Dispositivos Dell EMC PowerProtect de la serie DP

Guía de instalación y actualización

2.7.1

Diciembre de 2021
Rev. 01

DELL EMC

Notas, precauciones y advertencias

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Tabla de contenido

1

Introducción

Temas:

Alcance del documento y público de destino

En este documento, se describe PowerProtect DP Series Appliance cómo instalar el hardware (rack y pila) y realizar la configuración inicial de software después de configurar el hardware del dispositivo.

El público objetivo de este documento incluye personal de campo, partners y clientes que administran y operan PowerProtect DP Series Appliance.

Convenciones de denominación de productos y cambios de terminología

En la siguiente tabla, se describen los cambios recientes de nombre y terminología en IDPA/PowerProtect DP Series Appliance a partir de la versión 2.7.

Tabla 1. Convenciones de denominación de productos y cambios de terminología

Nombre de producto o componente existente	Nombre o terminología nuevos
Virtual Machines	Services
ESXi	Hypervisor
vSphere	Hypervisor Platform
vCenter/vCSA (VM)	Hypervisor Manager
vCenter service daemon	Hypervisor Manager Service Daemon
vSAN	Storage Pool
ACM (VM)	Appliance Configuration Manager (Service)
dpatools	Infrastructure Management Service
PT-Agent	Node Event Service
Avamar (VM)	Protection Software (Service)
Avamar Proxy/vProxy (VM)	VM Proxy (Service)
DD/DDVE	Protection Storage
DPC (VM)	Data Protection Central (Service)
DPA	Reporting & Analytics
(DP)Search	Search
CDRA (VM)	Cloud DR (Service)

Tabla 1. Convenciones de denominación de productos y cambios de terminología (continuación)

Nombre de producto o componente existente	Nombre o terminología nuevos
CDRS	Cloud DR Server
Cyber Recovery (VM)	Cyber Recovery (Service)
Integrated Dell Remote Access Controller (iDRAC)	iDRAC
iDRAC Service Module (iSM)/iSM service	iDRAC Service Module

Características del producto

PowerProtect DP Series Appliance proporciona una configuración simplificada y la integración de componentes de protección de datos en una solución consolidada.

Solución integrada

PowerProtect DP Series Appliance es una solución convergente que ofrece funcionalidades completas de respaldo, replicación, recuperación, desduplicación, acceso instantáneo, restauración, búsqueda, creación de informes y análisis, preparación para la nube con recuperación ante desastres y retención a largo plazo en la nube, todo en un solo dispositivo. El dispositivo está disponible en diversas configuraciones en función de sus requisitos y capacidad de almacenamiento.

- DP4400
- DP5900
- DP8400
- DP8900

El modelo DP4400 es un sistema de 2U hiperconvergente que un usuario puede instalar y configurar en el sitio.

DP4400 incluye una edición virtual del servidor de Protection Software (Protection Software (Service)) como el nodo de Protection Software, una edición virtual del sistema Protection Storage (Protection Storage) como el nodo de Protection Storage Cloud DR, Data Protection Central como una administración centralizada del sistema, un Appliance Configuration Manager (ACM) para la configuración y las actualizaciones simplificadas, Cyber Recovery, Search, Reporting & Analytics y un nodo de computación que aloja los componentes virtuales y el software.

DP4400 contiene un servidor de Hypervisor, que aloja todas estas ediciones virtuales de los productos puntuales mencionados anteriormente.

NOTA: El nodo Cloud DR está disponible en el dispositivo según la licencia que tenga.

Los componentes Search, Reporting & Analytics y Cloud DR son opcionales. Además, puede realizar las funciones de Search, Reporting & Analytics y Cloud DR en una implementación corporativa central con Data Protection Central.

La solución Cyber Recovery (CR) es compatible con las nuevas instalaciones de DP4400. Para obtener información sobre los requisitos previos, los requisitos de dirección IP, la configuración y la replicación, consulte Implementación de Cyber Recovery para PowerProtect DP4400 en la página 38.

Si su organización permite la comunicación a través de Internet, como parte de la configuración inicial del sistema, puede registrar el dispositivo PowerProtect DP Series Appliance los componentes Protection Software, Protection Storage y con Secure Remote Services (anteriormente ESRS). Secure Remote Services es un sistema de soporte de servicio al cliente seguro, basado en IP y distribuido que proporciona a los clientes de Dell EMC el comando, el control y la visibilidad de las actividades relacionadas con el soporte.

Administración centralizada

Data Protection Central proporciona funcionalidades avanzadas de monitoreo y administración de desde un solo panel e incluye las siguientes funciones PowerProtect DP Series Appliance.

- Un tablero integral que le permite administrar e incluye información sobre los componentes Protection Software, Protection Storage, Search y .
  - Actividades de respaldo
  - Actividades de replicación
  - Activos

- Capacity
- Estado
- Alertas

- Operaciones avanzadas de búsqueda y recuperación mediante la integración con Search.
- Funcionalidades integrales de creación de informes
- Respaldos en la nube.

Administración de dispositivos

ACM proporciona una interfaz basada en web para configurar, monitorear y actualizar el dispositivo.

El tablero de ACM muestra un resumen de la configuración de los componentes individuales. También permite a los administradores monitorear el dispositivo, modificar los detalles de configuración, como expandir la capacidad del disco Protection Storage, cambiar la contraseña común para el dispositivo, actualizar la información del cliente y cambiar los valores en el panel Configuración general. El panel Configuración general del tablero de ACM le permite cambiar la configuración de LDAP, muestra las zonas horarias, el estado del servidor NTP, el estado del servidor LDAP externo, el estado de FIPS, etc. El tablero ACM le permite actualizar el sistema y sus componentes. También muestra la información de estado del servidor del dispositivo y los componentes de VMware.

Administración de respaldo

PowerProtect DP Series Appliance utiliza servidores Protection Software (Service) para los modelos DP4xxx que realizan operaciones de respaldo, con los datos almacenados en un sistema Protection Storage.

También puede agregar un Protection Software NDMP Accelerator (debe configurar manualmente NDMP Accelerator) para habilitar el respaldo y la recuperación de sistemas NAS. Para obtener más información sobre los detalles de configuración, consulte Opciones de configuración para el modelo DP4400 en la página 9. El Protection Software NDMP Accelerator utiliza el protocolo de administración de datos en red (NDMP) para activar el respaldo y recuperación de sistemas de almacenamiento conectado en red (NAS). El acelerador lleva a cabo el procesamiento de NDMP y envía los datos directamente al servidor de Protection Storage (almacenamiento de Protection Storage)

Reporting and Analytics

La característica ofrece una funcionalidad muy sólida de creación de informes con secciones dedicadas para diversas funciones. Estos informes lo ayudan a recuperar información sobre Protection Storage y Protection Software. Con estos informes, puede identificar interrupciones en el ambiente, diagnosticar problemas, planificar tareas para disminuir los riesgos y pronosticar tendencias futuras. También puede ejecutar informes personalizados y del sistema, plantillas de tablero y programar la generación de informes según sus requisitos.

Buscar

La función Search proporciona una manera eficaz de buscar datos de respaldo dentro de PowerProtect DP Series Appliance y, a continuación, restaurar los datos de respaldo en función de los resultados de Search. Las actividades de recopilación programadas se utilizan para recopilar e indexar los metadatos (como palabra clave, nombre, tipo, ubicación, tamaño y servidor/cliente de respaldo, o contenido indexado) del respaldo, que luego se almacena en PowerProtect DP Series Appliance.

Recuperación ante desastres

Cloud DR es una solución que permite la recuperación ante desastres de una o más serviciosen las instalaciones a la nube. Cloud DR se integra con el software de respaldo en las instalaciones existente y un sistema Protection Storage para copiar los respaldos de VM a la nube. A continuación, puede ejecutar una prueba de recuperación ante desastres o una conmutación por error, que convierte una VM en una instancia de Elastic Compute Cloud (EC2) de Amazon Web Services y, a continuación, ejecuta esta instancia en la nube.

NOTA: La instalación de componentes Cloud DR, Search y (según) es opcional. Además, si estos componentes ya están configurados en el entorno, el dispositivo se puede configurar para usar la implementación central en el entorno. No es necesario configurar los componentes opcionales que se incluyen en PowerProtect DP Series Appliance nuevamente.

NOTA: Durante la configuración de la red, si selecciona protocolo de red IPv6, entonces Cloud DR y Search se deshabilitan.

Sin embargo, el tablero no muestra ningún dato asociado con Cloud DR, Search y . Además, debe administrar y configurar cualquiera de estas instancias externas. Además, PowerProtect DP Series Appliance no es compatible con Search local y Análisis (no forma parte de PowerProtect DP Series Appliance. pero se implementa de forma centralizada en el entorno del cliente) cuando estas funciones son realizadas por implementaciones externas.

Cyber Recovery

La solución de Cyber Recovery mantiene configuraciones de tecnología y datos empresariales de misión crítica en un entorno de 'vault' seguro y aislado físicamente de la red, que se puede utilizar para la recuperación o el análisis. Cyber Recovery Vault (CR Vault) está físicamente aislado del sistema de producción o de la red. La solución de Cyber Recovery permite el acceso a CR Vault solamente durante el tiempo suficiente para replicar los datos desde el sistema de producción. En todas las demás ocasiones, CR Vault se protege y se desconecta de la red. Se ejecuta un proceso de desduplicación en el entorno de producción para acelerar el proceso de replicación, de modo que el tiempo de conexión a Cyber Recovery sea lo más breve posible. Dentro de Cyber Recovery, el software de Cyber Recovery crea copias con bloqueo de retención de punto en el tiempo (PIT), que se pueden validar y utilizar para la recuperación del sistema de producción. La implementación de la solución Cyber Recovery como parte del dispositivo PowerProtect serie DP permite la protección de datos de misión crítica vulnerables a los ataques cibernéticos.

Consulte Implementación de Cyber Recovery para PowerProtect DP4400 en la página 38 para obtener más información.

Escalabilidad

Los modelos PowerProtect DP Series Appliance están diseñados para ser escalables, de modo que puedan escalar verticalmente con necesidades en constante cambio. Consulte la sección *Expanding storage capacity* en la *Guía de instalación PowerProtect DP Series Appliancede Dell EMC* para obtener más información sobre cómo agregar capacidad de almacenamiento.

- Para el modelo DP4400 con una capacidad de 8 TB a 24 TB, puede expandir la capacidad de almacenamiento en múltiplos de incrementos de 4 TB hasta 24 TB. Al agregar el kit de expansión de discos, también puede expandir la capacidad más allá de 24 TB en incrementos de 12 TB.
- Para el modelo DP4400 con una capacidad de 24 TB a 96 TB, puede expandir la capacidad de almacenamiento en incrementos de 12 TB y puede expandir la capacidad hasta un máximo de 96 TB.

En la siguiente tabla se detalla la configuración de los modelos PowerProtect DP Series Appliance.

Tabla 2. Configuración para el modelo PowerProtect DP Series Appliance

Modelo	Detalles de la configuración
DP4400	De 8 TB a 24 TB
	De 24 TB a 96 TB

Soporte unificado

El mismo equipo de Servicio al cliente es compatible con el hardware y el software utilizados en el dispositivo.

Configuración detallada

PowerProtect DP Series Appliance está disponible en los siguientes modelos:

Tabla 3. Opciones de configuración para el modelo DP4400

Modelo	Modelo de Protection Storage	Opciones de configuración de Protection Storage (TB utilizables)	Protection Software	Nodo acelerador de Protection Software para respaldo de NDMP/NAS (opcional)
DP4400	Protection Storage	8, 12, 16, 20 o 24 TB	Protection Software (Service) 3 TB	NDMP Accelerator (1)
DP4400	Protection Storage	24, 36, 48, 60, 72, 84 o 96 TB	Protection Software (Service) 3 TB	NDMP Accelerator (1)

2

Instalar y configurar PowerProtect DP Series Appliance para DP4400

En esta sección, se detalla cómo instalar PowerProtect DP Series Appliance para el hardware de DP4400. También se explica cómo realizar la configuración inicial de software después de configurar el hardware del dispositivo.

Temas:

Instalar el hardware de PowerProtect DP Series Appliance

Esta sección está diseñada para el personal que instala, configura y mantiene el PowerProtect DP Series Appliance para DP4400, y por lo que debe estar familiarizado con el equipo de almacenamiento digital y el cableado.

Requisitos previos

Los siguientes son los requisitos previos para instalar el hardware de PowerProtect DP Series Appliance.

Requisitos previos

Verifique que tenga los siguientes componentes:

- Sistema DP4400 de 2U
- Kit de rieles, que incluye:
  - Dos rieles deslizantes
  - Dos tiras de velcro
  - Cuatro tornillos
  - Cuatro arandelas
- Dos cables de alimentación
- Bisel
- Destornillador Phillips con punta magnética (no suministrado)
- Muñequera antiestática y almohadilla de espuma conductora

Tabla 4. Cables Ethernet calificados

Tipo de switch	Tipo de NIC	Velocidad	Cable requerido
SFP+ de 10 Gb	SFP+ (óptico)	10 GB	LC a LC con GBIC ópticos SR o Twinax
RJ45 de 1 Gb o 10 Gb	SFP+ con 1 GbBASE-T GBIC	1 GB	UTP con RJ45 (Cat5e o Cat6)
RJ45 de 1 Gb o 10 Gb	10 GbBASE-T (RJ45)	1 Gb o 10 Gb (según el switch)	UTP/STP con RJ45 (Cat6a o Cat7)

Instale las guías

Sobre esta tarea

Los rieles están etiquetados a la izquierda y a la derecha, y no pueden intercambiarse. El frente de cada riel tiene la etiqueta **Parte frontal izquierda** o **Parte frontal derecha** cuando se ve desde la parte frontal del gabinete.

Pasos

1. Determine dónde montar el sistema y use cinta de enmascarar o una lapicera con punta de fieltro para marcar la ubicación en la parte frontal y posterior del gabinete.

   NOTA: Instale el ensamblaje del riel izquierdo primero.

2. Extienda completamente el soporte deslizante trasero del riel.
3. Coloque la pieza del extremo del riel con la etiqueta **Parte frontal izquierda** hacia adentro y oriente la pieza del extremo posterior para alinearla con los orificios en los rebordes de la carcasa posterior.
4. Empuje el riel hacia la parte posterior del rack hasta que el pestillo quede fijo en su lugar.

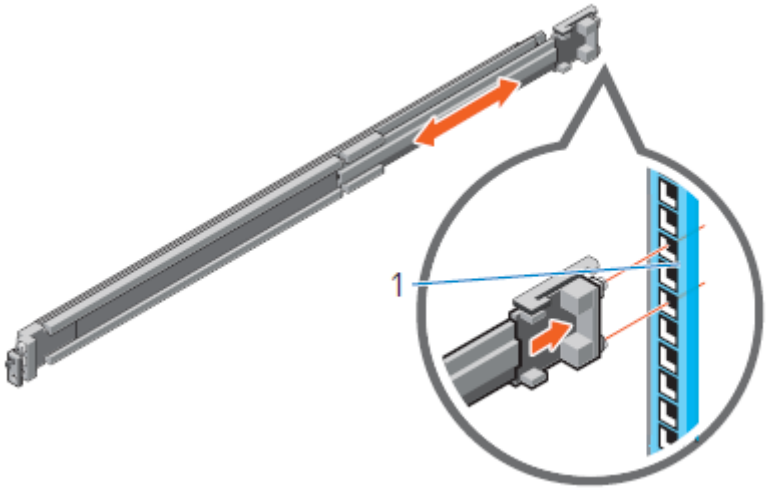

Ilustración 1. Instalación de la parte posterior del riel

5. Para la pieza de la parte frontal, gire el pestillo hacia afuera y extraiga el riel hacia adelante hasta que los pasadores se deslicen en el reborde; luego, suelte el pestillo para ajustar el riel en su lugar.

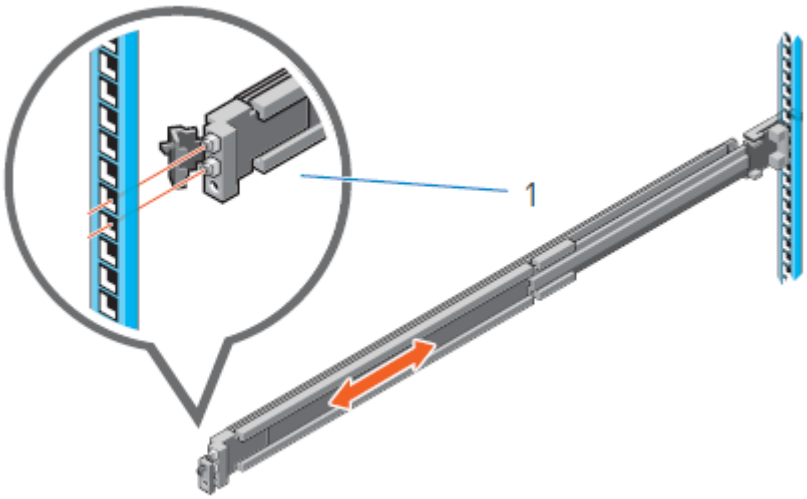

Ilustración 2. Instalación de la parte frontal del riel

6. Repita los pasos anteriores para instalar el ensamblaje del riel derecho.

Fijación de los rieles al gabinete

Los tornillos y las arandelas suministrados se usan para fijar los ensamblajes de rieles en las partes frontal y posterior del gabinete.

Sobre esta tarea

NOTA: Para los gabinetes con orificios cuadrados, coloque la arandela cónica proporcionada antes de instalar el tornillo. Para los gabinetes con orificios redondos sin rosca, instale solo el tornillo sin la arandela cónica.

Pasos

1. Alinee los tornillos con los espacios U designados en los rebordes frontales y posteriores del rack.

   Asegúrese de que los orificios para tornillos en la pestaña del soporte de retención del sistema estén colocados en los espacios U designados.
2. Inserte y apriete los dos tornillos utilizando el destornillador Phillips n.º 2.

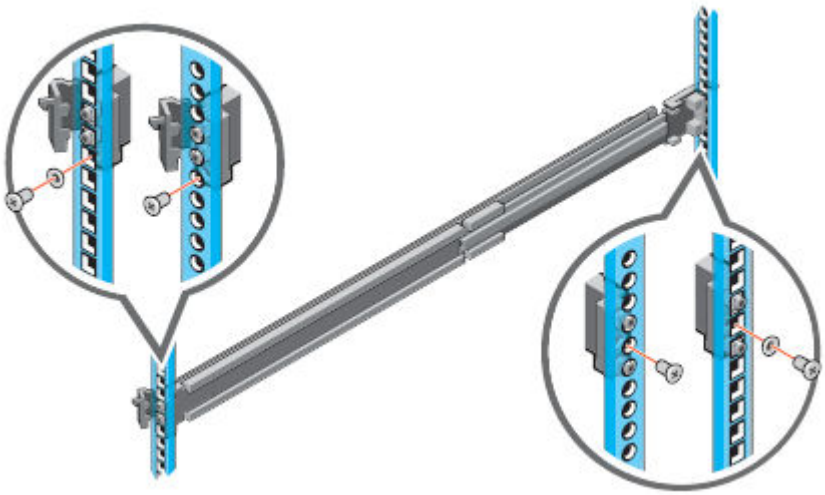

Ilustración 3. Instalación de tornillos

Instale el sistema en el gabinete

Sobre esta tarea

AVISO: El sistema es pesado. Para evitar lesiones o daños en el equipo, no intente instalar el sistema en un gabinete sin la ayuda de un elevador mecánico o de otra persona.

Pasos

1. En la parte frontal del gabinete, deslice los rieles internos hacia fuera del gabinete hasta que se bloqueen en su lugar.

Ilustración 4. Deslice los rieles internos hacia fuera del gabinete

2. Busque los separadores de rieles posteriores en cada lado del sistema. Posicione el sistema por encima de los rieles e introduzca los separadores de rieles posteriores en las ranuras J posteriores en los ensamblajes de correderas.
3. Gire el sistema hacia abajo hasta que todos los separadores de rieles estén ubicados en las ranuras J.

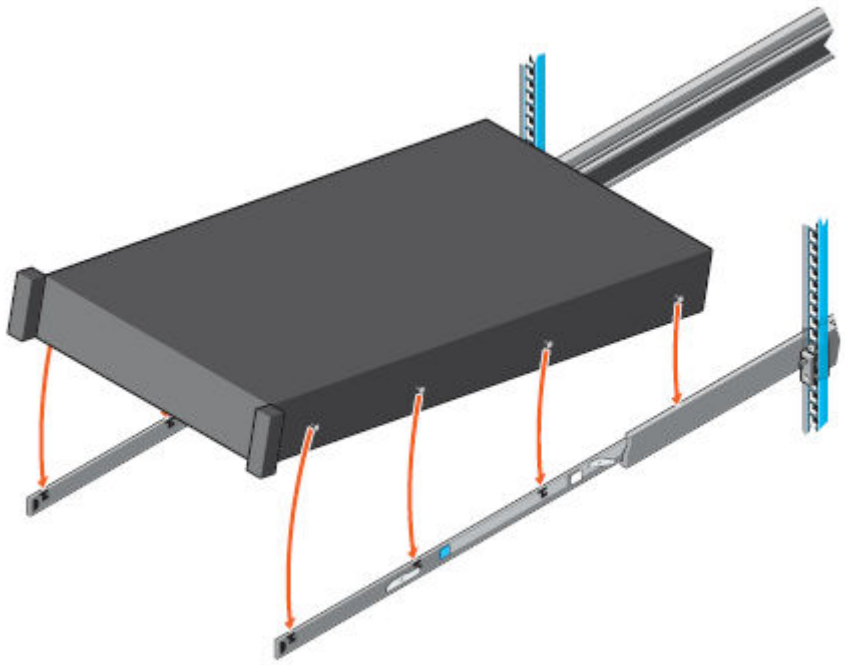

Ilustración 5. Instale el sistema sobre los rieles

4. Empuje el sistema hacia dentro hasta que los pestillos de bloqueo encajen en su sitio.
5. Tire de las pestañas de desbloqueo deslizantes azules hacia adelante y deslice el sistema dentro del gabinete. Los pestillos de cierre se acoplarán para asegurar el sistema en el gabinete.

   NOTA: Asegúrese de que el riel interno se deslice completamente hacia dentro del riel central. El riel central se bloquea si el riel interno no está completamente acoplado.

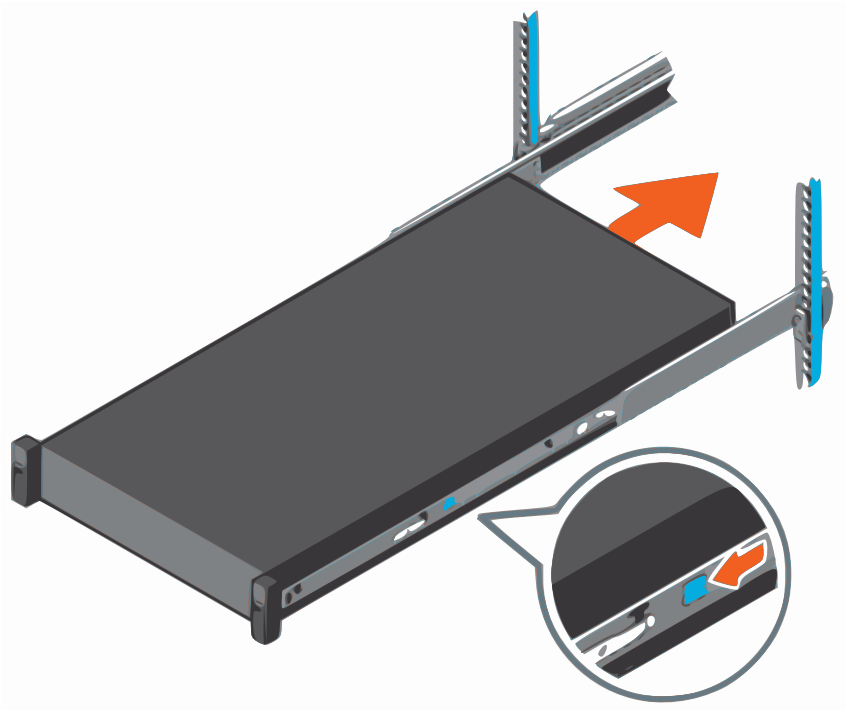

Ilustración 6. Deslice el sistema dentro del gabinete

Instale el bisel

Pasos

1. Alinee e inserte el extremo derecho del bisel en el sistema.
2. Presione el botón de liberación y ajuste el extremo izquierdo del bisel en el sistema.
3. Bloquee el bisel usando la llave.

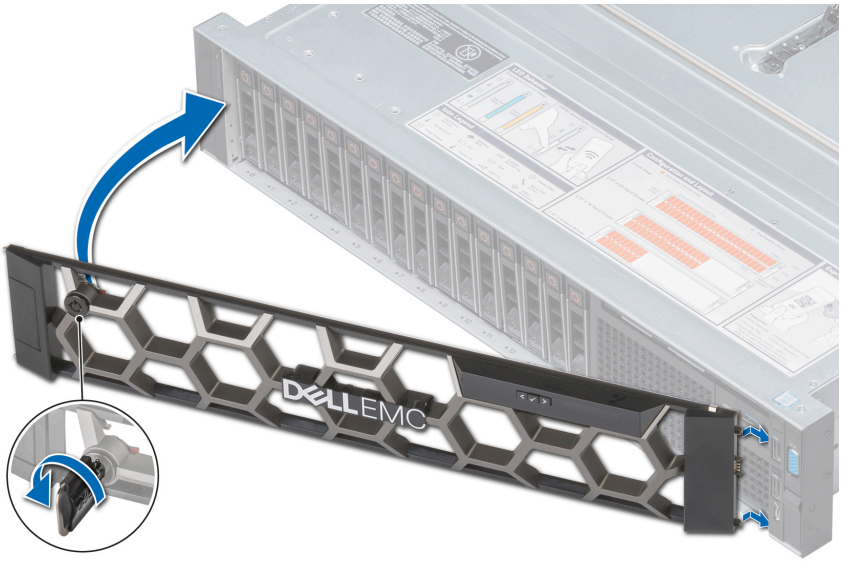

Ilustración 7. Instalación del bisel frontal

Conexión del sistema a la red

En la siguiente figura, se muestra la ubicación de los puertos de red de DP4400 y el puerto iDRAC.

Sobre esta tarea

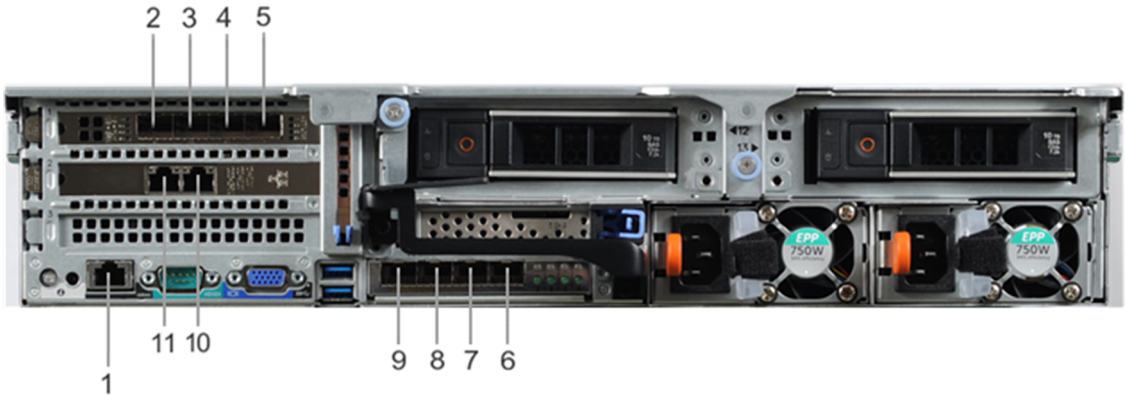

Ilustración 8. Conexiones de red de DP4400 y iDRAC

Pasos

1. Utilice un cable Ethernet de cobre Cat5e o Cat6 UTP para conectar un puerto de 1 GbE (10) con el equipo de servicio.
2. Si DP4400 contiene tarjetas de red SFP de 10 Gb, utilice cables de fibra con un SFP óptico de 10 Gb para conectar los cuatro puertos de 10 GbE necesarios (2, 3, 8, 9) para acceder a los puertos del switch en la red.

3. Si DP4400 contiene tarjetas de red BASE-T de 10 Gb, utilice cables de cobre Cat6a UTP o Cat7 para conectar los cuatro puertos de 10 GbE necesarios (2, 3, 8, 9) para acceder a los puertos del switch en la red
4. Utilice un cable Ethernet de cobre Cat5e o Cat6 para conectar el puerto de iDRAC (1) en la esquina inferior izquierda del chasis del sistema a la red.

   Según la ilustración anterior, en la siguiente tabla se detalla el tipo de puerto y su número de leyenda asociado.

Puertos de DP4400

En función de la ilustración anterior, en esta tabla se detalla el tipo de puerto y su número de leyenda asociado.

Tabla 5. Puertos de DP4400

Número de llamada	Tipo de puerto
1	iDRAC
2	10 GbE (obligatorio)
3	10 GbE (obligatorio)
4	10 GbE (sin usar)
5	10 GbE (sin usar)
6	10 GbE (sin usar)
7	10 GbE (sin usar)
8	10 GbE (obligatorio)
9	10 GbE (obligatorio)
10	1 GbE (obligatorio)
11	1 GbE (sin usar)

NOTA:

- Los puertos 2 y 9 son para el equipo de red de vSwitch0. Los puertos 3 y 8 son para el equipo de red de vSwitch1 y se utilizan durante la configuración del dispositivo.
- Asegúrese de que los cuatro puertos necesarios de 10 GbE (2, 3, 8 y 9) estén conectados a los puertos de acceso del switch en la red.
- Para obtener más información sobre la red de administración independiente, sus requisitos previos y el procedimiento asociado, consulte Requisitos de red de administración separados en la página 20.
- La MTU del switch debe ser de 1528 o superior. No se admiten tramas jumbo. En ocasiones, PowerProtect DP4400 puede fallar con el siguiente mensaje de error: `Adding back-end storage. Exception occurred while executing Avamar integration task. Failed to add Data Domain as Avamar back-end storage`. Para resolver este problema, debe quitar la MTU o aumentarla a 1518 o superior. Para obtener más información, consulte el artículo de la base de conocimientos 539946.

Conexión de los cables de alimentación y encendido del sistema

En este tema, se describe cómo conectar los cables de alimentación y encender el sistema

Sobre esta tarea

NOTA: Utilice una fuente de alimentación ininterrumpida (UPS) para protegerse contra la pérdida de datos causada por interrupciones de alimentación no planificadas.

Pasos

1. Conecte las fuentes de alimentación al rack.

Es posible que el sistema no se encienda automáticamente después de conectar los cables de alimentación AC. El botón de identificación del sistema ubicado en la parte posterior del chasis, en la parte izquierda inferior, se ilumina de color azul cuando la alimentación está activada.

2. Si el sistema no se enciende automáticamente después de conectar los cables de alimentación, presione el botón de encendido en el panel de control derecho en la parte frontal del chasis para encender el sistema.

Configurar PowerProtect DP Series Appliance con un switch Juniper

Sobre esta tarea

En las siguientes secciones de este capítulo, se describen las tareas de configuración para una implementación de PowerProtect DP Series Appliance mediante un switch Dell. Si la implementación de PowerProtect DP Series Appliance utiliza un switch Juniper con hosts Hypervisor que ejecutan una tarjeta NIC 10G X710, debe realizar las siguientes tareas de configuración.

Pasos

1. Deshabilite el protocolo Data Center Bridging Capability Exchange (DCBX) en el puerto del switch Juniper.
   Para obtener más información, consulte el artículo de de la base de conocimientos 000057774.
2. Instale el controlador de i40e, desinstale el controlador i40en y, a continuación, reinicie Hypervisor.
   Puede descargar el controlador i40e desde https://my.vmware.com/group/vmware/downloads/details?%20downloadGroup=DT-ESXI60-INTEL-I40E-207&productId=743.
   Para obtener más información, consulte el artículo de la base de conocimientos 000042326.

Configure iDRAC

Debe configurar iDRAC para las operaciones de actualización y mantenimiento del sistema. Además, PowerProtect DP Series Appliance es compatible con el uso de iDRAC para cambiar la configuración de seguridad y le permite encender el sistema de manera remota.

Requisitos previos

Conéctese a la unidad mediante un monitor VGA con un teclado o un puerto serie, encienda el dispositivo y realice los siguientes pasos:

NOTA: No utilice iDRAC para cambiar la configuración de almacenamiento, la configuración del dispositivo o la configuración del BIOS, ya que realizar cambios afectará la funcionalidad del sistema. Póngase en contacto con el servicio de soporte si se requieren cambios en cualquiera de estas áreas.

Pasos

1. Durante el proceso de arranque del sistema, presione **F2** para acceder al menú de BIOS.
2. En la página **System Setup Main Menu**, haga clic en **iDRAC Settings**.
   Se muestra la página iDRAC Settings.
3. Haga clic en **Network**.
   Se muestra la página Network.
4. En **Configuración de IPv4**, especifique detalles de la dirección IP estática.
5. Presione **Esc** para volver al menú anterior.
6. Seleccione **User Configuration**.
   a. Habilite el usuario root.
   b. Cambie la contraseña del usuario root.
      Tenga en cuenta que la contraseña predeterminada es *ldpa_1234*.

Instalar el software DP4400

En los siguientes temas, se proporcionan instrucciones detalladas sobre cómo instalar y configurar el software PowerProtect DP4400.

Requisitos previos a la instalación

Antes de instalar el software PowerProtect DP4400, debe cumplir con los siguientes requisitos previos a la instalación.

Conectividad de cables

En la siguiente imagen, se muestra la ubicación de los puertos de red de DP4400 y el puerto iDRAC.

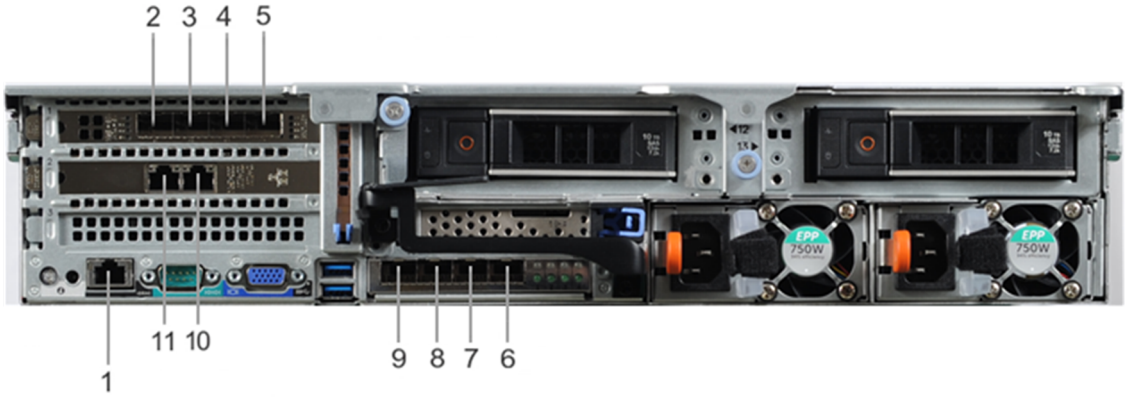

Ilustración 9. Conexiones de red de DP4400 y de iDRAC

1. Los puertos 2 y 9 son para el equipo de red de vSwitch0. Los puertos 3 y 8 son para el equipo de red de vSwitch1 y se utilizan durante la configuración del dispositivo.
2. Asegúrese de que los cuatro puertos necesarios de 10 GbE (2, 3, 8 y 9) estén conectados a los puertos de acceso del switch en la red.

NOTA: Todos los puertos del switch deben estar en "Access mode or untagged" y la MTU no debe ser inferior a 1528 bytes. Todos los puertos del switch deben estar activos y no deben configurarse en LACP.

NOTA: Si la seguridad del puerto del switch CISCO está habilitada en los puertos de PowerProtect DP Series Appliance, la implementación de PowerProtect DP Series Appliance falla debido a problemas de ping de redes esporádicos. Una máquina virtual no puede hacer ping a ningún otro host en la red física o no puede hacer ping a la dirección IP de la gateway debido a la restricción de seguridad del puerto de Cisco. Encuentre una explicación detallada, consulte https://kb.vmware.com/s/article/1002811

Requisitos de dirección IP

En las siguientes tablas, se detallan las direcciones IP requeridas por PowerProtect para diversos componentes.

Sobre esta tarea

El uso de un rango es el método preferido, ya que simplifica la asignación y reduce la posibilidad de errores al ingresar las direcciones IP.

Cuando reserva las direcciones IP, debe asignar las direcciones IP a un nombre de dominio calificado (FQDN) en el servidor DNS. El siguiente es el formato compatible para un FQDN:

- Caracteres compatibles:
  - Letras mayúsculas o minúsculas (A-z, a-z)
  - Números (0-9)
  - Guion (-)
- No debe superar el límite de 255 caracteres.
- No debe incluir caracteres especiales, símbolos, espacios ni signos de puntuación que no sean un guion (-).

Las etiquetas son las cadenas en el FQDN que están separadas por un punto (.). Utilice un punto solo como separador entre las etiquetas. El siguiente es el formato compatible para las etiquetas:

- Cada etiqueta debe comenzar con una letra o un número.
- No debe superar el límite de 63 caracteres.
- Cada etiqueta debe tener al menos una letra.
- Una etiqueta no debe comenzar ni terminar con un guion (-)

Cuando configure los ajustes del servidor DNS durante la configuración del dispositivo, asegúrese de configurar los ajustes correctamente. Después de configurar el nombre de host y el nombre de dominio de los productos de punto, no puede modificar los nombres de host de los productos de punto. Sin embargo, puede modificar la dirección IP del servidor DNS en los productos de punto después de configurar el dispositivo.

Asegúrese de que el nuevo servidor DNS tenga el mismo nombre de host y los mismos nombres de dominio que están asociados con las direcciones IP del producto de punto correspondientes. Para obtener más información sobre cómo modificar la dirección IP del servidor DNS, consulte el artículo de la base de conocimientos 537628.

Asegúrese de tener una dirección IP de NTP válida a la que se pueda acceder desde el dispositivo.

NOTA: Asegúrese de que la diferencia horaria entre el servidor NTP y el hipervisor no sea superior a 10 minutos. Si la diferencia de tiempo entre los dos servidores es de más de 10 minutos, la configuración de red del dispositivo puede fallar.

En caso de que no haya una dirección IP válida para DNS, NTP y gateway, el dispositivo se puede configurar mediante la dirección IP de ACM. Consulte Implementación autónoma (opcional) para obtener más información.

Cuando se utiliza un rango de direcciones IP durante la configuración de PowerProtect, se asignan las direcciones IP en un orden estándar. Una vez asignada, cada IP se debe registrar en DNS con entradas de búsqueda directa e inversa.

Se necesita un total de 13 direcciones IP para todos los componentes y una para Hypervisor y ACM. La cantidad total de requisitos de dirección IP varía según la selección del componente opcional (que se muestra en la siguiente tabla). iDRAC también requiere una dirección IP.

Tabla 6. Requisitos de dirección IP

Cantidad de direcciones IP requeridas	Componente	Entrada de DNS requerida
1	Appliance Configuration Manager	Sí
1	PowerProtect DP Series Appliance Hypervisor	Sí
1	PowerProtect DP Series Appliance Hypervisor Manager	Sí
1	Protection Storage (administración)	Sí
2	Protection Storage (respaldo)	No
1	Protection Software	Sí
1	Proxy interno de Protection Software	Sí
1	Data Protection Central para PowerProtect DP Series Appliance	Sí

Tabla 6. Requisitos de dirección IP (continuación)

Cantidad de direcciones IP requeridas	Componente	Entrada de DNS requerida
2	Reporting and Analytics (opcional)	Sí
1	Search (opcional)	Sí
1	Cloud DR (opcional)	Sí

Se recomienda asignar el rango de direcciones IP en la siguiente secuencia. La tabla también muestra cómo se asignarán estas IP a diferentes componentes cuando se selecciona una opción de rango de IP durante la implementación en el asistente de ACM.

Tabla 7. Asignación de direcciones IP para una sola red para el modelo DP4400

Asignación de rango de IP	Ejemplo	Componente	Campo asignado
+0	`192.0.2.1`	Hypervisor Manager (Service)	servicio de servidor de VMware Hypervisor Manager (Service)
+1	`192.0.2.2`	Protection storage	IP de administración
+2	`192.0.2.3`	Protection storage	IP de respaldo 1
+3	`192.0.2.4`	Protection storage	IP de respaldo 2
+4	`192.0.2.5`	Protection Software	IP del servidor
+5	`192.0.2.6`	Proxy interno de PProtection Software	Protection Software Proxy servicio
+6	`192.0.2.7`	Data Protection Central	VM de Data Protection Central
+7	`192.0.2.8`	Reporting and Analytics (opcional)	Host del servidor de aplicaciones servicio
+8	`192.0.2.9`	Reporting and Analytics (opcional)	Host del servidor del área de almacenamiento de datos servicio
+9	`192.0.2.10`	Search (opcional)	Indexar host de nodo primario servicio
+10	`192.0.2.11`	Cloud DR (opcional)	CDRA (opcional) dispositivo virtual complementario

Requisitos de red de administración separados

Puede configurar una red de administración independiente en PowerProtect DP Series Appliance durante la instalación del dispositivo.

Flujo de datos y de control

En PowerProtect DP Series Appliance, Infrastructure Management Service (Protection Software) almacena solo la información de metadatos sobre el respaldo y los datos de respaldo reales almacenados en Protection Storage. En una red de administración independiente, Protection Software permanece en la red de administración y Protection Storage está configurado con IP de respaldo y de administración.

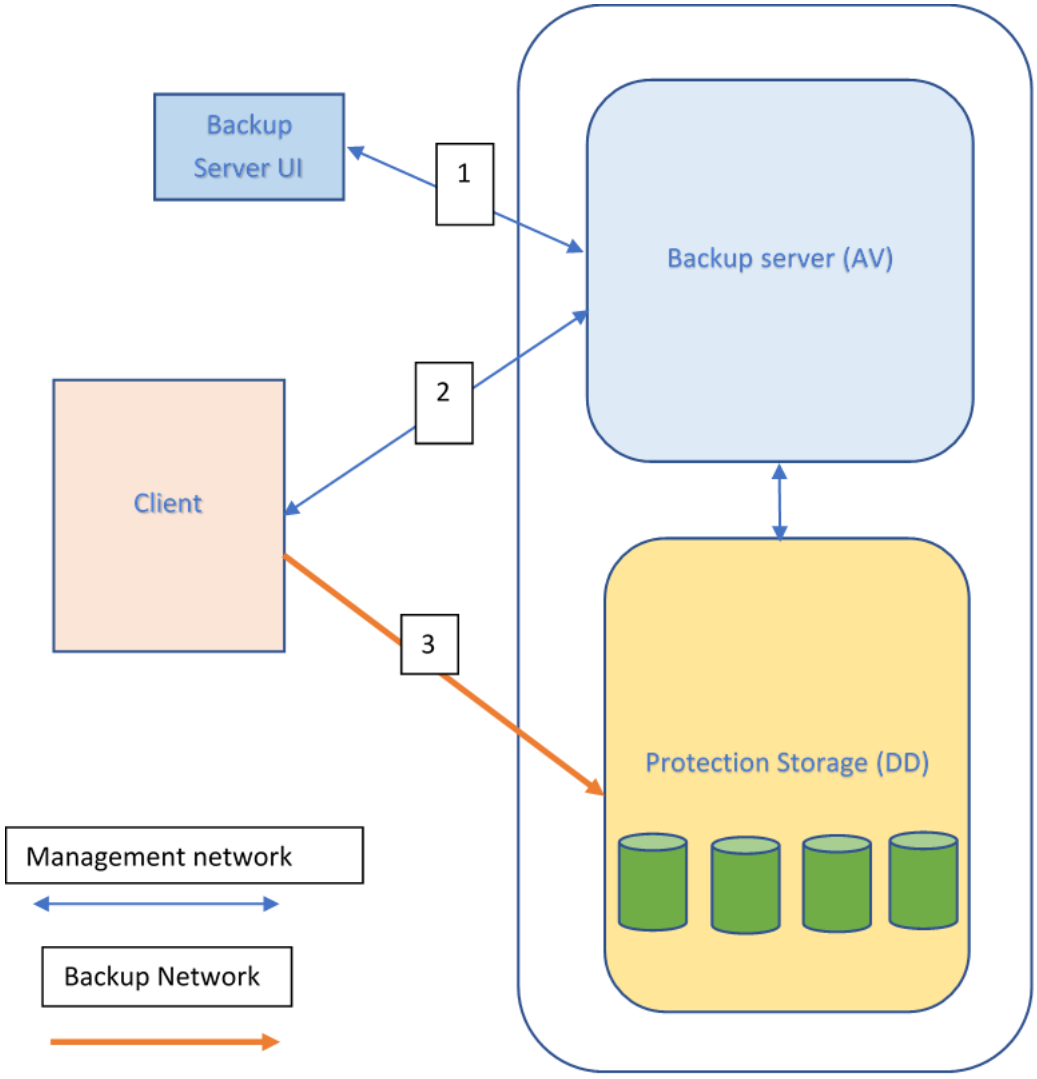

Ilustración 10. Flujo de datos y de control

1. El usuario inicia la solicitud de respaldo desde la interfaz del usuario del servidor de respaldo.
2. Infrastructure Management Service inicia la comunicación con el cliente a través de la red de administración.
3. El cliente recibe los detalles de Protection Storage para respaldar los datos e inicia el respaldo de datos a través de la red de respaldo.

NOTA: La administración (o la red corporativa) y la red de respaldo deben ser accesibles desde el cliente.

Requisito de dirección IP para una red de administración independiente

En las siguientes tablas, se detallan las direcciones IP requeridas por PowerProtect DP Series Appliance para diversos componentes.

Sobre esta tarea

El uso de un rango es el método preferido, ya que simplifica la asignación y reduce la posibilidad de errores al ingresar las direcciones IP.

Cuando se utiliza un rango de direcciones IP durante la configuración de PowerProtect DP Series Appliance, se asignan las direcciones IP en un orden estándar. Una vez asignada, cada IP se debe registrar en DNS con entradas de búsqueda directa e inversa.

Se necesita un total de 14 direcciones IP para todos los componentes y una para Hypervisor y ACM. La cantidad total de requisitos de dirección IP varía según la selección del componente opcional (que se muestra en la siguiente tabla). iDRAC también requiere una dirección IP.

En las siguientes tablas se detallan los requisitos totales de dirección IP.

Tabla 8. Requisitos de dirección IP de la red de administración para el DP4400

Cantidad de direcciones IP requeridas	Componente	Entrada de DNS requerida
1	Appliance Configuration Manager	Sí
1	PowerProtect DP Series Appliance Hypervisor	Sí
1	PowerProtect DP Series Appliance Hypervisor Manager	Sí
1	Protection Storage (administración)	Sí
1	Protection Software (respaldo)	Sí
1	Proxy interno de Protection Software	Sí
1	Data Protection Central	Sí
2	Reporting & Analytics (opcional)	Sí
1	Search (opcional)	Sí
1	Cloud DR (opcional)	Sí

Tabla 9. Requisitos de dirección IP de red de respaldo para el DP4400

Cantidad de direcciones IP necesarias para la entrada de DNS de componentes	Componente	Entrada de DNS requerida
2	Protection Storage	No
1	Proxy interno de Protection Software	No

Se recomienda asignar un rango de direcciones IP que estén en secuencia. En la siguiente tabla, se muestra cómo se asignarán estas direcciones IP cuando se seleccione la opción de rango de IP durante la implementación.

Tabla 10. Asignación de rango IP de administración

Asignación de rango IP de administración	Componente	Campo asignado
+0	Hypervisor Manager (Service)	servicio de servidor de VMware Hypervisor Manager (Service)
+1	Protection storage	IP de administración
+2	Protection Software	IP del servidor
+3	Proxy interno de Protection Software	Proxy de Protection Storage servicio
+4	Data Protection Central	Data Protection Central servicio
+5	Reporting & Analytics (opcional)	Host del servidor de aplicaciones servicio
+6	Reporting & Analytics (opcional)	Host del servidor del área de almacenamiento de datos servicio

Tabla 10. Asignación de rango IP de administración (continuación)

Asignación de rango IP de administración	Componente	Campo asignado
+7	Search (opcional)	Indexar host de nodo primario servicio
+8	Cloud DR (opcional)	CDRA (opcional) dispositivo virtual complementario

Consulte las siguientes tablas para ver las asignaciones de rango de direcciones IP de respaldo con la red de respaldo dedicada

Tabla 11. Asignaciones de rango de direcciones IP de respaldo con red de respaldo dedicada

Asignación de rango de IP de respaldo	Componente	Campo asignado
+0	Protection Storage	IP de respaldo 1
+1	Protection Storage	IP de respaldo 2
+2	Proxy interno de Protection Software	servicio de Protection Software

Instale Network Validation Tool

Network Validation Tool (NVT) para PowerProtect DP Series Appliance ejecuta varias pruebas automatizadas para validar la configuración de red. Debe ejecutar NVT para PowerProtect DP Series Appliance desde un sistema en la red de administración.

Antes de instalar PowerProtect DP Series Appliance, se debe completar la configuración de red para el centro de datos. Después de completar todas las configuraciones de red necesarias para la instalación de PowerProtect DP Series Appliance, instale y ejecute Network Validation Tool para validar los requisitos de red para una implementación correcta de PowerProtect DP Series Appliance en el centro de datos. Para descargar NVT, y para obtener más información acerca de NVT, consulte https://central.dell.com/solutions/NVT-PP.

Puertos del firewall

Para que PowerProtect DP Series Appliance 2.7.1 funcione correctamente, los puertos del firewall deben estar abiertos. Para obtener más información, consulte la sección Apéndice.

Secure Remote Services (SRS)

Si su organización permite la comunicación a través de Internet, como parte de la configuración inicial del sistema, puede registrar los componentes de PowerProtect DP Series Appliance, Protection Software, Protection Storage y Reporting and Analytics con Secure Remote Services. Secure Remote Services es un sistema de soporte de servicio al cliente seguro, basado en IP y distribuido que proporciona a los clientes de Dell EMC el comando, el control y la visibilidad de las actividades relacionadas con el soporte.

Se recomienda enfáticamente completar el proceso de registro de Secure Remote Services. Para preparar el entorno de PowerProtect DP Series Appliance para el registro de Secure Remote Services, agregue los ID del sitio del cliente al gateway de SRS y confirme que el ID del sitio sea visible a través de ServiceLink.

El servidor SRS debe tener una versión `v3.20.00.08` o superior y tener acceso a PowerProtect DP Series Appliance. DataProtection-ACM se puede configurar con SRS durante el proceso de instalación o se puede configurar más adelante desde el tablero de ACM. El nombre de host de la gateway de SRS debe estar registrado en el DNS y la búsqueda directa e inversa debe funcionar.

La información completa sobre SRS está disponible en el sitio de soporte en línea. El registro de SRS lo realiza el servicio al cliente (CS) durante la implementación o el arquitecto de soluciones (SA).

Se recomienda completar el proceso de registro de SRS, que le permite tener las siguientes ventajas:

- Dell EMC ofrece informes de eventos de productos, como alertas de error, lo que aumenta considerablemente la disponibilidad de su infraestructura de información.
- Dell EMC proporciona servicios remotos rápidos, ya sea a través de reconocimiento y notificación automatizados o a través de interpretación y respuesta cuando se produce un evento de soporte, lo que elimina la necesidad de visitas de soporte en sitio.
- Proporciona una mayor protección de su información
- Reducción de riesgos
- Mejor tiempo de reparación

Si el cliente opta por no implementar el SRS, el administrador de proyectos (PM) debe iniciar sesión en http://gcsdocs.corp.emc.com y completar los detalles en el formulario de exclusión.

Soporte en línea

Para crear una cuenta de soporte en línea, vaya a https://www.dell.com/support. Se requieren su nombre de usuario y su contraseña para la configuración de Secure Remote Services

ID del sitio

Se crea un ID de sitio en los sistemas de soporte para cada ubicación de su organización donde se han instalado productos de Dell EMC. Se requiere su ID de sitio durante la configuración inicial. Para verificar el número de ID del sitio en el servicio de soporte en línea, realice los siguientes pasos:

1. Inicie sesión en el soporte en línea con sus credenciales.
2. Coloque el cursor sobre su nombre de usuario y seleccione **Manage Company Information**.
3. Haga clic en **View Sites**.

NOTA: También puede buscar un site y agregarlo a la lista Mis sites. Si no está disponible un ID de site o si el ID de site correcto no aparece en la lista, debe notificar al representante de campo local para solicitar uno.

Licencias

Necesita una licencia para usar PowerProtect DP Series Appliance. Para usar todas las funciones de PowerProtect DP Series Appliance, debe activar la licencia que recibió. Para activar las licencias, debe estar conectado a una red con una conexión a Internet para la activación dentro del producto o debe haber recibido la carta del código de activación de licencia (LAC) por correo electrónico durante el proceso de cumplimiento para activar manualmente las licencias. La carta de LAC incluye el código de autorización de licencia asociado con su pedido, las instrucciones para descargar archivos binarios de software y las instrucciones para activar los derechos en línea a través de Dell EMC Software Licensing Central.

Las licencias de PowerProtect DP Series Appliance se descargan automáticamente. En caso de que se encuentre en un sitio oscuro o si tiene alguna restricción de red, y si las licencias no se descargan automáticamente, debe activar manualmente la licencia. Consulte el Activación manual en la página 24 para obtener más detalles.

Activación dentro del producto

La activación de la licencia en el producto es una función en la que ACM descarga automáticamente las licencias para productos de punto de **Protection Storage**, **Backup Server** y **Reporting and Analytics** desde el servidor ELMS.

Asegúrese de que el dispositivo esté conectado a una red para descargar automáticamente las licencias. Una vez que las licencias se descargan correctamente, no se muestra la pestaña **License** de la página Configuración de PowerProtect DP Series Appliance. Si las licencias no se descargan correctamente durante la configuración de red, la pestaña **License** se muestra en la página Configuration de PowerProtect DP Series Appliance con el botón **Check online for licenses**. Puede hacer clic en **Check online for licenses** para descargar las licencias desde el servidor de ELMS.

NOTA: La activación de la licencia en el producto no es compatible en los siguientes casos:

- En una red habilitada para IPv6
- Cuando se utiliza ACM como DNS

NOTA: Si el sistema no puede descargar las licencias automáticamente desde el servidor de ELMS, se muestra un mensaje de error y debe activar manualmente las licencias. Para obtener más información sobre cómo activar manualmente las licencias, consulte Activación manual en la página 24.

Activación manual

La función de activación manual de licencia le permite cargar y activar las licencias que descargó desde el servidor de ELMS.

Sobre esta tarea

Para activar manualmente las licencias, descargue los archivos de licencia para Protection Storage, Protection Software y Reporting & Analytics desde Dell EMC Software Licensing Central.

La persona de contacto mencionada en su orden de venta debe haber recibido la carta del Código de autorización de licencia (LAC) a través de un correo electrónico durante el proceso de cumplimiento de pedidos. Esta carta de LAC incluye el código de autorización de

licencia asociado con su pedido, las instrucciones para descargar archivos binarios de software y las instrucciones para activar los derechos en línea a través de Dell EMC Software Licencing Central.

Configurar el software DP4400

En los siguientes temas, se describe la forma de configurar el software DP4400.

Conéctese a ACM

Conéctese a la interfaz del usuario de ACM y comience el proceso de configuración. Para obtener una experiencia sin inconvenientes, habilite las conexiones de red pública y privada en su computadora de servicio.

Requisitos previos

- Después de encender el dispositivo, espere 5 minutos para que finalice el arranque.
- Verifique que la computadora de servicio esté conectada al puerto GbE identificado como (10) en Conexiones de red de DP4400 y de iDRAC en la página 25.
- En la computadora de servicio, registre la configuración de la dirección IP para la interfaz de Ethernet que está conectada a DP4400.

NOTA: PowerProtect DP Series Appliance utiliza las direcciones IP `192.168.100.xxx` para los componentes internos. Asegúrese de que la red `192.168.100` no se utilice en su entorno. Si las direcciones de red están en uso, comuníquese con el servicio al cliente para obtener ayuda.

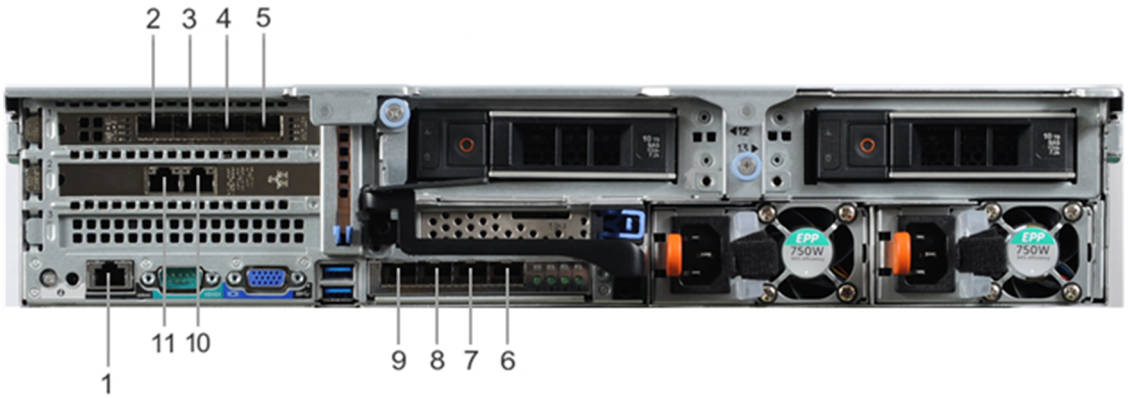

Ilustración 11. Conexiones de red de DP4400 y de iDRAC

Pasos

1. En la computadora de servicio, asigne la dirección IP estática **`192.168.100.98`** y la máscara de subred **`255.255.255.224`** para la interfaz de Ethernet que está conectada a DP4400.

   El gateway predeterminado no es obligatorio.
2. Verifique que ACM responda a un ping en la dirección IP predeterminada de ACM, **`192.168.100.100`**.
3. Para conectarse a la interfaz del usuario de ACM, escriba **`https://192.168.100.100:8543/`** en una ventana del navegador.
4. Inicie sesión en ACM con el nombre de usuario y la contraseña predeterminados de la cuenta del sistema:
   - **Nombre de usuario:** `root`
   - **Contraseña:** `Idpa_1234`

   Puede configurar el ACM de las siguientes maneras:
   - GUID-A3032316-0CED-4EEF-8649-073314E203F9.xml
   - GUID-A46BAAA2-20D3-4977-B46F-724CA6F63ED8.xml

Configurar ACM con rango de IP

Después de un inicio de sesión correcto, se muestra la pantalla **Change Appliance Password**.

Pasos

1. Inicie sesión en ACM con el nombre de usuario y la contraseña predeterminados de la cuenta del sistema:
2. Se muestra la página **Change Appliance Password**.

   La página **Change Appliance Password** consta de *Update Appliance Password*.

   - Actualizar contraseña del dispositivo

     Esta contraseña se asignará a todos los componentes del dispositivo. Debe contener entre 9 y 20 caracteres e incluir al menos un carácter compatible de cada tipo.

     Los siguientes tipos de caracteres son compatibles:

     - Letras en mayúscula (**A**-**Z**)
     - Letras en minúscula (**a**-**z**)
     - Números (**0**-**9**)
     - Caracteres especiales: punto (**.**), guion (**-**) y guion bajo (**_**).

       La contraseña no debe incluir nombres comunes o nombres de usuario como **root** o **admin**. Además, la contraseña no debe comenzar con un guion (**-**) y terminar con un punto (**.**).

3. Una vez que cambie correctamente las contraseñas, el sistema cierra su sesión. Debe iniciar sesión nuevamente con sus nuevas credenciales.
4. En la pantalla **End User License Agreement**, acepte el EULA.

   Se muestra la pantalla **Network Configuration**.

   Después de aceptar el EULA, configure la conectividad de red inicial con el dispositivo de DP4400. PowerProtect DP Series Appliance es compatible con redes habilitadas para IPv4 e IPv6. El asistente de configuración de red configurará la red pública para Appliance Configuration Manager y el servidor Hypervisor.

Configurar los ajustes de ACM para una sola red

Según el tipo de red que haya seleccionado (IPv4 o IPv6), proporcione la siguiente información para configurar ACM para una sola red.

Pasos

- **Red IPv4**

  Máscara de subred Máscara de dirección IP que identifica el rango de direcciones IP en la subred donde se conecta el dispositivo.

- **Red IPv6**

  Longitud del prefijo Longitud de la dirección IP que identifica el rango de direcciones IP donde se conecta el dispositivo.

Dirección IP de Appliance Configuration Manager	Esta es la dirección IP para asignar a ACM. Esta es la primera dirección IP de las 13 direcciones IP reservadas para ACM.
Dirección IP/ nombre de host ESXi	Esta es la dirección IP que se asignará al servidor de Hypervisor. Esta es la segunda dirección IP de las 13 direcciones IP reservadas para Hypervisor.
Dirección IP de gateway	La dirección IP de gateway predeterminada del dispositivo.
Nombre de dominio	Nombre de dominio para el ambiente de red.
Nombre de host o dirección IP del servidor NTP	La dirección IP del servidor NTP para el entorno de red
Dirección IP del servidor DNS principal	Servidor DNS principal para el ambiente de red.

Dirección IP del servidor DNS secundario	Servidor DNS secundario para el ambiente de red.

Configure the ACM settings for separate management network

If you want to configure the ACM settings for separate management and backup network, perform the following steps.

Steps

1. Click the **Separate Management Network** check box.
2. Provide the following information to configure the **Management network settings**:

Appliance Configuration Manager IP Address/ Hostname	The IP address to assign to the ACM. This is the first IP address of the 14 IPs that is reserved for the ACM.
ESXi IP Address/ Hostname	The IP address to assign to the Hypervisor server. This is the second IP address of the 14 IPs that is reserved for Hypervisor.
Subnet mask	The IP address mask that identifies the range of IP addresses in the subnet where the appliance is connected.
Gateway IP address	The default gateway IP address of the appliance.
Domain name	The domain name for your network environment.
NTP server IP Address/ Hostname	The NTP server IP address for your network environment.
Primary DNS server IP address	The primary DNS server for your network environment.
Secondary DNS server IP address	The secondary DNS server for your network environment.

3. Click **Yes** to continue.

   After you configure the basic networking infrastructure, your web browser automatically redirects to the ACM IP address assigned during the network configuration.

   For automatic forwarding to work correctly, the system that you use to complete the configuration must be connected to the same network as the configured ACM IP address.

   If you cannot have connections to both public and private networks simultaneously, disconnect from the private appliance configuration network and then connect to the network that the ACM IP address is on, to complete the rest of the configuration.

   Once the network configuration is complete, revert the network adapter IP address settings on the service computer to their previous state.

   If the network configuration fails, you can click **Retry** to revert all the settings. You must review the settings, make any changes if required, and then configure the network settings again.
4. Login to the ACM using the public IP Address.

   The SRS page appears.
5. On the **Dell EMC Secure Remote Services** configuration for PowerProtect DP Series Appliance, perform the following steps:
   a. Specify the SRS Gateway IP address.
   b. Specify the online support credentials in the *Username* and *Password* fields.
   c. Click **Configure**.

      If the SRS configuration fails, you will get an error message. Refer to SRS Troubleshooting section to resolve the issue and configure again.

      It is strongly recommended that skip the SRS configuration and configure it from the ACM dashboard later.

6. The PowerProtect DP Series Appliance configuration page appears. On the PowerProtect DP Series Appliance configuration page, perform the following steps.

   NOTE: Ensure that you click the prerequisites link available on the **Welcome** page and read them before you continue.

   a. On the **Welcome** page, select the optional components that you want to install in the configuration and click **Next**.

      NOTE: If you have selected IPv6 as your network, then the optional components such as Search and CDR are not available to install as they do not support IPv6-enabled networks.

7. If you are connected to the network with an Internet connection, the system automatically downloads the licenses for Protection Storage, Protection Software, and Reporting and Analytics point products.

   In-product activation is not supported on IPv6-enabled network and dark site appliance. If you are not connected to the network or the licenses are not downloaded from the ELMS Server, click **Browse** to locate and upload the license files manually. The system validates the license files with the following checks:

   - The maximum storage capacity for the appliance cannot be more than 24 TB (appliance with 8 TB to 24 TB capacity) and 96 TB (appliance with capacity of 24 TB to 96 TB) based on the appliance you have. Depending on the appliance you have, you can upgrade the storage capacity from 8 TB to 24 TB in increments of 4 TB or 24 TB to 96 TB in increments of 12 TB.
   - The license file should not have the hash (#) character.
   - The license must be in multiples of 4 TB.

8. Click **Next**.

   The General settings page is displayed.

9. On the **General settings** page, perform the following actions:
   - Verify the number in the **Serial Number** field, which is the *Locking ID* mentioned in the *Dell EMC software license activation notification* email.
   - Select the **Time zone** from the list.
   - Select and enter the IP address in the **IP address range (11)** field. The system automatically assigns 11 IP addresses in a chronological order, which is based on the IP address that you specify to configure the other components of the appliance. For example, if you specify `10.200.1.10`, the system automatically generates a range of IP address from 10.200.1.10 to 20.

     NOTE: If any of the optional components such as Reporting & Analytics, Search, and CDR is not selected on **Welcome** page, then the IP address range will be reduced here.
   - If you have configured separate management network, specify the IP addresses in the IP address range (9) and IP address range (3) fields in the Management network settings and Backup network settings sections respectively.

     NOTE: If any of the optional components such as Reporting & Analytics, Search, and CDR is not selected on **Welcome** page, then the IP address range will be reduced here.
   - Click **Validate**.

     The system validates the availability of the IP addresses and allocates them to the PowerProtect DP Series Appliance components. To view the list of IP addresses allocated to the individual components, hover on the green check mark.

     NOTE: If you do not select the IP address range checkbox, you must manually configure and specify the IP addresses for each component. See Configuración de red única sin rango de IP on page 29 for more info.

10. Click **Next**.

    The **Customer Information Settings** page is displayed.

11. On the **Customer information settings** page, perform the following actions:

    a. On the **Customer information** section, enter information in the mandatory fields.
       - Enter the name of the company in the **Company name** field.
       - Enter the name of the administrator in the **Admin contact name** field.
       - Enter the contact number of the administrator in the **Admin contact number** field.
       - Enter the location in the **Location** field.
       - Enter the site ID in the **Site ID** field.

         NOTE: If you select the **Email notification** checkbox, the **Email Configuration** section is displayed.

    b. In the **Email Configuration** section, enter information in the mandatory fields.

       NOTE: If you select the **Email notification** check box, the **Email Configuration** section is displayed .

       - Enter the SMTP server IP address in the **SMTP server** field.
       - Enter the port number in the **Port** field.

NOTE: The **Port** field is auto populated and is the default SMTP port.

- Enter the email address of the administrator in the **Administrator email** field.
- Click **Test Email** to send a test email to the administrator's email address.

12. Click **Next**.
13. In the **Summary** page, review the information that you entered and click **Submit** to start the configuration.
14. Click the **Submit** button. A confirmation message is displayed.
15. Click **Yes** to continue to configure the Appliance.

Configurar ACM sin rango de IP

La configuración de ACM sin rango de IP consta de dos partes: configuración de red única sin rango de IP y configuración de red independiente sin rango de IP.

Configuración de red única sin rango de IP

El siguiente procedimiento detalla la configuración del ACM sin rango de IP.

Pasos

1. En la página **Network Configuration**, asegúrese de no seleccionar la casilla de verificación **Separate Management Network**.
2. En la página **General Settings**, asegúrese de no seleccionar la casilla de verificación **IP address range** en la sección **Network**.
3. Haga clic en **Next**.
   Se muestra la página **Customer Information**.
4. Proporcione todas las entradas necesarias en la página **Customer Information**.
5. Haga clic en **Next**.
   Se muestra la página **Hypervisor Manager Configuration** .
6. **En la página Hypervisor Manager Configuration** , especifique una dirección IP única en el campo **IP address** para configurar el Hypervisor Manager (Service)interno. El nombre de host asociado se completará automáticamente en el lado derecho.
7. Haga clic en **Next**.
   Se muestra la página Protection Storage Configuration.
8. En la página **Protection Storage Configuración**, especifique direcciones IP únicas en las secciones Protection Storage y Red de datos para los siguientes campos:
   - Management Network IP Address.
   - Dirección IP de respaldo 1.
   - Dirección IP de respaldo 2.
9. Haga clic en **Next**.
   Se muestra la página Protection Software.
10. En la página **Protection Software Configuration**, especifique una dirección IP única en la sección **Backup Node and Image Proxy** para los siguientes campos:
    - IP de nodo de respaldo.
    - Dirección IP del proxy de imagen.
11. Haga clic en **Next**.
    Se muestra la página Data Protection Central.
12. En la página Data Protection Central, especifique una dirección IP única en el campo **Management Network IP**.
13. Haga clic en **Next**.
14. Si seleccionó cualquier componente opcional, como Reporting and Analytics, Search o Cloud DR en la **página Welcome**, especifique una dirección IP única para el componente opcional.
15. Haga clic en **Next** y vaya a la página **Summary**.
16. Revise la información que especificó y haga clic en **Submit** para iniciar la configuración.
17. En la página **Configuration progress**, puede descargar lo siguiente cuando PowerProtect DP Series Appliance está configurado correctamente:
    - ID de la solución.

- Configuración.
- Archivo XML de configuración.

18. Haga clic en **Finish**. Se muestra el mensaje de confirmación **First Security Officer User Update**.
19. Haga clic en **OK**.

    Se muestra la configuración de Secure Remote Services para las páginas de Protection Software, Sistema operativo de Protection Storage y Reporting and Analytics. Si lo desea, puede omitir la configuración de Secure Remote Services, ya que tiene una opción para configurar Secure Remote Services desde el tablero ACM.

20. El PowerProtect DP Series Appliance se instala e implementa.

    Se le solicitará que inicie sesión en DPC en una nueva ventana del navegador. El nombre de usuario predeterminado para DPC es `Idpauser`. En caso de que se tarde más en iniciar sesión, actualice el navegador e inicie sesión en el tablero de ACMACM.

Configuración de red independiente sin rango de IP

El siguiente procedimiento detalla la configuración de una red independiente sin rango de IP.

Pasos

1. En la página **Network Configuration**, asegúrese de seleccionar la casilla de verificación **Separate Management Network**.
2. En la página **General Settings**, asegúrese de no seleccionar la casilla de verificación **IP address range** en la sección **Network**.
3. Haga clic en **Next**.

   Se muestra la página **Customer Information**.
4. Proporcione todas las entradas necesarias en la página **Customer Information**.
5. Haga clic en **Next**.

   Se muestra la página **Hypervisor Manager Configuration** .
6. **En la página Hypervisor Manager Configuration**, especifique una dirección IP única en el campo **IP address** para configurar el Hypervisor Manager (Service) interno. El nombre de host asociado se completará automáticamente en el lado derecho.
7. Haga clic en **Next**.

   Se muestra la página Protection Storage Configuration.
8. En la página **Protection Storage Configuración**, especifique direcciones IP únicas en las secciones Protection Storage y Red de datos para los siguientes campos:
   - Management Network IP Address.
   - Dirección IP de respaldo 1.
   - Dirección IP de respaldo 2.
9. Haga clic en **Next**.
10. Se muestra la página **Protection Software**. En la página **Protection Software**, especifique una dirección IP única en la sección **Backup Node** e **Image Proxy** para los siguientes campos:
    - IP de nodo de respaldo
    - Dirección IP del proxy de imagen
    - Dirección IP del proxy de respaldo
11. Haga clic en **Next**.

    Se muestra la página **Data Protection Central**.
12. En la página **Data Protection Central**, especifique una dirección IP única en el campo **Management Network IP**.
13. Haga clic en **Next**.
14. Si seleccionó algún componente opcional, como Reporting and Analytics, Search o Cloud DR en la **página Welcome**, especifique una dirección IP única en el campo **Management Network IP** para el componente opcional.
15. Haga clic en **Next** y vaya a la página **Summary**.
16. Revise la información que especificó y haga clic en **Submit** para iniciar la configuración.
17. En la página **Configuration progress**, puede descargar lo siguiente cuando PowerProtect DP Series Appliance está configurado correctamente:
    - ID de la solución.
    - Configuración.
    - Archivo XML de configuración.

18. Haga clic en **Finish**.

    Se muestra la configuración de Secure Remote Services para las páginas de Protection Software, Sistema operativo de Protection Storage y Reporting and Analytics. Si lo desea, puede omitir la configuración de Secure Remote Services, ya que tiene una opción para configurar Secure Remote Services desde el tablero ACM.

19. El PowerProtect DP Series Appliance se instala e implementa.

    Se le solicitará que inicie sesión en DPC en una nueva ventana del navegador. El nombre de usuario predeterminado para DPC es **`Idpauser`**. En caso de que se tarde más tiempo en iniciar sesión, actualice el navegador e inicie sesión en ACM ACM mediante la URL <https:<ACM_IPAddress>:8543/dataprotection>, con las credenciales comunes.

Solución de problemas de fallas de instalación

Esta sección contiene información sobre la solución de problemas básica para ayudar a resolver los posibles problemas.

Reintentar la instalación

Si la instalación falla, puede continuar desde el punto en que falló la instalación.

Sobre esta tarea

Durante la implementación del dispositivo, si alguno de los componentes críticos no se instala, puede reintentar la instalación del componente desde el punto en que falló la instalación. Para volver a intentar la instalación, realice las siguientes acciones.

Pasos

1. Haga clic en **Retry** en la página **Configuration progress**.

   Si la operación **Retry** se realiza después de 5 días de falla de configuración, se muestra un mensaje de advertencia de `Note that the user can retry without destroying file system .`

   Se muestra el cuadro de diálogo **Retry Configuration**.

   NOTA: ACM revierte los cambios realizados en el componente que falló durante la instalación y reanuda la configuración del dispositivo.

2. Haga clic en **Yes** para continuar la instalación.
   Aparece la página **Configuration progress**. La instalación continúa desde el punto en que falló la instalación.

   NOTA: Si ACM se está reiniciando o el servicio web de ACM se está reiniciando durante la implementación de PowerProtect DP Series Appliance, la opción **Retry** no está disponible, solo puede realizar **Rollback** a la instalación.

Instalación de reversión

Si la instalación falla, puede revertir la instalación cuando la funcionalidad **Retry** no resuelve el problema y seguir el asistente para configurar e implementar PowerProtect DP Series Appliance.PowerProtect DP Series Appliance. La función **Rollback** revierte los cambios realizados en la configuración del dispositivo. Puede revisar los ajustes e iniciar la instalación y la configuración del dispositivo nuevamente.

Requisitos previos

Asegúrese de hacer clic en **Download log bundle** para descargar los registros antes de iniciar **Rollback**.

Sobre esta tarea

Para realizar **Rollback** a la configuración del dispositivo, lleve a cabo las siguientes acciones.

Pasos

1. Haga clic en **Rollback** en la página **Configuration progress**.
   Se muestra la página **Rollback Configuration**.

   NOTA: ACM revierte los cambios realizados en la configuración del dispositivo.

Si la operación **Retry** se realiza después de 5 días de falla de configuración, se muestra un mensaje de advertencia de `Note that without destroying the filesystem on Protection Storage, next configuration can be submitted .`

2. Haga clic en **Yes** para continuar la instalación.
   Aparece la página **Configuration progress**. El sistema revierte todos los cambios realizados en el dispositivo.
   NOTA: Puede ver los detalles del progreso del **Rollback** de todos los componentes en la página **Configuration progress**.

Resultados

Una vez que **Rollback** se realiza correctamente, se muestra la página **Configuration Welcome**. Configure el dispositivo desde la página **Configuration Welcome**.

Creación y descarga de un paquete de registro

Puede crear y descargar un paquete de registro que se puede analizar o enviar al servicio al cliente.

Pasos

1. En el tablero de ACM, haga clic en el icono del paquete de registro en la esquina superior derecha y seleccione **Create log bundle**.
2. En el cuadro de diálogo **Create log bundle**, seleccione los componentes que desee incluir en el paquete de registro y haga clic en **OK**.
3. Cuando se cree el paquete de registro, vuelva a seleccionar el icono del paquete de registro y seleccione **Download log bundle**. .
4. Especifique la ubicación de descarga y haga clic en **OK**.

Cuenta de usuario del primer director de seguridad

Después de hacer clic en el botón **Finish** para completar la instalación del dispositivo, se muestra la ventana emergente **Actualización del usuario del primer director de seguridad**.

Se recomienda crear la cuenta de usuario del director de seguridad de Protection Storage para los requisitos de cumplimiento de normas y seguridad. Consulte la sección *Crear primer usuario director de seguridad* en la *Guía del producto del dispositivo de la serie DP de PowerProtect* y crear una cuenta de usuario del director de seguridad en el sistema.

Acceso a Hypervisor Manager (Service)

Si necesita iniciar sesión en Hypervisor Manager (Service) para solucionar un problema encontrado durante la instalación, utilice el usuario **`idpauser@localos`** y la contraseña común para PowerProtect DP Series Appliance. Esta cuenta de usuario tiene privilegios limitados, pero tiene acceso a información que puede ayudar a identificar y solucionar problemas.

Solución de problemas de Secure Remote Services

Para el modelo DP4400, el ID de serie del dispositivo siempre se completa automáticamente en la página de configuración de Secure Remote Services.

Sobre esta tarea

Después de verificar los números de serie del producto de dispositivo y componente, continúe registrando el dispositivo y los componentes con Secure Remote Services, mediante los siguientes pasos:

Pasos

1. Configure Secure Remote Services mediante para el dispositivo de ACM, Protection Storage, Protection Softwarey Reporting and Analytics, y durante la instalación nueva a través del asistente de ACM o desde el tablero de ACM.
2. Ingrese la IP de gateway de Secure Remote Services del cliente.
3. Ingrese las credenciales del servicio de soporte en línea (nombre de usuario y contraseña).
   En caso de que se produzca algún problema, consulte la siguiente tabla para conocer algunos problemas comunes y la resolución asociada.

Tabla 12. Problemas comunes y resolución durante la solución de problemas de Secure Remote Services

Problema	Solución	Punto de contacto
Falla de autenticación	Verificar las credenciales	Equipo de seguridad
Errores de autorización si la dirección de la cuenta de usuario no está asignada al ID del sitio: • Usuario no autorizado • Se produjo un error durante la comunicación con el servicio DRM	Abra un incidente de TI en SNOW para solicitar asistencia sobre estos errores de registro de Secure Remote Services.	
Incompatibilidad de dispositivos • Es posible que el número de serie no esté asociado con el ID de sitio correcto • Es posible que el número de serie no se agregue en la extracción del dispositivo Secure Remote Services	• Verifique que el ID del sitio se haya agregado en el gateway de Secure Remote Services. • Verifique el SWID desde el correo electrónico de notificación de activación de licencia. • Verifique y solicite el número de serie (SWID), el ID del sitio (ID de envío a la parte/registro de SO) y el número de referencia SWID (número de elemento). • Los dispositivos se pueden registrar con una ID de sitio diferente. Verifique desde la página Extracción del dispositivo y actualice los ID del sitio en el gateway de Secure Remote Services del cliente, según corresponda.	Soporte de Secure Remote Services
Falla en el registro de dispositivo, Protection Storage, Protection Software y Reporting and Analytics.	• Si el archivo ACM `server.log` tiene una entrada para el error que se produjo durante la comunicación con el servicio DRM, reinicie los servicios en el servidor de gateway de Secure Remote Services del cliente. • Si el archivo ACM `server.log` tiene una entrada con el mensaje de error `Failed to register device: SSL peer certificate or SSH remote key was not OK`, asegúrese de que el nombre de host de gateway exacto utilizado durante la implementación de gateway también se utilice en este comando.	Soporte de Secure Remote Services o chatee con el equipo de licencias.

Volver a registrar el Secure Remote Services y actualizar el número de serie del dispositivo

Los siguientes son algunos de los casos en los que se requiere volver a registrar el número de serie del dispositivo:

Caso 1

El número de serie del dispositivo incorrecto está registrado con Secure Remote Services

Caso 2

Se configuró un número de serie ficticio en el dispositivo durante la instalación, pero no se registró con Secure Remote Services

Pasos generales para resolver el caso 1 y el caso 2

1. Obtenga el número de serie del dispositivo correcto para volver a registrarse.
2. Anule el registro del dispositivo si ya está registrado con Secure Remote Services.
3. Configure el número de serie del dispositivo correcto en el dispositivo.
4. Registre o vuelva a registrar el dispositivo con Secure Remote Services una vez más.

Archivos que se deben editar para volver a registrar el dispositivo

- `esrsconfigstatus.xml`: Este archivo contiene el estado de la configuración de registro de Secure Remote Services para los componentes de Protection Storage, Protection Software (Service), Reporting and Analytics y del dispositivo. Este archivo se lee para comprobar el estado del registro de Secure Remote Servicescuando se recibe una solicitud de configuración de Secure Remote Services.
- `selskuconfig.xml`: este archivo contiene el ID de serie del dispositivo. Este archivo se lee cuando se recibe la solicitud para configurar el Secure Remote Services para el dispositivo.
  - Si el número de serie no coincide en el archivo `selskuconfig.xml`, comuníquese con el equipo de escalación de licencia a través del chat.
- `solutionId.xml`: este archivo también contiene el número de serie del dispositivo.

Realización de tareas de alto nivel

1. Obtenga el número de serie del dispositivo correcto para volver a registrarse.

   Para el caso 1, comuníquese con el soporte.

   Para el caso 2, el número de serie del dispositivo correcto se puede obtener de la orden de venta.

2. Anule el registro del dispositivo si ya está registrado con Secure Remote Services.
   - a. Inicie sesión en el gateway de Secure Remote Services del cliente.
   - b. Haga clic en la pestaña **Device** y haga clic en **Manage Device**.
   - c. Seleccione la casilla de verificación del modelo con el número de serie de dispositivo incorrecto correspondiente que desea cancelar de registro
   - d. Haga clic en el botón **Remove**.
3. Póngase en contacto con el soporte de Secure Remote Services para aprobar el estado *Pending Delete* del dispositivo en el servidor de Secure Remote Services ServiceLink (https://servicelink.emc.com).
4. Configure el número de serie del dispositivo correcto en el dispositivo.
   a. Conéctese al ACM mediante SSH.
   b. Abra el archivo `/usr/local/dataprotection/var/configmgr/server_data/config/esrsconfigstatus.xml`.
   c. Quite la etiqueta `product` del archivo `esrsconfigstatus.xml`. A continuación, se proporciona un ejemplo del archivo `esrsconfigstatus.xml`

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EsrsConfigStatus>
<isAcmRegistered>true</isAcmRegistered>
<isComponentRegistered>false</isComponentRegistered>
<isDdRegistered>false</isDdRegistered>
<isDpaRegistetred>false</isDpaRegistetred>
<product>
<productName>ACM</productName>
<ipAddress>10.241.180.37</ipAddress>
<serialNumber>DPAPPLIANCEDEV09-ACM</serialNumber>
<deviceKey>uKsnjbSc7zjmrK5G4Wpe4xszfGkYPNc0EOTqKQTpnK9A0QrGj8DPTOFV6a7Ejc7m1Zb1KnzICqXzrd
UaR1kTAEsp58ZU+6jXEjy+zMYI3e2FJ1TKPdtbrhC0O8pZbwJ60mCTUMr4Q9T9Lo0DHGDQM0kgGw6uC57Ab/
```

```
ULG8ougWqJpKVEZtNtYqntEequSnt53qtXAkLuUtk3g1WP</deviceKey>
</product>
</EsrsConfigStatus>
```

d. Cambie el valor del parámetro `isAcmRegistered` a *false* si es *true*. A continuación, se proporciona un ejemplo del parámetro `isAcmRegistered`

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EsrsConfigStatus>
    <isAcmRegistered>true</isAcmRegistered>
    <isComponentRegistered>false</isComponentRegistered>
    <isDdRegistered>false</isDdRegistered>
    <isDpaRegistetred>false</isDpaRegistetred>
</EsrsConfigStatus>
```

e. Abra el archivo `/usr/local/dataprotection/var/configmgr/server_data/skuconfig/selskuconfig.xml`. A continuación, se proporciona un ejemplo

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VCEDPA>
<Model Name="Integrated Data Protection Appliance" Version="4400S">
<SerialID>IDP00180200001</SerialID>
<singleNetworkIpCount>10</singleNetworkIpCount>
<MultipleNetworkIpCount>
<managementNetworkIpCount>0</managementNetworkIpCount>
          <backupNetworkIpCount>0</backupNetworkIpCount>
...
```

f. Actualice el parámetro `SerialID` con el nuevo número de serie de ACM. A continuación, se proporciona un ejemplo

```
<SerialID>IDP00180200001</SerialID>
```

g. Abra el archivo `/usr/local/dataprotection/var/configmgr/server_data/config/solutionId.xml`. A continuación, se proporciona un ejemplo.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SolutionIdentifier>
<solutionName>Integrated Data Protection Appliance</solutionName>
<solutionSerialNumber>IDP00180200001</solutionSerialNumber>
<components>
...
```

h. Actualice el parámetro `solutionSerialNumber` con el nuevo número de serie del dispositivo. A continuación, se proporciona un ejemplo.

```
<solutionSerialNumber>IDP00180200001</solutionSerialNumber>
```

i. Ejecute el comando `rm` para eliminar el siguiente archivo.

```
/usr/local/dataprotection/var/configmgr/server_data/config/
DataProtectionConfiguration.pdf
```

```
DataProtectionConfiguration.pdf
/usr/local/dataprotection/var/configmgr/server_data/config/
DataProtectionConfiguration.xml
```

j. Utilice el botón **Refresh** en el tablero de ACM ACM para reflejar estos cambios.

5. Vuelva a registrar el dispositivo con Secure Remote Services. Ahora puede volver a registrar el dispositivo desde el tablero de ACM.

Una vez que el registro de Secure Remote Services se realiza correctamente, el personal de soporte y los usuarios reciben notificaciones relacionadas con eventos críticos y fatales o errores en el dispositivo a través de la administración del ciclo de vida de conectividad (https://clm.isus.emc.com/clm-dashboard/dashboard/index.jsp).

Adición de ID de sitio al gateway de Secure Remote Services

La adición de ID de sitio al gateway de Secure Remote Services ya no es necesaria para el gateway Secure Remote Services versión 3.34 y superior.

Para gateway Secure Remote Services versión 3.34 y superior, la dirección de su cuenta se asigna al ID del sitio, de modo que pueda utilizar la dirección de cuenta de usuario especificada durante el registro de Secure Remote Services, sin tener que agregar el ID de sitio en el gateway Secure Remote Services.

Los errores encontrados si la dirección de la cuenta de usuario no está asignada al ID del sitio son los siguientes:

- Usuario no autorizado:
- Se produjo un error durante la comunicación con el servicio DRM.

Abra un incidente de TI en SNOW para solicitar asistencia los errores de registro de Secure Remote Services anteriores.

Para los usuarios con gateway Secure Remote Services versión 3.34 y anterior, realice los siguientes pasos para conectar y agregar ID de sitio al gateway de Secure Remote Services:

1. Conéctese al gateway de Secure Remote Services navegando a `https://srs_gateway_ip_address:9443/`.
2. Inicie sesión con su nombre de usuario y contraseña de gateway de Secure Remote Services.

   Si encuentra alguno de los siguientes problemas:

   - No se puede acceder al gateway de Secure Remote Services del cliente por IP o nombre de host: problema de red en el entorno del cliente

     Verifique que el nombre de host del gateway de Secure Remote Services del cliente esté registrado en las zonas de búsqueda directa e inversa de DNS. Asegúrese de que ping y nslookup sean correctos y válidos. El punto de contacto para este problema es el equipo/soporte de Secure Remote Services de TI del entorno del cliente.

   - SrS Gateway connection denied: credenciales incorrectas

     Inicie sesión directamente en el portal de soporte para validar las credenciales. Espere a que se revierta el token de SSO si está utilizando un token para la autorización entre intentos de inicio de sesión/registro. El punto de contacto para este problema es el equipo de soporte de IDPA/SRS.
3. Para verificar el estado de los servicios que se ejecutan en el gateway de Secure Remote Services, haga clic en la pestaña **Dashboard** > **Service Status** y verifique el estado de los servicios que se ejecutan en el sistema de gateway de Secure Remote Services.
4. Asegúrese de que la conectividad de red desde el gateway de Secure Remote Services a todos los servidores Dell EMC necesarios haciendo clic en **Configuration** > **Network Check** > **Run Test**.

Agregar SiteID a Secure Remote Services

Agregue ID de sitio al host de gateway de Secure Remote Services.

Pasos

1. En el menú **Devices**, seleccione **Manage Device**.

   En la siguiente figura se muestra la consola de Secure Remote Services y el menú **Devices**.

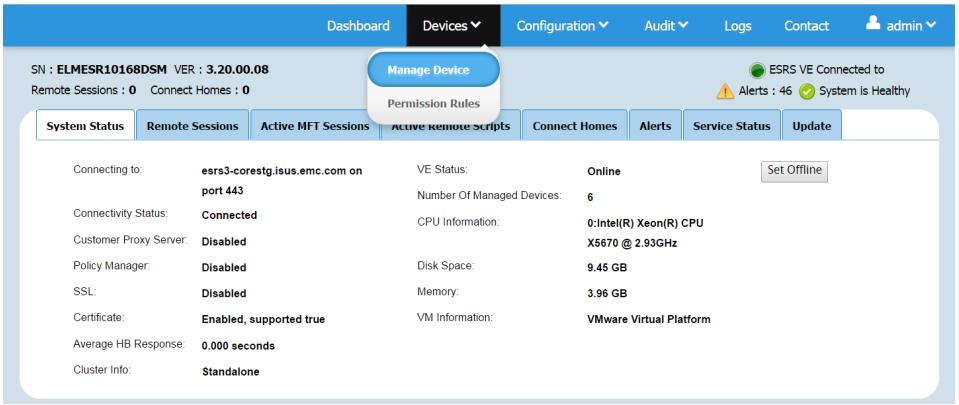

Ilustración 12. Menú Devices de Secure Remote Services

2. Haga clic en el botón **Add SiteID**.

   NOTA: No agregue el ID del sitio sin el permiso del cliente.

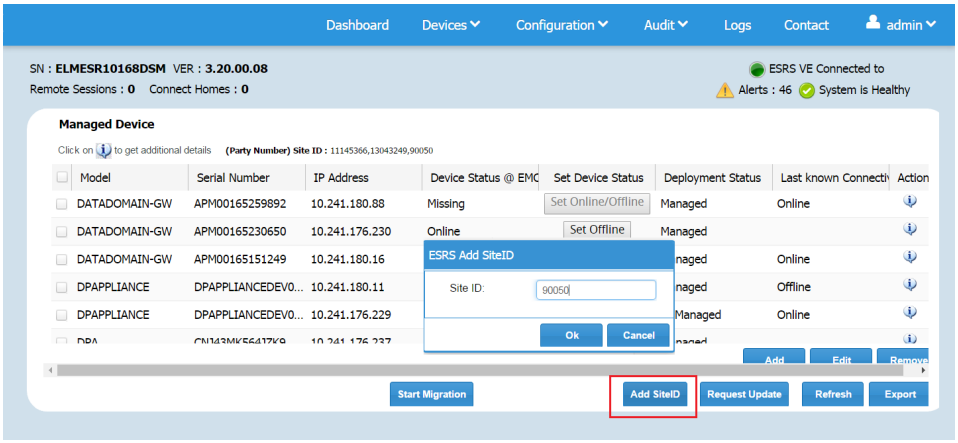

Ilustración 13. Ventana Add SiteID de Secure Remote Services

3. En la ventana Secure Remote Services **Add SiteID** , escriba el `Site ID`, a continuación, haga clic en **OK**.

   Si encuentra algún problema, consulte a continuación dónde se documentan los problemas comunes y sus resoluciones.

   - `The Site ID already exists, please enter another Site ID` o `The Site ID is invalid. Please contact your local EMC representative` or `The specified Site ID is not a valid site Number.`

     Verifique si se ingresó un ID de sitio válido. Puede encontrar el ID del sitio en (Ship to Party/Reg ID from SO). El punto de contacto para este problema es el equipo de cuentas.

ID en serie requeridos para PowerProtect DP Series Appliance, Protection Storage, Protection Software y Reporting and Analytics

El ID de serie que se requiere en la ventana de configuración de Secure Remote Services para los componentes del dispositivo, Protection Storage, Protection Software y Reporting and Analytics, se conoce de la siguiente manera:

- *Número de serie de activación*: en el correo electrónico de notificación de activación de la licencia de software de Dell EMC, en la sección ID de software o en el ID de bloqueo que aparece al principio del correo electrónico.
- *SWID o LOCKING_ID*: en los archivos de licencia de productos de componentes.

1. Obtenga los números de serie de activación para los componentes del dispositivo, Protection Storage, Protection Storage, Protection Software y Reporting and Analytics en la sección ID software del correo electrónico de notificación de activación de licencia de software de Dell EMC.

   En la siguiente tabla se muestra la entrada para el campo ID de serie en la ventana de configuración de Secure Remote Services:

Tabla 13. Secure Remote ServicesCampos de ID de serie

Componente	ID de software/número de serie
Modelo DP4400	ID de bloqueo (rellenado automáticamente)
Protection Storage (DP4400 modelo)	ID de bloqueo (rellenado automáticamente)
Protection Software/Protection Software (Service)	ID de software (rellenado automáticamente)
Reporting and Analytics	ID de software (rellenado automáticamente)

Si encuentra algún problema como el siguiente `Dell EMC software license activation notification email is not readily available with the customer`:

- El registro de Secure Remote Services se puede realizar más adelante después de configurar el dispositivo desde el tablero de ACM.
- Los ID de software (SWID) y los ID de bloqueo para los componentes del dispositivo, Protection Storage, Protection Software y Reporting and Analytics se pueden encontrar en los archivos de licencia de componentes correspondientes.

- El número de serie del dispositivo (DP4400) se puede encontrar en el archivo `selskuconfig.xml` . Más adelante en este documento, se proporciona más información sobre este archivo.
- El punto de contacto para este problema es el equipo de escalación de licencia.

  Además, para Protection Storage, donde los modelos de DP4400 tienen una instancia de Protection Storage en lugar de una Protection Storage física, el ID de software de la instancia se utiliza para el registro de Secure Remote Services. A continuación se proporciona un ejemplo:

  ```
  # system show serialno detailed
  Serial number: IDP00180200004
  System software-id: ELMDDV0218XCG5
  Instance software-id: ELMDDV04199S11
  ...
  ```

  En el modelo DP4400, para Protection Storage, el número de serie completado automáticamente que se muestra en el campo ID de serie es el mismo que el Locking_ID del dispositivo cuando se configura Secure Remote Services para Protection Storage.

  Sin embargo, el ID de instancia obtenido del comando anterior es lo que se utilizará para el registro de Secure Remote Services y se puede verificar desde la base de datos de extracción del dispositivo después de que el registro de Secure Remote Services se haya realizado correctamente.

Implementación de Cyber Recovery para PowerProtect DP4400

En esta sección, se describe la implementación de Cyber Recovery para DP4400.

> ⚠ Cyber Recovery is supported for new installation of DP4400 and DP5900 systems only. It is not supported for any existing IDPA/PowerProtect DP series deployments.
> Specific licenses and installation services are required for deploying Cyber Recovery. Contact the Dell Technologies Sales Team for assistance if these requirements are not met.
> Continuing without verifying the pre-requisites may cause the system to be unusable.

Requisitos previos

En esta sección, se describen los requisitos previos para instalar el dispositivo con modo de vault.

El sistema de vault contiene solo Protection Software, Protection Storage y Cyber Recovery, junto con componentes de la infraestructura, incluido ACM.

NOTA: Cuando configure el dispositivo, asegúrese de que la IP y el nombre de host para Protection Software sean los mismos que los del Protection Software de producción.

- Una dirección IP y un nombre de host registrados en DNS con entradas de búsqueda directa e inversa para el servicio CR.

  En caso de que no haya una dirección IP válida para DNS, NTP y gateway, el dispositivo se puede configurar mediante la dirección IP de ACM. Consulte Implementación independiente (opcional) en la página 83 para obtener más información.

- Compatible solo con la red IPv4.
- Los componentes opcionales, como Data Protection Central, Reporting & Analytics, Cloud DR y Search, no deben estar presentes en el dispositivo.
- Asegúrese de que la IP y el FQDN para Protection Software sean los mismos que los del Protection Software de producción.
- Los puertos de firewall requeridos deben estar abiertos. Consulte Cyber Recovery en la página 121 para obtener más información.
- El dispositivo no debe estar habilitado para FIPS. Cyber Recovery no cumple con FIPS.
- Licencia válida de Cyber Recovery.
- Licencia de Protection Storage válida en caso de que esté configurando el bloqueo de retención como Gobierno corporativo.

Requisitos de dirección IP

Se requiere un total de 10 direcciones IP para configurar Cyber Recovery en el dispositivo.

Tabla 14. Requisitos de dirección IP para la configuración de CR

Cantidad de direcciones IP requeridas	Componente	Entrada de DNS requerida
1	Appliance Configuration Manager	Sí
1	Hipervisor de dispositivos PowerProtect serie DP	Sí
1	PowerProtect DP Series Appliance Hypervisor Manager	Sí
1	Protection Storage (administración)	Sí
2	Protection Storage (respaldo)	No
1	Aplicación de respaldo	Sí
1	Proxy interno del servidor de respaldo	Sí
1	DPC del dispositivo PowerProtect serie DP	Sí
1	Cyber Recovery	Sí
1	Replicación de Cyber Recovery	Sí

NOTA:

- Después de configurar Cyber Recovery, necesita +1 dirección IP para Protection Storage a fin de configurar el par de replicación. En caso de que la conexión directa esté configurada, se puede utilizar la dirección IP privada.
- En caso de que no haya una dirección IP válida para DNS, NTP y gateway, el dispositivo se puede configurar mediante la dirección IP de ACM. Consulte Implementación independiente (opcional) en la página 83 para obtener más información.
- Como parte de la implementación de VM de CR, ACM configura los respaldos diarios de recuperación ante desastres (DR) de cr. Para obtener más información acerca de la configuración de respaldo de DR, consulte la *Guía del producto del dispositivo PowerProtect serie DP*. Asegúrese de que los respaldos de CR se ejecuten cuando no haya otros trabajos en ejecución. Si el trabajo programado está configurado para ejecutarse mientras se ejecutan otros trabajos de CR, los respaldos fallan.

Instalar el parche posterior a la instalación de PowerProtect DP Series Appliance en DataProtection-ACM

Realice los siguientes pasos para instalar un parche posterior a la instalación:

Requisitos previos

NOTA: Si no se actualiza el firmware antes de ejecutar el flujo de trabajo de actualización de software (instalación de los parches previos o posteriores a la instalación), se pierde la funcionalidad de recibir alertas de fallas de hardware en ACM.

Debe revisar el archivo Léame disponible junto con este parche posterior a la instalación para verificar si hay alguna tarea de preinstalación que debe realizar antes de aplicar este parche posterior a la instalación.

Pasos

1. Identifique la versión actual de PowerProtect DP Series Appliance mediante la ejecución del siguiente comando:

   ```
   # rpm -qa | grep dataprotection
   ```

2. Vaya a https://support.emc.com/downloads/41849_Integrated-Data-Protection-Appliance para ver si hay parches posteriores a la instalación disponibles para su versión de PowerProtect DP Series Appliance. Si hay algún parche posterior a la instalación disponible, descárguelo en su carpeta local.

3. Extraiga el contenido de este archivo `Idpa_post_update_N.N.N.nnnnnn.zip`.
   Este archivo zip contiene el parche `Idpa_post_update_N.N.N.nnnnnn.tar.gz` y un archivo `ReadMe.txt` asociado.

   Donde:

   `N.N.N` es la versión más reciente del parche posterior a la instalación.
   `nnnnnn` es el número de compilación.
4. Copie el archivo `Idpa_post_update_N.N.N.nnnnnn.tar.gz` en la ubicación `/data01/upgrade` en ACM.

   NOTA: Asegúrese de que solo exista el archivo de parche posterior a la instalación en esta carpeta y que no existan otros paquetes. Si hay otros archivos de instalación en esta carpeta, debe eliminarlos antes de instalar el parche.
5. Asegúrese de tener el permiso ejecutable para el paquete de instalación que copió en el directorio `/data01/upgrade`. Si no tiene el permiso ejecutable, ejecute el comando `chmod 644 Idpa_post_update_<version.build number>.tar.gz` para obtener el permiso.
6. Inicie sesión en ACM y haga clic en la pestaña **Upgrade**.
   El archivo de paquete de actualización más reciente se detecta automáticamente y aparece en **Upgrade Binary Location**.
7. Haga clic en **Extraer**.
   El navegador se redirige a *https://<acm_configured_public_ip>:9443* con un número de puerto modificado.

   NOTA: El proceso de validación tarda aproximadamente 15 minutos y ACM puede agotar el tiempo de espera. Para reanudar la sesión, debe iniciar sesión una vez más.

   El sistema realiza lo siguiente:

   - Estado de VLAN
     - Valida si puede conectarse a los 3 servidores de Hypervisor
     - Valida la cantidad de clústeres de Storage Pool
     - Valida si el almacén de datos de Storage Pool es mayor que 16,2 TB.
   - Valida la conexión a todos los componentes.
   - Valida el estado de la licencia.
   - Valida si los servicios de Protection Software se están ejecutando.
   - Valida para asegurarse de que no haya trabajos de respaldo en ejecución en Protection Software.
   - Valida si la capacidad utilizada de DD es inferior al 85 %.
   - Validación del punto de control de Protection Software
   - Requisitos de Storage Pool:
     - Sirve para buscar objetos o máquinas virtuales inaccesibles de Storage Pool.
     - Comprueba si el clúster de Storage Pool requiere un rebalanceo de datos de disco.
     - Comprueba si una tarea de reconstrucción de componentes está en curso en el clúster de Storage Pool.
     - Comprueba los requisitos de espacio de disco suficiente (30 %).
   - Requisitos previos de actualización de ESX:
     - Requiere puntos de conexión válidos para todos los servidores de Hypervisor requeridos.
     - Requiere que los servidores de Hypervisor correspondientes estén en modo de mantenimiento.
     - Requiere que la versión de Hypervisor Manager sea superior a la versión de Hypervisor. En caso de que haya una actualización importante a Hypervisor Manager, la dirección IP privada de Hypervisor Manager, 192.168.100.108, no debe estar en uso.

   NOTA: La dirección IP privada de Hypervisor Manager, 192.168.100.108, solo se requiere temporalmente durante el proceso de actualización.

   En una tabla, se muestra la versión actual, la nueva versión y el tipo (por ejemplo, principal, parche) de cada componente para el que está disponible una actualización.

   Si la validación no se realiza correctamente, compruebe los errores que se muestran cuando pase el cursor sobre el signo de exclamación. Resuelva todos los errores y haga clic en **Extract**.
8. Haga clic en **Upgrade**, escriba la contraseña de ACM y haga clic en **Authenticate**.
9. Para iniciar la actualización, haga clic en **Yes**.
   Se inicia el proceso de actualización.

   NOTA: El proceso de actualización puede tardar entre cinco y seis horas, durante el cual toda la actividad en PowerProtect DP Series Appliance debe estar en modo inactivo. No se puede acceder al sistema mientras se realizan partes de la actualización.

   AVISO: Si el proceso de actualización aún está en ejecución, no apague ni reinicie ACM ni reinicie el servicio *dataprotection_webapp*. Si por algún motivo apagó o reinició ACM, o reinició el servicio *dataprotection_webapp*

mientras el proceso de actualización aún está en ejecución, y si no puede ver el progreso de la actualización después de reiniciar ACM, comuníquese con un profesional de soporte técnico.

Upgrade Progress muestra lo siguiente:

- La barra de progreso de actualización de ACM con el porcentaje de progreso y la descripción del paso de actualización en curso
- Barra de progreso de actualización de componentes individuales con porcentaje de progreso y descripción del paso de actualización en curso

10. Una vez que todos los componentes se actualicen correctamente y la barra de progreso general de actualización de PowerProtect DP Series Appliance muestre el 100 %, haga clic en **Finish**.
11. Haga clic en **OK** en la ventana **Upgrade Finish**.

NOTA: Una vez finalizada la actualización, puede enfrentarse a un escenario en el que Protection Software está en modo de mantenimiento y los trabajos no se pueden ejecutar. Una vez que Protection Software sale del modo de mantenimiento, se ejecutan los trabajos.

NOTA: Una vez finalizada la actualización, confirme la notificación Event Connect EMC notification failed en el administrador de Protection Software. Esta notificación se genera durante la actualización cuando se desconecta el servicio de MC.

NOTA: Una vez finalizada la actualización, hay una advertencia en Hypervisor Manager acerca de un posible problema vulnerable que se describe en CVE-2018-3646. PowerProtect DP Series Appliance utiliza la versión de Hypervisor que tiene la corrección para esta vulnerabilidad; sin embargo, esta corrección no está habilitada de manera predeterminada, ya que tiene un impacto grave en el rendimiento. Para obtener más información, consulte la *Guía de configuración de seguridad de PowerProtect DP Series Appliance*.

NOTA: Si agregó nodos de NDMP Accelerator a PowerProtect DP Series Appliance, debe actualizarlos manualmente. Para actualizar los nodos de NDMP Accelerator, consulte la sección *Actualización de software acelerador* en la *Guía del usuario de Dell EMC Avamar NDMP Accelerator para sistemas NAS de Dell EMC*.

El tablero con todos los productos y sus versiones actualizadas se muestra junto con ACM recientemente configurado.

Si la actualización de algún componente falla, el proceso de actualización se detiene hasta que soluciona el problema y resuelve el error. Sin embargo, si hay advertencias no críticas, el proceso de actualización continúa. Estas advertencias se deben resolver una vez que se completa el proceso de actualización.

3

Actualice a PowerProtect DP Series Appliance 2.7.1

En este capítulo, se describe cómo actualizar PowerProtect DP Series Appliance en los modelos DP4400 y DP5900. El software, el firmware y los componentes de infraestructura se actualizan en la actualización del dispositivo.

Se actualizan los siguientes componentes:

- Protection Software
- Protection Storage
- Data Protection Central
- Reporting and Analytics (opcional)
- Búsqueda (Opcional) .
- Cloud DR (opcional)
- ACM
- Administrador de hipervisor
- Firmware de servidor e hipervisor

Los componentes se actualizan en la siguiente secuencia:

1. Protection Software, Protection Storage, Data Protection Central, Reporting and Analytics, Search, Cloud DR y ACM.
2. Administrador de hipervisor, hipervisor y firmware del servidor.

Comuníquese con el soporte de Dell EMC para actualizar los nodos NDMP o para actualizar el switch ToR S4148-ON en el modelo DP5900.

NOTA: No se admite la actualización de infraestructura antes de la actualización de software.

Temas:

Rutas de actualización soportadas

En la siguiente tabla, se detallan las rutas de actualización compatibles con PowerProtect DP Series Appliance 2.7.1 en DP4400 modelos DP5900 y DP5900.

NOTA: Para verificar si está actualizando el dispositivo desde una versión compatible, haga clic en el icono **About** en la esquina superior izquierda del tablero de ACM.

Tabla 15. Rutas de actualización soportadas

Versión actual	Ruta de actualización compatible
PowerProtect DP Series Appliance versión 2.6	Actualice PowerProtect DP Series Appliance a la versión 19.7.1
PowerProtect DP Series Appliance versión 2.6.1	Actualice PowerProtect DP Series Appliance a la versión 19.7.1
PowerProtect DP Series Appliance versión 2.7	Actualice PowerProtect DP Series Appliance a la versión 19.7.1

Para obtener información sobre las rutas de actualización compatibles con las versiones 2.5 y anteriores del dispositivo, consulte la *Guía de instalación y actualización de Integrated Data Protection Appliance*.

Requisitos previos

En esta sección, se proporciona información sobre los requisitos previos que debe completar antes de comenzar el procedimiento de actualización.

ACM

- Asegúrese de que el archivo binario `idpa-hw-upgrade_<version>.tar.gz` de la actualización se descargue desde el soporte de Dell EMC y se copie a la carpeta `/data01/upgrade` en ACM.

  NOTA: La carpeta `/data01/upgrade` no debe contener ningún otro paquete de parche previo o posterior.

  NOTA: Si está actualizando tanto el software como los componentes de la infraestructura, puede eliminar el binario de actualización, que es de aproximadamente 50 GB, de la ubicación de origen después de transferir el archivo al ACM. Sin embargo, si está actualizando solo los componentes de software (de la versión 2.4.x y 2.5), debe conservar el binario de actualización, ya que tendrá que volver a copiar el mismo archivo en ACM para la actualización de infraestructura.
- Inicie sesión en la IP del servicio de ACM mediante SSH. y, a continuación, ejecute el siguiente comando para validar el paquete de actualización mediante el proceso de suma de comprobación SHA256: `sha256sum -c <*tar.gz.sha256 file name>`
- Asegúrese de tener permiso ejecutable para el paquete de actualización descargado. Para obtener el permiso ejecutable, ejecute el siguiente comando: `chmod 644 idpa-hw-upgrade_<version>.tar.gz.`

Protection Software

- La actualización de PowerProtect DP Series Appliance se debe realizar durante una ventana de mantenimiento cuando no hay otras actividades de mantenimiento o trabajos de replicación de respaldo en curso.
- Asegúrese de que las políticas de replicación estén deshabilitadas y de que no haya trabajos de replicación que se activen desde el servidor de origen de Protection Software mientras la actualización está en curso, ya sea en los servidores de Protection Software de origen o de destino. Consulte Detener trabajos de respaldo y replicación si no puede cancelar el trabajo de replicación o respaldo.

Cloud DR

Esta sección solo se aplica si el Cloud DR implementado en el dispositivo PowerProtect serie DP está configurado con Cloud DR Server.

Los siguientes son los requisitos de Cloud DR y Cloud DR Server antes de actualizar el dispositivo:

- Cloud DR (servicio) se debe actualizar manualmente a la versión 19.5.x o 19.6.x
- Cloud DR Server se debe actualizar manualmente a la versión 19.8.x

Cloud DR se actualiza automáticamente a su versión 19.8.x con la actualización del dispositivo.

NOTA: Si Cloud DR Server no está configurado con Cloud DR, puede continuar directamente con la actualización del dispositivo a medida que se actualiza con la actualización del dispositivo Cloud DR.

Las versiones de Cloud DR Server y Cloud DR no tienen que ser idénticas y no es necesario actualizarlas simultáneamente (a menos que se indique lo contrario). Cuando cargue un paquete de actualización, si la versión del paquete de actualización no es compatible, recibirá una notificación.

Cuando actualiza desde la versión de Cloud DR Server/Cloud DR después de 18.3, puede actualizar directamente a una versión cuatro veces posterior a la versión actual (por ejemplo, 18.3 > 19.3 > 19.5).

Secuencia de actualización manual de Cloud DR o Cloud DR Server

En la siguiente tabla se describen las rutas de actualización y la secuencia en la que Cloud DR y Cloud DR Server se deben actualizar.

Tabla 16. Secuencia de actualización de Cloud DR o Cloud DR Server

Versión del dispositivo	Versión de CDR correspondiente	Pasos de actualización de Cloud DR Server y Cloud DR
PowerProtect DP Series Appliance 2.6	19.5	Actualice Cloud DR Server de la versión 19.5 a la 19.8.
PowerProtect DP Series Appliance 2.6.1	19.6	Actualice Cloud DR Server de la versión 19.6 a la 19.8.

Cargar paquetes de actualización

Sobre esta tarea

Realice los siguientes pasos para descargar los paquetes de actualización y cargarlos desde el sistema Cloud DR:

Pasos

1. Descargue el `multi_package` de **Cloud Disaster Recovery Upgrade** desde el sitio de soporte de Dell EMC.
2. En el menú Cloud DR Server **System**, seleccione **Upgrades**.
3. Para cargar el paquete de actualización que acaba de descargar, haga clic en **Upload Package**.
4. Para reemplazar el paquete cargado actualmente por otro paquete de Cloud DR, haga clic en **Upload Different Package**.

   NOTA: Después de cargar un paquete de actualización para Cloud DR Server, se muestra el botón **Upgrade Cloud DR Server**.

   NOTA: Después de cargar un paquete de actualización para Cloud DR, un mensaje indica que `CDRA upgrade is pending`. Si el paquete de actualización incluye Cloud DR Server y Cloud DR, la actualización de Cloud DR se inicia después de la actualización de Cloud DR Server. **Cloud DR restore ova package** se actualiza como parte del proceso de actualización de Cloud DR.

   NOTA: No actualice el Cloud DR Server mientras se ejecuta el proceso de recuperación rápida. Si actualiza Cloud DR Server mientras se ejecuta el proceso de recuperación rápida, el proceso no se monitorea después de la actualización y se pierde la imagen de la máquina.

   Para obtener información detallada sobre cómo actualizar Cloud DR/Cloud DR Server, consulte el capítulo *Actualización de CDRS y CDRA* de la *Guía de instalación y administración de Dell EMC Cloud Disaster Recovery*, que se puede obtener en el sitio de soporte de Dell EMC.

Actualice el Cloud DR Server

Para actualizar Cloud DR Server a PowerProtect DP Series Appliance 2.7.1, realice los siguientes pasos.

Requisitos previos

Descargue el paquete de actualización (Cloud DR Server o Cloud DR, o ambos) desde el sitio de soporte de Dell EMC.

Asegúrese de que no haya ningún proceso de recuperación rápida en ejecución.

Pasos

1. En la opción del menú Cloud DR Server **System**, seleccione **Upgrades**.

   NOTA: Si hay una operación de recuperación ante desastres en curso, el proceso de actualización se deshabilita.

2. Haga clic en **Upgrade Cloud DR Server**.
3. En el cuadro de diálogo **Cloud DR Server Upgrade**, haga clic en **Upgrade**.

   Espere un breve tiempo de inactividad durante la actualización mientras se reinicia Cloud DR Server. No puede realizar operaciones de recuperación ante desastres hasta que se complete la actualización y reinicie el navegador.
4. Reinicie el navegador e inicie sesión en la interfaz de Cloud DR Server.

Resultados

Una vez que la actualización de Cloud DR Server se realiza correctamente, los cambios pueden tardar entre 10 y 15 minutos en reflejarse en la interfaz de usuario de Cloud DR. El tiempo que tardan los cambios en reflejarse depende de la conexión de red entre Cloud DR y Cloud DR Server. Espere a que la actualización de Cloud DR Server se refleje en la interfaz de usuario de Cloud DR y, a continuación, continúe con la actualización de Cloud DR si es necesario.

Actualización del Cloud DR

Para actualizar Cloud DR a PowerProtect DP Series Appliance 2.7.1, realice los siguientes pasos.

Pasos

1. En la opción del menú Cloud DR **System**, seleccione **Upgrades**.
   La página **Upgrades** muestra y proporciona información sobre la versión actual y el estado de actualización de Cloud DR.
2. Si hay un paquete de actualización disponible para Cloud DR, haga clic en **Upgrade Cloud DR Add-on**.
   Cloud DR se actualizó a la nueva versión. Es posible que se produzca un breve tiempo de inactividad durante la actualización mientras Cloud DR se reinicia. Al final del proceso de actualización, se muestra la página de inicio de sesión de Cloud DR.
3. Reinicie el navegador e inicie sesión en la interfaz de Cloud DR.

Actualice el PowerProtect DP Series Appliance

Sobre esta tarea

En esta sección, se describe cómo actualizar el dispositivo a su versión 2.7.1. Tanto el software como los componentes de infraestructura se actualizan en este proceso de actualización.

- **Actualización de software**: actualiza Protection Storage, Protection Software, Data Protection Central, Reporting & Analytics, Search, Cloud DR y ACM.
- **Actualización de la infraestructura**: actualiza Hypervisor Manager y Hypervisor y el firmware del servidor PowerEdge.

Pasos

1. Inicie sesión en la interfaz del usuario de ACM mediante `https://<ACM_hostname>:8543`.
   Se recomienda usar el nombre del host de ACM para conectarse a la interfaz de usuario de ACM en lugar de usar la dirección IP.

   NOTA: Asegúrese de que no haya errores ni operaciones en curso en el tablero de ACM antes de pasar al paso siguiente.

   Si no puede conectarse a la interfaz de usuario de ACM mediante el nombre de host, agregue la siguiente entrada en el archivo hosts: *<ACM IP address> <ACM hostname>* y reinicie el navegador.
   - Para computadoras con Windows, el archivo de hosts se encuentra en `C:\Windows\System32\drivers\etc\hosts`
   - Para computadoras Linux, el archivo de hosts se encuentra en `/etc/hosts`
2. Verifique que el archivo `tar.gz` se complete automáticamente en el campo **Upgrade File Location** de la pestaña **Upgrade**.
   Si el archivo `tar.gz` no se rellena automáticamente, escriba la ruta en el campo **Upgrade File Location**.

   NOTA: Asegúrese de que el nombre del archivo de actualización `tar.gz` comience con `idpa`.

   Si la ruta o el nombre del archivo son incorrectos, se muestra un mensaje de error.
3. Haga clic en **Upgrade Readiness**.
   Una vez que la preparación para la actualización se completa correctamente, se muestra la página **End User License Agreement** de la actualización.

   NOTA: Si no se muestra la página **End User License Agreement**, asegúrese de que el puerto 9443 esté abierto en el firewall de la red y, a continuación, acceda a la ui de actualización desde el siguiente enlace: `https://<ACM_FQDN_OR_IP_ADDRESS>:9443/dataprotection-upgrade`

   Consulte No se puede acceder a la interfaz del usuario de ACM si no puede acceder a la URL anterior.
4. Lea Dell EMC **End User License Agreement** y haga clic en **Agree** para continuar las validaciones de la actualización.
   Si hace clic en **Disagree** y, a continuación, en **Cancel**, se lo dirigirá nuevamente al tablero de ACM.

5. Compruebe las opciones de actualización y, a continuación, haga clic en **Validate** para realizar comprobaciones de validación de los componentes que se actualizarán.

   Software Upgrade e **Infrastructure Upgrade** están seleccionados de forma predeterminada. Elija el valor predeterminado de **Software Upgrade** e **Infrastructure Upgrade** o sencillamente **Software Upgrade**.

   NOTA: Si deselecciona **Infrastructure Upgrade**, debe actualizar los componentes de la infraestructura más adelante. No se le permitirá actualizar a versiones futuras de PowerProtect DP Series Appliance sin actualizar los componentes de infraestructura correspondientes. Se recomienda utilizar este método únicamente si puede permitirse dos ventanas de actualización comparativamente más breves en lugar de una ventana de actualización larga.

   NOTA: Cuando se actualizan solo los componentes de software de las versiones PowerProtect DP Series Appliance 2.5 y anteriores, el paquete de actualización `tar.gz` no se conserva en ACM. Cuando realice la actualización de los componentes de la infraestructura, tendrá que copiar manualmente el paquete tar de actualización en la carpeta ACM `/data01/upgrade` nuevamente.

6. Espere a que se completen las comprobaciones de validación.

   El software de verifica los requisitos para realizar la actualización en función de las opciones seleccionadas en la página **Upgrade validation**. Consulte Solucionar errores de validación de actualización si experimenta algún error de validación de actualización. Consulte Posibles errores con la actualización de firmware si experimenta algún error de validación relacionado con el firmware.

   NOTA:

   Si seleccionó la opción Infrastructure Upgrade, **Current Version** de la fila **Server Firmware** puede aparecer como **N/A** o como **Unknown**.

   N/A se muestra cuando el proceso de validación de actualización no puede recuperar la versión de bloque de firmware, que puede ser una excepción o puede deberse a un error de tiempo de ejecución. **Unknown** se muestra cuando el proceso de validación de actualización no puede identificar la versión de bloque de firmware de la información recuperada, ya que los componentes de hardware en el nodo del servidor tienen diferentes versiones de firmware del bloque de firmware conocido.

   Continúe con el paso siguiente, ya que esto no afecta el proceso de actualización.

7. Haga clic en **Upgrade** y, a continuación, haga clic e n **OK** después de que se completen todas las validaciones.

   La página **Upgrade Progress** muestra los detalles del progreso de la actualización. Este proceso puede tardar algunas horas en completarse según las opciones de actualización seleccionadas en la página **Upgrade Validation**. Si la actualización de algún componente falla, el proceso de actualización se detiene hasta que soluciona el problema y resuelve el error. Consulte Solucionar errores de actualización si experimenta algún error de actualización. Consulte Posibles errores con la actualización de firmware si experimenta algún error de actualización de firmware.

   NOTA: La sesión del navegador puede agotar el tiempo de espera si la página **Upgrade Progress** está inactiva durante algún tiempo. Actualice el navegador e inicie sesión nuevamente en ACM para volver a conectarse a la página **Upgrade Progress**.

   NOTA: Si hace clic en **Cancel** en lugar de **Upgrade**, se le redirigirá al tablero de ACM. Cuando vuelve a continuar con el proceso de actualización, la página **End User License Agreement** no se muestra, ya que **End User License Agreement** ya está aceptado.

   NOTA: Durante la actualización, el flujo de trabajo de actualización realiza algunas operaciones en los componentes individuales, como el cambio de nombre o el reinicio de los componentes, lo que genera alertas. Puede ignorar estas alertas, ya que forman parte del flujo de trabajo del proceso de actualización. Sin embargo, si hay alertas críticas relacionadas con el hardware, comuníquese con el personal de soporte técnico de Dell EMC.

8. Opcional: haga clic en **Download Logs** para recopilar los registros después de que se complete el proceso de actualización.
9. Haga clic en **Finish** y, a continuación, en **OK** para finalizar la operación de actualización.
   Espere el tiempo que se muestra en la ventana emergente, después del cual se lo redirige al tablero de ACM. No vaya a otra pantalla cuando aparezca el temporizador en la ventana emergente.

   NOTA: Si cierra la ventana emergente antes de la hora especificada, debe abrir manualmente el tablero de ACM en el navegador. Sin embargo, es posible que no se pueda acceder al tablero de ACM o que el estado de algunos componentes se muestre incorrectamente debido al inicio posterior a la actualización, el cual está en curso. Debe esperar al menos 30 minutos después de hacer clic en Finish hasta que se reinicie ACM y otros servicios del dispositivo.

NOTA: Si el dispositivo se actualizó desde la versión 2.4.x o la versión 2.5, el tablero de ACM tardará más en mostrarse. Durante este tiempo, no intente eliminar ni encender ninguno de los servicios de ACM (especialmente el servicio ACM -old).

El servidor Hypervisor se reinicia junto con todos los servicios del dispositivo de servidor alojados en él. El dispositivo DP4400 tarda entre 5 y 45 minutos en iniciarse según las rutas de actualización. El dispositivo DP5900 tarda aproximadamente 10 minutos en iniciarse. Consulte No se puede iniciar el dispositivo después de la actualización si el dispositivo no se inicia.

10. Verifique que todos los componentes se hayan iniciado y que no haya errores en el tablero de ACM.

    Si realizó la actualización predeterminada de software e infraestructura en el paso 6, el dispositivo se actualizó correctamente a su versión 2.7.1.

    NOTA: Si se muestran errores en el tablero de ACM, cierre la ventana del navegador existente y abra la interfaz del usuario de ACM en una nueva ventana del navegador.

    NOTA: Es posible que la versión del firmware aparezca como **N/A** o **Unknown** cuando mueva el cursor junto a **Hardware Version** en la interfaz del usuario de ACM. Para obtener más información, consulte la nota en el paso 6

    NOTA: Si habilitó FIPS cuando actualizó a PowerProtect DP Series Appliance 2.7.1, el proxy de VM interno de Protection Software no se actualizará. Durante la actualización, el proxy de VM interno de Protection Software se apaga porque no cumple con el cumplimiento de normas de FIPS. Después de la actualización, el proxy de VM interno de Protection Software permanecerá en 19.3 (no en 19.4.x.x).

11. Si deseleccionó la casilla de verificación **Infrastructure Upgrade** en el paso 6, el tablero de ACM muestra una notificación que indica que la actualización de los componentes de la infraestructura está pendiente. Vaya a la pestaña **Upgrade** y repita todos los pasos de actualización nuevamente para actualizar los componentes de la infraestructura.

    NOTA: Cuando se actualizan solo los componentes de software de las versiones PowerProtect DP Series Appliance 2.5 y anteriores, el paquete de actualización `tar.gz` no se conserva en ACM. Cuando realice la actualización de los componentes de la infraestructura, tendrá que copiar manualmente el paquete tar de actualización en la carpeta ACM `/data01/upgrade` nuevamente.

    NOTA: El paquete de actualización `tar.gz` es el mismo que el que se usa para la actualización de software.

Actualizar el VM Proxy externo

Requisitos previos

- Asegúrese de que todos los hot fixes necesarios estén instalados en Protection Software antes de actualizar los proxies internos y externos.
- Asegúrese de que se haya completado la actualización de la versión de Protection Software.
- Asegúrese de que no haya ningún respaldo o restauración de VMware en curso.

Sobre esta tarea

Realice los siguientes pasos para actualizar el proxy mediante **Proxy Deployment Manager (PDM)**. .

NOTA:

- La actualización del proxy mediante PDM solo es posible si el proxy se implementó anteriormente mediante PDM.
- El proxy no estándar no se puede actualizar mediante PDM, por ejemplo, más de una NIC.

Pasos

1. Desde un navegador, conéctese a **Avamar Administrator** mediante la URL:
   `https://hostname/aui`
2. Seleccione **Proxy Management**.
3. En la sección **Config**, seleccione **vCenter** en la lista desplegable.
4. Haga clic en **Create Recommendation**.

   Se crea la recomendación y el proxy que se debe actualizar se muestra con un relámpago.

5. Haga clic en **Apply**.
6. En el cuadro de diálogo **Upgrade pending**, haga clic en **Continue**.

7. Verifique que el proxy actualizado se implemente en Hypervisor Manager y que los respaldos que usan el proxy recién implementado se realicen correctamente.
8. Elimine el VM Proxy antiguo de la interfaz del usuario del servidor Hypervisor Manager.

   Estos pasos también se enumeran en el artículo de la base de conocimientos 20235. Si no puede implementar el proxy mediante los pasos del artículo de la base de conocimientos 20235, consulte Actualizar el proxy de VM externo manualmente.

Actualizar la base de datos de HCL del pool de almacenamiento (aplicable solo para el modelo DP5900)

En esta sección, se describe cómo actualizar la base de datos de HCL del pool de almacenamiento.

Requisitos previos

NOTA: Para acceder al cliente web de Hypervisor Manager:

- Agregue la dirección IP de Hypervisor Manager al archivo de hosts en la máquina desde la que puede acceder al cliente web. La entrada debe tener el siguiente formato:

  ```
  <Hypervisor Manager IP address>     dpappliance-vcsa.idpa.local
  ```

- Si Hypervisor Manager no tiene un proxy o no está conectado a Internet, asegúrese de haber descargado el archivo `all.json` desde https://partnerweb.vmware.com/service/vsan/all.json.

Pasos

1. Inicie sesión en el servidor de Hypervisor Manager como usuario raíz y con las credenciales predeterminadas mediante el cliente web.
2. Vaya al clúster **vSAN,** haga clic en **Monitor** y, a continuación, haga clic en **Health**.
3. Expanda la prueba **Hardware compatibility** y, a continuación, seleccione **vSAN HCL DB up-to-date**
4. Seleccione el método online u offline para cargar la base de datos de HCL.
   - Haga clic en **Get latest version online** si Hypervisor Manager está conectado a Internet.
   - Haga clic en **Update from file** si no tiene un proxy o Hypervisor Manager no está conectado a Internet. Utilice el archivo `all.json` descargado.
5. Haga clic en **Retest**.

Solución de problemas de validación de actualización y fallas de actualización

- Consulte Solucionar errores de validación de actualización para cualquier problema encontrado con comprobaciones de validación realizadas durante el proceso de actualización.
- Consulte Solucionar errores de actualización para cualquier problema que encuentre durante la actualización del dispositivo.

NOTA: Para cualquier falla de validación de actualización relacionada con el pool de almacenamiento, comuníquese con el soporte de Dell.

Solucionar errores de validación de actualización

En esta sección, se describen algunas de las posibles fallas de validación de actualización y su solución alternativa.

No se puede acceder a la interfaz del usuario de ACM durante la actualización del dispositivo

Sobre esta tarea

Si no puede acceder a la interfaz del usuario de ACM desde `https://<ACM_FQDN_OR_IP_ADDRESS>:9443/dataprotection-upgrade`, realice los siguientes pasos para cancelar el proceso de actualización manualmente.

.

Pasos

1. Detenga el servicio tomcat de ACM mediante el siguiente comando: `service dataprotection_webapp stop` .
2. Use el siguiente comando para detener el servicio tomcat de actualización de ACM si se está ejecutando: `service dataprotection_webapp_upgrade stop`
3. Use el siguiente comando para comprobar si el servicio tomcat ACM está en ejecución: `service dataprotection_webapp status`
4. Use el siguiente comando para comprobar si el estado del dispositivo es `ESRS_AV_CONFIGURED` en el archivo `applianceStatus.xml`: `cat /usr/local/dataprotection/var/configmgr/server_data/status/applianceStatus.xml | grep applianceState`
5. Use el siguiente comando para copiar los registros de Tomcat de actualización desde la carpeta`/usr/local/dataprotection/upgrade-tomcat/logs/`: `cp -R /usr/local/dataprotection/upgrade-tomcat/logs/ /data01/upgrade-tomcat-logs-backup/`
6. Use el siguiente comando para eliminar la carpeta `upgrade-tomcat` de la carpeta `/usr/local/dataprotection/`: `rm -rf /usr/local/dataprotection/upgrade-tomcat`
7. Copie los registros de actualización desde `/data01/tmp/patch/logs` y, a continuación, elimine la carpeta de parches de la ruta`/data01/tmp/`
8. Ejecute el siguiente comando para iniciar el servicio Tomcat de ACM: `service dataprotection_webapp start`
9. Vuelva a intentar la operación de actualización del dispositivo. Si no puede acceder a la URL, comuníquese con el soporte de Dell.

Protection Storage

En esta sección, se describen las posibles soluciones para fallas de validación de actualización de Protection Storage. Debe realizar los pasos dados en este capítulo mediante un cliente SSH y conectarse a Protection Storage con la cuenta de usuario sysadmin.

Realice lo siguiente para corregir las posibles fallas de validación de actualización:

- Ejecute el siguiente comando para comprobar que el consumo de almacenamiento de Protection Storage sea inferior al 99 %: `filesys show space`

  Si el consumo de almacenamiento es superior al 99 %, comuníquese con el soporte de Dell.

- Compruebe el estado del sistema de archivos mediante la ejecución del siguiente comando: `filesys status`

  Si el sistema de archivos está en buen estado, pero está ocupado, espere a que se complete la tarea y vuelva a intentar la validación de la actualización.

- Ejecute el siguiente comando para comprobar si hay operaciones de limpieza en curso: `filesys clean status`

  Espere a que se complete la tarea de limpieza y vuelva a intentar la validación de la actualización.

- Compruebe si hay alertas críticas mediante el siguiente comando: `alerts show current`

  Corrija los problemas para borrar las alertas y vuelva a intentar la validación de la actualización.

La capacidad utilizada de la partición / en Search supera el 55 %

Sobre esta tarea

La validación de la actualización puede fallar si la capacidad utilizada de la partición / en Search supera el 55 %.

Siga los siguientes pasos:

Pasos

1. Mediante una conexión SSH, con credenciales raíz, conéctese a Search.
2. Ejecute el siguiente comando para verificar el espacio utilizado en Search:
   `df -h`
3. Verifique que el espacio utilizado de la partición / sea del 55 % o superior.
4. Cambie el directorio a la carpeta `/var/log/`.
5. Elimine todos los archivos con la extensión `.xz`. El siguiente comando proporciona un ejemplo:
   `rm *.xz`
6. Borre los archivos de registro grandes, de ser necesario. Por ejemplo, puede borrar los archivos de mensajes.
7. Verifique que el espacio utilizado de la partición / sea inferior al 55 %.
8. Si el espacio utilizado de la partición / sigue siendo del 55 % o más, siga los pasos que se mencionan en el artículo de la base de conocimientos 000186645.

Used capacity of the partitions other than the / partition on Search exceeds 90 percent

About this task

The upgrade validation may fail if the used capacity of the partitions other than the / on Search exceeds 90 percent.

Perform the following steps:

Steps

1. Using an SSH connection, with root credentials, connect to the Search.
2. Verify the used space on Search by running the following command:
   `df -h`
3. Identify the partitions that are using 90 percent and above of the storage space.
4. For the partition mounted on `/mnt/es_data`, you can reduce the used space by deleting the indices from the Search Web UI.
5. For the partition mounted on `/mnt/search`, you can reduce the used space by deleting the older or unwanted log files.
6. Ensure the Search services are running.
   - Verify the status of Search services.
     - `service elasticsearch status`
     - `service search-cis-core status`
   - If the services are in a stopped state, then start the service.
     - `service elasticsearch start`
     - `service search-cis-core start`
   - If the services fail to start, restart the Search VM, and then check the status of the services again.
     - `reboot`

Protection Software

En esta sección, se describen las posibles soluciones para fallas de validación de actualización de Protection Software (servicio). Debe realizar los pasos que se indican en este capítulo sobre el Protection Software mediante un cliente SSH.

Realice lo siguiente para corregir las posibles fallas de validación de actualización:

- Para comprobar si hay al menos 38 GB de espacio libre en el directorio `/space` en el servidor de Protection Software, ejecute el siguiente comando `df -h`. Si el espacio libre en el directorio es inferior a 38 GB, elimine los archivos no deseados del directorio.

  Si el tamaño total de la partición `/space` es inferior a 96 GB, consulte el artículo de la base de conocimientos 000190523 sobre cómo aumentar el tamaño de la partición en el Protection Software (servicio).

- Compruebe si hay políticas activadas. Todas las políticas se deben deshabilitar antes de la actualización de un dispositivo.
- Compruebe si un servidor de replicación está configurado. Las validaciones de actualización pueden fallar si se configura un servidor de replicación.

Póngase en contacto con el soporte de Dell para validar la configuración mediante la comprobación de AV Proactive más reciente y continuar con la actualización.

- Compruebe si los agentes y clientes de respaldo de Protection Software se actualizaron manualmente antes de la actualización del servidor de Protection Software.

  Póngase en contacto con el soporte de Dell para validar la configuración mediante la comprobación de AV Proactive más reciente y continuar con la actualización.

Crear un punto de control validado

Requisitos previos

- Ejecute el siguiente comando para comprobar si tiene un punto de control validado que no tenga más de 24 horas con un `HFScheck`: `status.dpn`

Sobre esta tarea

La validación de la actualización puede fallar si no tiene un punto de control validado en Protection Software. El punto de control validado no debe tener más de 24 horas, con un `HFScheck` que no tenga más de 36 horas. Para crear un nuevo punto de control validado, realice los siguientes pasos:

Pasos

1. Inicie sesión en el servidor de Protection Software con la cuenta de usuario `admin`.
2. Ejecute el siguiente comando para crear un punto de control: `mccli checkpoint create --override_maintenance_scheduler=true --wait=0`
3. Ejecute el siguiente comando para ver el punto de control creado: `cplist --lscp`
4. Ejecute el siguiente comando para validar el punto de control: `mccli checkpoint validate --cptag=CheckpointTagFromPreviousCommand --override_maintenance_scheduler=true --wait=0`

Finalizar sesiones suspendidas

Sobre esta tarea

La validación de la actualización puede fallar si hay sesiones suspendidas en ejecución en el proxy de VM (servicio). Para finalizar estas sesiones suspendidas, realice los siguientes pasos:

Pasos

1. Inicie sesión en el sistema de Protection Software como usuario administrador con Putty.
2. Ejecute el siguiente comando para ver las sesiones activas en el sistema: `avmaint sessions | grep "path\|sessionid\|starttime"`
   - path: muestra la ruta del cliente.
   - sessionid: muestra el identificador único de la sesión.
   - starttime: muestra el registro de fecha y hora de UNIX de cuando comenzó la sesión.
3. Traduzca el valor del parámetro starttime a un formato legible mediante la ejecución del siguiente comando: `t.pl <starttime>`
4. Compare el valor con el programador de respaldo para confirmar si la sesión está en ejecución. Si la sesión se inició hace varios días y no está configurada como **overtime**, es posible que sea una sesión suspendida.
5. Ejecute el siguiente comando para eliminar las sesiones suspendidas: `avmaint kill <sessionid>`
6. Después de quitar todas las sesiones suspendidas, ejecute el siguiente comando para ver la lista de sesiones que se ejecutan en el servidor de Protection Software: `avmaint sessions --full`

Detener trabajos de respaldo y replicación

Sobre esta tarea

La actualización del dispositivo PowerProtect serie DP se debe realizar durante una ventana de mantenimiento cuando no hay otras actividades de mantenimiento de Protection Software, trabajos de respaldo o replicación en ejecución. Para asegurarse de esto, realice los siguientes pasos.

Pasos

1. Conéctese al nodo de utilidad mediante SSH e inicie sesión como usuario administrador.
2. Ejecute el siguiente comando para verificar si el estado del servidor es inactivo: `opstatus.dpn`
3. Ejecute los siguientes comandos:
   - `avmaint sessions | grep path`: para comprobar si hay trabajos de respaldo en curso.
   - `mccli activity show --active | grep Replication` : para comprobar si hay trabajos de replicación en curso.

   Ejemplo de salida:

   ```
   admin@dp5900-08-10:~/>: avmaint sessions | grep path
   path="/AVI_BACKUPS"
   path="/"
   admin@dp5900-08-10:~/>: mccli activity show --active | grep Replication
   9163194680374209 Running 0 2021-09-18 02:33 EDT 00h:02m:10s 2021-09-19 02:33 EDT Replication
   Source 133.4 MB 83%  dp5900-08-10.datadomain.com /MC_SYSTEM
   1631946917158146 Running 0 2021-09-18 02:35 EDT 00h:00m:14s 2021-09-19 02:33 EDT Replication
   Source 140.2 MB 2.1% EM_BACKUPS                  /
   admin@dp5900-08-10:~/>:
   ```

   Si hay trabajos de respaldo o replicación en ejecución, puede esperar a que estos trabajos se completen o puede finalizarlos. También puede comunicarse con el soporte de Dell para finalizar estos trabajos de respaldo.
4. Ejecute el siguiente comando para finalizar los trabajos de respaldo o replicación: `mccli activity cancel --id=<job_id>`
5. Ejecute los siguientes comandos para confirmar que los trabajos ya no están en curso.
   - `avmaint sessions | grep path`: para comprobar si hay trabajos de respaldo en curso.
   - `mccli activity show --active | grep Replication` : para comprobar si hay trabajos de replicación en curso.

Reporting and Analytics

Sobre esta tarea

El tamaño de la partición `/data01` en el servicio Reporting and Analytics DataStore no debe superar los 60 GB. Si el tamaño de la partición `/data01` es superior a 60 GB, la validación de la actualización fallará.

Para verificar el tamaño de la partición `/data01`, realice los siguientes pasos

Pasos

1. Conéctese al servicio Reporting and Analytics DataStore mediante SSH con credenciales raíz.
2. Verifique el tamaño de la partición `/data01` mediante el siguiente comando:`df -h`
3. Verifique el valor en la columna `size` de la partición `/data01`.
4. Si el tamaño es superior a 60 GB, comuníquese con el soporte de Dell para actualizar los componentes de informes y análisis.

Data Protection Central

Si configuró un servidor LDAP externo, asegúrese de que esté configurado desde el tablero de ACM.

Requisitos previos

Si configuró un servidor LDAP externo en Data Protection Central manualmente (no a través del tablero de ACM), la validación de la actualización para la actualización de componentes de Reporting & Analytics fallará.

NOTA: No se admite la configuración de un LDAP externo desde Data Protection Central.

Sobre esta tarea

Realice los siguientes pasos para comprobar si los ajustes de LDAP se configuran a través del tablero de ACM:

Pasos

1. Inicie sesión en el tablero de ACM.
2. Haga clic en el ícono a la izquierda de **Shutdown Appliance** y descargue la configuración actual para ver el archivo PDF de configuración del dispositivo con los detalles de configuración del dispositivo actual.
3. Para conectarse a Data Protection Central, especifique el nombre de usuario mencionado en la configuración de LDAP del PDF de configuración de PowerProtect DP Series Appliance. Si inicia sesión correctamente con el nombre de usuario proporcionado, esto indica que la configuración de LDAP está sincronizada.
   Si no puede iniciar sesión con el nombre de usuario mencionado en la configuración de LDAP del PDF de configuración de PowerProtect DP Series Appliance, vuelva a configurar la configuración de Data Protection Central LDAP con el nombre de host de ACM (generalmente idpauser) como servidor LDAP. Consulte la sección *Revert to internal LDAP environment* en la *Guía del producto de PowerProtect DP Series Appliance* para obtener más información.
4. Vuelva a configurar el LDAP externo desde el tablero de ACM. Consulte la *sección Configuración de un entorno LDAP externo* en la *Guía del producto de PowerProtect DP Series Appliance* para obtener más información.

Cloud DR

Sobre esta tarea

La validación de la actualización del componente Cloud DR puede fallar por el siguiente motivo:

- Si el Cloud DR Server no está conectado al Cloud DR.
- Si Cloud DR está configurado con su cuenta de nube y destino de Cloud DR, pero no con el Cloud DR Server

Realice los siguientes pasos para configurar el Cloud DR Server con el Cloud DR.

Pasos

1. En la barra de menú, haga clic en el servidor de Cloud DR.
   - Si no hay ninguna instancia de Cloud DR Server implementada, se abre la página **Deploy Cloud DR Server**.
   - Si ya hay una instancia de Cloud DR Server implementada, se abre la página **Cloud DR Server**. No se pueden implementar instancias de Cloud DR Server adicionales.
2. En la sección **Cloud DR Server Configuration**, seleccione el destino de Cloud DR en el que desee implementar **Cloud DR Server**.
3. Para asignar direcciones IP para la solución Cloud DR, proporcione **IPV4 CIDR Range**.
4. En la sección **User Configuration**, ingrese y confirme las contraseñas para los usuarios admin de Cloud DR Server y monitor de Cloud DR Server.

   Las contraseñas deben cumplir con lo siguiente:
   - Una longitud mínima de ocho caracteres.
   - Al menos un carácter en minúscula (a-z)
   - Al menos un carácter en mayúscula (A-Z)
   - Al menos un número (0-9)
   - Al menos un carácter especial (no alfanumérico)

   a. Ingrese y confirme las contraseñas para los usuarios Cloud DR Server Admin y Cloud DR Server Monitor.
   b. Introduzca una dirección de correo electrónico para las solicitudes de restablecimiento de contraseña de DD Cloud DR.
   Cuando se instala correctamente el servidor de Cloud DR, AWS envía un correo electrónico a esta dirección para la verificación. Siga las instrucciones que aparecen en el correo electrónico en un plazo de 24 horas desde la implementación.
5. Para confirmar que acepta los términos de Marketplace, haga clic en la casilla de verificación **I have accepted the AWS Marketplace terms**.
6. Haga clic en **Deploy** Cloud DR Server.

   El servidor de Cloud DR comienza la implementación de Cloud DR Server en el destino de Cloud DR. Si se produce un error durante la implementación, haga clic en **Cleanup** para eliminar los recursos de nube que crea Cloud DR Server y vuelva a intentar la implementación.

   La implementación de Cloud DR Server puede tardar hasta 30 minutos.

   Si la implementación se realiza correctamente, aparece la página Cloud DR Server, que enumera el nombre del host de Cloud DR Server y la región. También se implementa lo siguiente:
   - Una nube privada virtual (VPC).

- Un catálogo de servicios de base de datos relacionales (RDS) de Amazon, a fin de mantener los datos persistentes.
- Una subred privada para la comunicación entre RDS y Cloud DR Server.
- Una subred pública (modo estándar) o una subred privada (modo profesional) con acceso a Internet para utilizar mediante Cloud DR Server.
- La instancia EC2 de Cloud DR Server.

EL tipo de instancia M4.Large se utiliza para la instancia de Cloud DR Server. Para reducir los costos de implementación, es posible que desee adquirir instancias reservadas de AWS; de lo contrario, se utiliza una instancia por demanda. Una dirección IP elástica se asigna automáticamente a la instancia de Cloud DR Server. No puede cambiar esta dirección IP.

NOTA: Varios dispositivos de complemento de Cloud DR pueden conectarse a una sola instancia del servidor de Cloud DR. Sin embargo, un dispositivo Cloud DR Add-on no se puede conectar a múltiples instancias de Cloud DR Server.

Resultados

Haga clic en el nombre de host de Cloud DR Server después de implementar el Cloud DR Server para conectarse a Cloud DR Server.

ACM, Hypervisor Manager y Hypervisor

En esta sección, se describen las posibles soluciones para las fallas de validación de actualización de ACM, Hypervisor Manager y Hypervisor.

Realice lo siguiente para corregir las posibles fallas de validación de actualización:

- Compruebe si las direcciones IP privadas `192.168.100.108` utilizadas por el componente administrador del hipervisor y `192.168.100.113` utilizadas por el componente de ACM están disponibles para la validación de la actualización. Si las direcciones IP no están disponibles, la validación de la actualización fallará. Asegúrese de que estas direcciones IP estén disponibles y, a continuación, vuelva a intentar la validación de la actualización.

  Si se utiliza un rango de direcciones IP interno personalizado, actualice la dirección IP temporal y el gateway ACM en el archivo `/data01/tmp/patch/ip_details.properties`.

- Compruebe si ha creado o copiado máquinas virtuales, carpetas o archivos en los servidores del hipervisor o del administrador de hipervisor del dispositivo. Asegúrese de lo siguiente y vuelva a intentar la validación de la actualización:
  - No hay VM que no sean PowerProtect DP Series Appliance, vApps, pools de recursos ni ajustes personalizados implementados o configurados en el dispositivo.
  - No existen archivos y carpetas personalizados en los servidores del hipervisor y del administrador de hipervisor (Servicio).
  - No se copian archivos en las particiones del servidor del hipervisor o del administrador de hipervisor (Servicio). Estos incluyen ISO, VIB u otros archivos binarios copiados manualmente en las particiones de almacenamiento del servidor del hipervisor o del administrador de hipervisor (Servicio).

Configurar el nombre de host correcto en el servidor del hipervisor

Sobre esta tarea

La validación de la actualización puede fallar si el nombre de host (corto y FQDN) no está configurado correctamente en el servidor de hipervisor. Para asegurarse de tener el nombre de host correcto para el servidor de hipervisor que se refleja en iDRAC, realice los siguientes pasos:

Pasos

1. Conéctese al servidor de ACM mediante una conexión SSH
2. Ejecute el siguiente comando para ver el nombre de host de las direcciones IP asociadas con el servidor de hipervisor: `nslookup`
3. Conéctese al servidor del hipervisor mediante una conexión SSH.
4. Ejecute los siguientes comandos para verificar si el nombre de host coincide con el recuperado del comando `nslookup`:
   - `hostname -s`
   - `hostname -f`
5. Si el nombre de host en el hipervisor es incorrecto, ejecute los siguientes comandos:
   - `esxcli system hostname set --host=hostname`
   - `esxcli system hostname set --fqdn=fqdn`
6. Inicie sesión en la consola de iDRAC.

7. Vaya a **System Panel** en el **iDRAC dashboard** y verifique el valor en el campo **Host Name** .

   Si no puede acceder a la consola de iDRAC para ninguno de los servidores de Hypervisor, siga los pasos que se indican en el artículo de la base de conocimientos 21500.
8. Si el nombre de host no se refleja correctamente en el **iDRAC Dashboard**, actualice la consola y verifique el nombre de host.
9. Si el nombre de host no se refleja correctamente incluso después de actualizar la consola, detenga y reinicie el servicio de iDRAC:
   a. Ejecute el siguiente comando: `esxcli system wbem set -e=true`
   b. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/sfcbd-watchdog stop`
   c. Ejecute el siguiente comando para volver a iniciar el servicio: `/etc/init.d/sfcbd-watchdog start`

Reduzca el espacio de almacenamiento en la partición de Hypervisor Manager

Sobre esta tarea

La validación de Hypervisor Manager puede fallar con si el espacio de almacenamiento utilizado para la partición `/storage/log` es superior al 90 %. Para reducir el espacio de almacenamiento utilizado en `/storage/log`, realice los siguientes pasos:

Pasos

1. Mediante un cliente SSH, conéctese al Servidor de Hypervisor Manager servicio como usuario raíz.
2. Cambie al aviso de Shell: `shell`
3. Ejecute los siguientes comandos para asegurarse de que los servicios de Hypervisor Manager estén en ejecución: `service-control --all --status`
4. Ejecute el siguiente comando para verificar el tamaño de la partición /storage/log: `df -h`

   NOTA: Esta partición está en uso en más del 90 %. Elimine los archivos no deseados y lleve este valor porcentual por debajo del 90 % para asegurarse de que las validaciones de actualización se realicen correctamente.
5. Ejecute el siguiente comando para identificar los 20 archivos principales con un alto uso de disco: `du -a /storage/log | sort -n -r | head -n 20`
6. Elimine los archivos enumerados en la salida del comando anterior.
7. Ejecute el siguiente comando para verificar que el valor `% Use` de la partición `/storage/log` sea inferior al 90 %: `df -h`
8. Repita los pasos del 5 al 7 hasta que la partición `/storage/log` esté por debajo del 90 %.
9. Ejecute el siguiente comando para reiniciar todos los servicios de Hypervisor Manager y los servicios de Platform Services Controller: `service-control --start --all`
10. Ejecute el siguiente comando para asegurarse de que todos los servicios de Hypervisor Manager estén en ejecución antes del inicio del procedimiento de actualización: `service-control --all --status`

Solución de problemas de fallas de actualización

En esta sección, se describen los posibles problemas que puede encontrar cuando actualiza el dispositivo a su versión 2.7.1.

No se puede iniciar el dispositivo después de la actualización

Sobre esta tarea

Si el dispositivo no se inicia después de hacer clic en **Finish**, conéctese a la interfaz del usuario de Hypervisor y realice las siguientes tareas:

Pasos

1. Compruebe si el servidor Hypervisor está en modo de mantenimiento.
2. Salga del modo de mantenimiento.
3. Encienda la VM de **Data-Protection-ACM**.

   NOTA: No encienda ninguna de las otras VM (especialmente la VM ACM-old). Una vez que se enciende la VM **data-protection-ACM**, puede monitorear el progreso del inicio del dispositivo desde la interfaz del usuario de ACM

Protection Software

En esta sección, se describen los posibles errores de actualización que puede encontrar con Protection Software y su posible solución alternativa.

Protection Software no se puede iniciar después de la actualización

Es posible que Protection Software no se inicie o que tenga problemas de funcionalidad si instaló certificados SSL personalizados no compatibles en el Protection Software. Comuníquese con el soporte de Dell para resolver el problema.

Instale la CLI necesaria del instalador de Protection Software

Sobre esta tarea

La actualización de Protection Software puede fallar si la versión requerida de `avi-cli` no está instalada en Appliance Configuration Manager (ACM). Para instalar la versión correcta de `avi-cli`, realice los siguientes pasos:

Pasos

1. Mediante un cliente SSH, conéctese a ACM como usuario raíz.
2. Ejecute el siguiente comando para verificar que estén instalados los siguientes archivos binarios: `rpm -qa emc-avi-cli emc-ruby emc-tools`

   Tome nota de las versiones de estos archivos binarios.
3. Navegue hasta la carpeta `/data01/tmp/patch/products/ACM/AVICLI/binaries/` con el siguiente comando: `cd /data01/tmp/patch/products/ACM/AVICLI/binaries/`
4. Ejecute el siguiente comando para enumerar los archivos en la carpeta: `ls`

   NOTA: Esta carpeta contiene las versiones pertinentes de los RPM necesarios para instalar `avi-cli`.
5. Verifique si los números de versión de los archivos binarios instalados en el servicio de ACM del paso 3 corresponden a los archivos de la carpeta actual.

   NOTA: Si los valores de la versión de RPM son los mismos que los de la carpeta actual, comuníquese con el soporte de Dell EMC para obtener ayuda. Si los valores de la versión de RPM son diferentes a los valores de la carpeta actual, continúe con los pasos que se indican a continuación para actualizar los archivos binarios de la carpeta actual.
6. Desinstale los archivos binarios obsoletos existentes.
   a. Ejecute el siguiente comando para desinstalar el binario `emc-avi-cli` existente: `rpm -e emc-avi-cli`
   b. Ejecute el siguiente comando para desinstalar el binario `emc-ruby` existente: `rpm -e emc-ruby`
   c. Ejecute el siguiente comando para desinstalar el binario `emc-tools` existente: `rpm -e emc-tools`
7. Instale los RPM pertinentes desde la carpeta actual.
   a. Ejecute el siguiente comando para instalar el RPM `emc-tools` requerido: `rpm -ivh /data01/tmp/patch/products/ACM/AVICLI/binaries/emc-tools*.rpm --force`
   b. Ejecute el siguiente comando para instalar el RPM `emc-ruby` requerido: `rpm -ivh /data01/tmp/patch/products/ACM/AVICLI/binaries/emc-ruby*.rpm --force`
   c. Ejecute el siguiente comando para instalar el RPM `emc-avi-cli` requerido: `rpm -ivh /data01/tmp/patch/products/ACM/AVICLI/binaries/emc-avi-cli*.rpm --force`

La búsqueda se desconecta de Protection Software después de la actualización de PowerProtect DP Series Appliance

Sobre esta tarea

Después de actualizar PowerProtect DP Series Appliance, es posible que Búsqueda se desconecte de Protection Software. Si este es el caso, habrá un icono de vínculo rojo roto en el **idpa-backupServer** incluido en la página **Search UI** > **Manage: Avamar** > **Administration** > **Sources**. Para conectar la Búsqueda a Protection Software, realice los siguientes pasos.

Pasos

1. En la esquina superior derecha de la interfaz del usuario de búsqueda, en el campo **Manage:**, seleccione **Avamar** en el menú desplegable.
2. En el panel de navegación izquierdo, haga clic en **Administration** > **Sources**.

   Aparece una lista de fuentes de Búsqueda de Protection Software.
3. Haga clic en dentro de la fila que contiene **idpa-backupServer**.
4. Haga clic en el botón **Repair Agent** (icono de martillo y llave inglesa) en la barra de herramientas vertical derecha.
   Esto ejecuta un trabajo del agente de reparación para conectar la Búsqueda a Protection Software.

Actualizar el VM Proxy externo manualmente

En esta sección, se describen los pasos para actualizar VM Proxy manualmente. Si el VM Proxy existente no está disponible para la actualización en Proxy Deployment Manager (PDM), elimine el proxy servicio existente e implemente un nuevo proxy de servicio.

Requisitos previos

NOTA: Asegúrese de que todos los hot fixes necesarios estén instalados en Protection Software antes de actualizar los proxies internos y externos.

Pasos

1. Conéctese a la VM Proxy y recopile todos los detalles relacionados con la red, como la dirección IP asignada, DNS, Gateway, máscara de red y direcciones IP del servidor NTP.
2. Conéctese a la interfaz del usuario de Hypervisor Manager Server mediante un navegador en `https://<vCenter Server IP>`.
3. En la vista **Hosts and Clusters**, en el panel de navegación izquierdo, navegue hasta el nodo del servidor de Hypervisor Manager y seleccione la VM Proxy.
4. Anote el nombre de la servicio, el almacén de datos en el que está alojada, la red que utiliza. Haga clic con el botón secundario en VM Proxy y seleccione **Power** > **Shut Down Guest OS**.
5. Haga clic con el botón secundario en VM Proxy y seleccione **Rename**.
6. Cambie el nombre de VM Proxy agregando `-old` al nombre original.
7. Conéctese a la interfaz de usuario de Protection Software mediante `<https://<Avamar Server IP>`.
8. Implemente un nuevo proxy de servicio en el mismo Hypervisor Manager al que se conectó en el paso 6.
   a. Seleccione **Proxy Management** en el panel izquierdo.
   b. En la pestaña **Proxy Deployment**, en **Config Window**, seleccione el Hypervisor Manager.
   c. Verifique todas las demás configuraciones y haga clic en **CREATE RECOMMENDATION**.
   d. El **New Proxy** se muestra en la ventana **Recommendations**.
   e. Seleccione **New Proxy** y haga clic en el botón **Edit**.
   f. Cambie **Name** y configúrelo al mismo nombre que el nombre del antiguo servidor proxy de VM Proxy en Hypervisor Manager Server.
   g. Proporcione la misma dirección IP y todos los demás detalles que el VM Proxy anterior.
   h. Ejecute el siguiente comando para verificar que la dirección IP y el nombre de host del VM Proxy se puedan resolver mediante DNS:

      ```
      host -W 10 -T <Avamar_Proxy_VM_IP_Address>
      ```

      El comando anterior debe devolver el nombre de host de la IP de VM Proxy si se puede acceder al servidor DNS y si la IP de proxy está registrada en el servidor DNS.

      Consulte el artículo de la base de conocimientos 168924 para obtener ayuda.
   i. Haga clic en **Save**.
   j. Haga clic en **Apply Changes** para implementar el nuevo VM Proxy.
9. Realice un respaldo de una de las Hypervisor Manager para asegurarse de que los respaldos se ejecuten correctamente con el nuevo VM Proxy.
10. Elimine la **-old** VM Proxy de la interfaz del usuario de Hypervisor Manager Server.

Posibles errores con la actualización de firmware

Si se produce un problema con la actualización del firmware, la actualización del dispositivo falla y aparece un mensaje de error y su código de error correspondiente en la interfaz del usuario de ACM. Consulte la siguiente tabla para obtener los pasos de resolución de los errores. En la columna de operación, se describe el proceso de actualización del firmware en el que se produce el error. Después de resolver el error, haga clic en **Retry** para continuar con la actualización del dispositivo.

Tabla 17. Errores y resolución de actualización de firmware

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
9,000	Cualquier operación.	Error interno del servidor: el servicio de administración de infraestructura encontró una condición inesperada que impedía que se cumpliera la solicitud. Póngase en contacto con el servicio de soporte.	Es posible que aparezca este error si faltan los scripts de tareas del cliente que fallan en el host de Hypervisor. Esto puede ocurrir si el host de Hypervisor no realiza un ciclo de apagado y encendido en el proceso de reimaginación. Para resolver este problema, realice las siguientes tareas: 1. Inicie sesión en el host de Hypervisor mediante SSH y anote la lista de archivos en la carpeta `/scratch/dell/extern`. 2. Inicie sesión en ACM mediante SSH y anote la lista de archivos en la carpeta `/usr/local/dpatools/bin/clienttask`. 3. Si los archivos de la carpeta Hypervisor no están presentes en la carpeta ACM, utilice el comando de copia segura (scp) para copiar los archivos en el host de Hypervisor. 4. Vuelva a intentar la operación de actualización desde la interfaz del usuario de ACM. Si no se resuelve el problema, comuníquese con el soporte de Dell.
9001	Consulta de versiones de firmware	No se pudo conectar al servicio de eventos de nodo. Compruebe el estado del servicio de eventos del nodo o la conexión IP.	1. Inicie sesión en el host de Hypervisor mediante SSH y ejecute el siguiente comando para cambiar la configuración del servicio de eventos de nodo **rest_ip**: `/opt/dell/DellPTAgent/tools/pta_cfg set rest_ip=https:// <host internal IP> 8086` 2. Ejecute el siguiente comando para comprobar el estado del servicio de eventos de nodo: `/etc/init.d/DellPTAgent status` • Si el servicio de eventos de nodo está inactivo, ejecute el siguiente comando para iniciar el servicio: `/etc/init.d/DellPTAgent start` • Si el servicio de eventos de nodo está en funcionamiento, ejecute el siguiente comando para reiniciar el servicio: `/etc/init.d/DellPTAgent restart` 3. Para evitar más fallas de comprobación previa, inicie sesión en todos los hosts de Hypervisor y repita los pasos 1 y 2.
9002	Consulta de versiones de firmware	No se pudo consultar el inventario de software desde el servicio de eventos de nodo (HttpStatus. SERVICE_UNAVAILABLE).	Para comprobar el estado de iSM, realice los siguientes pasos:

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
		Verifique el estado del iDRAC Service Module o del iDRAC.	1. Inicie sesión en el host en el que se observan los problemas de iSM. 2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` ● Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` ● Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop` 2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft` Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`
9003	Consulta de versiones de firmware	No se pudo consultar el inventario de software desde el servicio de eventos de nodo (HttpStatus. BAD_GATEWAY). Verifique el estado del iDRAC o del iDRAC Service Module.	Para comprobar el estado de iSM, realice los siguientes pasos: 1. Inicie sesión en el host en el que se observan los problemas de iSM. 2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` ● Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` ● Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop` 2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft`

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
			Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`
9004	Comprobación previa del firmware	No se pudo conectar al servicio de eventos de nodo. Compruebe el estado del servicio de eventos del nodo o la conexión IP.	1. Inicie sesión en el host de Hypervisor mediante SSH y ejecute el siguiente comando para cambiar la configuración del servicio de eventos de nodo **rest_ip**: `/opt/dell/DellPTAgent/tools/pta_cfg set rest_ip=https:// <host internal IP> 8086` 2. Ejecute el siguiente comando para comprobar el estado del servicio de eventos de nodo: `/etc/init.d/DellPTAgent status` ● Si el servicio de eventos de nodo está inactivo, ejecute el siguiente comando para iniciar el servicio: `/etc/init.d/DellPTAgent start` ● Si el servicio de eventos de nodo está en funcionamiento, ejecute el siguiente comando para reiniciar el servicio: `/etc/init.d/DellPTAgent restart` 3. Para evitar más fallas de comprobación previa, inicie sesión en todos los hosts de Hypervisor y repita los pasos 1 y 2.
9005	Comprobación previa del firmware	No se pudo consultar el inventario de software desde el servicio de eventos de nodo (HttpStatus. SERVICE_UNAVAILABLE). Verifique el estado del iDRAC Service Module o del iDRAC.	Para comprobar el estado de iSM, realice los siguientes pasos: 1. Inicie sesión en el host en el que se observan los problemas de iSM. 2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` ● Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` ● Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop` 2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft`

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
			Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`
9006	Comprobación previa del firmware	No se pudo consultar el inventario de software desde el servicio de eventos de nodo (HttpStatus. BAD_GATEWAY). Verifique el estado del iDRAC o del iDRAC Service Module.	Para comprobar el estado de iSM, realice los siguientes pasos: 1. Inicie sesión en el host en el que se observan los problemas de iSM. 2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` • Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` • Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop` 2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft` Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`
9012	Actualización del firmware	No se pudo desempaquetar la carga útil del firmware. Compruebe si la línea de espera de trabajos de LC de iDRAC está desactivada.	Comuníquese con el soporte de Dell para resolver el problema.
9013	Actualización del firmware	No se pudo conectar al servicio de eventos de nodo. Compruebe el estado del servicio de eventos del nodo o la conexión IP.	1. Inicie sesión en el host de Hypervisor mediante SSH y ejecute el siguiente comando para cambiar la configuración del servicio de eventos de nodo **rest_ip**: `/opt/dell/DellPTAgent/tools/pta_cfg set`

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
			`rest_ip=https:// <host internal IP> 8086` 2. Ejecute el siguiente comando para comprobar el estado del servicio de eventos de nodo: `/etc/init.d/DellPTAgent status` ● Si el servicio de eventos de nodo está inactivo, ejecute el siguiente comando para iniciar el servicio: `/etc/init.d/DellPTAgent start` ● Si el servicio de eventos de nodo está en funcionamiento, ejecute el siguiente comando para reiniciar el servicio: `/etc/init.d/DellPTAgent restart` 3. Para evitar más fallas de comprobación previa, inicie sesión en todos los hosts de Hypervisor y repita los pasos 1 y 2.
9014	Actualización del firmware	No se pudo procesar la carga útil del firmware con el servicio de eventos de nodo (HttpStatus. SERVICE_UNAVAILABLE). Verifique el estado del iDRAC Service Module o del iDRAC.	Para comprobar el estado de iSM, realice los siguientes pasos: 1. Inicie sesión en el host en el que se observan los problemas de iSM. 2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` ● Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` ● Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop` 2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft` Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`
9015	Actualización del firmware	No se pudo procesar la carga útil del firmware con el servicio de eventos de nodo (HttpStatus. BAD_GATEWAY). Verifique el	Para comprobar el estado de iSM, realice los siguientes pasos: 1. Inicie sesión en el host en el que se observan los problemas de iSM.

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
		estado del iDRAC o del iDRAC Service Module.	2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` ● Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` ● Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop` 2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft` Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`
9017	Comprobación previa del firmware	Sin perfil de firmware. Asegúrese de que esté instalado el módulo de ID correcto.	Comuníquese con el soporte de Dell para resolver el problema.
9018	Tareas posteriores a la actualización	No se pudo recuperar el estado de vSAN. Asegúrese de que vSAN esté en buen estado.	Comuníquese con el soporte de Dell para resolver el problema.
9019	Tareas posteriores a la actualización del firmware	El servicio de eventos de nodo no pudo procesar la solicitud de reinicio. Compruebe el estado del servicio de eventos del nodo.	1. Inicie sesión en el host de Hypervisor mediante SSH y ejecute el siguiente comando para cambiar la configuración del servicio de eventos de nodo **rest_ip**: `/opt/dell/DellPTAgent/tools/pta_cfg set rest_ip=https:// <host internal IP> 8086` 2. Ejecute el siguiente comando para comprobar el estado del servicio de eventos de nodo: `/etc/init.d/DellPTAgent status` ● Si el servicio de eventos de nodo está inactivo, ejecute el siguiente comando para iniciar el servicio: `/etc/init.d/DellPTAgent start` ● Si el servicio de eventos de nodo está en funcionamiento, ejecute el siguiente comando para reiniciar el servicio: `/etc/init.d/DellPTAgent restart`

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
			3. Para evitar más fallas de comprobación previa, inicie sesión en todos los hosts de Hypervisor y repita los pasos 1 y 2.
9020	Tareas previas a la actualización del firmware	No se pudo reiniciar el servicio de eventos de nodo. Compruebe si el servicio de eventos del nodo es un estado de error y asegúrese de que esté instalado correctamente.	Comuníquese con el soporte de Dell para resolver el problema.
9021	Tareas previas a la actualización del firmware	No se pudieron realizar tareas de requisitos previos debido a un error interno. Revise los registros de actualización para obtener más detalles.	Comuníquese con el soporte de Dell para resolver el problema.
9022	Actualización del firmware	No se encuentra el archivo de carga útil del firmware. Agregue la ruta de carga útil del firmware al cuerpo de la solicitud y vuelva a intentar la API de actualización de firmware.	Comuníquese con el soporte de Dell para resolver el problema.
9023	Actualización del firmware	No se pudo actualizar el firmware debido a un error interno. Compruebe el estado del servicio de eventos del nodo, del iDRAC Service Module o del iDRAC y los registros de revisión para obtener más detalles	Comuníquese con el soporte de Dell para resolver el problema.
9024	Tareas previas a la actualización del firmware	No se pudo conectar al servicio de eventos de nodo. Compruebe el estado del servicio de eventos del nodo o la conexión IP.	1. Inicie sesión en el host de Hypervisor mediante SSH y ejecute el siguiente comando para cambiar la configuración del servicio de eventos de nodo **rest_ip**: `/opt/dell/DellPTAgent/tools/pta_cfg set rest_ip=https:// <host internal IP> 8086` 2. Ejecute el siguiente comando para comprobar el estado del servicio de eventos de nodo: `/etc/init.d/DellPTAgent status` • Si el servicio de eventos de nodo está inactivo, ejecute el siguiente comando para iniciar el servicio: `/etc/init.d/DellPTAgent start` • Si el servicio de eventos de nodo está en funcionamiento, ejecute el siguiente comando para reiniciar el servicio: `/etc/init.d/DellPTAgent restart` 3. Para evitar más fallas de comprobación previa, inicie sesión en todos los hosts de Hypervisor y repita los pasos 1 y 2.
9025	Tareas posteriores a la actualización del firmware	No se pudo conectar al servicio de eventos de nodo. Compruebe el estado del servicio de eventos del nodo o la conexión IP.	1. Inicie sesión en el host de Hypervisor mediante SSH y ejecute el siguiente comando para cambiar la configuración del servicio de eventos de nodo **rest_ip**: `/opt/dell/DellPTAgent/tools/pta_cfg set`

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
			`rest_ip=https:// <host internal IP> 8086` 2. Ejecute el siguiente comando para comprobar el estado del servicio de eventos de nodo: `/etc/init.d/DellPTAgent status` • Si el servicio de eventos de nodo está inactivo, ejecute el siguiente comando para iniciar el servicio: `/etc/init.d/DellPTAgent start` • Si el servicio de eventos de nodo está en funcionamiento, ejecute el siguiente comando para reiniciar el servicio: `/etc/init.d/DellPTAgent restart` 3. Para evitar más fallas de comprobación previa, inicie sesión en todos los hosts de Hypervisor y repita los pasos 1 y 2.
9028	Tareas posteriores a la actualización del firmware	No se pudieron realizar tareas posteriores a la actualización debido a un error interno. Compruebe el estado de vSAN y revise los registros de actualización para obtener más detalles.	Comuníquese con el soporte de Dell para resolver el problema.
9029	Cualquier operación.	Tiempo de espera agotado mientras se espera que se complete una tarea interna. Compruebe el estado del servicio de eventos del nodo, del iDRAC Service Module o del iDRAC y compruebe los registros para obtener más detalles.	Comuníquese con el soporte de Dell para resolver el problema.
9030	Tareas posteriores a la actualización del firmware	El hipervisor no pudo salir del modo de mantenimiento. Compruebe el estado del hipervisor y asegúrese de que vSAN esté en buen estado.	Comuníquese con el soporte de Dell para resolver el problema.
9031	Tareas posteriores a la actualización del firmware	Tiempo de espera agotado mientras espera para volver a conectarse y actualizar el siguiente host. Compruebe el estado del hipervisor y asegúrese de que vSAN esté en buen estado.	Comuníquese con el soporte de Dell para resolver el problema.
9032	Actualización del firmware	Se superó el tiempo de espera máximo para el restablecimiento del sistema. Compruebe el estado del servicio de eventos de nodo e iDRAC.	Comuníquese con el soporte de Dell para resolver el problema.
9033	Comprobación de la preparación para la actualización del firmware	No se pudo verificar si el firmware actual es válido. Compruebe el inventario de software de iDRAC y el registro de actualización para obtener más información.	Comuníquese con el soporte de Dell para resolver el problema.
9034	Comprobación previa del firmware	No se pudo obtener el perfil de firmware. Compruebe la carga útil del firmware instalado y los	Comuníquese con el soporte de Dell para resolver el problema.

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
		registros de actualización para obtener más detalles.	
9035	Comprobación previa del firmware	No se pudo obtener versiones de firmware debido a la falta de perfiles de firmware. Compruebe la versión del servicio de administración de infraestructura instalada y los registros de actualización para obtener detalles.	Comuníquese con el soporte de Dell para resolver el problema.
9036	Actualización del firmware	No se pudieron borrar los trabajos pendientes en la línea de espera de trabajos de iDRAC. Compruebe el estado del servicio de eventos del nodo, del iDRAC Service Module o del iDRAC y compruebe los registros de actualización para obtener más detalles.	Comuníquese con el soporte de Dell para resolver el problema.
N/D	Comprobación de la preparación para la actualización del firmware	No se pudo conectar al servicio de eventos de nodo. Compruebe el estado del servicio de eventos del nodo o la conexión IP.	1. Inicie sesión en el host de Hypervisor mediante SSH y ejecute el siguiente comando para cambiar la configuración del servicio de eventos de nodo **rest_ip**: `/opt/dell/DellPTAgent/tools/pta_cfg set rest_ip=https:// <host internal IP> 8086` 2. Ejecute el siguiente comando para comprobar el estado del servicio de eventos de nodo: `/etc/init.d/DellPTAgent status` ● Si el servicio de eventos de nodo está inactivo, ejecute el siguiente comando para iniciar el servicio: `/etc/init.d/DellPTAgent start` ● Si el servicio de eventos de nodo está en funcionamiento, ejecute el siguiente comando para reiniciar el servicio: `/etc/init.d/DellPTAgent restart` 3. Para evitar más fallas de comprobación previa, inicie sesión en todos los hosts de Hypervisor y repita los pasos 1 y 2.
N/D	Comprobación de la preparación para la actualización del firmware	No se pudo consultar el resumen del host desde el servicio de eventos de nodo (HttpStatus. SERVICE_UNAVAILABLE). Compruebe el estado de iSM o iDRAC.	Para comprobar el estado de iSM, realice los siguientes pasos: 1. Inicie sesión en el host en el que se observan los problemas de iSM. 2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` ● Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` ● Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop`

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
			2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft` Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`
N/D	Comprobación de la preparación para la actualización del firmware	No se pudo consultar el resumen del host desde el servicio de eventos de nodo (HttpStatus. BAD_GATEWAY). Compruebe el estado de iDRAC o iSM.	Para comprobar el estado de iSM, realice los siguientes pasos: 1. Inicie sesión en el host en el que se observan los problemas de iSM. 2. Ejecute el siguiente comando para comprobar el estado de iSM: `/etc/init.d/dcism-netmon-watchdog status` • Ejecute el siguiente comando si se detiene el servicio: `/etc/init.d/dcism-netmon-watchdog start` • Si el estado es **iSM is active (not running)**, realice los siguientes pasos: 1. Ejecute el siguiente comando para detener el servicio: `/etc/init.d/dcism-netmon-watchdog stop` 2. Ejecute el siguiente comando para reiniciar iSM: `/etc/init.d/dcism-netmon-watchdog start` 3. Inicie sesión en iDRAC mediante SSH. 4. Ejecute el siguiente comando para restablecer iDRAC: `racadm racreset soft` Si la GUI de iDRAC muestra el error **Not running (TLS error)**, realice los siguientes pasos: 1. Se observa el problema de inicio de sesión en el host en iSM. 2. Ejecute el siguiente comando para detener iSM: `/etc/init.d/dcism-netmon-watchdog stop` 3. Ejecute el siguiente comando para reinstalar iSM a fin de establecer una nueva conexión TLS con iDRAC: `/etc/init.d/dcism-netmon-watchdog start install`

Tabla 17. Errores y resolución de actualización de firmware (continuación)

Código de error	Operación	Mensaje de error y corrección que se muestran en la interfaz del usuario de ACM	Solución
N/D	Comprobación de la preparación para la actualización del firmware	iDRAC está en el modo de recuperación. Borre el modo de recuperación antes de la actualización del firmware.	Comuníquese con el soporte de Dell para resolver el problema.
N/D	Comprobación de la preparación para la actualización del firmware	Hay algunos trabajos pendientes en la línea de espera de trabajos de iDRAC. Borre la línea de espera de trabajos de iDRAC antes de actualizar el firmware.	1. Inicie sesión en iDRAC mediante SSH. 2. Ejecute el siguiente comando para borrar todos los trabajos de la línea de espera de trabajos: `racadm jobqueue delete -i JID_CLEARALL_FORCE` **NOTA:** Se recomienda utilizar `JID_CLEARALL` en lugar de `JID_CLEARALL_FORCE`. Utilice `JID_CLEARALL_FORCE` solo para recuperar el iDRAC Lifecycle Controller desde un estado fallido o cuando un trabajo de trabajo en ejecución no está progresando. **NOTA:** Es necesario restablecer iDRAC después de utilizar `JID_CLEARALL_FORCE` para asegurarse de que iDRAC tenga un buen estado de funcionamiento 3. Espere 5 minutos para que iDRAC se establezca.
N/D	Comprobación de la preparación para la actualización del firmware	El firmware actual de iDRAC es anterior a 3.30.30.30. No se admite la actualización directa a la versión de destino. Primero, el firmware de iDRAC se debe actualizar a 3.36.103.36.	1. Inicie sesión en ACM mediante SSH 2. Ejecute el siguiente comando para verificar si el servicio de administración de infraestructura es de la versión 2.3.0 o superior: `rpm -qa | grep dpatools` 3. Compruebe si el paquete de firmware `IDPA-10.308-10.308.tar.gz` está disponible en `/usr/local/dpatools/bin/payload` 4. Ejecute el siguiente comando para instalar iDRAC versión 3.36.103.36 en los nodos: `dpacli -fwupdate /usr/local/dpatools/bin/payload/IDPA-10.308-10.308.tar.gz -skipReboot` 5. Haga clic en **Revalidate** en la interfaz de usuario de actualización de ACM para volver a ejecutar las comprobaciones previas de la actualización.

Actualización manual del firmware del servidor de PowerProtect DP Series Appliance

Para los modelos Gen 14, si la versión de firmware de iDRAC es inferior a 3.30.30.30, no podrá continuar con la actualización del dispositivo. Debe actualizar la versión de firmware de iDRAC a 3.36.103.36 mediante *dptools* para iniciar la actualización antes de continuar con la actualización del dispositivo

Si el firmware del se actualizó a un bloque de firmware de PowerProtect DP Series Applianceincluido con PowerProtect DP Series Appliance 2.7.1, no es necesario actualizar el firmware en el PowerProtect DP Series Appliance.

Asegúrese de lo siguiente antes de actualizar el firmware del servidor:

- Asegúrese de estar conectado y haber configurado el iDRAC.
- Asegúrese de que ACM esté en funcionamiento.

  NOTA: La sesión de Appliance Configuration Manager SSH está configurada para agotar el tiempo de espera después de 10 minutos de inactividad. Actualice la sesión para mantenerla activa o cambie el valor de tiempo de espera. Para obtener más información, consulte la *sección Tiempo de espera de sesión agotado* en la PowerProtect DP Series Appliance*Guía de configuración de seguridad de* .
- Asegúrese de tener puntos de conexión válidos para el servidor de Hypervisor requerido.
- Ponga en pausa todas las actividades en PowerProtect DP Series Appliance, incluida la servicios.
- Asegúrese de que todos los servicios en ACM tengan marcas de verificación verdes que indiquen que todos están en buen estado, en funcionamiento y configurados correctamente. Si alguno de los servicios no está en verde, inicie sesión en ese servicio en particular y reinícielo.
- Descargue los paquetes de actualización de firmware necesarios desde el sitio web de soporte de Dell EMC a su carpeta local.
- Utilice el proceso de validación de suma de comprobación `sha256` para verificar su integridad.
- Asegúrese de que ACM esté en funcionamiento.
- Descargue el paquete del servicio de administración de infraestructura más reciente desde el sitio web de soporte de Dell EMC a su carpeta local y utilice la suma de comprobación `sha256` para verificar su integridad.
- En la GUI de ACM, haga clic en **Download Current Configuration** para generar el archivo `DataProtectionConfiguration.xml` necesario para habilitar el modo de servicio.

  NOTA: El archivo `DataProtectionConfiguration.xml` se genera automáticamente para PowerProtect DP Series Appliance versión 2.5 y superior.

  NOTA: La sesión de Appliance Configuration Manager SSH está configurada para agotar el tiempo de espera después de 10 minutos de inactividad. Actualice la sesión para mantenerla activa o cambie el valor de tiempo de espera. Para obtener más información, consulte la *sección Tiempo de espera de sesión agotado* en la PowerProtect DP Series Appliance*Guía de configuración de seguridad de* .

Para actualizar el firmware del servidor manualmente, realice lo siguiente:

1. Instale el paquete del servicio de administración de infraestructura
2. Instalar el paquete de actualización de firmware
3. Actualice el firmware (solo sistemas configurados para ACM)

Instalar el paquete de Infrastructure Management Service

Pasos

1. Mediante un cliente SSH, conéctese a ACM como usuario raíz.
2. Para crear un nuevo directorio, ejecute el siguiente comando:

   `mkdir /root/firmware/`
3. Desde el paquete Infrastructure Management Service más reciente que descargó desde el sitio web de soporte de Dell EMC (https://www.dell.com/support/home/en-in), copie el `dpatools-<version>.rpm` al nuevo directorio `/root/firmware/`.
4. En la sesión de SSH, verifique la versión de Infrastructure Management Service instalada en ACM.

   `rpm -qa dpatools`. El siguiente es un ejemplo de salida de este comando:

   `dpatools-<version>.noarch`
5. Si la versión que descargó es una versión posterior a la ya instalada, actualice el paquete de Infrastructure Management Service mediante la ejecución de lo siguiente.

   `rpm -Uvh --force dpatools-<version>.rpm`

Instalar el paquete de actualización de firmware

Pasos

1. Mediante un cliente SSH, conéctese a ACM como usuario raíz.
2. Verifique la versión del firmware en el dispositivo.

   `dpacli -fwversions`

El comando `dpacli -fwversions` muestra la versión de firmware de todos los componentes en el servidor del dispositivo.

3. Desde el paquete de actualización de firmware más reciente que descargó desde el sitio web de soporte de Dell EMC (https://www.dell.com/support/home/en-in), mediante WinSCP o cualquier otra aplicación de emulación de terminal, copie el `dpafw-<version>.rpm` al directorio raíz.
4. Ejecute el siguiente comando:

   `rpm -Uvh --force dpafw-<version>.rpm`

Actualizar el firmware (solo para sistemas configurados para ACM)

Pasos

1. Conéctese al ACM mediante a un cliente SSH.
2. En ACM, inicie el flujo de trabajo de actualización de firmware mediante la ejecución del siguiente comando:

   `dpacli -fwworkflow /usr/local/dpatools/bin/payload/IDPA-<version>-<version>.tar.gz`

   Por ejemplo: **`dpacli -fwworkflow /usr/local/dpatools/bin/payload/IDPA-2.310-2.310.tar.gz`**

   a. Si el PowerProtect DP Series Appliance está en un estado no configurado (solo la VM de ACM está presente en el dispositivo), ejecute el siguiente comando:

      `dpacli -fwupdate /usr/local/dpatools/bin/payload/IDPA-<version>-<version>.tar.gz`

      Por ejemplo: **`dpacli -fwupdate /usr/local/dpatools/bin/payload/IDPA-2.310-2.310.tar.gz`**
3. Monitoree el archivo de registro de `dpacli` mediante la ejecución del siguiente comando:

   `tail -f /usr/local/dpatools/logs/dpacli.log`
4. De manera opcional, puede supervisar el progreso de la actualización del firmware en la GUI de iDRAC navegando a **Maintenance** > **Job Queue**.

   NOTA: El proceso de actualización del firmware, incluido el reinicio del servidor, puede tardar hasta 45 minutos en completarse.

   Después de que las actualizaciones de firmware se completen correctamente, el pool de almacenamiento debe estar en buen estado. Puede ejecutar el comando `dpacli -fwprecheck` en ACM para validar si el firmware se actualizó correctamente.

   Si el pool de almacenamiento no está en buen estado, puede recuperarlo mediante los siguientes pasos:

   a. Habilite el modo de mantenimiento en todos los hosts de hipervisor.
   b. Apague todos los hosts de hipervisor (apague).
   c. Encienda los hosts de hipervisor uno a la vez.

   NOTA: Asegúrese de que el host del hipervisor esté en funcionamiento antes de encender el siguiente host de hipervisor. Las evaluaciones del estado fallarán hasta que el segundo host del hipervisor se haya unido al clúster.

Versiones de bloques de firmware

Una vez que se actualice el firmware, revise la tabla a continuación para validar si la versión de bloque de firmware para los componentes de hardware es correcta.

En la siguiente tabla, se enumeran las versiones de firmware de los componentes de hardware PowerProtect DP Series Appliance 2.7.1.

NOTA: Puede verificar la versión de bloque de firmware en PowerProtect DP Series Appliance mediante la ejecución del comando `dpacli -fwversions` desde ACM servicio. Muestra la versión de bloque de firmware de todos los componentes de hardware en el servidor PowerProtect DP Series Appliance.

Tabla 18. Versiones de bloques de firmware de los componentes de hardware de DP4400 PowerProtect DP Series Appliance 2.7.1

Componente	DP4400	
	Versión de bloque de firmware	SWB
BIOS	2.10.2	N63PX
iDRAC	4.40.10.00	MGD5F

Tabla 18. Versiones de bloques de firmware de los componentes de hardware de DP4400 PowerProtect DP Series Appliance 2.7.1 (continuación)

Adaptador de BOSS-S1	2.5.13.3024	3P39V
Adaptador de red convergente Ethernet Intel(R) X710	19.5.12	YP4R0
Intel(R) Ethernet 10G X710 rNDC Intel(R) Ethernet 10G 4P X710 SFP+ rNDC Intel(R) Ethernet 10G 4P X710 SFP+ rNDC	19.5.12	YP4R0
Adaptador Intel(R) Ethernet 10G 4P X550 rNDC Intel(R) Gigabit 2P I350-t	19.5.12	40NTK
Firmware de la PSU Lite_on de 1100 W	00.23.32	PT6KV
Firmware de la PSU de Delta de 1100 W	00.1D.7D	C4M76
Firmware del backplane de almacenamiento no expansor	4.35_06	VV85D
Placa posterior expansora	2.52	60K1J
SSD PCIe NVMe Dell Express Flash 1725	KPYABD3Q	WM6VX
SSD PCIe NVMe Dell Express Flash 1725a	1.1.2	NMDM2
SSD PCIe NVMe Dell Express Flash 1725b	1.1.0	DYC3X
SSD PCIe NVMe Dell Express Flash 1735	2.0.2	68GR1v
Disco SAS Hitachi Leo-A de 12 TB	NS06	C6PNG
Disco SAS Seagate Mobula de 12 TB	RSL2	JWKDW
Disco SAS Toshiba MG07 de 12 TB	EI07	F66RN
H730P PERC	25.5.8.0001	WRF3Y
Intel M.2 (para BOSS)	DL43	CHJGV
Tarjeta Intel Youngsville 240G M2	DL6N	5WH9V
Micron M.2 (para BOSS)	E012	6FGD4

Tabla 19. Versiones de bloques de firmware de los componentes de hardware de DP5900 PowerProtect DP Series Appliance 2.7.1

Componente	**DP 5900**	
	Versión de bloque de firmware	**SWB**
BIOS	2.10.2	N63PX
iDRAC	4.40.10.00	MGD5F
Adaptador de BOSS-S1	2.5.13.3024	3P39V
Adaptador de red convergente Ethernet Intel(R) X710	19.5.12	YP4R0
Intel(R) Ethernet 10G X710 rNDC Intel(R) Ethernet 10G 4P X710 SFP+ rNDC Intel(R) Ethernet 10G 4P X710 SFP+ rNDC	19.5.12	YP4R0
Firmware de la PSU Lite_on de 1100 W	00.23.32	PT6KV
Firmware de la PSU de Delta de 1100 W	00.1D.7D	C4M76
Firmware de PSU Artesyn de 750 W	00.1B.53	8R0NM
Firmware del backplane de almacenamiento no expansor	4.35_06	VV85D

Tabla 19. Versiones de bloques de firmware de los componentes de hardware de DP5900 PowerProtect DP Series Appliance 2.7.1 (continuación)

SSD SATA Toshiba HK4 RI de 1920 GB y 6 Gbps 2,5	DACB	H3XHN
DISCO SAS SEAGATE DE 1,8 TB	ST53	JV3YW
Intel M.2 (para BOSS)	DL43	CHJGV
Tarjeta Intel Youngsville 240G M2	DL6N	5WH9V
Micron M.2 (para BOSS)	E012	6FGD4
SSD de 1,92 TB, SATA de 6 Gbps, 2,5, 512e, 5200 RI ISE	F003	VVF8D
Unidad de conexión en caliente SAMSUNG 1,92 TB SSD SATA RI 512n de 6 Gbps y 2,5", P863, ISE	GA3A	YJ52X
Unidad de conexión en caliente SAMSUNG 1,92 TB SSD SATA RI 512n de 6 Gbps y 2,5", P863a, ISE	GC5B	P2YRJ
Unidad de conexión en caliente SAMSUNG 1,92 TB SSD SATA RI 512n de 6 Gbps y 2,5", P883a, ISE	HE57	4DN2V
Unidad de conexión en caliente Intel 1,92 TB SSD SATA RI 512n de 6 Gbps y 2,5", Youngsville s4500, ISE	DL5C	V141M
Unidad de conexión en caliente Intel 1,92 TB SSD SATA RI 512n de 6 Gbps y 2,5", Youngsville s4510, ISE	DL63	8VGP8
Disco duro de conexión en caliente Toshiba SAS de 1,8 TB, 10K r/min y 12 Gbps 512e de 2,5", AL14SE, ISE	EB04	NYK8R
Disco duro de conexión en caliente Toshiba SAS de 1,8 TB, 10K r/min y 12 Gbps 512e de 2,5", AL15SE, ISE	EF05	YMJY5
HBA330 Mini	16.17.00.05	YXWY1

4

Administrar Data Protection Central después de la instalación de PowerProtect DP Series Appliance

Después de instalar PowerProtect DP Series Appliance correctamente, el sistema abre Data Protection Central en una nueva ventana o pestaña del navegador. Puede realizar un respaldo de servicio, restaurar un respaldo de servicio y generar informes para Protection Software y Protection Storage mediante Data Protection Central.

Esta sección contiene los siguientes temas:

Temas:

Realizar un respaldo de VM

En esta sección, se proporciona información sobre cómo respaldar un cliente de VMware mediante la interfaz de usuario de Data Protection Central.

Descripción general del respaldo de VM

Tan pronto como su ambiente esté en funcionamiento, puede seguir los pasos de esta sección para respaldar un cliente de VMware.

Si es la primera vez que utiliza Protection Software, en la sección se incluyen tareas de preparación, como la definición de clientes de vCenter y VMware, y la implementación de un proxy de VM Proxy.

Todo el proceso está organizado en los siguientes procedimientos:

- Definición de los clientes de vCenter y VMware
- Implementar el proxy de VM (servicio)
- Creación y ejecución de la política de respaldo

Para obtener más información acerca de los respaldos de Protection Software, se encuentra disponible la documentación de Protection Software, incluida la *Guía de administración de Avamar* y la *Guía de usuario de los clientes de respaldo de Avamar*.

Definición de los clientes de vCenter y VMware

Este procedimiento muestra cómo crear los clientes de vCenter y servicio y agregar un conjunto de datos al cliente de VM.

Sobre esta tarea

Para crear vCenter y los clientes de servicio y agregar un conjunto de datos al cliente de VM, realice las siguientes acciones.

Pasos

1. Abra un navegador e ingrese `https://<ACM IP address>:8543` para acceder a la interfaz de usuario de ACM.
2. Haga clic en **DPC Web UI** e inicie sesión en **DPC**.
   Se mostrará la página del tablero **DPC**.
3. Haga clic en **System Management** en el panel izquierdo para mostrar la página Data Protection Central.

4. Haga clic en los puntos suspensivos verticales de Protection Software-Protection Software y seleccione **Protection Software Restore**.
   Se muestra la página **Asset Management** en la interfaz de usuario de Protection Software.
5. Para agregar VMware vCenter Server como un cliente de respaldo, realice las siguientes acciones.
   a. Haga clic en los puntos suspensivos verticales junto a **ADD CLIENT** y seleccione **Add VMware vCenter**.

      NOTA: Asegúrese de que se encuentra en el dominio **root**.

      Se muestra la pantalla **New vCenter Client**.
   b. Seleccione o ingrese los detalles que se requieren en los campos para crear un cliente de vCenter mediante la siguiente tabla. Haga clic en **Next** para continuar con la página siguiente.

Tabla 20. Incorporación de clientes de vCenter

Página	Campo	Descripción
Información del cliente	Client Type	Seleccione VMware vCenter.
	New Client Name or IP	Nombre del cliente o dirección IP.
	Client Domain	Nombre del dominio.
vCenter Information	User Name	El nombre de usuario del administrador de vCenter Server.
	Password	La contraseña del administrador.
	Verify Password	Ingrese la misma contraseña para verificar si son idénticas.
	Puerto	El número de puerto HTTPS de vCenter.
Avanzado	Auto Discovery • Habilitar importación dinámica de VM por regla • Habilitar Change Block Tracking	Seleccione la casilla de verificación para activar las opciones. Este es un campo opcional. **NOTA:** La casilla de verificación **Enable Changed Block Tracking** modificados solo se habilita cuando selecciona **Enable Dynamic VM import by rule**.
Optional Information	Optional Information • Contact • Teléfono • Correo electrónico • Ubicación	Ingrese la información pertinente en los campos. Todos los campos son opcionales para esta tarea.

   c. Haga clic en **ADD** en la página **Summary**. Luego, actualice la pantalla para verificar el nuevo cliente de vCenter.
   d. Haga clic en **OK** en la página **Finish**.
   Se agrega el cliente de vCenter y se muestra la página **Asset Management**

NOTA: Actualice la página para verificar si se agregó el cliente de vCenter.

6. Para agregar el cliente de VMware, realice las siguientes acciones.
   a. En el panel **Domain**, expanda el nuevo cliente de vCenter y haga clic en **VirtualMachines**.
   b. En el panel **Asset Management**, haga clic en **ADD CLIENT**.
   Se muestra la página **Select VMware Entity**.
   c. En la ventana **Select VMware Entity**, expanda el árbol de hosts o clústeres y seleccione el clúster que aloja la VM que desea respaldar.

      NOTA: Para ver los detalles del host o del clúster, alterne el botón **Host/Cluster**.

      Las máquinas virtuales asignadas al clúster se muestran en el panel derecho.
   d. En el panel derecho, haga clic en el ícono **+** para seleccionar la VM que desea respaldar y haga clic en **YES**.
7. Para agregar el conjunto de datos, realice las siguientes acciones.
   a. Haga clic en **Setting** en la sección **Adminstration** en el panel izquierdo.

NOTA: Asegúrese de que se encuentra en el dominio **root**.

b. Haga clic en la pestaña **Dataset** en el panel **Setting**. y, a continuación, haga clic en el signo más (**+**) para mostrar la ventana **Create DataSet**.
c. Haga clic en **+ ADD**.
   Se muestra la ventana **Create Dataset**.
d. En el campo **Dataset Name**, ingrese un nombre para el conjunto de datos.
e. Seleccione **Windows VMware Image** desde la lista de **Plugins** disponibles.

   NOTA: Puede seleccionar un plug-in diferente de la lista de complementos disponibles. Las opciones de configuración y los datos de origen son diferentes para los diferentes plug-ins.

   Las opciones **Windows VMware Image** se muestran en la pestaña **Options**.
f. Seleccione la casilla de verificación **Index VMware Image Backups**.
g. Haga clic en la pestaña **Source Data** para ver las opciones de configuración.
   Las opciones disponibles en la pestaña de datos de origen le permiten respaldar los datos de origen en función de su selección.
h. Haga clic en **Submit**.
   La aplicación muestra el mensaje **Dataset created successfully** en la página del tablero de Protection Software.

NOTA: La indexación se utiliza para la restauración de archivos específicos y es opcional para el respaldo de servicios completas. Si la selecciona aquí, le permitirá restaurar archivos específicos, como se describe en Restauración de archivos específicos.

Implementar el proxy de VM (servicio)

En esta sección, se proporciona información sobre cómo implementar el proxy de Protection Software.

Sobre esta tarea

Implemente el proxy de VM (servicio) en cada vCenter que desee proteger.

Pasos

1. Abra un navegador e ingrese `https://<ACM IP address>:8543` para acceder a la interfaz de usuario de ACM.
2. Haga clic en **DPC Web UI** e inicie sesión en **DPC**.
   Se mostrará la página del tablero **DPC**.
3. Haga clic en **System Management** en el panel izquierdo para mostrar la página Data Protection Central.
4. Haga clic en los puntos suspensivos verticales de Protection Software-Protection Software y seleccione **Protection Software Proxy Deployment**.
   Se muestra la página **Proxy Management** en la interfaz de usuario de Protection Software.
5. En el panel derecho, haga clic en los puntos suspensivos verticales frente a PowerProtect DP Series Appliance Protection Software y seleccione **Protection Software Proxy Deployment**.
6. En la sección **Config**, realice las siguientes acciones. **Data Change Rate** y **Backup Window**. A continuación, seleccione la casilla de verificación.
   a. Seleccione el vCenter que agregó. Para obtener más información sobre cómo agregar un vCenter, consulte Definir vCenter y clientes de VMware
   b. Ingrese la tasa de cambio de datos en el campo **Data Change Rate (%)**
   c. Ingrese la cantidad de minutos en el campo **Backup Window (minutes)**.
   d. Seleccione la casilla de verificación **Protect Virtual Machines on Local Storage**.
7. Haga clic en **CREATE RECOMMENDATION**.
   La sección **Recommendations** muestra los nuevos proxies propuestos en cada host.
8. Expanda los listados en el panel **Recommendations** y seleccione **New proxy** en el host del servidor Hypervisor.
9. Haga clic en ✎.
   Se muestra la ventana **Proxy**.
   a. Escriba el nombre de host del proxy en el campo **Name**.
   b. Seleccione el **Domain** del servidor de Protection Software donde reside este proxy.
   c. Escriba la dirección IP en el campo **IP**.
   d. Seleccione un área de almacenamiento de datos en la lista **Datastore**.
   e. Seleccione una red de la lista **Network**.
   f. Ingrese el nombre del servidor o la dirección IP en el campo **DNS**.
   g. Escriba la dirección IP del gateway de red en el campo **Gateway**.
   h. Escriba la máscara de red en el campo **Netmask**.
   i. Escriba la dirección IP en el campo **NTP**.
   j. Haga clic en **SAVE**.
10. Haga clic en ✓ en la sección **Recommendations** para implementar el proxy.
    La implementación del proxy se muestra en el panel inferior.

Creación y ejecución de la política de respaldo

En esta sección, se proporciona información sobre cómo crear una política de respaldo. La política de respaldo se crea para proteger al cliente VMware.

Sobre esta tarea

Para crear la política, realice las siguientes acciones.

Pasos

1. Haga clic en **DPC Web UI** e inicie sesión en **DPC**.
   Se mostrará la página del tablero **DPC**.
2. Haga clic en **System Management** en el panel izquierdo para mostrar la página Data Protection Central.
3. Haga clic en los puntos suspensivos verticales de Protection Software-Protection Software y seleccione **Manage Policies**.
   Se muestra la página **System Management > Manage Policies**.
4. En la página **Manage Policies**, haga clic en más (**+**).
   Se muestra la ventana **Add policy**.
5. Seleccione o ingrese los detalles que se requieren en los campos para crear una nueva política de respaldo mediante la siguiente tabla. Haga clic en **Next** para continuar con la página siguiente.

Tabla 21. Incorporación de políticas

Página	Campo	Descripción
Información	Nombre	El nombre de la política.
	Domain	Acepte la entrada predeterminada.
	Habilitado	Haga clic para habilitar la política.
	Conjunto de datos	Seleccione **VMware Image Dataset**.
	Programa	Seleccione **Daily Schedule**.
	Retention	Seleccione **Default Retention**.
Clientes (Opcional)	Clientes disponibles	Seleccione el cliente de máquina virtual definido anteriormente en esta guía.
Proxies (Optional)	Proxies disponibles	Seleccione el proxy definido anteriormente en esta guía.

6. Haga clic en **Finish**.
   La nueva política se muestra en la lista de políticas.
7. Para ejecutar la política, seleccione la política de la lista y haga clic en **BACKUP NOW**.
8. Monitoree la política haciendo clic en **Systems** en **Job Activities** en el panel de navegación.

Restauración de un respaldo de VM

En esta sección, se describen los tres métodos diferentes para restaurar el respaldo de vm mediante la interfaz de usuario de Data Protection Central para PowerProtect DP Series Appliance.

- Restaurar una VM en la página 77
- Restauración mediante acceso instantáneo en la página 79
- Restauración de archivos específicos en la página 80

Restaurar una VM

En esta sección, se proporciona información sobre el procedimiento básico de restauración de VM.

Requisitos previos

Debe existir un respaldo de la máquina virtual a fin de realizar una restauración.

Sobre esta tarea

Para restaurar una máquina virtual, realice las siguientes acciones.

Pasos

1. Haga clic en **DPC Web UI** e inicie sesión en **DPC**.
   Se mostrará la página del tablero **DPC**.
2. Haga clic en **System Management** en el panel izquierdo para mostrar la página Data Protection Central.
3. Haga clic en los puntos suspensivos verticales de Protection Software-Protection Software y seleccione **Protection Software Restore**.
   Se muestra la página **Asset Management** en la interfaz de usuario de Protection Software.
4. Expanda el vCenter que agregó al panel **Domain** y seleccione **Virtual machines** para visualizar los clientes de VM que pertenecen a ese vCenter.
5. En la lista de clientes, seleccione al cliente de VM que desee restaurar.
6. Haga clic en **VIEW MORE** para ver la lista de todos los respaldos.
7. Seleccione el respaldo más reciente de la lista y haga clic en **RESTORE**.
   Se muestra la ventana **Select Restore Content**.
8. Seleccione el contenido que desea restaurar y haga clic en **NEXT**.
   Se mostrará la ventana **Restore**.
9. Seleccione o ingrese los detalles que se requieren en los campos para restaurar desde una máquina virtual mediante la siguiente tabla. Haga clic en **Next** para continuar con la página siguiente.

   Utilice la siguiente tabla para completar cada página del asistente. Haga clic en **NEXT** para avanzar a la próxima página.

Tabla 22. Restauración desde una máquina virtual

Página del asistente	Campo	Descripción
Basic Config	Destination	Seleccione **Restore to new Virtual Machine**.
	Post Restore Options	Seleccione **Do not power on VM after restore**.
	Proxy	Seleccione **Automatic**.
	Utilice CBT para aumentar el rendimiento	Seleccione la casilla de verificación para aumentar el rendimiento mediante CBT.
Advanced Config	vCenter	Seleccione la dirección IP de vCenter para administrar la máquina virtual restaurada.
	Nombre de VM	Introduzca un nombre para la VM restaurada.
Ubicación		Expanda el árbol y seleccione la VM donde desee ejecutar la restauración.
Host/Cluster		Expanda el árbol y seleccione el host/clúster de Hypervisor.
Pool de recursos		Expanda el árbol y seleccione el pool de recursos.
Datastore		Seleccione el almacén de datos ESX de destino.

NOTA: Las opciones del asistente **de restauración** cambian en función de las opciones que seleccione durante el procedimiento de restauración.

10. En la página **Summary**, revise sus entradas y haga clic en **FINISH** para ejecutar la restauración.

NOTA: Para monitorear los resultados, seleccione **Activity** en el árbol de navegación de la interfaz de usuario de Protection Software y visualice los resultados del procesamiento en el panel **Activity** derecho.

Restauración mediante acceso instantáneo

Puede usar la función de acceso instantáneo para realizar la recuperación de una VM prácticamente en tiempo real. Protection Software monta una imagen de copia de seguridad de VM en un recurso compartido NFS en su entorno de respaldo y activa la máquina virtual para que pueda administrarse en vCenter.

Sobre esta tarea

Para restaurar una VM mediante la función de acceso instantáneo, realice las siguientes acciones.

NOTA: Después de completar estos pasos, debe mover la máquina virtual de su entorno de respaldo al sistema de producción.

.

Pasos

1. Haga clic en **DPC Web UI** e inicie sesión en **DPC**.
   Se mostrará la página del tablero **DPC**.
2. Haga clic en **System Management** en el panel izquierdo para mostrar la página Data Protection Central.
3. Haga clic en los puntos suspensivos verticales de Protection Software-Protection Software y seleccione **Protection Software Restore**.
   Se muestra la página **Asset Management** en la interfaz de usuario de Protection Software.
4. Expanda el Hypervisor Manager (Service) que agregó al panel **Domain** y seleccione **Virtual machines** para visualizar los clientes de VM que pertenecen a ese Hypervisor Manager (Service).
5. En la lista de clientes, seleccione al cliente de VM que desee restaurar.
6. Haga clic en **RESTORE**.
   Se muestra el cuadro de diálogo **Quick Restore**.
   NOTA: La función de restauración rápida restaura el respaldo más reciente.
7. Haga clic en **OK**.
   Se muestra la ventana **Select Restore Content**.
8. Seleccione el contenido que desea restaurar y haga clic en **NEXT**.
   Se mostrará la ventana **Restore**.
9. Seleccione o ingrese los detalles que se requieren en los campos para restaurar desde una máquina virtual mediante la siguiente tabla. Haga clic en **NEXT** para continuar con la página siguiente.
   Utilice la siguiente tabla para completar cada página del asistente. Haga clic en **NEXT** para avanzar a la próxima página.

Tabla 23. Restauración mediante acceso instantáneo

Página del asistente	Campo	Descripción
Basic Config	Destination	Seleccione **Instant Access**.
	Proxy	Seleccione **Automatic**.
Advanced Config	vCenter	Seleccione la dirección IP de vCenter para administrar la máquina virtual restaurada.
	Nombre de VM	Introduzca un nombre para la VM restaurada.
Ubicación		Expanda el árbol y seleccione la VM donde desee ejecutar la restauración.
Host/Cluster		Expanda el árbol y seleccione el host/clúster de Hypervisor.
Pool de recursos		Expanda el árbol y seleccione el pool de recursos.

NOTA: Las opciones del asistente **Restore** cambian en función de las opciones que seleccione durante el procedimiento de restauración.

10. En la página **Summary**, revise sus entradas y haga clic en **FINISH** para ejecutar la restauración.
    NOTA: Para monitorear los resultados, seleccione **Activity** en el árbol de navegación de la interfaz de usuario de Protection Software y visualice los resultados del procesamiento en el panel **Activity** derecho.

Restauración de archivos específicos

Puede restaurar archivos específicos directamente desde los resultados de búsqueda.

Requisitos previos

Asegúrese de que Protection Software indexe sus imágenes de VM respaldadas. Para obtener instrucciones, consulte la *Guía del administrador de búsqueda de Dell EMC*.

Sobre esta tarea

En este procedimiento, se utiliza la aplicación Search para buscar y restaurar archivos específicos en un respaldo de VM. Para restaurar archivos específicos, realice las siguientes acciones.

Pasos

1. Haga clic en **DPC Web UI** e inicie sesión en **DPC**.
   Se mostrará la página del tablero **DPC**.
2. Haga clic en **Search and Recovery** en el panel izquierdo.
   La aplicación abre la página **Search**.
3. En el campo **Search**, introduzca una consulta para recuperar archivos específicos y haga clic en **Search**. (También puede usar las opciones de filtro para refinar los resultados de búsqueda).
   La aplicación muestra la lista de archivos en función de su consulta.
4. Seleccione los archivos que desee restaurar y haga clic en **Restore** para visualizar el cuadro de diálogo **Restore**.
5. Seleccione o ingrese los detalles que se requieren en los campos para restaurar a partir de los resultados de búsqueda mediante la siguiente tabla. Haga clic en **Next** para continuar con la página siguiente.

Tabla 24. Restauración de archivos específicos

Campo	Descripción
Original path / Destination path	Selección de la ubicación de la restauración. Cuando corresponda, haga clic en **Overwrite** y seleccione **Restore Access Control List** para proteger el archivo con la misma configuración de lista de control de acceso.
Client	Cuando esté seleccionada la opción **Destination Path**, seleccione el cliente donde desee guardar el archivo.
Restore to	Especifique la ruta donde desee guardar el archivo.
Username / Password	Especifique el nombre de usuario de VM y la contraseña.

6. Haga clic en **Restore** para iniciar el proceso de restauración.
7. Para monitorear los resultados, haga clic en **View Jobs** debajo del campo **Search** y actualice la pantalla para ver las acciones en curso.

Generación de informes

En esta sección, se proporciona información sobre cómo generar informes mediante la interfaz del usuario de Data Protection Central para PowerProtect DP Series Appliance.

Creación de un informe

Esta función le permite generar informes para sistemas Protection Software y Protection Storage. Puede generar 11 informes preconfigurados.

Sobre esta tarea

Para obtener más información acerca de estos informes, consulte la *Guía del producto de Dell EMC Data Protection Advisor*.

Si desea generar sus propios informes, consulte la *Guía de creación de informes personalizada de Dell EMC Data Protection*.

Pasos

1. Haga clic en **DPC Web UI** e inicie sesión en **DPC**.
   Se mostrará la página del tablero **DPC**.
2. Haga clic en **Reports** en el panel izquierdo.

   En el panel derecho, se muestra cada tipo de informe. El panel muestra los informes Protection Software y Protection Storage. Puede seleccionar las casillas de verificación Protection Software y Protection Storage, o ambas, en la parte superior derecha para filtrar los informes que se muestran.

   El período de informe para cada informe se muestra en la esquina inferior derecha. El período de informe predeterminado es la semana anterior, pero puede cambiarlo; para ello, haga clic en **LAST WEEK** y seleccione otro período.
3. Para generar un informe, haga clic en **RUN REPORT** debajo del nombre del informe.
   PowerProtect DP Series Appliance genera el informe y muestra **View Last Report** con el registro de fecha y hora al finalizar.
4. Haga clic en **View Last Report** para visualizar el informe en una nueva ventana.

5

Recursos adicionales

Temas:

Recursos de capacitación de PowerProtect DP Series Appliance

Hay videos paso a paso, demostraciones y explicaciones de características del producto disponibles en línea.

Puede obtener más información y capacitación de PowerProtect DP Series Appliance en https://education.emc.com:

A

Implementación independiente (opcional)

La implementación autónoma se refiere a la configuración de la red del dispositivo mediante la IP de ACM para DNS, NTP y Gateway. Esta es una tarea opcional. Realice esta tarea solo si no tiene una dirección IP válida para DNS, NTP y Gateway. Después de implementar y configurar correctamente el dispositivo, puede cambiar el DNS, NTP y gateway desde el tablero de ACM.

Requisitos previos

- La implementación independiente solo es compatible con la red IPv4.

  NOTA: No puede configurar ACM como DNS y NTP en una red IPv6.
- En una configuración de red única, debe haber al menos dos enlaces ascendentes conectados al switch.

  Realice la siguiente solución alternativa temporal si no tiene dos enlaces ascendentes:

  Asigne dos direcciones IP temporales en subredes diferentes (la subred debe ser diferente de la IP de administración de Protection Storage) a las IP de respaldo del Protection Storage. Estas IP no requieren entradas de DNS. Después de la implementación, cambie las IP de Protection Storage asignadas a estas NIC y actualice el Protection Storage `ifgroup`. Esta solución alternativa evita la falla de configuración de Protection Storage.

Sobre esta tarea

Realice los siguientes pasos cuando esté en la página **Network Configuration** en ACM.

Pasos

1. Abra una sesión SSH como usuario **`root`** en ACM mediante una IP privada.
2. Ejecute el comando:

   `cd /usr/local/dataprotection/var/configmgr/server_data/config/`
3. Abra el archivo `commonconfig.xml` mediante el editor vi:

   `vi commonconfig.xml`
4. Busque las siguientes etiquetas:

   `<configureAcmDNS>false</configureAcmDNS>`

   `<configureAcmNTP>false</configureAcmNTP>`
5. Cambie los valores de las etiquetas según el modo de implementación:
   - Para configurar DNS, establezca el valor de la etiqueta `configureAcmDNS` como `true`
   - Para configurar NTP, establezca el valor de la etiqueta `configureAcmNTP` como `true`
6. Guarde el archivo `commonconfig.xml`.
7. Siga estos pasos para configurar DNS.
   a. Ejecute el comando: `cd /usr/local/dataprotection/customscripts/`
   b. Abra el archivo `dns_ip_hostname_mappings.properties` mediante el editor vi:

      `vi dns_ip_hostname_mappings.properties`

      El contenido del archivo depende del modelo del dispositivo. Verifique si las claves necesarias están presentes en el archivo; de lo contrario, puede agregarlas manualmente.
   c. Ingrese las direcciones IP requeridas, el mapeo de nombre de host y otros detalles según las claves presentes en el archivo. Consulte las siguientes reglas para actualizar el archivo:
      - Para usar el rango de IP para asignar direcciones IP y nombres de host a los componentes respectivos, consulte Requisitos de dirección IP en la página 19.

        NOTA: La validación del rango de IP no es compatible con la implementación independiente.
      - Para una sola red, deje los campos de red de respaldo independientes en blanco.
      - **NOTA:** Ingrese el nombre de host corto y no el FQDN.
      - Las entradas de nombre de host no deben contener guion bajo (_).

- Ingrese la dirección IP o el nombre de host para los componentes opcionales (Reporting and Analytics, Search, Cloud DR y Cyber Recovery). Si las direcciones IP o los nombres de host correspondientes no se agregan en el archivo durante la implementación, los componentes opcionales no se pueden implementar desde el tablero de ACM más adelante mientras ACM se utiliza como DNS.

d. Guarde el archivo `dns_ip_hostname_mappings.properties`.

e. Vaya a la página ACM **Network Configuration** en el navegador de Internet y actualice la página.

La página **Network Configuration** se debe completar automáticamente si el archivo `dns_ip_hostname_mappings.properties` se actualiza con todos los campos obligatorios.

8. Ingrese la IP de ACM en el campo **NTP server IP Address**.
9. Haga clic en **Submit**.

Resultados

- Después de configurar las redes básicas, el navegador web redirigirá automáticamente a la dirección IP de ACM asignada durante la configuración de redes.

  NOTA: Para que el envío automático funcione correctamente, la computadora que utilice para completar la configuración debe estar conectada a la misma red que la dirección IP configurada de ACM.
- Si no puede tener conexiones a redes públicas y privadas al mismo tiempo, desconéctese de la red de configuración de dispositivos privados y, luego, conéctese a la red en la que se encuentra la dirección IP de ACM para completar el resto de la configuración.
- Si la configuración de red falla, puede hacer clic en **Rollback** para revertir todos los ajustes. Revise los ajustes, modifíquelos si es necesario y, a continuación, vuelva a configurar los ajustes de red.

Siguientes pasos

- Una vez que se complete la configuración de red, restablezca la configuración de la dirección IP del adaptador de red en la computadora de servicio a su estado anterior.
- Después de completar la configuración de red, consulte Configurar el software DP4400 en la página 25 para conocer los pasos para instalar e implementar el dispositivo.
- Para agregar nuevas direcciones IP y entradas de nombre de host en el DNS que se ejecuta como ACM, consulte Agregar direcciones IP y entradas de nombre de host en la página 84.
- Después de implementar el dispositivo, puede cambiar las direcciones IP de DNS, NTP y Gateway desde el tablero de ACM. Para obtener más información, consulte la *Guía del producto del dispositivo PowerProtect serie DP*.

Temas:

Agregar direcciones IP y entradas de nombre de host

En esta sección, se describen los pasos para agregar las direcciones IP y las entradas de nombre de host al servidor DNS que se ejecuta como ACM.

Sobre esta tarea

Realice estos pasos para agregar las direcciones IP y las entradas de nombre de host:

Pasos

1. Vaya al directorio `/var/lib/named/master` en ACM mediante el comando:

   ```
   cd /var/lib/named/master
   ```
2. Agregue direcciones IP y entradas de nombre de host (similar a otras entradas presentes en el archivo) al final de los dos archivos siguientes. Asegúrese de agregar `.` al final del FQDN mientras agrega las entradas.

   NOTA: Además de agregar direcciones IP y nombres de host nuevos a los archivos, no modifique ningún otro contenido.

   - Búsqueda directa: archivo *<domain_name>*

     Donde *domain_name* es el nombre de dominio que se menciona en el archivo `usr/local/dataprotection/customscripts/dns_ip_hostname_mappings.properties` durante la configuración de red.

   - Búsqueda inversa: archivo *<first three octets of reverse subnet IP>*`.in-addr.arpa`

Por ejemplo: *xx.xx.xx*.in-addr.arpa

Donde *xx.xx.xx* es la subred inversa mencionada en el archivo `/usr/local/dataprotection/customscripts/dns_ip_hostname_mappings.properties` durante la configuración de red.

3. Reinicie el servicio con nombre mediante el comando:
   `service named restart`

B

Puertos de red

Este apéndice contiene información sobre los puertos de red para los siguientes componentes:

Temas:

Protection Software

La siguiente tabla muestra los requisitos de puertos de Protection Software.

Tabla 25. Requisitos de puertos

Puerto/Protocolo	Source	Destination	Descripción
29000/TCP	Nodo de utilidad	Nodo de almacenamiento	Subsistema de Protection Software mediante SSL
29000/TCP	Nodo de almacenamiento	Nodo de utilidad	Subsistema de Protection Software mediante SSL
30001/TCP	Nodo de utilidad	Nodo de almacenamiento	MCS a través de SSL
30001/TCP	Nodo de almacenamiento	Nodo de utilidad	MCS a través de SSL
30002/TCP	Servidor Protection Software	Cliente Protection Software.	Cliente Protection Software a través de SSL
30002/TCP	Cliente Protection Software.	Servidor Protection Software	Cliente Protection Software a través de SSL
30003/TCP	Nodo de utilidad	Nodo de almacenamiento	MCS a través de SSL
30003/TCP	Nodo de almacenamiento	Nodo de utilidad	MCS a través de SSL

Para obtener información detallada acerca de los puertos, consulte el *Apéndice de requisitos de puertos* en la *Guía de seguridad del producto Dell EMC Avamar 19.4*.

Puertos entrantes requeridos del nodo de utilidad

En la tabla de esta sección, se describen los puertos entrantes que deben estar abiertos en un nodo de utilidad de Protection Software.

En la siguiente tabla se describen los puertos entrantes que deben estar abiertos en un nodo de utilidad de Protection Software. Para cada puerto que se enumera en esta tabla, el nodo de utilidad de Protection Software es el destino y el origen se enumera en la columna Equipo de origen.

NOTA: Protection Software 7.5.1 elimina la compatibilidad con el acceso HTTP a los puertos TCP 80 y 7580. Utilice los puertos HTTPS 443 y 7543 para acceder a estos servicios en su lugar.

Tabla 26. Puertos entrantes requeridos en el nodo de utilidad

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
N/D	ICMP Tipos 3, 8 y 11	ICMP	• Clientes de Protection Software • Otros servidores Protection Software • Sistema Protection Storage	Los clientes de Protection Software hacen ping periódicamente al servidor Protection Software para determinar la mejor interfaz para comunicarse con MCS. El servidor Protection Software envía una respuesta ICMP. Los servidores Protection Software también hacen ping a los sistemas asociados, como destinos de replicación y Protection Storage.
22	TCP	Protocolo SSH	• Computadoras del administrador • Otros nodos de servidor de Protection Software	Acceso seguro al shell.
69	TCP	TFTP	Switch interno	
123	TCP/UDP	NTP	Servidores de hora NTP	Proporciona sincronización de reloj desde servidores de Network Time Protocol.
163	UDP	SNMP	Sistema Protection Storage	Puerto de captador/establecedor para objetos SNMP desde un sistema Protection Storage. Se requiere cuando se almacenan respaldos de clientes Protection Software en un sistema Protection Storage.
443	TCP	Protocolo HTTPS a través de TLS/SSL	• Clientes del navegador web • Servidor web proxy inverso • AvInstaller • Host del servicio de descarga de Protection Software • Administrador de claves de Protection Software	Proporciona a los navegadores web acceso HTTPS a los servicios Protection Software. Se puede utilizar un servidor web proxy inverso para limitar el acceso a este puerto.
700	TCP/UDP	Login Manager	• Clientes del navegador web • Servidor web proxy inverso	
703	TCP	Servicio AKM	Nodos de servidor de Protection Software	Se utiliza para la administración de claves.

Tabla 26. Puertos entrantes requeridos en el nodo de utilidad (continuación)

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
1234	TCP	HTTPS de la utilidad de instalación Protection Software	Clientes del navegador web	Solo abra este puerto para la instalación de Protection Software. Solo permita el acceso desde computadoras de administrador de confianza que se utilizan durante la instalación de software. **NOTA:** Cierre este puerto cuando finalice la instalación de Protection Software. Los servicios de Protection Software no escuchan en el puerto 1234.
2888	TCP	AVDTO	Nodo de acceso a medios y retención ampliada de Protection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad con Protection Software Extended Retention.
5555	TCP	Administrador de servidor de PostgreSQL	• Clientes que ejecutan Protection Software Client Manager y Reporting and Analytics • Computadoras cliente administrador de PostgreSQL	Este puerto está abierto de manera predeterminada. En la sección *Protección del puerto del firewall de Postgres* en la *Guía de seguridad del producto Avamar*, se proporcionan más instrucciones para habilitar el acceso selectivo. Limite el acceso a computadoras de administrador de confianza.
5568	TCP	PostgreSQL	Nodo de acceso a medios y retención ampliada de AProtection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad con Protection Software Extended Retention.
5671	TCP	Bus de mensajes	• localhost • Otros nodos de utilidad de Protection Software • Computadoras con retención extendida de Protection Software • Computadoras de Backup and Recovery Manager	El bus de mensajes es un agente de mensajes que se utiliza para mejorar la comunicación entre procesos asíncrona.
6667	TCP	Evento de servicio de archivo	Nodo de acceso a medios y retención ampliada de Protection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad

Tabla 26. Puertos entrantes requeridos en el nodo de utilidad (continuación)

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
				con Protection Software Extended Retention.
7,000	TCP	Apache Tomcat	Nodo de acceso a medios y retención ampliada de Protection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad con Protection Software Extended Retention.
7443	TCP	Apache Tomcat	Nodo de acceso a medios y retención ampliada de Protection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad con Protection Software Extended Retention.
7543	HTTPS/SSL	Update Manager	Clientes del navegador web	Los clientes del navegador web utilizan este puerto para crear conexiones HTTPS a Protection Software Installation Manager. Limite el acceso a computadoras de administrador de confianza.
7544	TCP	Update Manager	Clientes de conector Jetty	Los clientes de conector Jetty utilizan este puerto para enviar una señal de apagado a su servidor web Jetty. Limite el acceso a computadoras de administrador de confianza.
7778–7781	TCP	RMI	Consola de administración del administrador de Protection Software	Se utiliza para las conexiones desde la consola Protection Software. Limite el acceso a computadoras de administrador de confianza.
8105	TCP	Apache Tomcat	Computadoras de cliente de Protection Software	Utilizado por Protection Software Desktop/ Laptop.
8109	TCP	Apache Tomcat	Computadoras de cliente de Protection Software	Utilizado por Protection Software Desktop/ Laptop.
8181	TCP	Apache Tomcat	Computadoras de cliente de Protection Software	Las conexiones desde computadoras del cliente de Protection Software y desde hosts AvInstaller se redirigen a este puerto.
8444	TCP	Apache Tomcat	Clientes del navegador web	Las conexiones del navegador web desde computadoras del cliente de escritorio/laptop de Protection Software se redirigen a este puerto.

Tabla 26. Puertos entrantes requeridos en el nodo de utilidad (continuación)

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
8505	TCP	Apache Tomcat	Utilidad del servidor de nodos o de un único nodo	La computadora de escritorio/laptop de Protection Software utiliza este puerto para enviar un comando de apagado a su servidor Apache Tomcat. Limite el acceso al nodo de utilidad o al servidor de un solo nodo.
8580	TCP	AvInstaller	Clientes del navegador web	Se utiliza para las conexiones desde el equipo del Servicio de descarga de Protection Software y para el acceso a AvInstaller desde otros clientes del navegador web.
9443	TCP	RMI: servicios web de la consola de administración de Protection Software	Clientes del navegador web	
19000	TCP/UDP	Subsistema de Protection Software (también conocido como GSAN)	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
19500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
20000	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
20500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25000	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26000	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
27000	TCP	Servidor Protection Software	• Computadoras de cliente de Protection Software • Nodos de servidor de Protection Software • Nodos de Protection Software que actúan como un origen replicador	Comunicación del subsistema de Protection Software. Este puerto está bloqueado de manera predeterminada para las instalaciones nuevas de Protection Software. Abra este

Tabla 26. Puertos entrantes requeridos en el nodo de utilidad (continuación)

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
				puerto para permitir respaldos no cifrados.
27500	TCP	Servidor Protection Software	• Nodos de servidor de Protection Software • Nodos de Protection Software que actúan como un origen replicador	Comunicación del subsistema de Protection Software.
28001	TCP	• CLI del servidor Protection Software • MCS • Avagent	• Computadoras de cliente de Protection Software • Proxy de VMware • Origen de replicación • Destino de replicación	• Comandos de la CLI desde computadoras cliente. • Comunicación de Avagent a MCS. • La comunicación bidireccional entre avagent y MCS funciona en el servidor Protection Software de origen de replicación y el servidor Protection Software de destino de replicación para permitir el intercambio de claves de autenticación.
28002–28011	TCP		Nodo de acceso a medios y retención ampliada de Protection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad con Protection Software Extended Retention.
28009	TCP	avagent	Proxy de VMware	Comunicación no segura con el proxy de VMware.
28810-28819	TCP	ddrmaint	localhost	Uso interno solo para la autenticación basada en token cuando se conecta a Protection Storage; solo el host local puede usarla.
29000	TCP	SSL del servidor Protection Software	• Computadoras de cliente de Protection Software • Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
30001	TCP	MCS	• Computadoras de cliente de Protection Software • Proxy de VMware • Nodos de servidor de Protection Software	• Comunicación de conector seguro de 2 vías. • Comunicación de Avagent a MCS. • Comunicación de MCS a través de SSL.
30002	TCP	avagent	Computadoras de cliente de Protection Software	Comunicación del cliente a través de SSL.

Tabla 26. Puertos entrantes requeridos en el nodo de utilidad (continuación)

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
30003	TCP	MCS	• Computadoras de cliente de Protection Software • Nodos de servidor de Protection Software	Comunicación de MCS a través de SSL.
30102–30109	TCP	avagent	Proxy de VMware	Comunicación asegurada con el proxy de VMware.
61617	TCP	Apache ActiveMQ SSL	Nodo de acceso a medios y retención ampliada de Protection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad con Protection Software Extended Retention.

Puertos entrantes opcionales del nodo de utilidad

En esta sección, se describen los puertos entrantes recomendados, pero opcionales, para un nodo de utilidad de Protection Software.

En la siguiente tabla se describen los puertos entrantes recomendados, pero opcionales, para un nodo de utilidad de Protection Software. Para cada puerto que se enumera en esta tabla, el nodo de utilidad de Protection Software es el destino y el origen se enumera en la columna Equipo de origen.

Tabla 27. Puertos entrantes opcionales en el nodo de utilidad

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
514	UDP	syslog	Utilidad del servidor de nodos o de un único nodo	El servidor de Protection Software se conecta a este puerto para comunicar eventos al registro del sistema.
8509	TCP	Apache Tomcat	Utilidad del servidor de nodos o de un único nodo	El protocolo Apache JServ (A VGA) utiliza el puerto 8509 para equilibrar la carga de trabajo de varias instancias de Tomcat.

Puertos de salida requeridos del nodo de utilidad

En esta sección, se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde un nodo de utilidad Protection Software.

En la siguiente tabla se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde un nodo de utilidad Protection Software. Para cada fila, el nodo de utilidad es el equipo de origen que debe tener acceso saliente al puerto indicado en la computadora de destino indicada.

Tabla 28. Puertos de salida requeridos para el nodo de utilidad

Puerto	Protocolo	Equipo de destino	Información adicional
N/D	ICMP Tipos 3, 8 y 11	• Clientes de Protection Software • Otros servidores Protection Software • Sistema Protection Storage	Los clientes de Protection Software hacen ping periódicamente al servidor Protection Software para determinar la mejor interfaz para comunicarse con MCS. El servidor Protection Software envía una respuesta ICMP. Los servidores Protection Software

Tabla 28. Puertos de salida requeridos para el nodo de utilidad (continuación)

Puerto	Protocolo	Equipo de destino	Información adicional
			también hacen ping a los sistemas asociados, como destinos de replicación y Protection Storage.
7	TCP	Sistema Protection Storage	Se requiere para registrar un sistema Protection Storage para almacenar respaldos de clientes de Protection Software.
23	TCP	Interno	Se requiere para la comunicación con switches internos y para actualizaciones de firmware.
25	TCP	Servicio al cliente de Protection Software	Se requiere para permitir que ConnectEMC realice una conexión SMTP con el servicio al cliente.
53	TCP/UDP	DNS	Se requiere para la resolución de nombres y las transferencias de zonas DNS. Los nodos proxy de VMware requieren la conexión TCP a DNS.
88		Centro de distribución de claves (KDC)	Se requiere para acceder al sistema de autenticación Kerberos.
111	TCP/UDP	Servicio del asignador de puertos RPC en el sistema Protection Storage	Solo se requiere cuando los respaldos se almacenan en un sistema Protection Storage. Acceso a la funcionalidad del asignador de puertos RPC y NFS en un sistema Protection Storage.
123	TCP/UDP	Servidores de hora NTP	Proporciona sincronización de la hora del sistema desde los servidores de Network Time Protocol.
161	UDP	Servicio SNMP en el sistema Protection Storage	Solo se requiere cuando los respaldos se almacenan en un sistema Protection Storage.
389	TCP/UDP	LDAP	Brinda acceso a los servicios de directorio.
443	• API de Hypervisor Platform • TCP	• Hypervisor Manager • Administrador de claves de Protection Software	
464	TCP	Centro de distribución de claves (KDC)	Se requiere para acceder a la contraseña de cambio/ configuración de Kerberos.
902	TCP	Servicio proxy del servidor de Hypervisor	
2049	TCP/UDP	Demonio de NFS en el sistema Protection Storage	Solo se requiere cuando los respaldos se almacenan en un sistema Protection Storage.

Tabla 28. Puertos de salida requeridos para el nodo de utilidad (continuación)

Puerto	Protocolo	Equipo de destino	Información adicional
2052	TCP/UDP	Proceso de montaje de NFS en el sistema Protection Storage	Solo se requiere cuando los respaldos se almacenan en un sistema Protection Storage. La comunicación saliente debe estar abierta para los protocolos TCP y UDP.
5671	TCP	• localhost • Otros nodos de utilidad de Protection Software • Computadoras con retención extendida de Protection Software • Computadoras de Backup and Recovery Manager	Mensajería de bus de mensajes. El bus de mensajes es un agente de mensajes que se utiliza para mejorar la comunicación asíncrona entre procesos.
5696	TCP	Servidor de administración de claves en conformidad con KMIP	Puerto recomendado para la operación de administración de claves externa de AKM.
7443	TCP	Nodo de acceso a medios que aloja la retención extendida de Protection Software	Solo se requiere cuando se utiliza la función de retención extendida de Protection Software.
7444	TCP	Hypervisor Manager	Para las configuraciones de nodos de utilidad que también ejecutan el dispositivo de respaldo de VMware, este puerto se abre mediante una cláusula if/then en las reglas de firewall. De lo contrario, este puerto no es necesario. Se utiliza para probar las credenciales de Hypervisor Manager.
7543	HTTPS/SSL	Update Manager	Los clientes del navegador web utilizan este puerto para crear conexiones HTTPS a Protection Software Installation Manager. Limite el acceso a computadoras de administrador de confianza.
7544	TCP	Update Manager	Los clientes de conector Jetty utilizan este puerto para enviar una señal de apagado a su servidor web Jetty. Limite el acceso a computadoras de administrador de confianza.
7543	HTTPS	Update Manager	Se utiliza para las conexiones desde la computadora del servicio de descarga de Protection Software y para acceder a Update Manager desde otros clientes del navegador web.
8080	TCP	Servidor NetWorker	Para las configuraciones de nodos de utilidad que también ejecutan el dispositivo de respaldo de VMware, este

Tabla 28. Puertos de salida requeridos para el nodo de utilidad (continuación)

Puerto	Protocolo	Equipo de destino	Información adicional
			puerto se abre mediante una cláusula if/then en las reglas de firewall. De lo contrario, este puerto no es necesario. Se utiliza para registrarse en un servidor de NetWorker.
8580	TCP	Computadora que ejecuta el servicio de descarga de Protection Software	Se utiliza para realizar solicitudes de descargas de paquetes desde la computadora del servicio de descarga de Protection Software.
9443	TCP	Servidores administrados de Protection Software	Los servicios web de la consola de administración de Protection Software utilizan este puerto de salida para la comunicación RMI a través de un puerto asignado dinámicamente en servidores administrados de Protection Software.
19000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
19500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
20000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
20500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
27000	TCP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
28001	TCP	Sistema de origen de replicación y sistema de destino de replicación	La replicación requiere acceso bidireccional entre el servidor de Protection Software de origen de replicación y el servidor de Protection Software de destino de replicación para permitir el intercambio de claves de autenticación.
28009	TCP	Proxy de VMware	Acceso de MCS a registros de proxy.
28011	TCP	Nodo de acceso a medios y retención ampliada de Protection Software	Las reglas de firewall abren este puerto cuando instala la compatibilidad con Protection Software Extended Retention.

Tabla 28. Puertos de salida requeridos para el nodo de utilidad (continuación)

Puerto	Protocolo	Equipo de destino	Información adicional
29000	TCP	Nodos de servidor de Protection Software	Comunicación del subsistema Protection Software a través de SSL.
30001	TCP	Nodos de servidor de Protection Software	Comunicación de MCS a través de SSL.
30002	TCP	Computadoras de cliente de Protection Software	Comunicación con avagent.
30003	TCP	Nodos de servidor de Protection Software	Comunicación de MCS a través de SSL.
30002 a 30009	TCP	Proxy de VMware	Puerto de paginación de Avagent. Comunicación asegurada con el proxy de VMware.
30102	TCP	Proxy de VMware	Puerto de paginación de Avagent. Comunicación asegurada con el proxy de VMware.
61617	TCP	Nodo de acceso a medios que aloja la retención extendida de Protection Software	Solo se requiere cuando se utiliza la función de retención extendida de Protection Software.
61619	TCP	Computadora que ejecuta Backup and Recovery Manager.	Necesario para permitir la comunicación con Backup and Recovery Manager.

Puertos entrantes necesarios para el nodo de almacenamiento

En esta sección, se describen los puertos entrantes que deben estar abiertos en cada nodo de almacenamiento Protection Software.

En la siguiente tabla se describen los puertos entrantes que deben estar abiertos en cada nodo de almacenamiento Protection Software. Para cada puerto que se enumera en esta tabla, el nodo de almacenamiento Protection Software es el destino y el origen aparece en la columna Equipo de origen.

Tabla 29. Puertos entrantes requeridos en cada nodo de almacenamiento

Puerto	Protocolo	Nombre del servicio	Source	Información adicional
22	TCP	Protocolo SSH	• Computadoras del administrador • Otros nodos de servidor de Protection Software	Acceso seguro al shell.
123	TCP/UDP	NTP	• Servidores de hora NTP • Nodo de utilidad Protection Software	Permite la sincronización del reloj desde servidores de Network Time Protocol (exócrono) y desde el nodo de utilidad (isócrono).
19000	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
19500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.

Tabla 29. Puertos entrantes requeridos en cada nodo de almacenamiento (continuación)

Puerto	Protocolo	Nombre del servicio	Source	Información adicional
20000	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
20500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25000	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26000	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26500	TCP/UDP	Subsistema de Protection Software	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
27000	TCP	Servidor de Protection Software	• Computadoras de cliente de Protection Software • Nodos de Protection Software que actúan como un origen replicador	Comunicación del subsistema de Protection Software. Este puerto está bloqueado de manera predeterminada para las instalaciones nuevas. Abra este puerto para permitir respaldos no cifrados.
29000	TCP	SSL del servidor Protection Software	• Computadoras de cliente de Protection Software • Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
30001	TCP	SSL MCS	Nodos de servidor de Protection Software	Comunicación MCS
30003	TCP	SSL MCS	Nodos de servidor de Protection Software	Comunicación MCS

Puertos entrantes opcionales del nodo de almacenamiento

En esta sección, se describen los puertos entrantes recomendados, pero opcionales, para un nodo de almacenamiento de Protection Software.

En la siguiente tabla se describen los puertos entrantes recomendados, pero opcionales, para un nodo de almacenamiento de Protection Software. Para cada puerto que se enumera en esta tabla, el nodo de almacenamiento Protection Software es el destino y el origen aparece en la columna Equipo de origen.

Tabla 30. Puertos entrantes opcionales en el nodo de almacenamiento

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
623	UDP	IPMI	Clientes de administración remota	Los clientes de administración se conectan a este puerto para emitir comandos IPMI al sistema operativo del nodo y

Tabla 30. Puertos entrantes opcionales en el nodo de almacenamiento

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
				a BMC. Este puerto es independiente de los puertos de consola RMC remotos que se describen en la sección *Puertos de interfaz de administración remota* de la *Guía de seguridad del producto de Dell EMC Protection Software.*

Puertos de salida requeridos del nodo de almacenamiento

En esta sección, se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde cada nodo de almacenamiento de Protection Software.

En la siguiente tabla se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde cada nodo de almacenamiento Protection Software. Para cada fila, el nodo de almacenamiento es el equipo de origen que debe tener acceso saliente al puerto indicado en la computadora de destino indicada.

Tabla 31. Puertos de salida requeridos para cada nodo de almacenamiento

Puerto	Protocolo	Destination	Información adicional
53	TCP/UDP	DNS	Se requiere para la resolución de nombres y las transferencias de zonas DNS. Los nodos proxy de VMware requieren la conexión TCP a DNS.
123	TCP/UDP	Servidores de hora NTP y el nodo de utilidad de Protection Software	Permite la sincronización del reloj desde servidores de Network Time Protocol (exócrono) y desde el nodo de utilidad (isócrono).
703	TCP	Nodo de utilidad	Permite el acceso al servicio AKM en el nodo de utilidad.
19000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
19500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
20000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
20500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
25500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26000	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
26500	TCP/UDP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.
27000	TCP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software.

Tabla 31. Puertos de salida requeridos para cada nodo de almacenamiento (continuación)

Puerto	Protocolo	Destination	Información adicional
29000	TCP	Nodos de servidor de Protection Software	Comunicación del subsistema de Protection Software a través de SSL.
30001	TCP	Nodos de servidor de Protection Software	Comunicación de MCS a través de SSL.
30003	TCP	Nodos de servidor de Protection Software	Comunicación de MCS a través de SSL.

Puertos entrantes requeridos por el cliente de Protection Software

En esta sección, se describen los puertos entrantes que deben estar abiertos en un cliente de Protection Software.

En la siguiente tabla se describen los puertos entrantes que deben estar abiertos en un cliente de Protection Software. Para cada puerto que se enumera en esta tabla, un cliente de Protection Softwarees el destino y el origen aparece en la columna Equipo de origen.

Tabla 32. Puertos entrantes requeridos en un cliente de Protection Software

Puerto	Protocolo	Nombre del servicio	Source	Información adicional
28002	TCP	avagent	Servidor Protection Software	Proporciona la funcionalidad de administración del administrador de Protection Software.
30001	TCP	MCS	Nodo de utilidad Protection Software	Conector seguro de 2 vías
30002	TCP	avagent	Nodo de utilidad Protection Software	

Puertos de salida requeridos por el cliente de Protection Software

En esta sección, se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde un cliente de Protection Software.

En la siguiente tabla se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde un cliente de Protection Software. Para cada fila, el cliente de Protection Software es el equipo de origen que debe tener acceso saliente al puerto indicado en la computadora de destino indicada.

NOTA: Protection Software 7.5.1 elimina la compatibilidad con el acceso HTTP al puerto TCP 80. Utilice el puerto HTTPS 443 para acceder a estos servicios en su lugar.

Tabla 33. Puertos de salida requeridos para un cliente de Protection Software

Puerto	Protocolo	Destination	Información adicional
53	TCP/UDP	DNS	Se requiere para la resolución de nombres y las transferencias de zonas DNS.
111	TCP/UDP	Sistema Protection Storage	Se requiere para respaldar clientes en Protection Storage.
123	UDP	Servidores de hora NTP	Proporciona sincronización de reloj desde servidores de Network Time Protocol.
443	TCP	Servicio HTTPS del servidor de Protection Software	Se requiere para utilizar la interfaz del usuario del navegador web de escritorio/

Tabla 33. Puertos de salida requeridos para un cliente de Protection Software (continuación)

Puerto	Protocolo	Destination	Información adicional
			laptop de Protection Software y la interfaz del usuario del navegador web de restauración web de Protection Software.
2049	TCP/UDP	Sistema Protection Storage	Se requiere para respaldar clientes en Protection Storage.
2052	TCP/UDP	Sistema Protection Storage	Se requiere para respaldar clientes en Protection Storage.
3008	TCP	Servicio de nivel de archivo en el sistema Protection Storage	Solo se requiere cuando los respaldos se almacenan en un sistema Protection Storage y se usa un nivel de archivo.
8105	TCP	Servidor Protection Software	Utilizado por Protection Software Desktop/Laptop.
8109	TCP	Servidor Protection Software	Utilizado por Protection Software Desktop/Laptop.
8181	TCP	Puerto de redireccionamiento HTTP del servidor Protection Software	Se requiere para utilizar la interfaz del usuario del navegador web de escritorio/ laptop de Protection Software y la interfaz del usuario del navegador web de restauración web de Protection Software.
8444	TCP	Puerto de redireccionamiento HTTPS del servidor Protection Software	Se requiere para utilizar la interfaz del usuario del navegador web de escritorio/ laptop de Protection Software y la interfaz del usuario del navegador web de restauración web de Protection Software.
27000	TCP	Servidor Protection Software	Comunicación del subsistema de Protection Software.
28001	TCP	Servidor Protection Software	Comandos de la CLI desde computadoras cliente.
29000	TCP	Servidor Protection Software	Comunicación del subsistema de Protection Software.
30001	TCP	Nodo de utilidad Protection Software	MCS
30003	TCP	Nodo de utilidad Protection Software	MCS

Puerto entrante requerido para el host del servicio de descarga de Protection Software

En esta sección, se describe el puerto de entrada que debe estar abierto en un host del servicio de descarga de Protection Software.

En la siguiente tabla se describe el puerto de entrada que debe estar abierto en un host del servicio de descarga de Protection Software. Para el puerto que se indica en esta tabla, un host del servicio de descarga de Protection Software es el destino y el origen se enumera en la columna Equipo de origen.

Tabla 34. Puerto entrante requerido en un host de servicio de descarga de Protection Software

Puerto	Protocolo	Nombre del servicio	Source	Información adicional
8580	TCP	Servicio de descarga de Protection Software	Servidor Protection Software	El servidor de Protection Software se conecta a este puerto para acceder al servicio de descarga de Protection Software.

Puertos salientes necesarios para el host del servicio de descarga de Protection Software.

En esta sección, se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde un host de servicio de descarga de Protection Software.

En la siguiente tabla se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde un host de servicio de descarga de Protection Software. Para cada fila, un host del servicio de descarga de Protection Software es el equipo de origen que debe tener acceso saliente al puerto indicado en la computadora de destino indicada.

NOTA: Protection Software 7.5.1 elimina la compatibilidad con el acceso HTTP al puerto TCP 80. Utilice el puerto HTTPS 443 para acceder a estos servicios en su lugar.

Tabla 35. Puertos de salida necesarios para un host de servicio de descarga de Protection Software

Puerto	Protocolo	Destination	Información adicional
21	TCP	Servidor FTP de Protection Software	Proporciona al servicio de descarga de Protection Software acceso FTP a actualizaciones, paquetes acumulativos de seguridad, revisiones y parches.
53	TCP/UDP	DNS	Se requiere para la resolución de nombres y las transferencias de zonas DNS.
123	UDP	Servidores de hora NTP	Proporciona sincronización de reloj desde servidores de Network Time Protocol.
443	TCP	Servicio HTTPS del servidor de Protection Software	Proporciona acceso de HTTPS al servicio de AvInstaller.

Puertos necesarios cuando se utiliza un sistema Protection Storage

En la siguiente tabla se describen los requisitos generales de puertos cuando se implementa un sistema Protection Software con un sistema Protection Storage como destino de almacenamiento:

Tabla 36. Puertos necesarios cuando se utiliza un sistema Protection Storage

Puerto	Protocolo	Source	Destination	Servicio	Información adicional
7	TCP	Nodo de utilidad	Sistema Protection Storage	ECHO	Se requiere para registrar un sistema Protection Storage para almacenar respaldos de clientes de Protection Software.
22	TCP	Nodo de utilidad	Sistema Protection Storage	Protocolo SSH	Comunicación de shell seguro con el sistema Protection Storage.

Tabla 36. Puertos necesarios cuando se utiliza un sistema Protection Storage (continuación)

Puerto	Protocolo	Source	Destination	Servicio	Información adicional
111	TCP/UDP	Nodo de utilidad	Sistema Protection Storage	Servicio del asignador de puertos RPC	Acceso a la funcionalidad del asignador de puertos RPC y NFS en un sistema Protection Storage.
		Cliente Protection Software.			
161	UDP	Nodo de utilidad	Sistema Protection Storage	SNMP	Este es el puerto getter/setter para objetos SNMP de un nodo de utilidad.
163	UDP	Sistema Protection Storage	Nodo de utilidad	SNMP	Ninguno
2049	TCP/UDP	Nodo de utilidad	Sistema Protection Storage	Demonio NFS	Ninguno
		Cliente Protection Software.	Sistema Protection Storage	Demonio NFS	Solo se requiere cuando los respaldos se almacenan en un sistema Protection Storage.
2052	TCP/UDP	Nodo de utilidad	Sistema Protection Storage	Proceso mountd de NFS	La comunicación saliente debe estar abierta para ambos protocolos: TCP y UDP.
		Cliente Protection Software.	Sistema Protection Storage	Proceso mountd de NFS	Solo se requiere cuando los respaldos se almacenan en un sistema Protection Storage.
3008	TCP	Cliente Protection Software.	Sistema Protection Storage	Servicio de nivel de archivo	Solo se requiere cuando se utiliza el nivel de archivo.
3009	TCP	Cliente Protection Software.	Sistema Protection Storage	Servicio de nivel de archivo	Solo se requiere cuando se utiliza el nivel de archivo en la API REST.

Puertos entrantes requeridos del nodo acelerador de NDMP

En esta sección, se describen los puertos entrantes que deben ser accesibles para los paquetes de red que se envían a cada nodo acelerador de Protection Software.

En la siguiente tabla, se describen los puertos entrantes que deben ser accesibles para los paquetes de red que se envían a cada nodo acelerador de Protection Software. Para cada fila, el nodo acelerador es el destino y el origen se enumera en la columna Equipo de origen:

Tabla 37. Puertos entrantes necesarios para cada nodo acelerador

Puerto	Protocolo	Source	Información adicional
7543	HTTP/SSL	Clientes del navegador web	Los clientes del navegador web utilizan este puerto para crear conexiones HTTPS a Protection Software Installation Manager. Limite el acceso a las computadoras de administrador de confianza.
Entre 28002 y 28202	TCP	Agente/cliente de Protection Software	

Tabla 37. Puertos entrantes necesarios para cada nodo acelerador (continuación)

Puerto	Protocolo	Source	Información adicional
Entre 30002 y 30202	TCP	Agente/cliente de Protection Software	

Puertos de salida requeridos del nodo acelerador de NDMP

En esta sección, se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde cada nodo acelerador de Protection Software.

En la siguiente tabla se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde cada nodo acelerador de Protection Software. Para cada fila, el nodo acelerador es la computadora de origen que debe tener acceso saliente al puerto indicado en la computadora de destino indicada.

Tabla 38. Puertos de salida requeridos para cada nodo acelerador

Puerto	Protocolo	Destination	Información adicional
7	TCP	Sistema Protection Storage	
25	TCP	Servicio al cliente	Se requiere para las conexiones SMTP entre ConnectEMC y Servicio al cliente.
111	TCP/UDP	Sistema Protection Storage	
443	TCP	Servicio al cliente	Comunicación LDLS con Servicio al cliente.
2049	TCP/UDP	Sistema Protection Storage	
2052	TCP/UDP	Sistema Protection Storage	
3008	TCP	Sistema Protection Storage	
3009	TCP	Sistema Protection Storage	
8080	TCP	Isilon	Se requiere para el acceso a la API de la plataforma Isilon.
8580	TCP	Computadora que ejecuta el servicio de descarga de Protection Software	Se utiliza para realizar solicitudes de descargas de paquetes desde la computadora del servicio de descarga de Protection Software.
9443	TCP	RMI: servicios web de la consola de administración de Protection Software	
10 000	TCP	Filer NAS	Se requiere para los mensajes de control de NDMP.
28001	TCP	Consola de administración del administrador de Protection Software	
30001	TCP	Consola de administración del administrador de Protection Software	
30003	TCP	Nodos de servidor de Protection Software	Comunicación de MCS a través de SSL.

Puertos entrantes de interfaz de administración remota

En esta sección, se describen los puertos entrantes que deben estar abiertos en la interfaz de administración remota de todos los nodos Protection Software basados en Gen4T y Gen4S.

En la siguiente tabla se describen los puertos entrantes que deben estar abiertos en la interfaz de administración remota de todos los nodos Protection Software basados en Gen4T. Los puertos reales que deben estar abiertos dependen del entorno de red. Para cada puerto que se enumera en esta tabla, la interfaz de administración remota en el nodo es el destino y el origen se enumera en la columna Equipo de origen.

Tabla 39. Puertos entrantes para la interfaz de administración remota en todos los nodos basados en Gen4T

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
80	TCP	HTTP	Computadoras del administrador	Acceso de HTTP
443	TCP	Protocolo HTTP a través de TLS/SSL	Computadoras del administrador	Acceso de HTTPS
2068	TCP	Consola virtual y redirección de medios	Computadoras del administrador	Teclado/mouse de consola virtual, servidor de medios virtuales, servicio seguro de medios virtuales y video de consola virtual

En la siguiente tabla se describen los puertos entrantes que deben estar abiertos en la interfaz de administración remota de todos los nodos Protection Software basados en Gen4S. Los puertos reales que deben estar abiertos dependen del entorno de red. Para cada puerto que se enumera en esta tabla, la interfaz de administración remota en el nodo es el destino y el origen se enumera en la columna Equipo de origen.

Tabla 40. Puertos entrantes para la interfaz de administración remota en todos los nodos basados en Gen4S

Puerto	Protocolo	Nombre del servicio	Equipo de origen	Información adicional
80	TCP	HTTP	Computadoras del administrador	Acceso de HTTP
443	TCP	HTTPS	Computadoras del administrador	Acceso de HTTPS
5120	TCP	Redireccionamiento de medios CDROM	Computadoras del administrador	
5123	TCP	Redireccionamiento de medios de disquete/USB	Computadoras del administrador	
7578	TCP	Teclado, video, mouse	Computadoras del administrador	

Los nodos Protection Software basados en Gen4 han llegado al final de su vida útil. En versiones anteriores de esta guía, se proporciona más información sobre los nodos Protection Software basados en Gen4.

NOTA:

Asegúrese de que el entorno de red local permita la creación de estas conexiones.

Si utiliza una intranet privada, configure la configuración del firewall y la traducción de direcciones de red (NAT) según corresponda.

Asegúrese de abrir los puertos de manera bidireccional en el nivel del firewall.

Puertos de salida de interfaz de administración remota

En esta sección, se describen los puertos de salida que deben ser accesibles para los paquetes de red que se envían desde la interfaz de administración remota en todos los nodos Protection Software.

En la siguiente tabla se describen los puertos salientes a los que deben acceder los paquetes de red que se envían desde la interfaz de administración remota en todos los nodos Protection Software. Los puertos reales que deben estar abiertos dependen del entorno de red. De manera predeterminada, ninguno de estos puertos salientes está configurado para estar en uso. Debe modificar la configuración para usar esos protocolos. Para cada fila, el nodo es el equipo de origen que debe tener acceso saliente al puerto indicado en la computadora de destino indicada.

Tabla 41. Puertos de salida para la interfaz de administración remota en todos los nodos Protection Software

Puerto	Protocolo	Equipo de destino	Información adicional
25	TCP	Computadoras del administrador	Se requiere para establecer una conexión SMTP con computadoras del administrador.
53	TCP/UDP	Servidor DNS	Se requiere para las consultas de DNS.
68	UDP	Computadoras del administrador	Se requiere para la dirección IP asignada por DHCP.
69	UDP	Computadoras del administrador	Se requiere para transferencias triviales de archivos (TFTP).
162	UDP	Computadoras del administrador	Se requiere para enviar traps SNMP.
636	TCP/UDP	Servidor de LDAPS	Se requiere para realizar consultas de LDAP seguro.
3269	TCP/UDP	Servidor de LDAPS	Se requiere para el catálogo global (CG) de LDAPS.

NOTA:

Asegúrese de que el entorno de red local permita la creación de estas conexiones.

Si utiliza una intranet privada, configure la configuración del firewall y la traducción de direcciones de red (NAT) según corresponda.

Asegúrese de abrir los puertos de manera bidireccional en el nivel del firewall.

Puertos entrantes de proxy combinado de Protection Software VMware

En esta sección, se describen los requisitos de puertos entrantes para el proxy combinado de Protection Software VMware.

En la siguiente tabla se describen los requisitos de puertos entrantes para el proxy combinado de Protection Software VMware:

Tabla 42. Puertos entrantes necesarios para el proxy combinado de Protection Software VMware

Puerto	Protocolo	Source	Información adicional
22	TCP/SSH TCP/SSH	Administrador de Protection Software	La compatibilidad con diagnósticos es opcional, pero se recomienda.
902	Servicio de proxy de TCP Hypervisor Server	Servidor Protection Software	
5489	Servicio TCP/CIM	Implementación de Protection Software	Se usa para registrar el proxy.
28009	Registros de proxy de TCP/ acceso	Protection Software MCS	
30102-30109	Puerto de paginación TCP/ avagent	Protection Software MCS	

Tabla 42. Puertos entrantes necesarios para el proxy combinado de Protection Software VMware (continuación)

Puerto	Protocolo	Source	Información adicional
30002 a 30009	Puerto de paginación TCP/ avagent	Servidor Protection Software	Comunicación segura con el servidor Protection Software (nodo de utilidad).

Puertos de salida de proxy combinados de Protection Software VMware

En esta sección, se describen los requisitos de puertos salientes para el proxy combinado de Protection Software VMware.

En la siguiente tabla se describen los requisitos de puertos salientes para el proxy combinado de Protection Software VMware:

Tabla 43. Puertos de salida requeridos para el proxy combinado de Protection Software VMware

Puerto	Protocolo	Destination	Información adicional
53	UDP + TCP/DNS	Servidor DNS	UDP + TCP
111	TCP/UDP	Sistema Protection Storage	Acceso a la funcionalidad del asignador de puertos RPC y NFS en un sistema Protection Storage
443	API TCP/Hypervisor Platform	Hosts de Hypervisor	
443	API TCP/Hypervisor Platform	Hypervisor Manager	
902	TCP/VDDK	Hosts de Hypervisor	
2049	TCP/UDP	Sistema Protection Storage	
2052	TCP/UDP	Sistema Protection Storage	La comunicación saliente debe estar abierta para ambos protocolos: TCP y UDP
8543	TCP	Servidor Protection Software	Se utiliza para las operaciones de instantáneas de VMware.
27000	Comunicación TCP/GSAN	Servidor Protection Software	Comunicación no segura.
28001	TCP/Protection Software MCS/avagent	Servidor Protection Software	
28002 a 28010	TCP/Protection Software MCS/avagent	Servidor Protection Software	
29000	Comunicación TCP/GSAN	Servidor Protection Software	Comunicación segura.
30001	Comunicación de TCP/avagent a MCS	Protection Software MCS	Protection Software 7.2
30002 a 30010	TCP/Protection Software MCS/avagent	Servidor Protection Software	
30102-30109	Puerto de paginación TCP/ Avagent	Servidor Protection Software	Comunicación segura con el nodo de utilidad del servidor de Protection Software

Protection Software Hypervisor Platform Puertos proxy combinados

En esta sección, se describen los puertos necesarios para el Protection Software Hypervisor Platform proxy combinado.

En la siguiente tabla se describen los puertos necesarios para el Protection Software Hypervisor Platform proxy combinado:

Tabla 44. Puertos necesarios para el Protection Software Hypervisor Platform proxy combinado

Puerto	Protocolo	Source	Destination
443	API TCP/Hypervisor Platform	Administrador de implementación de Protection Software	Hosts de Hypervisor
443	API TCP/Hypervisor Platform	Protection Software MCS	Hypervisor Manager (Service)
7444	TCP/Credenciales de prueba de Hypervisor Manager	Protection Software MCS	Hypervisor Manager (Service)

Puertos entrantes para el grupo de seguridad de red de Azure

En esta sección se describen las reglas que se deben agregar a un grupo de seguridad de red de Azure.

En las siguientes tablas se describen las reglas que se deben agregar a un grupo de seguridad de red de Azure:

NOTA: Si desea restringir el tráfico de origen, configure el origen con un bloque CIDR IPv4 o IPv6 o una sola dirección IPv4 o IPv6.

NOTA: Protection Software ya no es compatible con el acceso HTTP al puerto TCP 80. Utilice los puertos HTTPS 443 para acceder a estos servicios en su lugar.

Para todas las entradas de tabla:

- Los campos **Source** y **Destination** son `Any`.
- El campo **Source port range** es `*`
- **Action** es `Allow`.
- Asigne un valor de prioridad único a cada regla, a partir de 100.
- Escriba una descripción única para cada regla. El valor debe ser único para las reglas entrantes y salientes.

Tabla 45. Puertos entrantes para el grupo de seguridad de red de Azure

Tipo	Protocolo	Rango de puertos de destino
Protocolo SSH	TCP	22
Regla de TCP personalizada	TCP	161
Regla de UDP personalizada	UDP	161
Regla de TCP personalizada	TCP	163
Regla de UDP personalizada	UDP	163
HTTPS	TCP	443
Regla de TCP personalizada	TCP	700
Regla de TCP personalizada	TCP	7543
Regla de TCP personalizada	TCP	Entre 7778 y 7781
Regla de TCP personalizada	TCP	8543
Regla de TCP personalizada	TCP	9090
Regla de TCP personalizada	TCP	9443
Regla de TCP personalizada	TCP	27000
Regla de TCP personalizada	TCP	Entre 28001 y 28002
Regla de TCP personalizada	TCP	Entre 28810 y 28819
Regla de TCP personalizada	TCP	29000
Regla de TCP personalizada	TCP	Entre 30001 y 30010

Puertos salientes para el grupo de seguridad de red de Azure

En esta sección se describen los puertos salientes para el grupo de seguridad de red de Azure.

NOTA: Si desea restringir el origen de tráfico, configure el origen con un bloque CIDR IPv4 o IPv6 o una sola dirección IPv4 o IPv6.

De manera predeterminada, Azure tiene una regla AllowInternetOutBound con prioridad `65001` para permitir todo el tráfico de Internet saliente. Reemplace esta regla agregando una regla con una prioridad (es decir, un número entero) mayor que la prioridad de todas las reglas personalizadas y menos de 65 000: **`source: *, destination: *, protocol: *, action: Deny`**. La documentación de Azure contiene información sobre la creación de una regla de firewall.

Para todas las entradas de tabla:

- Los campos **Source** y **Destination** son `Any`.
- El campo **Source port range** es `*`
- **Action** es `Allow`.
- Asigne un valor de prioridad único a cada regla, a partir de 100.
- Escriba una descripción única para cada regla. El valor debe ser único para las reglas entrantes y salientes.

Tabla 46. Puertos salientes para el grupo de seguridad de red de Azure

Tipo	Protocolo	Rango de puertos de destino
Regla de TCP personalizada	TCP	7
Protocolo SSH	TCP	22
SMTP	TCP	25
DNS (UDP)	UDP	53
Regla de TCP personalizada	TCP	111
Regla de UDP personalizada	UDP	111
Regla de TCP personalizada	TCP	161
Regla de UDP personalizada	UDP	161
Regla de TCP personalizada	TCP	163
Regla de UDP personalizada	UDP	163
HTTPS	TCP	443
Regla de TCP personalizada	TCP	700
Regla de TCP personalizada	TCP	2049
Regla de UDP personalizada	UDP	2049
Regla de TCP personalizada	TCP	2052
Regla de UDP personalizada	UDP	2052
Regla de TCP personalizada	TCP	3008
Regla de TCP personalizada	TCP	3009
Regla de TCP personalizada	TCP	8443
Regla de TCP personalizada	TCP	8888
Regla de TCP personalizada	TCP	9090
Regla de TCP personalizada	TCP	9443
Regla de TCP personalizada	TCP	27000
Regla de TCP personalizada	TCP	28001-28010
Regla de TCP personalizada	TCP	29000
Regla de TCP personalizada	TCP	30001-30010

Protection Storage

En esta sección, se muestra información sobre los puertos de red de Protection Storage.

Ajustes de seguridad para la comunicación

Los ajustes de seguridad de comunicación permiten establecer canales de comunicación seguros entre los componentes del producto y entre los componentes del producto y los sistemas o componentes externos.

En las siguientes tablas, se enumeran los puertos de entrada y salida para TCP y UDP:

Tabla 47. Puertos de comunicación entrantes del sistema Protection Storage

Servicio	Protocolo	Puerto	Puerto configurable	Predeterminado	Descripción
FTP	TCP	21	No	Deshabilitado	El puerto se utiliza solo si FTP está habilitado. Ejecute `adminaccess show` en el sistema Protection Storage para determinar si está habilitado.
SSH y SCP	TCP	22	Sí	Habilitado	El puerto se utiliza solo si SSH está habilitado. Ejecute `adminaccess show` en el sistema Protection Storage para determinar si está habilitado. SCP se encuentra activado de forma predeterminada.
Telnet	TCP	23	No	Deshabilitado	El puerto se utiliza solo si Telnet está habilitado. Ejecute `adminaccess show` en el sistema Protection Storage para determinar si está habilitado.
HTTP	TCP	80	Sí	Habilitado[a]	El puerto se utiliza solo si HTTP está habilitado. Ejecute `adminaccess show` en el sistema Protection Storage para determinar si está habilitado.
DD Boost/NFS (asignador de puertos)	TCP	111	No	Habilitado	Se utiliza para asignar un puerto aleatorio para el servicio `mountd` que utilizan DD Boost y NFS. El puerto de servicio `mountd` se puede asignar estáticamente y se puede ejecutar con el comando `nfs option set mountd-port`.
NTP	UDP	123	No	Deshabilitado	1. El puerto solo se utiliza si NTP está habilitado en el sistema de Protection Storage. Ejecute `ntp status` para determinar si está habilitado. 2. El sistema Protection Storage utiliza este puerto para sincronizarse con un servidor de hora.
SNMP	TCP/UDP	161	No	Deshabilitado	El puerto se utiliza solo si SNMP está habilitado. Ejecute `snmp status` para determinar si está habilitado.
HTTPS	TCP	443	Sí	Habilitado	El puerto se utiliza solo si HTTPS está habilitado. Ejecute `adminaccess show` en el sistema Protection Storage para determinar si está habilitado.
CIFS (Microsoft-DS)	TCP	445	No	Habilitado	Puerto principal que CIFS utiliza para la transferencia de datos.

Tabla 47. Puertos de comunicación entrantes del sistema Protection Storage (continuación)

Servicio	Protocolo	Puerto	Puerto configurable	Predeterminado	Descripción
DD Boost/NFS	TCP	2049	Sí	Habilitado	Puerto principal que utiliza NFS. Ejecute el comando `nfs option show` en el sistema Protection Storage para determinar el puerto actual del servidor NFS.
NFS v3/NFS v4	TCP	2049	Sí	Habilitado	Puerto principal que utiliza el servicio NFS. Ejecute `nfs status` para determinar si el servicio NFS v3 o NFS v4 está habilitado. Ejecute `nfs option show nfs3-port` o `nfs option show nfs4-port` en el sistema Protection Storage para determinar el puerto actual que está escuchando.
Replicación	TCP	2051	Sí	Habilitado	El puerto solo se utiliza si la replicación está configurada en el sistema de Protection Storage. Ejecute `replication show config` para determinar si está configurado. Este puerto se puede modificar mediante el comando `replication modify`.
NFS (`mountd`)	TCP/UDP	2052	Sí	Habilitado	Se puede codificar de forma rígida mediante el comando `nfs option set mountd-port`. (Este comando es modo SE, lo que significa que solo un ingeniero de servicio puede emitir este comando). Ejecute `nfs option show mountd-port` en el sistema Protection Storage para determinar el puerto actual en el que `mountd` escucha.
Puerto de Protection Storage Management Center	TCP	3009	No	Habilitado	Este puerto se utiliza solo si Protection Storage Management Center administra el sistema Protection Storage. No se puede configurar.

a. HTTP está habilitado de manera predeterminada, pero redirige automáticamente a HTTPS.

Tabla 48. Puertos de comunicación de salida del sistema Protection Storage

Servicio	Protocolo	Puerto	Puerto configurable	Predeterminado	Descripción
SMTP	TCP	25	No	Deshabilitado	El sistema Protection Storage utiliza este puerto para enviar alertas y soporte automático por correo electrónico.
SNMP	UDP	162	Sí	Deshabilitado	El sistema Protection Storage utiliza este puerto para enviar SNMP traps al host SNMP. Utilice `snmp show trap-hosts` para ver los hosts de destino y `snmp status` para mostrar el estado del servicio.
Syslog	UDP	514	No	Deshabilitado	Si está habilitado, el sistema Protection Storage utiliza este puerto para enviar mensajes de registro del sistema. Utilice `log host show` para mostrar los hosts de destino y el estado del servicio.
RMCP	UDP	623	Open	Habilitado	Acceda de forma remota a BMC a través de IPMI.

Para llegar a un sistema Protection Storage detrás de un firewall, es posible que deba habilitar estos puertos definidos en las tablas anteriores.

Utilice la funcionalidad de filtro de red para deshabilitar todos los puertos que no se utilizan.

Configuración del firewall

Tabla 49. Puertos que Protection Storage utiliza para el tráfico entrante

Puerto	Servicio	Nota
TCP 21	FTP	Solo se utiliza si se activa FTP (ejecute `adminaccess show` en el sistema Protection Storage para determinarlo).
TCP 22	Protocolo SSH	Solo se utiliza si se activa SSH (ejecute `adminaccess show` en el sistema Protection Storage para determinarlo).
TCP 23	Telnet	Solo se utiliza si se activa Telnet (ejecute `adminaccess show` en el sistema Protection Storage para determinarlo).
TCP 80	HTTP	Solo se utiliza si se activa HTTP (ejecute `adminaccess show` en el sistema Protection Storage para determinarlo).
TCP 111	DD Boost/NFS (asignador de puertos)	Se utiliza para asignar un puerto aleatorio para el servicio `mountd` utilizado por NFS y DD Boost. El puerto del servicio `mountd` puede ser estáticamente asignado.
UDP 111	DD Boost/NFS (asignador de puertos)	Se utiliza para asignar un puerto aleatorio para el servicio `mountd` utilizado por NFS y DD Boost. El puerto del servicio `mountd` puede ser estáticamente asignado.
UDP 123	NTP	Solo se utiliza si se activa NTP (ejecute `ntp status` en el sistema Protection Storage para determinarlo).
UDP 137	CIFS (servicio de nombre NetBIOS)	CIFS utiliza este puerto para la resolución de nombres de NetBIOS.
UDP 138	CIFS (servicio de datagrama de NetBIOS)	CIFS utiliza este puerto para el servicio de datagrama de NetBIOS.
TCP 139	CIFS (servicio de sesión de NetBIOS)	CIFS utiliza este puerto para la información de la sesión.
UDP 161	SNMP (consulta)	Solo se utiliza si se activa SNMP (ejecute `snmp status` en el sistema Protection Storage para determinarlo).
TCP 389	LDAP	El servidor LDAP monitorea este puerto para las solicitudes de cliente LDAP; de manera predeterminada, utiliza TCP.
TCP 443	HTTPS	Solo se utiliza si se activa HTTPS (ejecute `adminaccess show` en el sistema Protection Storage para determinarlo).
TCP 445	CIFS (Microsoft-DS)	Puerto principal que CIFS utiliza para la transferencia de datos.
TCP 464	Active Directory	Kerberos change/set password: necesario para unirse a un dominio Active Directory.
TCP 2049	DD Boost/NFS	Puerto principal utilizado por NFS; se puede modificar mediante el comando `nfs set server-port`, que requiere el modo SE.

Tabla 49. Puertos que Protection Storage utiliza para el tráfico entrante (continuación)

Puerto	Servicio	Nota
TCP 2051	Replicación/DD Boost/Duplicación optimizada	Se utiliza solamente si se configura la replicación (ejecute `replication show config` en el sistema Protection Storage para determinarlo). Este puerto se puede modificar con la replicación.
TCP 2052	NFS Mountd/DD Boost/Duplicación optimizada	Puerto principal que utiliza NFS Mountd.
TCP 3008	RSS	Necesario cuando el sistema Protection Storage tiene un nivel Archive.
TCP 3009	SMS (administración del sistema)	Se utiliza para administrar un sistema de manera remota con Protection Storage Data Protection Central (DPC). No es posible modificar este puerto. Este puerto se utiliza solamente en sistemas Protection Storage que ejecutan DD OS 4.7.x o versiones posteriores. Este puerto debe estar abierto si planea configurar la replicación dentro de Protection Storage DPC, ya que el partner de replicación se debe agregar a Protection Storage DPC.
TCP 5001	iPerf	iPerf lo utiliza de forma predeterminada. Para cambiar del puerto, se requiere la opción `-p` desde se iperf o la opción de puerto en el comando `net iperf`. El lado remoto debe poder escuchar el nuevo puerto.
TCP 10000	NDMP	NDMP utiliza este puerto.

Tabla 50. Puertos que Protection Storage sistemas para tráfico saliente

Puerto	Servicio	Nota
TCP 20	FTP	Solo se utiliza si se activa FTP (ejecute **`adminaccess show`** en el sistema Protection Storage para determinarlo).
TCP 25	SMTP	Solo se utiliza si se activa FTP (ejecute **`adminaccess show`** en el sistema Protection Storage para determinarlo).
UDP/TCP 53	DNS	Se utiliza para realizar búsquedas de DNS cuando está configurado DNS (ejecute **`net show dns`** en el sistema Protection Storage para revisar la configuración de DNS).
TCP 80	HTTP	Se utiliza para cargar archivos de registro para dar compatibilidad al sistema Dell EMC mediante carga de soporte.
TCP 443	HTTPS	Utilizado para cargar el paquete de compatibilidad (SUB).
UDP 123	NTP	Utilizado para sincronizar en un servidor horario.
UDP 162	SNMP (trap)	Utilizado para enviar traps de SNMP a un host SNMP. Utilizado para ver los hosts de destino y el estado snmp para mostrar el

Tabla 50. Puertos que Protection Storage sistemas para tráfico saliente (continuación)

Puerto	Servicio	Nota
		estado del servicio. Use el comando **`snmp show trap-hosts`**.
UDP 514	Syslog	Si está habilitado, se utiliza para enviar mensajes de registro del sistema. Utilice registro host show para mostrar los hosts de destino y el estado del servicio.
TCP 2051	Replicación/DD Boost/Duplicación optimizada	Solo se utiliza si está configurada la replicación (ejecute **`replication show config`** en el sistema Protection Storage para determinarlo).
TCP 3009	SMS (administración del sistema)	Se utiliza para administrar un sistema de manera remota mediante Protection Storage Data Protection Central (DPC). No es posible modificar este puerto. Este puerto se utiliza solamente en sistemas Protection Storage que ejecutan DD OS 4.7.x o versiones posteriores. Si planea configurar la replicación desde Protection Storage DPC, este puerto se debe abrir. El partner de replicación se debe agregar al Protection Storage DPC.
TCP 5001	iPerf	iPerf utiliza este puerto de forma predeterminada. Para cambiar de puerto, se requiere la opción **`-p`** desde se iperf o la opción de puerto desde **`net iperf`**. El lado remoto debe poder escuchar el nuevo puerto.
TCP 27000	Comunicaciones del cliente de Protection Software con el servidor de Protection Software	Hosts de red de cliente de Protection Software.
TCP 27000	Comunicaciones del servidor Protection Software con el servidor objetivo de Replicator (comunicación de propiedad de Protection Software)	Necesario si el servidor se emplea como origen de replicación.
TCP 28001	Comunicaciones del cliente Protection Software con el servidor de administración	Clientes de Protection Software requeridos.
TCP 28002	Comunicaciones del servidor de Protection Software con el cliente de Protection Software	Opcional para buscar clientes y cancelar respaldos desde la consola de administración del administrador de Protection Software.
TCP 29000	Comunicaciones de capa de conexión segura (SSL) del cliente Protection Software con el servidor Protection Software	Clientes de Protection Software requeridos.
TCP 29000	Comunicaciones de SSL del servidor Protection Software con el servidor objetivo de Replicator	Necesario si el servidor es el origen de replicación.

Data Protection Central

Data Protection Central utiliza puertos entrantes y salientes cuando se comunica con sistemas remotos.

Tabla 51. Puertos de salida

Número de puerto	Protocolo de capa 4	Servicio
7	TCP, UDP	ECHO
22	TCP	SSO
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	TCP	DHCP
80	TCP	HTTP
88	TCP, UDP	Kerberos
111	TCP, UDP	ONC RPC
123	TCP, UDP	NTP
161 a 163	TCP, UDP	SNMP
389	TCP, UDP	LDAP
443	TCP	HTTPS
448	TCP	API REST de administrador de Search
464	TCP, UDP	Kerberos
514	TCP, UDP	rsh
587	TCP	SMPT
636	TCP, UDP	LDAPS
902	TCP	Hypervisor
2049	TCP, UDP	NFS
2052	TCP, UDP	mountd, clearvisn
3009	TCP	API REST de Protection Storage
5671	TCP	Message Bus over amqp
8443	TCP	MCSDK 8443 es una alternativa para 443
9002	TCP	API REST de Reporting & Analytics
9443	TCP	Servicio web de la consola de administración de Protection Software

Tabla 52. Puertos entrantes

Número de puerto	Protocolo de capa 4	Servicio
22	TCP	Protocolo SSH
80	TCP	HTTP
443	TCP	HTTPS
5671	TCP	Message Bus over amqp

Search

En esta sección, se muestra información sobre los puertos de red de Search.

Uso de los puertos

Tabla 53. Puertos predeterminados

Componente	Servicio	Protocolo	Puerto	Descripción
Servicio de indexación común	NGINX	TCP/HTTPS	442	Acceso seguro a Elasticsearch.
API e interfaces del usuario de Search y de administrador	NGINX	TCP/HTTPS	443	Aplicación web de administración. Aplicación web Search. API REST de administrador. API REST Search.
Servicio de indexación común	NGINX	TCP/HTTPS	445	API REST DE CIS. El servicio de indexación común (CIS) proporciona una capa segura sobre Elasticsearch.
Puertos de clúster de Elasticsearch	NGINX	TCP/HTTPS	9300–9400	Puertos para la comunicación con Elasticsearch (nodos de datos de índice). Los puertos de clúster de Elasticsearch solo se abren de forma interna y no son para el acceso externo.
Puppet	Puppet	TCP	8140, 61613	Consola, agente y servidor principal puppet. Los puertos Puppet deben estar abiertos entre nodos de Search para permitir la comunicación durante una actualización automática.
Cliente de Protection Software	Cliente de Protection Software	TCP	28000-29000, 30000-31000	Puertos para que el cliente de Protection Software se comunique con el servidor de Protection Software. Cada cliente requiere dos puertos de cada rango de puertos.
Cliente de NetWorker	Cliente de NetWorker	TCP	7937-8100	Puertos para el cliente de NetWorker que se comunican con el servidor de NetWorker.
OpenLDAP	slapd	TCP	389	Los puertos para el nodo Search que se comunican con OpenLDAP y se sincronizan entre OpenLDAP solo se abren internamente.
Protocolo SSH	sshd	TCP	22	El cliente se conecta al servidor mediante ssh.
NFS	nfs	TCP	111, 2049	Los puertos para comunicarse con NFS solo se abren internamente.

Reglas de firewall

Search requiere acceso a los siguientes puertos externos (a nivel mundial):

- 442:445 (API Web/Rest)
- 28000-29000, 30000-31000 (cliente de Protection Software)
- 7937-8100 (cliente de NetWorker)
- 22 (SSH)

Search requiere acceso a los siguientes puertos internos:

- 389 (openLDAP)
- 8140 (solo el servidor principal puppet y el nodo de servidor principal)
- 61613 (Puppet)
- 9300:9400 (Elasticsearch)
- 111, 2049 (NFS)

Para usar los puertos 9300–9400, CIS proporciona acceso a las direcciones IP dentro de una subred. Una subred de ejemplo puede ser 128.222.162.

Los nodos de Elasticsearch utilizan los puertos 9300–9400 para formar un clúster y comunicarse con otros nodos de Elasticsearch.

Reporting & Analytics

En las siguientes tablas, se muestra información acerca de los puertos de red de Reporting & Analytics. Puertos adicionales pueden ser necesarios para los agentes de Reporting and Analytics, según los sistemas que se monitoreen.

Tabla 54. Configuración de puertos de aplicaciones de Reporting & Analytics

Puerto	Descripción	Dirección del tráfico
25	El puerto TCP se utiliza para el servicio SMTP	Conexión de salida al servidor SMTP
80	El puerto TCP se utiliza para el servicio SharePoint	Conexión de salida al servidor de SharePoint
22	El puerto TCP que se utiliza para SSH	Conexión bidireccional al servidor SSH.
161	El puerto UDP se utiliza para el servicio SNMP	Conexión de salida a dispositivos SNMP
389/636 (mediante SSL)	El puerto TCP se utiliza para la integración de LDAP	Conexión de salida al servidor LDAP
3741	Puerto TCP que se utiliza para las comunicaciones de agentes de Reporting and Analytics.	Conexión saliente a agentes de Reporting and Analytics
4447	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de entrada
4712	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
4713	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
5445	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
5455	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
8090	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
9002	El puerto TCP se utiliza para el servicio HTTPS.	Conexión de entrada mediante SSL desde clientes de API REST, interfaz de usuario y CLI.
9003	Puerto TCP que se utiliza para las comunicaciones del área de almacenamiento de datos de Reporting and Analytics.	Conexión saliente al área de almacenamiento de datos de Reporting and Analytics.
9005	El puerto TCP se utiliza para la administración de JBoss	Conexión de host local
9999	El puerto TCP se utiliza para la administración de JBoss	Conexión de host local

Tabla 55. Configuración de puertos del área de almacenamiento de datos de Reporting & Analytics

Puerto	Descripción	Dirección del tráfico
3741	Puerto TCP que se utiliza para las comunicaciones de agentes de Reporting and Analytics.	Conexión entrante desde el servidor de aplicación de Reporting and Analytics.
9002	El puerto TCP se utiliza para el servicio HTTPS.	Conexión saliente a través de SSL al servidor de aplicación de Reporting and Analytics.

Tabla 55. Configuración de puertos del área de almacenamiento de datos de Reporting & Analytics (continuación)

Puerto	Descripción	Dirección del tráfico
9003	Puerto TCP que se utiliza para las comunicaciones del área de almacenamiento de datos de Reporting and Analytics.	Conexión entrante desde el servidor de aplicación de Reporting and Analytics.

Tabla 56. Configuración de puertos del agente de Reporting & Analytics

Puerto	Descripción	Dirección del tráfico
3741	Puerto TCP que se utiliza para las comunicaciones de agentes de Reporting and Analytics.	Conexión entrante desde el servidor de aplicación de Reporting and Analytics.
9002	El puerto TCP se utiliza para el servicio HTTPS.	Conexión saliente a través de SSL al servidor de aplicación de Reporting and Analytics.

Tabla 57. Configuración de puertos del clúster de Reporting & Analytics

Puerto	Descripción	Dirección del tráfico
25	El puerto TCP se utiliza para el servicio SMTP	Conexión de salida al servidor SMTP.
80	El puerto TCP se utiliza para el servicio SharePoint	Conexión de salida al servidor de SharePoint.
161	El puerto UDP se utiliza para el servicio SNMP	Conexión de salida a dispositivos SNMP.
389/636 (mediante SSL)	El puerto TCP se utiliza para la integración de LDAP	Conexión de salida al servidor LDAP.
3741	Puerto TCP que se utiliza para las comunicaciones de agentes de Reporting and Analytics.	Conexión saliente a agentes de Reporting and Analytics
4447	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de entrada
4712	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
4713	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
5445	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión bidireccional para el clúster
5455	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión bidireccional para el clúster
7500	Multidifusión mediante UDP	Conexión bidireccional para el clúster
7600	Multidifusión mediante TCP	Conexión de entrada para el clúster
8090	El puerto TCP se utiliza para la comunicación interna de los servicios	Conexión de host local
9002	El puerto TCP se utiliza para el servicio HTTPS.	Conexión de entrada mediante SSL desde clientes de API REST, interfaz de usuario y CLI.
9003	Puerto TCP que se utiliza para las comunicaciones del área de almacenamiento de datos de Reporting and Analytics.	Conexión saliente al área de almacenamiento de datos de Reporting and Analytics.

Tabla 57. Configuración de puertos del clúster de Reporting & Analytics (continuación)

Puerto	Descripción	Dirección del tráfico
9005	El puerto TCP se utiliza para la administración de JBoss	Conexión de host local
9876	Multidifusión mediante TCP	Conexión bidireccional para el clúster
9999	El puerto TCP se utiliza para la administración de JBoss	Conexión de host local
23364	Multidifusión mediante TCP	Conexión bidireccional para el clúster
45688	Multidifusión mediante TCP	Conexión bidireccional para el clúster
45689	Multidifusión mediante TCP	Conexión bidireccional para el clúster
45700	Multidifusión mediante UDP	Conexión bidireccional para el clúster
54200	Multidifusión mediante UDP	Conexión bidireccional para el clúster
54201	Multidifusión mediante UDP	Conexión bidireccional para el clúster
55200	Multidifusión mediante UDP	Conexión bidireccional para el clúster
55201	Multidifusión mediante UDP	Conexión bidireccional para el clúster
57600	Multidifusión mediante TCP	Conexión bidireccional para el clúster

Secure Remote Services

Secure Remote Services (SRS) ejecuta sus servicios en los siguientes puertos:

Los siguientes puertos se deben abrir en el servidor de gateway de Secure Remote Services (SRS) servicio. Los componentes del dispositivo (Protection Software, Protection Storage, ACM y Reporting & Analytics) se comunican con SRS mediante estos puertos.

Tabla 58. Requisitos de puertos para dispositivos

Productos de Dell EMC	Protocolo o puerto TCP	Dirección abierta	Origen o destino	Nombre de la aplicación	Tipo de comunicación (tráfico de red)	Realizado por personal autorizado de Dell EMC Global Services: objetivo de soporte (frecuencia)
Protection Software	HTTPS 9443	Saliente	a SRS	REST	Notificación de servicio	N/C
	HTTPS			ConnectEMC		
	FTP pasivo (21)					
	SMTP (25)		a SRS o al servidor SMTP del cliente			
	22	Entrante	desde SRS	CLI (mediante SSH)	Soporte remoto	Administración (ocasional)
	443			AVInstaller		Solución de problemas (frecuentes)
	80, 443, 8778, 8779, 8780, 8781, 8580, 8543, 9443, 7778, 7779, 7780 y 7781			Administrador empresarial		
	7778, 7779, 7780, 7781 y 9443			MCGUI		
Protection Storage	HTTPS 9443	Saliente	a SRS	REST	Notificación de servicio	N/C

Tabla 58. Requisitos de puertos para dispositivos (continuación)

Productos de Dell EMC	Protocolo o puerto TCP	Dirección abierta	Origen o destino	Nombre de la aplicación	Tipo de comunicación (tráfico de red)	Realizado por personal autorizado de Dell EMC Global Services: objetivo de soporte (frecuencia)
	443,25,21			ConnectEMC		
	80443	Entrante	desde SRS	Administrador empresarial	Soporte remoto	Administración (ocasional)
	22			CLI (mediante SSH)		Solución de problemas (frecuentes)
Reporting & Analytics	HTTPS 9443	Saliente	a SRS	REST	Notificación de servicio	N/C
	HTTPS			ConnectEMC		
	FTP pasivo (21)					
	SMTP (25)					
	22	Entrante	desde SRS	CLI (mediante SSH)	Soporte remoto	Solución de problemas (frecuentes)
	9002, 9003, 9004			GUI de Reporting and Analytics		
	3389			Escritorio remoto		
PowerProtect DP Series Appliance	HTTPS 9443	Saliente	a SRS	REST	Notificación de servicio	N/C
	HTTPS			ConnectEMC		
	FTP pasivo (21)					
	SMTP (25)					
	22	Entrante	desde SRS	CLI (mediante SSH)	Soporte remoto	Solución de problemas (frecuentes)
	8543			ACM		
	443			Interfaz de usuario de búsqueda, cliente web de Hypervisor Platform, interfaz de usuario de iDRAC		

Administración remota de servidores (iDRAC)

En la siguiente tabla se enumeran los puertos que se requieren para acceder a iDRAC de manera remota a través del firewall. Estos son los puertos predeterminados que iDRAC escucha para las conexiones.

Tabla 59. Los puertos que iDRAC escucha para las conexiones

Número de puerto	Tipo	Función	Puerto configurable	Nivel máximo de cifrado
22	TCP	Protocolo SSH	Sí	SSL de 256 bits
23	TCP	TELNET	Sí	Ninguno
80	TCP	HTTP	Sí	Ninguno

Tabla 59. Los puertos que iDRAC escucha para las conexiones (continuación)

Número de puerto	Tipo	Función	Puerto configurable	Nivel máximo de cifrado
161	UDP	Agente SNMP	Sí	Ninguno
443	TCP	HTTPS	Sí	SSL de 256 bits
623	UDP	RMCP/RMCP+	No	SSL de 128 bits
5,000	TCP	iDRAC a iSM	No	SSL de 256 bits
NOTA: El nivel de cifrado máximo es SSL de 256 bits si iSM 3.4 o superior y el firmware de iDRAC 3.30.30.30 o superior están instalados.				
5900	TCP	Teclado de consola virtual y redirección de mouse, medios virtuales, carpetas virtuales y uso compartido de archivos remotos	Sí	SSL de 128 bits
5901	TCP	VNC	Sí	SSL de 128 bits
NOTA: El puerto 5901 se abre cuando la función VNC está activada.				

En la siguiente tabla, se enumeran los puertos que iDRAC utiliza como cliente:

Tabla 60. Los puertos que iDRAC se utiliza como cliente

Número de puerto	Tipo	Función	Puerto configurable	Nivel máximo de cifrado
25	TCP	SMTP	Sí	Ninguno
53	UDP	DNS	No	Ninguno
68	UDP	Dirección IP del DHCP-assigned	No	Ninguno
69	TFTP	TFTP	No	Ninguno
123	UDP	Protocolo de hora de red (NTP)	No	Ninguno
162	UDP	SNMP trap	Sí	Ninguno
445	TCP	Common Internet File System (CIFS)	No	Ninguno
636	TCP	LDAP mediante SSL (LDAPS)	No	SSL de 256 bits
2049	TCP	Network File System (NFS)	No	Ninguno
3269	TCP	LDAPS para catálogo global (GC)	No	SSL de 256 bits
5353	UDP	mDNS	No	Ninguno
NOTA: Cuando Group Manager está habilitado, iDRAC utiliza mDNS para comunicarse a través del puerto 5353. Sin embargo, cuando está deshabilitado, el firewall interno de iDRAC bloquea el puerto 5353 y aparece como puerto abierto|filtrado en los análisis de puertos.				
514	UDP	Syslog remoto	Sí	Ninguno

Cloud DR

Los siguientes puertos deben estar abiertos para la comunicación entre los componentes especificados:

Tabla 61. Puertos Cloud DR requeridos

Puerto	Descripción
111	Comunicación entre Protection Storage y Cloud DR
443	Comunicación entre Cloud DR y AWS/Azure

Tabla 61. Puertos Cloud DR requeridos (continuación)

Puerto	Descripción
443	Comunicación entre Cloud DR y Cloud DR Server
443	Comunicación entre Cloud DR y Hypervisor Manager (Service)
443	Comunicación entre la VM de restauración local de servicio y AWS/Azure
2049	Comunicación entre Protection Storage y Cloud DR
9443	Comunicación entre Protection Software y Cloud DR

Cyber Recovery

En la siguiente tabla se proporcionan los puertos de red necesarios y opcionales para la implementación de Cyber Recovery. Los puertos internos solo se utilizan y se accede a estos en el entorno Cyber Recovery. Los puertos externos permiten conexiones remotas.

NOTA: Deshabilite todos los puertos de red y las interfaces que no son necesarios para su entorno.

Tabla 62. Puertos de red

Puertos	Protocolos	Propósito	Descripción	Dirección	Obligatorio
22	TCP	Protocolo SSH	Proporciona comunicación bidireccional entre el cliente SSH y los sistemas remotos en el vault Cyber Recovery.	Saliente	Sí
25	TCP	Notificaciones	Se utiliza para notificaciones por correo electrónico SMTP sobre alertas y eventos.	Saliente	Opcional
111	TCP	Cliente NFS	Se utiliza para realizar montajes de NFS entre el sistema PowerProtect DD y el host de administración de Cyber Recovery.	Bidireccional	Sí
123	TCP	NTP	Controla la sincronización de hora de Cyber Recovery a otro origen de hora de referencia.	Entrante	No
14777	TCP	Nginx	Proporciona a los navegadores web acceso HTTPS a la interfaz de usuario de Cyber Recovery.	Entrante	Sí
14778	TCP	API REST	Proporciona la conexión HTTPS para el usuario y la interfaz rest de la interfaz del usuario.	Entrante	Sí
14779	TCP	Cyber Recovery Registro Docker	Se utiliza para cargar o descargar las imágenes del contenedor de Docker. Los scripts de instalación y actualización recuperan las imágenes del registro, si es necesario.	Entrante	Sí
14780	TCP	Swagger	Proporciona acceso a la documentación de API REST de Cyber Recovery.	Entrante	Opcional
2049	TCP	Cliente NFS	Se utiliza para realizar montajes de NFS entre el sistema PowerProtect DD y el host de administración de Cyber Recovery.	Bidireccional	Sí
2052	TCP	Cliente NFS	Se utiliza para montar en el sistema PowerProtect DD.	Bidireccional	Sí
27017	TCP	MongoDB	Proporciona acceso a la base de datos que contiene las configuraciones de Cyber Recovery. El proceso de instalación configura estos puertos.	Entrante	Sí

NOTA: Si utiliza NFSv4 en el sistema PowerProtect DD, asegúrese de que `NFSv4 ID Map Out Numeric option` esté configurado en siempre.

Índice