query-user ()
{
  <#
        .DESCRIPTION
            Obtains information needed to run the script by prompting the user for input.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs an object containing the obtained information.


        .EXAMPLE
            $userVals = query-user
    #>
  Write-Host "Restoring from backup is a destructive process, continue anyway?"


  $continue = 0
  do
  {
    $earlyExit = Read-Host
    if ($earlyExit[0] -eq 'n')
    {
      return
    }
    elseif ($earlyExit[0] -ne 'y')
    {
      Write-Host "Please respond with a y or n"
    }
    else
    {
      $continue = 1
    }


  } while ($continue -eq 0)


  do
  {
    Write-Host "Enter directory backup is located in (ie: C:\users\joe\)"
    $backupDirectory = Read-Host
    # Add trailing slash if needed
    if (!$backupDirectory.EndsWith("\"))
    {
       $backupDirectory = $backupDirectory + "\"
    }


    Write-Host "Enter name of backup (ie: appliance_vm1_backup_2012-07-07_555555.bkp)"
    $backupFile = Read-Host


    # Check if file exists
    $fullFilePath = $backupDirectory + $backupFile
    if (! (Test-Path $fullFilePath))
    {
       Write-Host "Sorry the backup file $fullFilePath doesn't exist."
    }
  } while (! (Test-Path $fullFilePath))



  Write-Host "Enter appliance IP address (ie: https://10.10.10.10)"
  $hostname = Read-Host
  # Correct some common errors
```

```
  $hostname  = $hostname.Trim().ToLower()
  if (!$hostname.StartsWith("https://"))
  {
     if ($hostname.StartsWith("http://"))
     {
        $hostname  = $hostname.Replace("http","https")
     } else {
        $hostname  = "https://" + $hostname
     }
  }


  Write-Host "Enter username"
  $secUsername = Read-Host -AsSecureString
  $username =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($secUsername))



  Write-Host "Enter password"
  $secPassword = Read-Host -AsSecureString
  $password =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($secPassword))

  $absolutePath = $backupDirectory + $backupFile


  Write-Host "If using Active Directory, enter the Active Directory domain"
  Write-Host "  (Leave this field blank if not using Active Directory.)"
  $ADName = Read-Host


  $loginVals = @{ hostname = $hostname; userName = $username; password = $password; backupPath = $absolutePath;

                 backupFile = $backupFile; authLoginDomain = $ADName; }


  return $loginVals
}


##### getApiVersion: Get X_API_Version #####
function getApiVersion ([int32] $currentApiVersion,[string]$hostname)
{
  <#
        .DESCRIPTION
            Sends a web request to the appliance to obtain the current Api version.
            Returns the lower of: Api version supported by the script and Api version
            supported by the appliance.

        .PARAMETER currentApiVersion
            Api version that the script is currently using

        .PARAMETER hostname
            The appliance address to send the request to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the new active Api version


        .EXAMPLE
            $global:scriptApiVersion = getApiVersion()
    #>


  # the particular Uri on the Appliance to reqest the Api Version
  $versionUri = "/rest/version"


  # append the Uri to the end of the IP address to obtain a full Uri
  $fullVersionUri = $hostname + $versionUri


  # use setup-request to issue the REST request api version and get the response
  try
  {
    $applianceVersionJson = setup-request -Uri $fullVersionUri -method "GET" -accept "application/json"
-contentType "application/json"
    if ($applianceVersionJson -ne $null)
    {
      $applianceVersion = $applianceVersionJson | convertFrom-Json
      $currentApplianceVersion = $applianceVersion.currentVersion
      if ($currentApplianceVersion -lt $currentApiVersion)
      {
        return $currentApplianceVersion
      }
      return $currentApiVersion
    }
```

```
  }
  catch [System.Exception]
  {
    if ($global:interactiveMode -eq 1)
    {
      Write-Host $error[0].Exception.Message
    }
    else
    {
      Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message

    }
  }
}


##### Send the login request to the appliance #####
function login-appliance ([string]$username,[string]$password,[string]$hostname,[string]$ADName)
{
  <#
        .DESCRIPTION
            Attempts to send a web request to the appliance and obtain an authorized sessionID.

        .PARAMETER username
            The username to log into the remote appliance

        .PARAMETER password
            The correct password associated with username

        .PARAMETER hostname
            The appliance address to send the request to (in https://{ipaddress} format)

        .PARAMETER ADName
            The Active Directory name (optional)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the response body containing the needed session ID.


        .EXAMPLE
            $authtoken = login-appliance $username $password $hostname $ADName
    #>


  # the particular URI on the Appliance to reqest an "auth token"
  $loginURI = "/rest/login-sessions"


  # append the URI to the end of the IP address to obtain a full URI
  $fullLoginURI = $hostname + $loginURI
  # create the request body as a hash table, then convert it to json format
  if ($ADName)
  {
    $body = @{ userName = $username; password = $password; authLoginDomain = $ADName } | convertTo-json
  }
  else  # null or empty
  {
    $body = @{ userName = $username; password = $password } | convertTo-json
  }


  try
  {
    # create a new webrequest object and give it the header values that will be accepted by the Appliance, get
 response
    $loginRequest = setup-request -Uri $fullLoginURI -method "POST" -accept "application/json" -contentType
"application/json" -Body $body
    Write-Host "Login completed successfully."
  }
  catch [System.Exception]
  {
    Write-Host $_.Exception.message
    Write-Host $error[0].Exception
    return
  }


  #the output for the function, a hash table which contains a single value, "sessionID"
  $loginRequest | convertFrom-Json
  return
}


##### Upload the backup file to the appliance #####
function uploadTo-appliance ([string]$filepath,[string]$authinfo,[string]$hostname,[string]$backupFile)
{
  <#
        .DESCRIPTION
            Attempts to upload a backup file to the appliance.  Tries to use the curl command.
            The curl command has significantly better performance especially for large backups.
```

```
            If curl isn't installed, invokes uploadTo_appliance-without-curl to upload the file.

        .PARAMETER filepath
            The absolute filepath to the backup file.

        .PARAMETER authinfo
            The authorized session ID returned by the login request

        .PARAMETER hostname
            The appliance to connect to

        .PARAMETER backupFile
            The name of the file to upload. Only used to tell the server what file is contained in the post
request.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The response body to the upload post request.


        .EXAMPLE
            $uploadResponse = uploadTo-appliance $filePath $sessionID $hostname $fileName
    #>


  $uploadUri = "/rest/backups/archive"
  $fullUploadUri = $hostname + $uploadUri
  $curlUploadCommand = "curl -s -k -X POST " +
    "-H 'content-type: multipart/form-data' " +
    "-H 'accept: application/json' " +
    "-H 'auth: " + $authinfo + "' " +
    "-H 'X-API-Version: $global:scriptApiVersion' " +
    "-F file=@" + $filepath + " " +
    $fullUploadUri


  Write-Host "Uploading backup file to appliance, this may take a few minutes..."
  try
  {
    $testCurlSslOption = curl -V
    if ($testCurlSslOption -match "SSL")
    {
      $rawUploadResponse = invoke-expression $curlUploadCommand
      if ($rawUploadResponse -eq $null)
      {
        return
      }
      $uploadResponse = $rawUploadResponse | convertFrom-Json


      if ($uploadResponse.status -eq "SUCCEEDED")
      {
        Write-Host "Upload complete."
        return $uploadResponse
      }
      else
      {
        Write-Host $uploadResponse
        return
      }
    }
    else
    {
        Write-Host "Version of curl must support SSL to get improved upload performance."
        return uploadTo-appliance-without-curl $filepath $authinfo $hostname $backupFile
    }
  }
  catch [System.Management.Automation.CommandNotFoundException]
  {
    return uploadTo-appliance-without-curl $filepath $authinfo $hostname $backupFile
  }
  catch [System.Exception]
  {
    Write-Host "Not able to upload backup"
    Write-Host $error[0].Exception
    return
  }
}


##### Upload the backup file to the appliance without using the curl command #####
function uploadTo-appliance-without-curl
([string]$filepath,[string]$authinfo,[string]$hostname,[string]$backupFile)
{
  <#
        .DESCRIPTION
            Attempts to upload a backup to the appliance without using curl.

        .PARAMETER filepath
            The absolute filepath to the backup file.
```

```
        .PARAMETER authinfo
            The authorized session ID returned by the login request

        .PARAMETER hostname
            The appliance to connect to

        .PARAMETER backupFile
            The name of the file to upload. Only used to tell the server what file is contained in the post
request.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The response body to the upload post request.


        .EXAMPLE
            $uploadResponse = uploadTo-appliance $filePath $sessionID $hostname $fileName
    #>


  $uploadUri = "/rest/backups/archive"
  $fullUploadUri = $hostname + $uploadUri
  $uploadTimeout =  43200000 # 12 hours
  $bufferSize = 65536 # bytes


  try
  {
    [net.httpsWebRequest]$uploadRequest = [net.webRequest]::create($fullUploadUri)
    $uploadRequest.method = "POST"
    $uploadRequest.Timeout = $uploadTimeout
    $uploadRequest.ReadWriteTimeout = $uploadTimeout
    $uploadRequest.SendChunked = 1
    $uploadRequest.AllowWriteStreamBuffering = 0
    $uploadRequest.accept = "application/json"
    $boundary = "----------------------------bac8d687982e"
    $uploadRequest.ContentType = "multipart/form-data; boundary=----------------------------bac8d687982e"
    $uploadRequest.Headers.Add("auth", $authinfo)
    $uploadRequest.Headers.Add("X-API-Version", $global:scriptApiVersion)
    $fs = New-Object IO.FileStream ($filepath,[System.IO.FileMode]::Open)
    $rs = $uploadRequest.getRequestStream()
    $rs.WriteTimeout = $uploadTimeout
    $disposition = "Content-Disposition: form-data; name=""file""; filename=""encryptedBackup"""
    $conType = "Content-Type: application/octet-stream"


    [byte[]]$BoundaryBytes = [System.Text.Encoding]::UTF8.GetBytes("--" + $boundary + "`r`n")
    $rs.write($BoundaryBytes,0,$BoundaryBytes.Length)


    [byte[]]$contentDisp = [System.Text.Encoding]::UTF8.GetBytes($disposition + "`r`n")
    $rs.write($contentDisp,0,$contentDisp.Length)


    [byte[]]$contentType = [System.Text.Encoding]::UTF8.GetBytes($conType + "`r`n`r`n")
    $rs.write($contentType,0,$contentType.Length)


    $fs.CopyTo($rs,$bufferSize)
    $fs.close()


    [byte[]]$endBoundaryBytes = [System.Text.Encoding]::UTF8.GetBytes("`n`r`n--" + $boundary + "--`r`n")
    $rs.write($endBoundaryBytes,0,$endBoundaryBytes.Length)
    $rs.close()
  }
  catch [System.Exception]
  {
    Write-Host "Not able to send backup"
    Write-Host $error[0].Exception
  }
  try
  {
    [net.httpsWebResponse]$response = $uploadRequest.getResponse()
    $responseStream = $response.getResponseStream()
    $responseStream.ReadTimeout = $uploadTimeout
    $streamReader = New-Object IO.StreamReader ($responseStream)
    $rawUploadResponse = $streamReader.readtoend()
    $response.close()


    if ($rawUploadResponse -eq $null)
    {
      return
    }


    $uploadResponse = $rawUploadResponse | convertFrom-Json


    if ($uploadResponse.status -eq "SUCCEEDED")
```

```
    {
      Write-Host "Upload complete."
      return $uploadResponse
    }
    else
    {
      Write-Host $rawUploadResponse
      Write-Host $uploadResponse
      return
    }
  }
  catch [Net.WebException]
  {
    Write-Host $error[0]
    $errorResponse = $error[0].Exception.InnerException.Response.getResponseStream()
    $sr = New-Object IO.StreamReader ($errorResponse)


    $frawErrorStream = $sr.readtoend()
    $error[0].Exception.InnerException.Response.close()
    $errorObject = $rawErrorStream | convertFrom-Json


    Write-Host $errorObject.errorcode $errorObject.message $errorObject.resolution
    return
  }
}


##### Initiate the restore process #####
function start-restore ([string]$authinfo,[string]$hostname,[object]$uploadResponse)
{
  <#
        .DESCRIPTION
            Sends a POST request to the restore resource to initiate a restore.

        .PARAMETER authinfo
            The authorized sessionID obtained from login.

        .PARAMETER hostname
                The appliance to connect to.

        .PARAMETER uploadResponse
            The response body from the upload request. Contains the backup URI needed for restore call.


        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the response body from the POST restore call.


        .EXAMPLE
            $restoreResponse = start-restore $sessionID $hostname $uploadResponse
    #>
  # append the appropriate URI to the IP address of the Appliance
  $backupUri = $uploadResponse.uri
  $restoreUri = "/rest/restores"
  $fullRestoreUri = $hostname + $restoreURI
  $body = @{ type = "RESTORE"; uriOfBackupToRestore = $backupUri } | convertTo-json
  # create a new webrequest and add the proper headers
  try
  {
   $rawRestoreResponse = setup-request -uri $fullRestoreUri -method "POST" -accept "application/json" -contentType
 "application/json" -authValue $authinfo -Body $body


    $restoreResponse = $rawRestoreResponse | convertFrom-Json
    return $restoreResponse
  }


  catch [Net.WebException]
  {
    Write-Host $_.Exception.message
  }
}


##### Check for the status of ongoing restore #####
function restore-status ([string]$authinfo = "foo",[string]$hostname,[object]$restoreResponse,[string]$recoveredUri
 = "")
{
  <#
        .DESCRIPTION
            Uses GET requests to check the status of the restore process.

        .PARAMETER authinfo
            **to be removed once no longer a required header**

        .PARAMETER hostname
            The appliance to connect to
```

```
       .PARAMETER restoreResponse
           The response body from the restore initiation request.

       .PARAMETER recoveredUri
         In case of a interruption in the script or connection, the Uri for status is instead obtained through
this parameter.

       .INPUTS
           None, does not accept piping

       .OUTPUTS
           None, end of script upon completion or fail.


       .EXAMPLE
           restore-status *$authinfo* -hostname $hostname -restoreResponse $restoreResponse

           or

           restore-status -hostname $hostname -recoveredUri $recoveredUri
   #>

 $retryCount = 0
 $retryLimit = 5
 $retryMode  = 0


 # append the appropriate URI to the IP address of the Appliance

 if ($recoveredUri -ne "")
 {
   $fullStatusUri = $hostname + $recoveredUri
   write-host $fullStatusUri
 }
 else
 {
   $fullStatusUri = $hostname + $restoreResponse.uri
 }
 do
 {
   try
   {
     # create a new webrequest and add the proper headers (new header, auth is needed for authorization
     $rawStatusResp = setup-request -uri $fullStatusUri -method "GET" -accept "application/json" -contentType
"application/json" -authValue $authinfo
     $statusResponse = $rawStatusResp | convertFrom-Json
     $trimmedPercent = ($statusResponse.percentComplete) / 5
     $progressBar = "[" + "=" * $trimmedPercent + " " * (20 - $trimmedPercent) + "]"
     Write-Host "`rRestore progress: $progressBar " $statusResponse.percentComplete "%" -NoNewline
   }
   catch [Net.WebException]
   {
     try
     {
       $errorResponse = $error[0].Exception.InnerException.Response.getResponseStream()
       $sr = New-Object IO.StreamReader ($errorResponse)


       $rawErrorStream = $sr.readtoend()
       $error[0].Exception.InnerException.Response.close()
       $errorObject = $rawErrorStream | convertFrom-Json


       Write-Host $errorObject.message $errorObject.recommendedActions
     }
     catch [System.Exception]
     {
         Write-Host "`r`n" $error[1].Exception
     }


     # The error may be transient; retry several times.  If it still fails, return with an error.
     $retryCount++
     $retryMode = 1
     if ($retryCount -le $retryLimit)
     {
         Write-Host "In restore-status retrying GET on $fullStatusUri.  retry count: $retryCount`r`n"
         sleep 5
         continue
     }
     else
     {
         Write-Host "`r`nRestore may have failed! Could not determine the status of the restore."
         return
     }
   }
   if ($statusResponse.status -eq "SUCCEEDED")
   {
     Write-Host "`r`nRestore complete!"
     return
   }
   if ($statusResponse.status -eq "FAILED")
```

```
    {
      Write-Host "`r`nRestore failed! System should now undergo a reset to factory defaults."
    }
    Start-Sleep 10
  } while (($statusResponse.status -eq "IN_PROGRESS") -or ($retryMode -eq 1))


  return
}


##### Recovers Uri to the restore resource if connection lost #####
function recover-restoreID ([string]$hostname)
{
  <#
        .DESCRIPTION
            Uses GET requests to check the status of the restore process.

        .PARAMETER hostname
            The appliance to end the request to.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The Uri of the restore task in string form.

        .EXAMPLE
            $reacquiredUri = recover-restoredID $hostname
    #>


  $idUri = "/rest/restores/"
  $fullIdUri = $hostname + $idUri
  try
  {
    $rawIdResp = setup-request -uri $fullIdUri -method "GET" -contentType "application/json" -accept
"application/json" -authValue "foo"
    $idResponse = $rawIdResp | convertFrom-Json
  }
  catch [Net.WebException]
  {
    $_.Exception.message
    return
  }
  return $idResponse.members[0].uri
}


function setup-request ([string]$uri,[string]$method,[string]$accept,[string]$contentType =
"",[string]$authValue="0", [object]$body = $null)
{
  <#
    .DESCRIPTION
        A function to handle the more generic web requests to avoid repeated code in every function.

    .PARAMETER uri
        The full address to send the request to (required)

    .PARAMETER method
        The type of request, namely POST and GET (required)

    .PARAMETER accept
        The type of response the request accepts (required)

    .PARAMETER contentType
        The type of the request body

    .PARAMETER authValue
        The session ID used to authenticate the request

    .PARAMETER body
        The message to put in the request body

    .INPUTS
        None

    .OUTPUTS
        The response from the appliance, typically in Json form.

    .EXAMPLE
       $responseBody = setup-request -uri https://10.10.10.10/rest/doThis -method "GET" -accept "application/json"

    #>
  try
  {
    [net.httpsWebRequest]$request = [net.webRequest]::create($uri)
    $request.method = $method
    $request.accept = $accept


    $request.Headers.Add("Accept-Language: en-US")
    if ($contentType -ne "")
```

```
    {
      $request.ContentType = $contentType
    }
    if ($authValue -ne "0")
    {
      $request.Headers.Item("auth") = $authValue
    }
    $request.Headers.Add("X-API-Version: $global:scriptApiVersion")
    if ($body -ne $null)
    {
      #write-host $body
      $requestBodyStream = New-Object IO.StreamWriter $request.getRequestStream()
      $requestBodyStream.WriteLine($body)


      $requestBodyStream.flush()
      $requestBodyStream.close()
    }


    # attempt to connect to the Appliance and get a response
    [net.httpsWebResponse]$response = $request.getResponse()


    # response stored in a stream
    $responseStream = $response.getResponseStream()
    $sr = New-Object IO.StreamReader ($responseStream)


    #the stream, which contains a json object is read into the storage variable
    $rawResponseContent = $sr.readtoend()
    $response.close()
    return $rawResponseContent
  }
  catch [Net.WebException]
  {
    try
    {
        $errorResponse = $error[0].Exception.InnerException.Response.getResponseStream()
        $sr = New-Object IO.StreamReader ($errorResponse)
        $rawErrorStream = $sr.readtoend()
        $error[0].Exception.InnerException.Response.close()
        $errorObject = $rawErrorStream | convertFrom-Json
        Write-Host "errorCode returned:" $errorObject.errorCode
        Write-Host "when requesting a $method on $uri`r`n"
        Write-Host $errorObject.message ";" $errorObject.recommendedActions
    }
    catch [System.Exception]
    {
        Write-Host $error[1].Exception.Message
    }
    throw
    return


  }
}




##### Begin main #####



#this checks to see if the user wants to just check a status of an existing restore
if ($args.count -eq 2)
{
  foreach ($item in $args)
  {
    if ($item -eq "-status")
    {
      [void]$foreach.movenext()
      $hostname = $foreach.current
      # Correct some common errors in hostname
      $hostname  = $hostname.Trim().ToLower()
      if (!$hostname.StartsWith("https://"))
      {
         if ($hostname.StartsWith("http://"))
         {
            $hostname  = $hostname.Replace("http","https")
         } else {
            $hostname  = "https://" + $hostname
         }
      }
    }
        else
        {
            Write-Host "Invalid arguments."
            return
```

```
        }
  }


  $reacquiredUri = recover-restoreID -hostname $hostname
  if ($reacquiredUri -eq $null)
  {
    Write-Host "Error occurred when fetching active restore ID. No restore found."
    return
  }
  restore-status -recoveredUri $reacquiredUri -hostname $hostname


  return
}
elseif ($args.count -eq 0)
{
  $loginVals = query-user
  if ($loginVals -eq $null)
  {
    Write-Host "Error passing user login vals from function query-host, closing program."
    return
  }


#determines the active Api version
  $global:scriptApiVersion = getApiVersion $global:scriptApiVersion $loginVals.hostname
  if ($global:scriptApiVersion -eq $null)
  {
    Write-Host "Could not determine appliance Api version"
    return
  }


  $authinfo = login-appliance $loginVals.userName $loginvals.password $loginVals.hostname
$loginVals.authLoginDomain
  if ($authinfo -eq $null)
  {
    Write-Host "Error getting authorized session from appliance, closing program."
    return
  }


  $uploadResponse = uploadTo-appliance $loginVals.backupPath $authinfo.sessionID $loginVals.hostname
$loginVals.backupFile
  if ($uploadResponse -eq $null)
  {
    Write-Host "Error attempting to upload, closing program."
    return
  }


  $restoreResponse = start-restore $authinfo.sessionID $loginVals.hostname $uploadResponse
  if ($restoreResponse -eq $null)
  {
    Write-Host "Error obtaining response from Restore request, closing program."
    return
  }
  restore-status -hostname $loginVals.hostname -restoreResponse $restoreResponse -authinfo $authinfo.sessionID

  return
}
else
{
  Write-Host "Usage: restore.ps1"
  Write-Host "or"
  Write-Host "restore.ps1 -status https://{ipaddress}"
  return
}
```

C Servicio de directorio de autenticación

Este Apéndice proporciona información adicional para ayudarle a aplicar correctamente campos de contexto de búsqueda para agregar un servicio de directorio de autenticación al dispositivo HPE OneView.

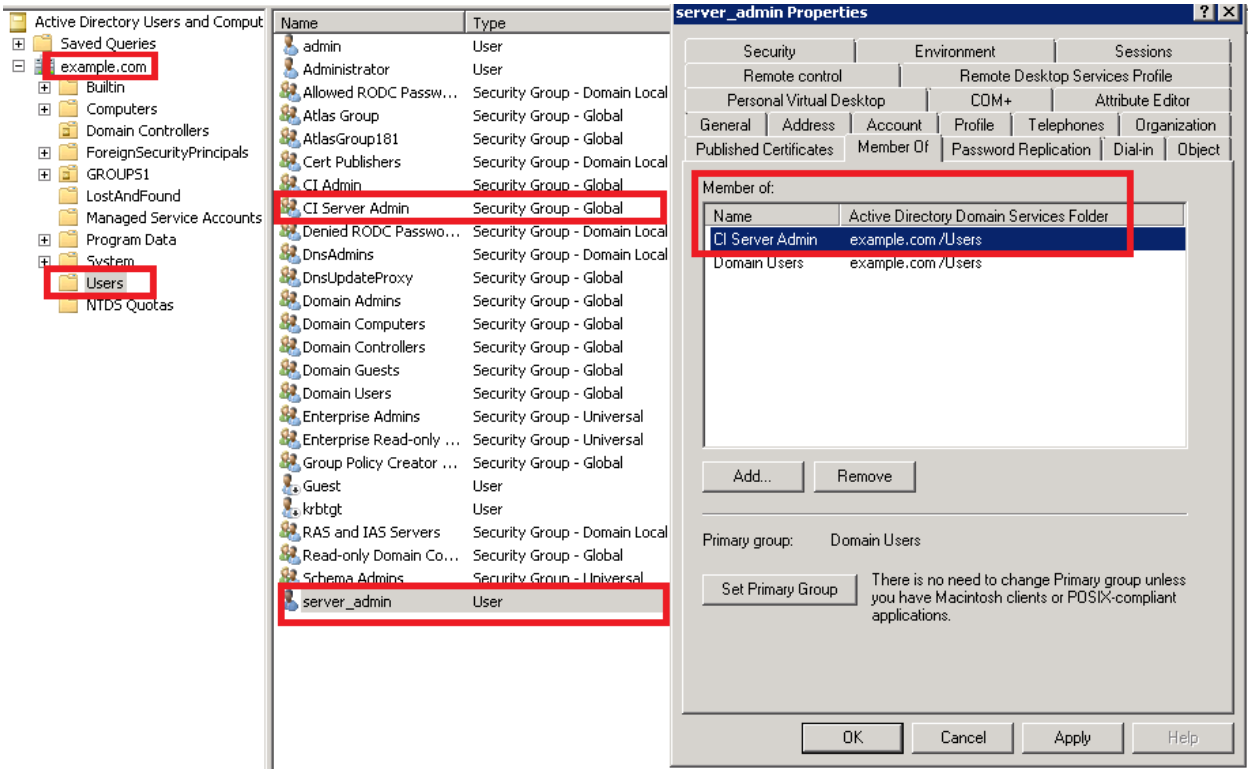
C.1 Configuraciones de Microsoft Active Directory

C.1.1 Usuarios y grupos en la misma OU

En la tabla siguiente se muestra la asignación general para los campos **Search context** (Contexto de búsqueda) de la pantalla **Add Directory** (Agregar directorio) para una configuración de Microsoft Active Directory en la que los usuarios y grupos pertenecen a la misma unidad organizativa (OU). Para obtener información sobre la pantalla **Add Directory** (Agregar directorio), consulte la ayuda en línea.

	Campo 1	Campo 2	Campo 3
Contexto de búsqueda	`CN`	`CN=Organizational_Unit`	`DC=domain,DC=domain`

En este ejemplo, el dominio es `example.com`, y los usuarios y grupos se encuentran en el contenedor `Users` (Usuarios), que es la unidad organizativa predeterminada.



Las entradas para los campos **Search context** (Contexto de búsqueda) que autenticarían al usuario denominado `server_admin` son:

	Campo 1	Campo 2	Campo 3
Contexto de búsqueda	`CN`	`CN=Users`	`DC=example,DC=com`

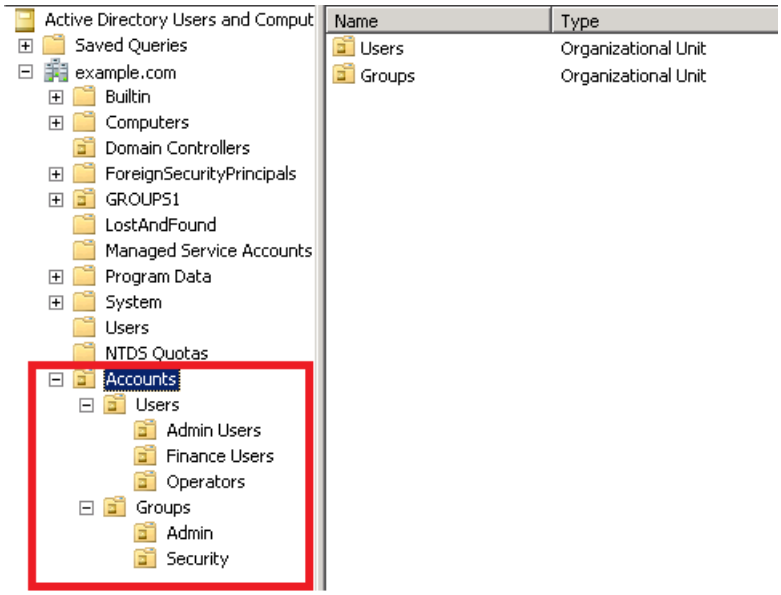
C.1.2 Usuarios y grupos en OU distintas, con la misma OU principal

En la tabla siguiente se muestra la asignación general para los campos **Search context** (Contexto de búsqueda) de la pantalla **Add Directory** (Agregar directorio) para una configuración de Microsoft Active Directory en la que los usuarios y grupos pertenecen a dos unidades organizativas distintas, pero ambas pertenecen a una misma OU principal. Para obtener información sobre la pantalla **Add Directory** (Agregar directorio), consulte la ayuda en línea.

	Campo 1	Campo 2	Campo 3
Contexto de búsqueda	`CN`	`OU=Organizational_Unit`	`DC=domain,DC=domain`

En este ejemplo, hay una OU principal denominada `Accounts` con dos OU secundarias, `Users` y `Groups`.

El dominio es `example.com`.



Las entradas para los campos **Search context** (Contexto de búsqueda) que autenticarían a un usuario de la OU `Users` son:

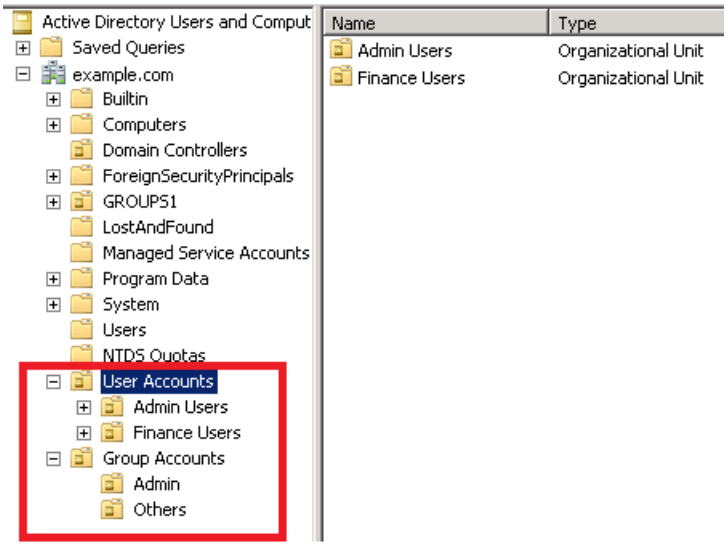
	Campo 1	Campo 2	Campo 3
Contexto de búsqueda	`CN`	`OU=Accounts`	`DC=example,DC=com`

C.1.3 Usuarios y grupos en OU distintas, con OU principales distintas

En la tabla siguiente se muestra la asignación general para los campos **Search context** (Contexto de búsqueda) de la pantalla **Add Directory** (Agregar directorio) para una configuración de Microsoft Active Directory en la que las cuentas de los usuarios y los grupos pertenecen a dos unidades organizativas distintas (que se muestran como OU1 y OU2). Para obtener información sobre la pantalla **Add Directory** (Agregar directorio), consulte la ayuda en línea.

	Campo 1	Campo 2	Campo 3
Contexto de búsqueda	`CN`	`OU=child_OU,OU=parent_OU` + ...	`DC=domain,DC=domain`

En este ejemplo, hay dos OU independientes, `User Accounts` y `Group Accounts` en el dominio `example.com`.



Para especificar la unidad organizativa se usa el siguiente formato:

`OU=child_OU,OU=parent_OU`

En el ejemplo, hay cuatro cuentas distintas que se pueden especificar:

`OU=Admin Users,OU=User Accounts,``DC=example.DC=com`
`OU=Finance Users,OU=User Accounts,``DC=example.DC=com`
`OU=Admin,OU=Group Accounts,``DC=example.DC=com`
`OU=Others,OU=Group Accounts,``DC=example.DC=com`

Puede combinar los contextos de búsqueda, hasta 10, utilizando el carácter + en el campo 2. Esta construcción se conoce como varios nombres completos relativos (RDN).

Para este ejemplo, las entradas de los campos **Search context** (Contexto de búsqueda) para autenticar a estos usuarios y grupos son:

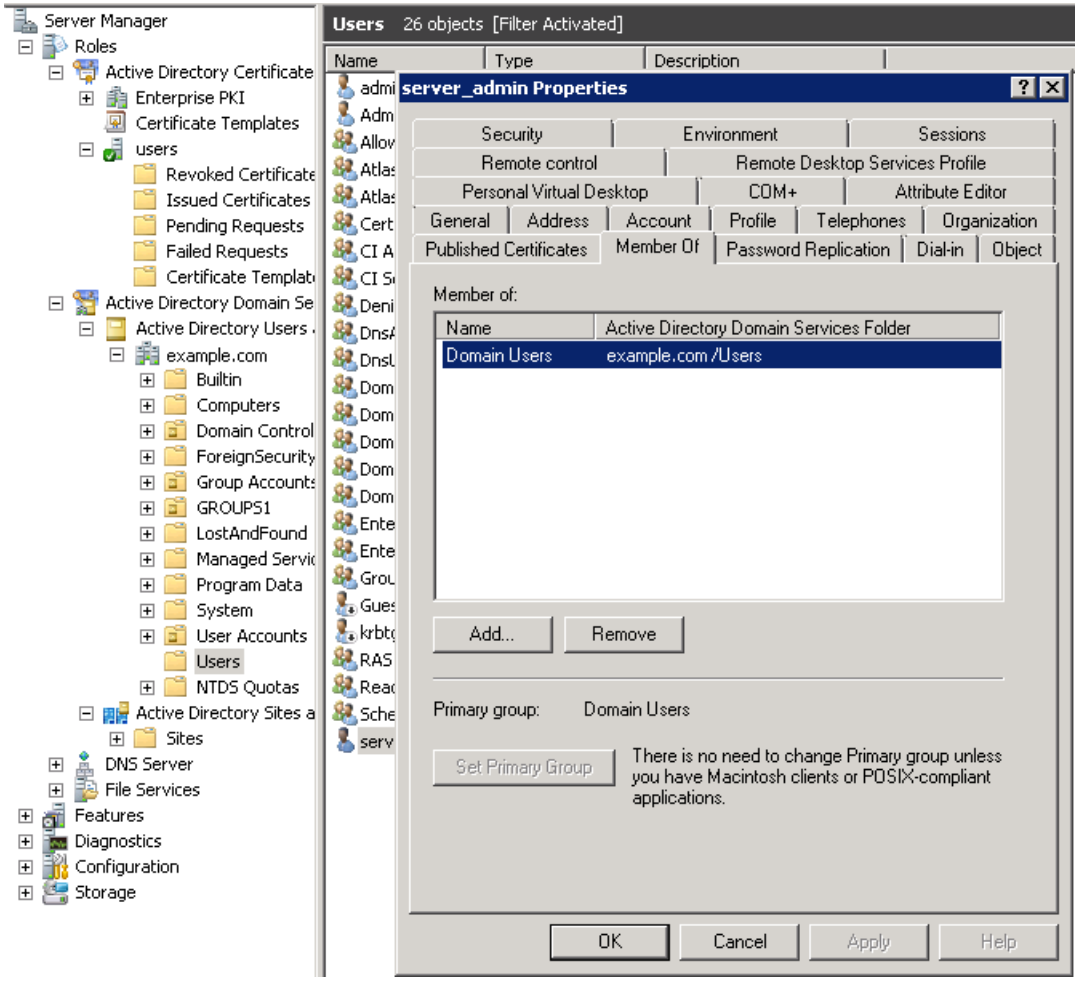
	Campo 1	**Campo 2**	**Campo 3**
Contexto de búsqueda	`CN`	`OU=Admin Users,OU=User Accounts + OU=Finance Users,OU=User Accounts + OU=Admin,OU=Group Accounts + OU=Others,OU=Group Accounts`	`DC=example,DC=com`

C.1.4 Grupos integrados

Microsoft Active Directory dispone de la función de grupos integrados, por la cual ciertos grupos se sitúan automáticamente en contenedores predefinidos. Estos grupos integrados son:

- Domain Users (Usuarios del dominio)
- Domain Admins (Administradores del dominio)
- Enterprise Admins (Administradores de empresas)

El grupo `Domain Users` (Usuarios del dominio) de Microsoft Active Directory contiene todos los usuarios que se han creado en el dominio. En este ejemplo, todas las cuentas de usuario situadas bajo `Users` (Usuarios) se incluyen en `Domain Users` (Usuarios del dominio):



Sin embargo, las cuentas de usuario del grupo `Domain Users` (Usuarios del dominio) no se autentican. Debe especificar la unidad o unidades organizativas.

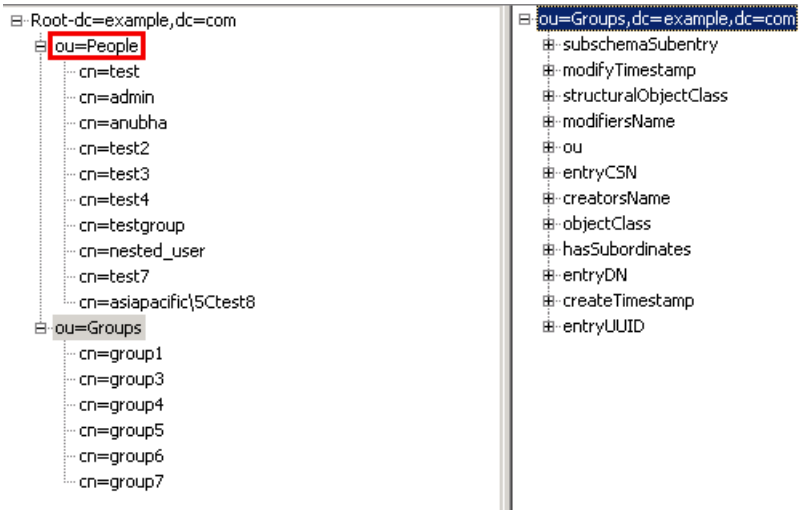
Para obtener más información sobre los grupos integrados y su comportamiento, consulte la documentación de Microsoft.

C.2 Configuración del directorio de OpenLDAP

En la tabla siguiente se muestra la asignación general para los campos **Search context** (Contexto de búsqueda) de la pantalla **Add Directory** (Agregar directorio) para una configuración de OpenLDAP en la que los usuarios y grupos pertenecen a unidades organizativas (OU) distintas. Para obtener información sobre la pantalla **Add Directory** (Agregar directorio), consulte la ayuda en línea.

	Campo 1	**Campo 2**	**Campo 3**
Contexto de búsqueda	`CN`	`OU=`*`Organizational_Unit`*	`DC=`*`domain`*`,DC=`*`domain`*

En este ejemplo, las cuentas de usuario se encuentran en la OU `People` (Personas) y los grupos se encuentran en la OU `Groups` (Grupos):



Para este ejemplo, las entradas de los campos **Search context** (Contexto de búsqueda) para autenticar a los usuarios, pero no a los grupos, son:

	Campo 1	Campo 2	Campo 3
Contexto de búsqueda	`CN`	`OU=People`	`DC=example,DC=com`

NOTA: La OU `Groups` (Grupos) no es válida para el campo 2 del contexto de búsqueda. De forma predeterminada, todos los grupos se buscan únicamente en la OU `Groups`. Para OpenLDAP, los grupos siempre se deben crear dentro de la OU `Groups`.

C.3 Validación de la configuración del servidor de directorio

Para obtener información sobre estos requisitos, consulte los detalles de la pantalla *Add Directory* (Agregar directorio) y los detalles de la pantalla *Add Directory Server* (Agregar servidor de directorio) en la ayuda en línea.

Asimismo, debe haber contextos de búsqueda válidos para que sea posible identificar y acceder al grupo o los grupos.

Utilice el procedimiento siguiente para comprobar que dispone de una configuración de servidor de directorio apropiada.

Requisitos previos

- Privilegios mínimos necesarios: administrador de infraestructuras.
- El servidor que alberga el servicio de directorio de autenticación debe:
  - Comunicarse a través de SSL.
  - Usar el mismo puerto SSL para LDAP.
  - Estar accesible a través de un nombre de dominio completo o una dirección IP.
  - Tener un certificado SSL disponible basado en un algoritmo RSA.

Validación de la configuración del servidor de directorio

1. Determine si existe una conexión con el servidor de directorio mediante el comando `ping`:
   `ping` *`nombre_de_host_del_servidor_de_directorio`*

2. Compruebe que la clave pública del certificado del servidor de directorio se basa en un algoritmo RSA.

   Si el servidor de directorio es en realidad una serie de servidores DNS que se ejecutan como un servidor DNS por turnos (DNS Round Robin), cada servidor de directorio tiene un certificado exclusivo. Utilice `nslookup` para obtener una lista de los servidores y elija uno.

   Conecte con un servidor mediante el comando `openssl s_client`. Especifique el nombre de host y el puerto.

   Copie el certificado del servidor en el campo Certificate (Certificado) de la pantalla Add Directory Server (Agregar servidor de directorio).

   Compruebe que el certificado especifica la clave pública como `RSA` (de *n* bits). La opción predeterminada para Microsoft Active Directory es RSA de 2048 bits.

3. Asegúrese de que la marca de tiempo del certificado es anterior a la hora del dispositivo.

   Esto puede ser motivo de preocupación si el dispositivo y el directorio se sincronizan con servidores de tiempo distintos o si se ejecutan en zonas horarias distintas.

4. Valide los contextos de búsqueda ejecutando el comando `ldapsearch` desde la consola del dispositivo.

Contexto de búsqueda	`CN`	`CN=Users`	`DC=example,DC=com` `Username: server_admin`

   En este ejemplo, el comando `ldapsearch`, utilizando TLS/SSL, debería ser parecido a este:

```
LDAPTLS_CACERT=location_of_certificate
ldapsearch -LLL
-Z -H ldaps://host_name:port
-b "base-DN"
-D "bind-DN"
-W [cn/uid/ssAMAccountName/userPrincipalName]
```

   En este ejemplo, el comando `ldapsearch`, sin utilizar TLS/SSL, debería ser parecido a este:

```
ldapsearch -LLL
-H ldap://IP_address:389
-b "cn=users,dc=example,dc=com"
-D "cn=server_admin,cn=users,dc=example,dc=com"
-W CN
```

C.4 Clases de objetos del esquema de LDAP

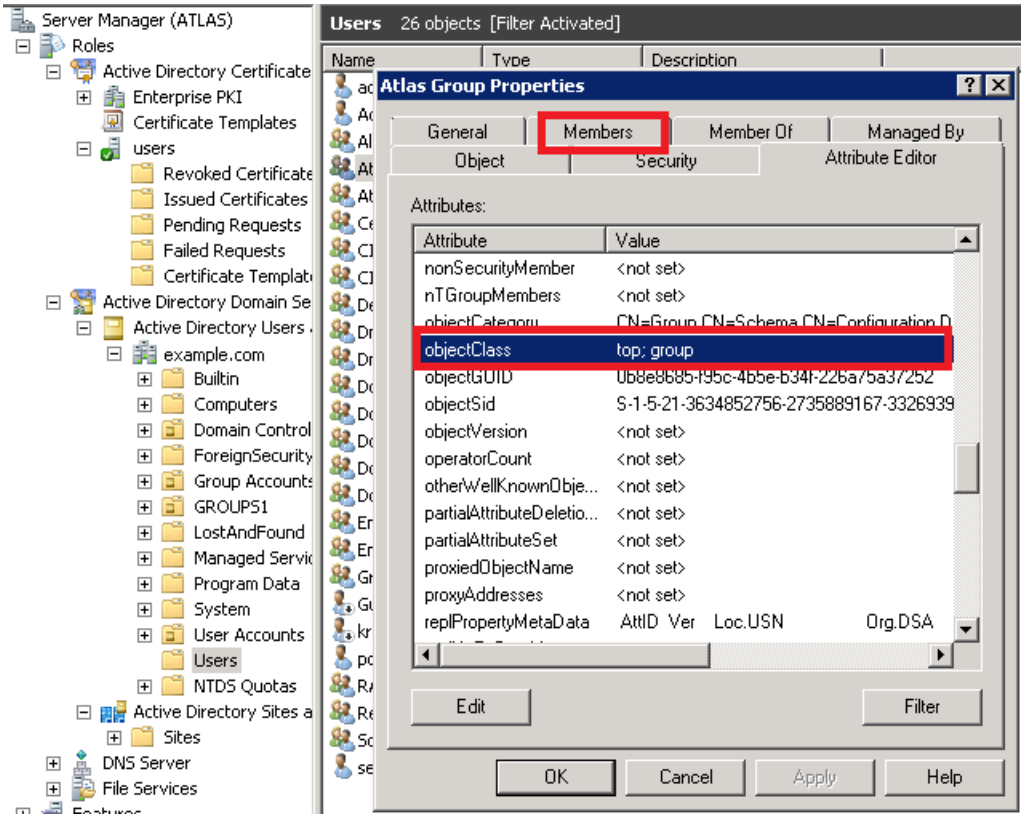
A continuación se ilustran los grupos, por tipo de directorio, creados con clases de objetos. Es necesario agregar dichos grupos LDAP a HPE OneView y asignarles roles. Consulte la ayuda en línea para obtener más información sobre cómo asignar roles.

Active Directory

En Active Directory, es posible crear un grupo con cualquiera de estas clases de objetos del esquema de LDAP:

- `groupofNames`
- `groups`
- `groupofUniqueNames`

Puede ver los miembros del grupo examinando las propiedades del nombre del grupo como se ilustra en este ejemplo:

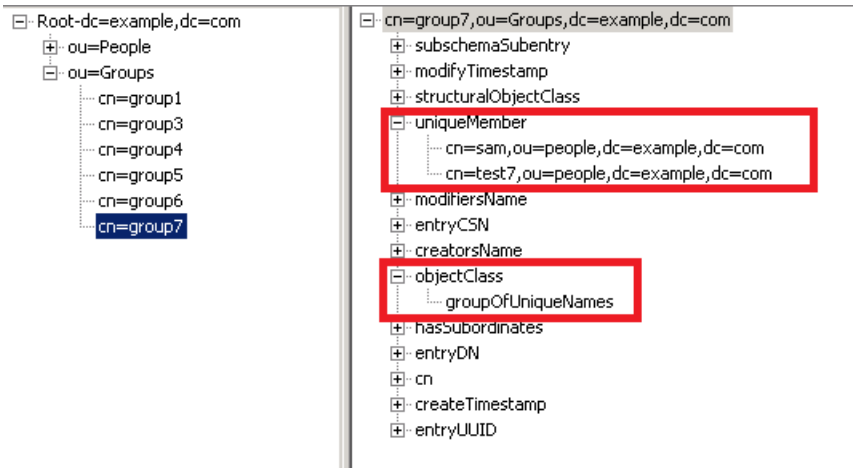


OpenLDAP

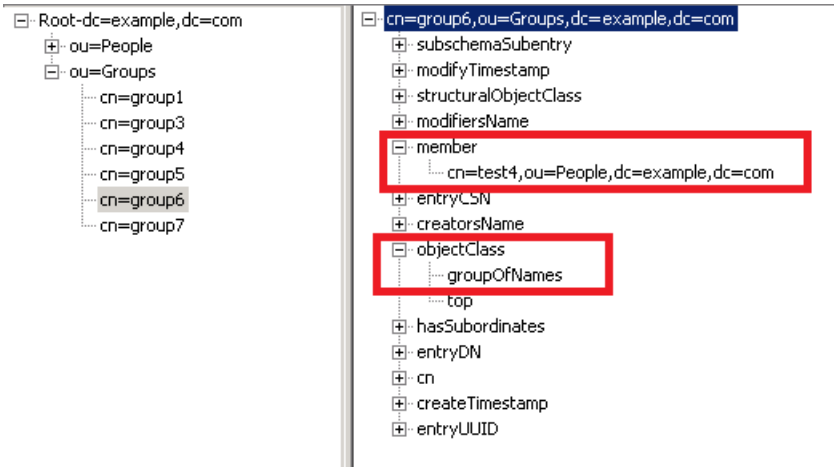
En OpenLDAP, se puede crear un grupo con cualquiera de estas clases de objetos del esquema de LDAP:

- `groupofUniqueNames`
- `groupofNames`

Los miembros de un grupo creado con la `objectClass` `groupOfUniqueNames` se encuentran en `uniqueMember`, como se ilustra en este ejemplo.



Los miembros de un grupo creado con la `objectClass` `groupOfNames` o `groups` se encuentran en `member`, como se muestra a continuación.


Root-dc=example,dc=com
ou=People
ou=Groups
cn=group1
cn=group3
cn=group4
cn=group5
cn=group6
cn=group7
cn=group6,ou=Groups,dc=example,dc=com
subschemaSubentry
modifyTimestamp
structuralObjectClass
modifiersName
member
cn=test4,ou=People,dc=example,dc=com
entryCSN
creatorsName
objectClass
groupOfNames
top
hasSubordinates
entryDN
cn
createTimestamp
entryUUID

D Instalación de HPE Smart Update Tools con HPE Insight Control server provisioning

Consulte la *Smart Update Tools User Guide* (Guía de usuario de Smart Update Tools) en **www.hpe.com/info/sut-docs** para obtener las instrucciones de instalación.Smart Update Tools (SUT) se puede instalar junto con el servidor HPE Insight Control que aprovisiona en servidores ProLiant.

SUT se instala en el modo Auto Deploy (Implementación automática). En el modo Auto Stage, SUT almacena provisionalmente los componentes en el servidor host en una ubicación temporal. Después de instalar instalado, para cualquier otra acción es necesario que el administrador del sistema operativo ejecute comandos desde la línea de comandos.

Para cambiar el modo de implementación de SUT a On Demand, Manual o modo de secuencia de comandos, que le permite controlar todas las solicitudes como argumentos de línea de comandos en el servidor, consulte la *Smart Update Tools User Guide* (Guía de usuario de Smart Update Tools) en **www.hpe.com/info/sut-docs**.

Para realizar implementaciones a escala en todos los servidores del centro de datos, consulte la *Smart Update Tools User Guide* (Guía de usuario de Smart Update Tools) en **www.hpe.com/info/sut-docs**.

NOTA: Cuando se configura SUT para ejecutarse en modo automático, SUT se ejecuta en el segundo plano del servidor del host. HPE OneView y SUT se comunican a través de la interfaz de HPE iLO REST. El estado de la instalación de firmware que se muestra en HPE OneView siempre se mantiene actualizado.

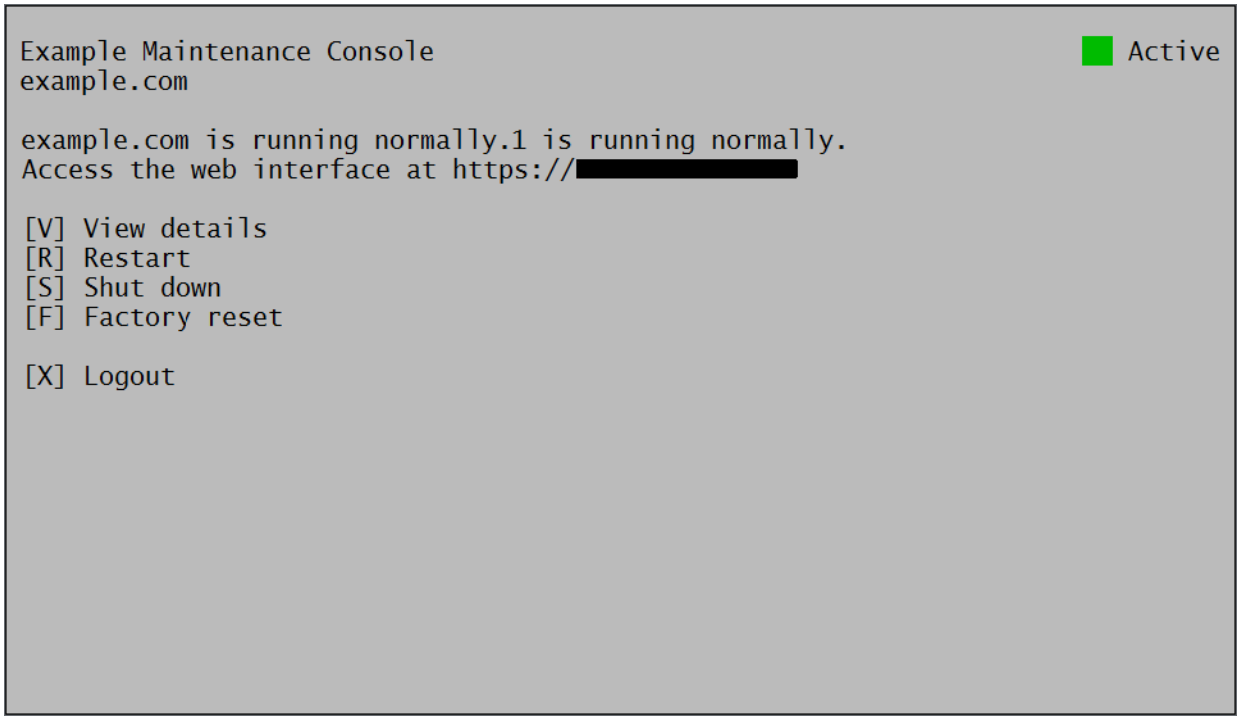
E Consola de mantenimiento

E.1 Acerca de la consola de mantenimiento

Para obtener información sobre el acceso a la consola de mantenimiento, consulte *Cómo acceder a la consola de mantenimiento*.

La consola de mantenimiento, que se muestra en la Figura 24, «Ejemplo del menú principal de la consola de mantenimiento», proporciona un conjunto limitado de comandos administrativos que podrían ser necesarios cuando no se puede acceder a la interfaz de usuario web del dispositivo (UI).

Figura 24 Ejemplo del menú principal de la consola de mantenimiento



En la parte superior izquierda de la mayoría de las pantallas de la consola de mantenimiento, se identifica el dispositivo local por su nombre de host.

La consola de mantenimiento muestra un icono y un mensaje sobre el estado del dispositivo, que puede indicar que está teniendo lugar una de las siguientes acciones:

- Funcionamiento normal
- El dispositivo está fuera de línea
- El dispositivo se está actualizando
- El dispositivo se está iniciando, apagando, reiniciando o no está disponible temporalmente
- El dispositivo se está restaurando desde un archivo de copia de seguridad
- Se está restableciendo la configuración predeterminada de fábrica del dispositivo

Comandos

El cuerpo del menú principal contiene comandos que se pueden utilizar para:

- Ver los detalles del dispositivo.
- Reiniciar el dispositivo local.
- Apagar el dispositivo.
- Restablecer la contraseña del administrador.
- Llevar a cabo una restauración a los valores de fábrica del dispositivo.
- Iniciar una consola de servicios, que un representante autorizado de soporte técnico puede utilizar para realizar un diagnóstico o reparar un problema.
- Cerrar la sesión de la consola de mantenimiento.

NOTA: Los comandos que muestra la consola de mantenimiento dependen del estado actual del dispositivo.

Navegación

- Utilice las teclas de flecha y de tabulador para desplazarse por la pantalla de la consola de mantenimiento.
- Los comandos se muestran con las correspondientes teclas de acceso directo. Estas teclas se muestran entre corchetes en la Figura 24, «Ejemplo del menú principal de la consola de mantenimiento». Al pulsar una tecla de acceso directo, se selecciona el comando.
- Puede utilizar la tecla **Intro** para invocar una selección. Es decir, después de realizar una selección, al pulsar **Intro** se ejecuta el comando.

Consulte también

- *Cómo acceder a la consola de mantenimiento*
- *Inicio de sesión en la consola de mantenimiento*
- *Visualización de los detalles del dispositivo*
- *Reinicio del dispositivo mediante la consola de mantenimiento*
- *Cómo apagar el dispositivo mediante la consola de mantenimiento*
- *Restablecimiento de la contraseña del administrador con la consola de mantenimiento*
- Lleve a cabo una restauración de fábrica del dispositivo utilizando la consola de mantenimiento

E.2 Sobre la contraseña de la consola de mantenimiento

La consola de mantenimiento no tiene ninguna contraseña inicial. Para configurarla, consulte «Restauración de la contraseña de la consola de mantenimiento».

Las contraseñas de la consola de mantenimiento deben cumplir los siguientes requisitos mínimos:

- Debe contener catorce (14) caracteres
- Una letra mayúscula alfa
- Una letra minúscula alfa
- Un número
- Un carácter especial

Las operaciones de copia de seguridad no hacen una copia de seguridad de la contraseña de la consola de mantenimiento. Asegúrese de poder recordar o recuperar la contraseña de la consola de mantenimiento de otra manera.

IMPORTANTE: La contraseña solo se puede reiniciar restaurando la aplicación a su configuración de fábrica original, que revierte la contraseña de la consola de mantenimiento a su configuración inicial: ninguna.

Más información

«Acerca de la consola de mantenimiento»
«Restauración de la contraseña de la consola de mantenimiento»
«Sobre la operación de restauración de fábrica»

E.3 Sobre la operación de restauración de fábrica

Una restauración de fábrica restaura el dispositivo a la configuración de fábrica original, pero no modifica la versión del firmware instalada.

⚠ **ATENCIÓN:** De forma predeterminada, la operación de restauración de fábrica borra los datos del dispositivo, incluidos los registros, los ajustes de red y la configuración de los dispositivos gestionados en HPE OneView. Tiene la opción de conservar explícitamente los registros y los ajustes de red.

Conservar los ajustes de red es la opción más segura cuando se intenta recuperar el dispositivo de un error porque el dispositivo sigue siendo accesible desde la red.

Asegúrese de tener un archivo de copia de seguridad reciente antes de realizar esta operación.

La operación de restauración de fábrica puede realizarse desde la interfaz de usuario o desde la consola de mantenimiento.

Utilice la operación de restauración de fábrica por cualquiera de estos motivos:

- Para dar de baja el dispositivo y migrar el hardware.
- Para devolver el dispositivo a un estado conocido para volver a utilizarlo (por ejemplo, para restaurar el dispositivo desde un archivo de copia de seguridad).

Más información

Restablecimiento del dispositivo a la configuración original de fábrica
Lleve a cabo una operación de restauración de fábrica utilizando la consola de mantenimiento
Acerca de la realización de copias de seguridad del dispositivo

E.4 Cómo acceder a la consola de mantenimiento

Acceda a la consola de mantenimiento a través de la consola virtual o de una conexión SSH.

NOTA: Utilice las credenciales para las credenciales del administrador de infraestructuras local cuando se le pidan. Puede restaurar la contraseña del administrador con la consola de mantenimiento.

Acceso a la consola de mantenimiento desde una conexión SSH

NOTA: Hewlett Packard Enterprise recomienda el uso de estas herramientas para acceder a la consola de mantenimiento a través de una conexión SSH:

- PuTTY
- MTPuTTY
- Consola vSphere/vCenter

Acceso a la consola de mantenimiento con SSH

1. Llame a una de las herramientas recomendadas al equipo local.
2. Acceda a la consola de dispositivos virtual especificando su nombre de dominio completamente cualificado o dirección IP.
3. Introduzca el nombre de usuario `maintenance` en el indicador de inicio de sesión.
4. Inicie la sesión en la consola de mantenimiento.

Acceso a la consola de mantenimiento desde la consola virtual

1. Acceda a la consola del dispositivo virtual.
2. Introduzca el nombre de usuario `maintenance` en el indicador de inicio de sesión.
3. Inicie la sesión en la consola de mantenimiento.

Más información

«Acerca de la consola de mantenimiento»

E.5 Inicio de sesión en la consola de mantenimiento

Cuando se accede a la consola de mantenimiento, se muestra una pantalla de inicio de sesión o el menú principal de la consola de mantenimiento:

- Si se accede a través de la consola del dispositivo, aparece inmediatamente el menú principal de la consola de mantenimiento.

  Después de introducir el primer comando y antes de que se ejecute, se presenta la pantalla de inicio de sesión.

  Hay dos excepciones: **Reset password** (Restablecer contraseña) y **Launch service console** (Iniciar la consola de servicios), que requieren una autorización de desafío/respuesta. Para obtener información sobre cómo restablecer la contraseña, consulte «Restablecimiento de la contraseña del administrador con la consola de mantenimiento».

- Si se accede a través de SSH, se muestra inmediatamente la pantalla de inicio de sesión.

Para iniciar sesión, escriba el nombre de usuario y la contraseña de una cuenta local de administrador de infraestructuras de este dispositivo.

NOTA: No se puede iniciar sesión usando una cuenta de administrador de infraestructuras que se autentica mediante un servicio de directorio de autenticación.

El inicio de sesión en la consola de mantenimiento es válido durante una hora. Tras una hora de inactividad, tendrá que volver a introducir la contraseña. La sesión de la consola de mantenimiento se cierra tras 24 horas de inactividad.

Más información

«Acerca de la consola de mantenimiento»
«Cómo acceder a la consola de mantenimiento»
«Detalles de la pantalla del menú principal de la consola de mantenimiento»

E.6 Detalles de la pantalla del menú principal de la consola de mantenimiento

Componente de la pantalla	Descripción
Título	Identifica la consola de mantenimiento de HPE OneView.
Identificador de dispositivo	Identifica un dispositivo por su nombre de host. Se encuentra justo debajo del título.
Icono	Indica el estado general del dispositivo. El icono se encuentra en la parte superior derecha de la pantalla de la consola.

Texto de estado	Muestra de una a tres líneas de texto adicional para explicar el estado indicado por el icono. Estos son algunos ejemplos de estados:
	`Restoring from backup (Restaurado desde una copia de seguridad)`
	`Starting (Iniciando)`

Componente de la pantalla	Descripción
Barra superior de notificación	Notifica o advierte de una situación relacionada con el dispositivo. La barra superior de notificación abarca toda la anchura de la consola de mantenimiento. La barra superior de notificación no se muestra cuando no hay ninguna notificación pendiente.

Comandos	Presenta una lista de los comandos disponibles que son apropiados para el estado del dispositivo. Estos son algunos ejemplos:
	`View details (Ver detalles)`
	`Restart (Reiniciar)`
	`Shut down (Apagar)`
	`Reset password (Restablecer contraseña)`
	`Restauración de fábrica`
	`Launch service console (Iniciar la consola de servicios)`

Consulte también

- «Acerca de la consola de mantenimiento»
- «Cómo acceder a la consola de mantenimiento»
- «Inicio de sesión en la consola de mantenimiento»
- «Visualización de los detalles del dispositivo»
- «Reinicio del dispositivo mediante la consola de mantenimiento»
- «Cómo apagar el dispositivo mediante la consola de mantenimiento»
- «Restablecimiento de la contraseña del administrador con la consola de mantenimiento»

E.7 Detalles de la pantalla Details de la consola de mantenimiento

El comando View Details (Ver detalles) muestra esta pantalla.

Componente de la pantalla	Descripción
Título	Identifica la consola de mantenimiento de HPE OneView.
Identificador de dispositivo	Identifica un dispositivo por su nombre de host. Se encuentra justo debajo del título.
Icono	Indica el estado general del dispositivo en la parte superior derecha.

Texto de estado	Muestra de una a tres líneas de texto adicional para explicar el estado del icono. Estos son algunos ejemplos de texto de estado:
	`Restoring from backup (Restaurado desde una copia de seguridad)`
	`Starting (Iniciando)`
	`Active (Activo)`

Barra superior de notificación	Notifica o advierte de una situación relacionada con el clúster del dispositivo. La barra superior de notificación abarca toda la anchura de la consola de mantenimiento. La barra superior de notificación está oculta cuando no hay ninguna notificación pendiente.
Nombre de host	Muestra el nombre de host del dispositivo.
Dirección IP	Muestra la dirección IP del dispositivo.
Modelo	El número de modelo del dispositivo en que se ejecuta HPE OneView.

Componente de la pantalla	Descripción
Firmware	El número de versión del firmware que se ejecuta en el dispositivo HPE OneView y la fecha en que se actualizó el firmware por última vez.
Número de serie	El número serie del dispositivo.

E.8 Estados de dispositivo de la consola de mantenimiento

La consola de mantenimiento muestra un icono y un mensaje en la esquina superior derecha sobre el estado del dispositivo. El estado puede depender de la situación, sobre todo para un clúster de dispositivos de alta disponibilidad, y también puede que sea necesaria una acción.

Estado de activación	Situación	Action (Acción)
Active (Activo)	El dispositivo local es el dispositivo activo del clúster de dispositivos y funciona con normalidad.	
Active (Activo) El disco ha fallado	No es un clúster de dispositivos.	Póngase en contacto con su representante de soporte autorizado para cambiar el disco estropeado
	El disco del dispositivo activo ha fallado. El dispositivo en espera asume el control como el único dispositivo.	Póngase en contacto con su representante de soporte autorizado para cambiar el disco estropeado
	El disco del dispositivo en espera ha fallado. El dispositivo activo sigue funcionando como dispositivo único.	Póngase en contacto con su representante de soporte autorizado para cambiar el disco estropeado
Active (Activo) En espera se está sincronizando	El dispositivo local funciona con normalidad. El dispositivo compañero se está sincronizando. Si se produce un error antes de que acabe la sincronización, no se puede activar.	
Active (Activo) No se puede conectar con el dispositivo en espera Cambios no sincronizados	El dispositivo local funciona con normalidad pero no puede contactar con el dispositivo compañero. El dispositivo compañero no se puede convertir en el dispositivo activo en caso de error.	Consulte las alertas que aparecen en la pantalla **Activity** (Actividad) para obtener más información y una solución.
Modo de espera.	El dispositivo local es el dispositivo en espera del clúster de dispositivos y funciona con normalidad.	
Modo de espera. El disco ha fallado	El disco del dispositivo local ha fallado. El dispositivo local ya no puede utilizarse como el dispositivo en espera en el clúster de dispositivos.	Póngase en contacto con su representante de soporte autorizado para cambiar el disco estropeado
	El disco del dispositivo compañero ha fallado. Actualmente, el dispositivo local es el dispositivo en espera, pero se activará automáticamente.	Póngase en contacto con su representante de soporte autorizado para cambiar el disco estropeado

Estado de activación	Situación	Action (Acción)
Modo de espera. Sincronización	El dispositivo local es el dispositivo en espera y se está sincronizando. Si se produce un error antes de que acabe la sincronización, no se puede activar.	
Sin conexión Se requiere acción manual	El dispositivo local no se puede activar automáticamente porque no puede confirmar que el dispositivo compañero no esté en ejecución.	Para obtener más información sobre la resolución del problema, consulte «El dispositivo está desconectado, se requiere acción manual.»
Sin conexión Error imposible de recuperar	El dispositivo ha fallado con un error imposible de recuperar.	Para obtener más información sobre la resolución del problema, consulte «Oops (¡Vaya!)».
Sin conexión Inservible (datos incompletos)	El dispositivo local no se puede activar porque no dispone de una copia completa de los datos del dispositivo.	Para obtener más información sobre la resolución del problema, consulte «El dispositivo está desconectado e inservible»
Resetting (Restableciendo)	Se está restableciendo la configuración predeterminada de fábrica del dispositivo. En un clúster de dispositivos, esta operación tiene lugar antes de que el dispositivo en espera se convierte en el dispositivo activo.	
Reiniciando	El dispositivo se está reiniciando y estará disponible en breve.	
Restoring from backup (Restaurado desde una copia de seguridad)	El dispositivo se reiniciará cuando se complete la restauración.	
Starting (Inicio)	El dispositivo local se está iniciando y estará disponible en breve.	
Starting (Inicio) Recuperación de un fallo	El dispositivo compañero ha sufrido un fallo y el dispositivo local se está activando.	Para obtener información sobre cómo determinar la causa del fallo, consulte «Apagado inesperado del dispositivo».
Apagado	El dispositivo local se está apagando.	
Temporarily unavailable (No disponible temporalmente)	El dispositivo local está en transición y su estado cambiará.	
Actualización	El dispositivo local está pasando por una actualización del software.	

E.9 Lleve a cabo una de restauración de fábrica utilizando la consola de mantenimiento.

Requisitos previos

- Asegúrese de que todos los usuarios han cerrado su sesión y de que todo el trabajo en curso está terminado.
- Realice una copia de seguridad de todos los archivos de usuario.
- Cree un archivo de volcado de soporte y guárdelo en una ubicación externa para mantenerlo a salvo.

Realización de una de restauración de fábrica utilizando la consola de mantenimiento

1. Acceda al menú principal de la consola de mantenimiento.

2. Seleccione **Factory reset** (Restauración de fábrica) en el menú principal.
3. En el cuadro de diálogo siguiente, realice una de las acciones siguientes:
   a. Escriba **Y** para seguir con la operación de restauración de fábrica.

   △ **ATENCIÓN:** Esta opción borra los registros y los ajustes de red.
   Utilice esta opción para dar de baja un dispositivo.

   b. Escriba **P** para continuar con la operación de restauración de fábrica, pero conservar los registros y los ajustes de red.
      Utilice esta opción si quiere restaurar una aplicación desde un archivo de copia de seguridad o si quiere aplicar una nueva configuración.
   c. Escriba **N** para cancelar la operación de restauración de fábrica y volver al menú principal.

   Confirme que desea llevar a cabo la restauración de fábrica en los cuadros de diálogo posteriores.
4. En el cuadro de diálogo siguiente, realice una de las acciones siguientes:
   a. Escriba **Y** para seguir con la operación de restauración de fábrica.
   b. Escriba **N** para cancelar la operación de restauración de fábrica y volver al menú principal.
5. Compruébelo observando la operación.

Más información

«Sobre la operación de restauración de fábrica»

E.10 Restablecimiento de la contraseña del administrador con la consola de mantenimiento

Si pierde u olvida la contraseña de administrador local, utilice el procedimiento siguiente para restablecerla.

Esta operación proporciona un **código de solicitud** exclusivo que debe usar al ponerse en contacto con su representante autorizado de soporte técnico.

⓵ **IMPORTANTE:** El **código de solicitud** es válido únicamente desde la pantalla **Password reset** (Restablecimiento de la contraseña) de la consola de mantenimiento. Si se vuelve al menú principal o se finaliza la sesión de la consola de mantenimiento, el código de solicitud no será válido. Necesitará volver a comenzar este procedimiento para adquirir un nuevo código de solicitud.

Necesitará ponerse en contacto con su representante autorizado de soporte técnico, que le enviará un **código de autorización** (también conocido como código de respuesta) después de verificar su información.

⓵ **IMPORTANTE:** El **código de autorización** debe introducirse antes de que pase una hora, o dejará de ser válido.

NOTA:

- Esta función no está disponible si ha accedido a la consola de mantenimiento a través de SSH. Si se conoce la contraseña de otro administrador de infraestructuras local, utilice la interfaz de usuario (UI) para restablecer la contraseña del administrador.
- Esta operación restablece la contraseña de una cuenta de administrador local en el dispositivo. No se aplica a las cuentas de administrador autenticadas por un servicio de directorio.
- Esta operación le permite establecer una contraseña de un solo uso para la cuenta local `administrator`.

  Utilice esa contraseña de un solo uso la próxima vez que inicie sesión en la interfaz de usuario con esta cuenta. El sistema le pedirá que establezca una contraseña nueva.

Para obtener información sobre cómo ponerse en contacto con Hewlett Packard Enterprise por teléfono, consulte Acceso al soporte de Hewlett Packard Enterprise.

Requisitos previos

- Debe tener acceso a la consola del dispositivo.

Restablecimiento de la contraseña de administrador con la consola de mantenimiento

1. Acceda a la consola del dispositivo virtual.
2. Acceda al menú principal de la consola de mantenimiento.
3. Seleccione **Reset password** (Restablecer contraseña).

   La consola de mantenimiento muestra un código de solicitud.
4. Llame por teléfono su representante autorizado de soporte técnico y proporciónele la información siguiente:
   - El nombre de la persona que solicita el restablecimiento de la contraseña.
   - El nombre de la empresa propietaria del dispositivo.
   - El código de solicitud de la consola de mantenimiento.

   El representante autorizado de soporte técnico comprueba la información y, a continuación, envía un mensaje a la dirección de correo electrónico autorizada que tiene registrada. Este mensaje contiene el código de autorización. El mensaje incluye una imagen ISO, que también es el código de autorización.
5. Realice una de las acciones siguientes para introducir el código de autorización en el campo de respuesta:
   - Si puede pegar información en la consola de mantenimiento, copie el código de autorización del mensaje de correo electrónico y péguelo en el campo de respuesta de la consola de mantenimiento.
   - Lea el código de autorización desde la imagen ISO:
     1. Guarde la imagen ISO que se incluye en el mensaje de correo electrónico.
     2. Monte la imagen ISO como un montaje de Virtual Media (un CD-ROM virtual).
     3. Seleccione **Read from ISO** (Leer desde ISO) en la consola de mantenimiento.
     4. La consola de mantenimiento lee la imagen ISO y, pasado un momento, rellena automáticamente el campo de respuesta con el código de autorización.
   - Introduzca el código de autorización en el campo de respuesta manualmente.
6. Elija una contraseña de administrador de un solo uso.
7. Cuando se le indique, escriba dos veces la contraseña nueva.
8. Seleccione **OK** (Aceptar) para definir la contraseña solo uso.
9. Inicie sesión en la interfaz de usuario con esta cuenta, utilizando la contraseña de un solo uso.
10. Establezca una contraseña nueva para esta cuenta en la pantalla que se visualiza.

11. Cierre la sesión y vuelva a iniciarla con la contraseña nueva para comprobar que funciona.

Más información

- «Acerca de la consola de mantenimiento»
- «Cómo acceder a la consola de mantenimiento»
- «Inicio de sesión en la consola de mantenimiento»
- Acceso al soporte de Hewlett Packard Enterprise

E.11 Restauración de la contraseña de la consola de mantenimiento

Requisitos previos

- Cree una nueva contraseña que cumpla los requisitos de la contraseña.
- Si olvida la contraseña de la consola de mantenimiento actual:
  1. Realice una copia de seguridad.
  2. Realice una copia de seguridad de todos los datos de usuario.
  3. Asegúrese de que todos los usuarios hayan cerrado sesión y de que no haya tareas en ejecución.
  4. Lleve a cabo una restauración de fábrica en el dispositivo.

     Tras una restauración de fábrica, la contraseña de la consola de mantenimiento no está habilitada.

Restauración de la contraseña de la consola de mantenimiento

1. Acceda a la consola del dispositivo virtual.
2. Inicie sesión con el nombre de usuario `maintenance` y la contraseña (si se ha configurado) en la ventana emergente del inicio de sesión.
3. Acceda al menú principal de la consola de mantenimiento.
4. Seleccione **Reset maintenance console password** (Restaurar la contraseña de la consola de mantenimiento).
5. Escriba la contraseña actual y la nueva dos veces, una vez para verificarla.
6. Seleccione **OK**.

E.12 Reinicio del dispositivo mediante la consola de mantenimiento

En este procedimiento se describe cómo utilizar la consola de mantenimiento para apagar y, a continuación, reiniciar el dispositivo.

Requisitos previos

- Asegúrese de que todos los usuarios han cerrado su sesión y de que todo el trabajo en curso está terminado.

Cómo reiniciar el dispositivo mediante la consola de mantenimiento

1. Acceda al menú principal de la consola de mantenimiento.
2. Seleccione **Restart** (Reiniciar).

   Confirme que desea reiniciar el dispositivo.
3. Compruebe que el dispositivo se reinicia.

Consulte también

- «Cómo acceder a la consola de mantenimiento»
- «Inicio de sesión en la consola de mantenimiento»
- «Detalles de la pantalla del menú principal de la consola de mantenimiento»
- «Cómo apagar el dispositivo mediante la consola de mantenimiento»

E.13 Cómo apagar el dispositivo mediante la consola de mantenimiento

En este procedimiento se describe cómo utilizar la consola de mantenimiento para realizar un cierre correcto del dispositivo.

Requisitos previos

- Asegúrese de que todos los usuarios han cerrado su sesión y de que todo el trabajo en curso está terminado.

Apagado del dispositivo mediante la consola de mantenimiento

1. Acceda al menú principal de la consola de mantenimiento.
2. Seleccione **Shut down** (Apagar) en el menú principal.

   Confirme que desea apagar el dispositivo.
3. Compruebe que el dispositivo se apaga.

Consulte también

- «Cómo acceder a la consola de mantenimiento»
- «Inicio de sesión en la consola de mantenimiento»
- «Detalles de la pantalla del menú principal de la consola de mantenimiento»
- «Reinicio del dispositivo mediante la consola de mantenimiento»

E.14 Visualización de los detalles del dispositivo

Utilice este procedimiento para mostrar los detalles del dispositivo, como el estado, el nombre de host, la dirección IP, el modelo y el firmware.

Cómo ver de los detalles del dispositivo

1. Acceda al menú principal de la consola mantenimiento.
2. Seleccione **View details** (Ver detalles).

   Se muestra la pantalla de detalles de la consola de mantenimiento.

Consulte también

- «Detalles de la pantalla Details de la consola de mantenimiento»
- «Cómo acceder a la consola de mantenimiento»
- «Inicio de sesión en la consola de mantenimiento»

Índice

D

E

F

G

H

I

R

S

T

U

V

W