Dispositivo Dell EMC PowerProtect de la serie DP 2.7.3

Guía del producto para DP4400 y DP5900

Febrero de 2023
Rev. 02

Notas, precauciones y advertencias

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

PRECAUCIÓN: CAUTION indica la posibilidad de daños en el hardware o la pérdida de datos y le informa cómo evitar el problema.

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

Historial de revisiones

Tabla 1. Historial de revisiones de la guía del producto Dispositivo PowerProtect serie DP

Revisión	Fecha	Descripción
01	Noviembre de 2022	Primera versión de este documento para Dispositivo PowerProtect serie DP 2.7.3

Tabla de contenido

1

Introducción

En este capítulo, se proporciona una visión general de las características y configuraciones de hardware de Dispositivo PowerProtect serie DP.

Se abordarán los siguientes temas:

Temas:

Alcance del documento y público de destino

En este documento, se describen los detalles administrativos de Dispositivo PowerProtect serie DP.

El público objetivo de este documento incluye personal de campo, partners y clientes responsables de la administración y la operación de Dispositivo PowerProtect serie DP. Este documento se creó para personas que están familiarizadas con las soluciones de Protección de datos.

Convenciones de denominación de productos y cambios de terminología

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

Tabla 2. 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	Buscar

Tabla 2. Convenciones de denominación de productos y cambios de terminología (continuación)

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

Características del producto

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

Solución integrada

Dispositivo PowerProtect serie DP es una solución integrada que ofrece funcionalidades completas de respaldo, replicación, recuperación, desduplicación, acceso y restauración instantáneos, búsqueda, creación de informes y análisis, Cyber Recovery, 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 según sus requisitos y su capacidad de almacenamiento.

- DP4400
- DP5900

El modelo PowerProtect 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 como el nodo de Backup Server, una edición virtual del sistema Protection Storage como el nodo de Protection Storage, Recuperación ante desastres en la nube, Data Protection Central como una administración centralizada del sistema, un Appliance Configuration Manager(ACM) para la configuración y las actualizaciones simplificadas, Buscar, Reporting & Analytics, y un nodo de procesamiento que aloja los componentes virtuales y el software.

DP5900 se envía como una unidad completa, con los componentes de hardware montados y cableados en la fábrica. Los modelos DP5xxx tienen Protection Storage físico y Protection Software (Service). La instalación y la configuración inicial del dispositivo Dispositivo PowerProtect serie DP DP5900 se completa mediante Servicio al cliente. Además de Protection Software como el nodo de Backup Server y Protection Storage como el nodo de Protection Storage, estos modelos Dispositivo PowerProtect serie DP incluyen Data Protection Central, Reporting & Analytics, Recuperación ante desastres en la nube, nodos de computación, un switch de red y Appliance Configuration Manager.

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

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

Los modelos DP4400 y DP5900 también tienen la solución Cyber Recovery.

Si su organización permite la comunicación a través de Internet, como parte de la configuración inicial del sistema, puede registrar los componentes Dispositivo PowerProtect serie DP, Protection Storage y Reporting & Analytics con Secure Remote Services (anteriormente ESRS). Secure Remote Services es un sistema de soporte de servicio al cliente seguro, distribuido y basado en IP 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 Dispositivo PowerProtect serie DP desde un solo panel e incluye las siguientes características.

- Un tablero integral que le permite administrar e incluye información sobre los componentes Protection Software, Protection Storage, Buscar y Reporting & Analytics.
  - Actividades de respaldo
  - Actividades de replicación
  - Activos
  - Capacity
  - Estado

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

Administración de dispositivos

ACM proporciona una interfaz basada en la 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 la expansión de la capacidad de disco de Protection Storage, cambiar la contraseña común para el dispositivo, actualizar la información del cliente y cambiar los valores en el panel General Settings. El panel General Settings 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 de ACM le permite actualizar el sistema y sus componentes. También muestra la información de estado de los componentes Appliance Server y VMware.

Administración de respaldo

Dispositivo PowerProtect serie DP utiliza servidores para los modelos DP5xxx y DP4xxx para realizar operaciones de respaldo, con los datos almacenados en un sistema Protection Storage. Por lo general, cuando se utiliza Administrator Management Console de , todos los servidores de se ven y se comportan de la misma manera. Las principales diferencias entre las configuraciones del servidor de son la cantidad de nodos y unidades de disco que se informan en la consola de Server Monitor.

También puede agregar 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 cada modelo. NDMP Accelerator utiliza Network Data Management Protocol (NDMP) para activar el respaldo y la recuperación de sistemas de almacenamiento conectado en red (NAS). El acelerador realiza el procesamiento de NDMP y envía los datos directamente al servidor de Protection Storage.

NOTA: Dispositivo PowerProtect serie DP no es compatible con el NDMP virtual (vNDMP).

Reporting and Analytics

ofrece una funcionalidad muy sólida de generación de informes con secciones dedicadas para diversas características. 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 tableros y programar la generación de informes según sus requisitos.

Buscar

La característica Buscar proporciona una manera eficaz de buscar datos de respaldo dentro de Dispositivo PowerProtect serie DP y restaurarlos en función de los resultados de Buscar. 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 Dispositivo PowerProtect serie DP.

Recuperación ante desastres

Cloud DR es una solución que permite la recuperación ante desastres de una o más instancias de Cloud DR en 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 del servicio en la nube. A continuación, puede ejecutar una prueba de recuperación ante desastres o una conmutación por error, que convierte un servicio en una instancia de Elastic Compute Cloud (EC2) de Amazon Web Services o Microsoft Azure y ejecuta esta instancia en la nube.

NOTA: La instalación de los componentes de Cloud DR, Buscar yReporting & Analytics (basado en Data Protection Advisor) 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 Dispositivo PowerProtect serie DP nuevamente. Durante la configuración de red, si selecciona el protocolo de red IPv6, entonces Cloud DR y Buscar se deshabilitan.

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

Cyber Recovery

La solución 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 aislado físicamente del sistema de producción o la red. La solución Cyber Recovery permite el acceso a CR Vault apenas 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 a fin de acelerar el proceso de replicación para que el tiempo de conexión al vault de Cyber Recovery sea lo más breve posible. En el vault de Cyber Recovery, el software Cyber Recovery crea copias de un punto en el tiempo (PIT) con bloqueo de retención, que se pueden validar y utilizar para la recuperación del sistema de producción. La implementación de la solución Cyber Recovery como parte de Dispositivo PowerProtect serie DP permite la protección de datos de misión crítica que son vulnerables a los ataques cibernéticos. Para obtener más información, consulte Recuperación de dispositivos con Cyber Recovery.

La solución Cyber Recovery solo es compatible con la instalación nueva de los sistemas DP4400 y DP5900.

Escalabilidad

Los modelos Dispositivo PowerProtect serie DP están diseñados para ser escalables, lo que permite su escalamiento vertical con las necesidades en constante cambio. Consulte la sección Expansión de la capacidad de almacenamiento en la *Guía del producto Dell EMC Dispositivo PowerProtect serie DP* 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 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 hasta un máximo de 96 TB.
- También se puede ampliar la capacidad de almacenamiento del modelo DP5xxx. Para obtener más información relacionada con la ampliación de la capacidad de almacenamiento, consulte Opciones de configuración para cada modelo.

En la siguiente tabla se detalla la configuración de los modelos Dispositivo PowerProtect serie DP.

Tabla 3. Configuración de los modelos Dispositivo PowerProtect serie DP

Modelo	Detalles de la configuración
DP4400	De 8 TB a 24 TB
	De 24 TB a 96 TB
DP5900	De 96 TB a 288 TB

Soporte unificado

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

Arquitectura y componentes del sistema

Dispositivo PowerProtect serie DP combina múltiples componentes de protección de datos en un solo producto.

Configuración detallada

PowerProtect DP Series Appliance está disponible en los siguientes modelos:

Tabla 4. Opciones de configuración para cada modelo

Modelo	Modelo de Protection Storage	Opciones de configuración de Protection Storage (TB utilizables)	Backup Server	Nodo acelerador de Avamar para respaldo de NDMP/NAS (opcional)
DP4400	Protection Storage	8, 12, 16, 20 o 24 TB	Protection Software (Service) 3 TB	NDMP Accelerator (1)
DP5900	Protection Storage 6900	144, 96, 192, 240 o 288 TB	Protection Software (Service) 3 TB	NDMP Accelerator (1-3)

Hardware de base

El siguiente hardware se incluye con los modelos de Dispositivo PowerProtect serie DP, DP4400 y DP5900:

Tabla 5. Hardware de Dispositivo PowerProtect serie DP

Modelos Dispositivo PowerProtect serie DP	Hardware
DP4400	Servidor Dell PowerEdge R740

DP5900	• Tipo de bandeja compatible: DS60 con 4 TB
	• Rack Titan-P
	  ○ Alimentación monofásica
	  ○ Conexión trifásica delta
	  ○ Conexión trifásica en estrella
	• Tres servidores Dell R640
	• Switch de puerto S4148 de Dell
	  NOTA: Los puertos Fo 1/13, Fo 1/14, Fo 1/29 y Fo 1/30 están reservados para enlaces ascendentes al entorno de red.
	• Cableado interno

Software integrado

Después de la configuración inicial, se implementan y se configuran las siguientes aplicaciones:

- Appliance Configuration Manager
- Protection Storage (DP4400 solamente).
- VMware Hypervisor Server para DP4400.
- Data Protection Central.
- Reporting & Analytics (opcional)
  - Datastore Server
  - Application Server
- Buscar (opcional)
  - Nodo primario de índice de Search
- Complemento de Cloud Disaster Recovery (opcional)
- Cyber Recovery (opcional). Puede configurar Cyber Recovery desde el tablero.

Protección automática del sistema

Dispositivo PowerProtect serie DP está configurado para protegerse contra la pérdida de datos con las aplicaciones de almacenamiento y respaldo incluidas en el sistema. El sistema está protegido con trabajos de respaldo definidos e iniciados automáticamente, que se programan a diario y tienen un período de retención de 30 días. Los metadatos del sistema se protegen mediante respaldo de punto de control para el almacenamiento de destino interno.

Tabla 6. Trabajos de respaldo de los servicios de componentes

servicios	Trabajo de respaldo
ACM	Management_VM_Backup
Hypervisor Manager (Service)	vCenter_Backup
DPA	DataProtectionAdvisor_Backup
Data Protection Central	DataProtectionCentral_Backup
Cloud DR	DataDomainCloudDisasterRecovery_Backup

NOTA: (Se aplica únicamente al modelo DP5900) Si falla uno de los servidores del clúster de PowerProtect DP Series Appliance , debe iniciar sesión inmediatamente en la GUI de **Avamar Administrator** y deshabilitar los trabajos de respaldo en la tabla *Component VM backup jobs*. Para deshabilitar los trabajos de respaldo de , consulte la Guía de administración de Avamar.

NOTA: Los trabajos de respaldo se relacionan con los servicios alojados en Dispositivo PowerProtect serie DP. Si falla uno de los servidores del clúster, puede que no sea posible tomar una instantánea del servicio, lo que provoca una falla de respaldo. Una vez que los tres servidores del clúster estén en funcionamiento, debe volver a habilitar los trabajos de respaldo desde la interfaz del usuario de Protection Software. Para obtener más información sobre cómo volver a habilitar los trabajos de respaldo a través de la interfaz del usuario de , consulte la Guía de administración de Avamar de Dell EMC.

NOTA: El componente de Buscar solo indexa los respaldos y no almacena ningún dato; por lo tanto, no se respalda el componente de Buscar. Si tiene algún problema con el componente de Buscar, elimine el componente de Buscar y vuelva a implementarlo desde el panel ACM.

Descripción general de la conectividad de red

En las tablas a continuación, se detallan las direcciones IP requeridas por Dispositivo PowerProtect serie DP para diversos componentes. Se pueden asignar como un rango de direcciones o como direcciones individuales no contiguas. 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 Dispositivo PowerProtect serie DP, se asignan las direcciones IP en un orden estándar.

NOTA: Asegúrese de que el rango de IP que asigna no esté configurado con una máscara de subred /27, ya que el rango de IP interno del dispositivo se establece con la misma máscara de subred. Además, asegúrese de que el rango de IP no sea el mismo que el rango de IP interno del dispositivo de 192.168.100.

La implementación inicial de Dispositivo PowerProtect serie DP mediante ACM es compatible con redes habilitadas para IPv4 e IPv6. Sin embargo, debe configurar manualmente las redes de doble pila.

NOTA: Los componentes Buscar, Cloud DR y Cyber Recovery no son compatibles con redes habilitadas para IPv6.

NOTA: 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. 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.

Las siguientes tablas se separan para proporcionarle información basada en el modelo sobre la dirección IP que se debe asignar a un componente. La primera columna de cada tabla en “Asignaciones de rango de direcciones IP” es el valor que se debe agregar a la primera dirección IP del rango.

DP4400

El modelo Dispositivo PowerProtect serie DPDP4400 tiene las siguientes tablas:

NOTA: La cantidad de direcciones IP requeridas en la tabla de asignaciones de rango de direcciones IP puede variar en función de los componentes opcionales que seleccionó.

Tabla 7. Asignaciones de rango de direcciones IP

Asignación de rango de IP	Ejemplo	Componente	Campo asignado
+0	`192.0.2.1`	Hypervisor	VMwareHypervisor Server servicios
+1	`192.0.2.2`	Almacenamiento con protección	IP de administración
+2	`192.0.2.3`	Almacenamiento con protección	IP de respaldo 1
+3	`192.0.2.4`	Almacenamiento con protección	IP de respaldo 2
+4	`192.0.2.5`	Aplicación de respaldo	IP del servidor
+5	`192.0.2.6`	Aplicación de respaldo	Proxy servicios
+6	`192.0.2.7`	Data Protection Central	Data Protection Centralservicio
+7	`192.0.2.8`	Reporting & Analytics (opcional)	Servicio de host de Application Server
+8	`192.0.2.9`	Reporting & Analytics (opcional)	Servicio de host de Datastore Server
+9	`192.0.2.10`	Buscar (opcional)	Servicio de host del nodo primario del índice
+10	`192.0.2.11`	Cloud DR (opcional)	Dispositivo virtual Cloud DR
+11	`192.0.2.12`	Cyber Recovery	Cyber Recovery

NOTA: Para obtener más información sobre los puertos de red y firewall que se utilizan en Dispositivo PowerProtect serie DP, consulte *Puertos de red* en la *Guía de configuración de seguridad de Dispositivo PowerProtect serie DP*.

Tabla 8. Asignaciones de rango de direcciones IP de administración con red de respaldo dedicada

Asignación de rango IP de administración	Componente	Campo asignado
+0	Hypervisor	Servicio de VMwareHypervisor Server
+1	Almacenamiento con protección	IP de administración
+2	Aplicación de respaldo	IP del servidor
+3	Aplicación de respaldo	Servicio de proxy de
+4	Data Protection Central	Data Protection Centralservicio
+5	Reporting & Analytics (opcional)	Servicio de host de Application Server
+6	Reporting & Analytics (opcional)	Servicio de host de Datastore Server
+7	Buscar	Servicio de host del nodo primario del índice
+8	Cloud DR (opcional)	Dispositivo virtual Cloud DR

Tabla 9. Asignaciones de rango de direcciones IP de respaldo con red de respaldo dedicada

Asignación de rango de IP de respaldo	Componente	Campo asignado
+0	Almacenamiento con protección	IP de respaldo 1
+1	Almacenamiento con protección	IP de respaldo 2
+2	Aplicación de respaldo	Servicio de proxy de

Tareas de servicio al cliente

En esta sección, se describen los componentes de Dispositivo PowerProtect serie DP que requieren soporte al cliente para obtener asistencia adicional.

Tabla 10. Tareas de servicio al cliente

Tarea	Descripción	Modelos de Dispositivo PowerProtect serie DP aplicables
Licencias	• Si no puede encontrar las claves de licencia correctas para cualquiera de los componentes. • Si desea obtener licencias para una mayor capacidad de almacenamiento.	Todos los modelos.
Secure Remote Services (SRS)	Para registrar los ID del sitio del cliente en el gateway de SRS.	Todos los modelos.
Servidor NDMP físico	Durante la instalación, la configuración y la actualización nuevas.	Todos los modelos.
Las últimas actualizaciones de firmware, BIOS y controladores en todos los servidores Dell	Para actualizar los modelos de Dispositivo PowerProtect serie DP en servidores de 13.ª generación (13G) y 14.ª generación (14G).	DP5900
Los servidores Dell de 13.ª generación deben tener dos unidades adicionales agregadas por servidor, lo que equivale a 7 discos SAS por ESX Server	Para actualizar los modelos de Dispositivo PowerProtect serie DP en servidores de 13.ª generación (13G).	DP5800

2

Monitoreo y administración del dispositivo

En este capítulo, se presentan las características y funcionalidades del tablero ACM.

Se abordarán los siguientes temas:

Temas:

Acerca del tablero de ACM

El tablero de ACM le permite administrar la configuración del dispositivo y los componentes individuales, actualizar la información de soporte del cliente y actualizar el software del dispositivo y sus componentes. El tablero de ACM también realiza el monitoreo del estado del sistema para el hardware del dispositivo.

Para acceder al tablero, escriba **`https://<ACM IP address>:8543/`** en un navegador web e inicie sesión. El panel requiere Google Chrome versión 64 o versiones posteriores, o Mozilla Firefox 47.2 o versiones posteriores.

NOTA: El panel se activa solamente después de configurar Dispositivo PowerProtect serie DP.

En la vista inicial, se visualiza la página **Home** y las pestañas **Health** y **Upgrade**.

Tareas de administración básicas

El tablero de ACM le permite ver los detalles del sistema, cambiar la contraseña de los componentes del dispositivo y cerrar sesión en el tablero.

Cambio de la contraseña del dispositivo

La contraseña del dispositivo es común para todos los componentes de Dispositivo PowerProtect serie DP.

1. Haga clic en el icono **Change Password**.
2. Escriba la contraseña actual en **Current Password**.
3. Escriba la nueva contraseña en **New Password** y confírmela. La contraseña debe tener entre 9 y 20 caracteres, y debe 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 (**`_`**)

     NOTA: Una contraseña con un punto (**`.`**) como último carácter (por ejemplo, ldpa1234.) no se acepta como una contraseña válida.
   - No debe comenzar con un guion (**`-`**)
   - La contraseña no debe incluir nombres comunes o nombres de usuario como **`root`** o **`admin`**.
4. Haga clic en **Change Password**. Se inicia el proceso de cambio de contraseña para ACM y todos los demás componentes de Dispositivo PowerProtect serie DP . **Password change progress** muestra la barra de progreso con descripciones del estado.

   NOTA: El proceso de apagado del dispositivo tarda aproximadamente 40 minutos en completarse.

El usuario cambia la contraseña en la siguiente secuencia:

1. Usuario de LDAP interno **`idpauser`** de ACM
2. Usuario **`sysadmin`** de almacenamiento (Protection Storage)
3. Usuarios de Backup Server (Protection Software):
   a. **`admin`** del sistema operativo y **`root`** del sistema operativo

b. Usuarios del servidor de Protection Software: **root**, **mcuser**, **repluser** y **viewuser**

4. Usuario **root** del sistema operativo del proxy del servidor de respaldo
5. Usuarios de Data Protection Central (DPC): **admin** del sistema operativo y **root** del sistema operativo
6. Usuarios de Reporting and Analytics (DPA): **root** del sistema operativo de Application Server, **root** del sistema operativo de Datastore, **administrator** de Application Server
7. **root** del sistema operativo de Search (DPS) y **root** y **admin** del LDAP predeterminado de búsqueda
8. Cloud DR Contraseña de **admin**
9. Contraseña **idpauser** de Hypervisor Manager (Service) y ESXi.
10. Contraseña de **root** de ACM.

NOTA: Después de cambiar la contraseña, los usuarios de ACM deben cerrar la sesión e iniciar sesión nuevamente con la contraseña actualizada.

NOTA: Una vez configurado Cyber Recovery, se actualizan los usuarios **root**, **admin**, **crso**, **Lockbox** y **MongoDB**.

Visualización de detalles de versión y compilación

Haga clic en el icono **Information** (**i**). En el icono **About** y, por consiguiente, la pestaña **Appliance**, muestra detalles sobre la versión de software de PowerProtect DP Series Appliance, el número de compilación y la versión de hardware.

Cerrar sesión

Haga clic en el botón **Logout**.

Tablero Appliance Configuration Manager

La pestaña **Home** proporciona una visión general del estado y la configuración de los componentes de Dispositivo PowerProtect serie DP y también muestra la configuración general y la información del cliente de Dispositivo PowerProtect serie DP.

En la pestaña **Home** del panel, puede ver los detalles del producto y la configuración de red; administrar la contraseña, la zona horaria, SMTP y la configuración de NTP; y modificar la información de soporte del cliente.

También puede configurar los ajustes de LDAP, crear y descargar paquetes de registros, descargar la configuración actual del dispositivo, apagar el dispositivo, registrar componentes con Secure Remote Services (anteriormente ESRS) e instalar componentes opcionales, como Reporting & Analytics, Buscar y Cloud DR si aún no están instalados.

También puede configurar Cyber Recovery en los modelos DP4400 y DP5900.

NOTA: Secure Remote Services (SRS) es una aplicación independiente que se puede instalar e implementar. Para obtener más información sobre SRS, consulte https://www.dell.com/support/home/product-support/product/emc-secure-remote-services/overview.

Puede configurar Secure Remote Services presente en el panel **General Settings**. Si Secure Remote Services no está configurado, puede configurarlo haciendo clic en el icono **Edit**.

Descarga de los detalles de configuración

Para descargar un archivo PDF con los detalles actuales de la configuración de Dispositivo PowerProtect serie DP, haga clic en el icono de Adobe PDF.

Administración de los componentes del sistema

La pestaña **Home** contiene los paneles para cada una de las siguientes funciones:

- **Dispositivo PowerProtect serie DP**.
- **Data Protection Central**
- **Protection Software**
- **Protection Storage**.
- **Reporting & Analytics**.

- **Buscar**.
- **CDRA**.
- **Cloud DR**.
- **Customer Information**.
- **General Settings**.

NOTA: Si hay un componente al que no se puede acceder en la red o que tiene una credencial almacenada incorrecta, el panel correspondiente le indica al usuario que resuelva el problema.

Panel Data Protection Central

El panel **Data Protection Central** muestra la versión de Data Protection Central y la dirección IP del componente.

Puede pasar el cursor sobre **Services** para ver la información de estado de los servicios de **Data Protection Central**.

Para iniciar la interfaz web, haga clic en **Data Protection Central Web UI** e inicie sesión.

NOTA: Si no se configuró LDAP externo, utilice **`idpauser`** como nombre de usuario. Si se configuró LDAP externo, utilice el nombre de usuario de LDAP externo.

Para obtener más información sobre los flujos de trabajo y las funcionalidades de **Data Protection Central**, consulte la *Guía de administración de Data Protection Central*.

Panel Protection Software

El panel **Protection Software** muestra la dirección IP del componente, la versión de , los metadatos del almacenamiento de respaldo total y disponible, el estado de la licencia del nodo de Protection Software y si la instalación de agentes está en curso.

Puede pasar el cursor sobre **Services** para ver la información de estado de los servicios de Protection Software.

Haga clic en **Protection Software Web UI** para abrir la interfaz web de Protection Software e iniciar sesión. Hay un enlace dedicado para las descargas de clientes Protection Software que está separado de la interfaz web, desde donde puede descargar los clientes .

Para obtener más información acerca de la función de los agentes de respaldo y cómo instalarlos, consulte la *Guía de administración de* .

Panel Protection Storage

El panel **Protection Storage** muestra la versión de DD OS, la dirección IP del componente, el almacenamiento de respaldo total y disponible, el sistema de archivos y el estado de la licencia del nodo de Protection Storage, y las alertas que requieren su acción.

Para acceder a una funcionalidad adicional del componente, haga clic en el enlace **Protection Storage System Manager**.

NOTA: La instancia de Protection Storage Management Center (DDMC) no puede administrar Protection Storage.

NOTA: Data Protection Central es compatible con Single Sign On (SSO) para Protection Storage. Consulte las secciones Habilitación y deshabilitación de SSO y Configuración de grupos de Single Sign On (SSO) del tema Configuración de autenticación de SSO en la *Guía de administración de Dell EMC DD OS versión 7.2* para configurar SSO desde Data Protection Central.

Cuando utilice el servidor LDAP seguro interno de Dispositivo PowerProtect serie DP, utilice las siguientes credenciales mientras realiza los pasos descritos en la sección Configuración de grupos de Single Sign On (SSO) de la *Guía de administración de Dell EMC DD OS versión 7.2*.

1. En el campo **User Group**, especifique: **`dp_admin`**
2. En el campo **Domain name**, especifique: **`idpa.local`**
3. En la lista **Management Role**, seleccione: **`admin`**

Expansión de la capacidad de almacenamiento

Puede ampliar la capacidad de almacenamiento mediante la obtención de las licencias adicionales necesarias a través del servidor de licenciamiento de Dell.

Requisitos previos

NOTA: No se admite la adición de licencias para expandir el almacenamiento directamente desde la interfaz del usuario de Protection Storage.

Sobre esta tarea

Una vez que el sistema detecta el hardware, la opción **Expand storage** aparece disponible en el menú del icono de engranaje, en el panel **Protection Storage**. Para obtener más información sobre la expansión de la capacidad de almacenamiento, consulte la sección Expansión de almacenamiento de la *Guía de instalación y actualización de Dispositivo PowerProtect serie DP* Dell EMC más reciente.

Pasos

1. En el panel **Protection Storage**, active con el mouse el icono de engranaje en la parte superior derecha y haga clic en **Expand storage**.
   Se abre el asistente **Storage expansion and license upgrade**.
2. Haga clic en **Browse** y seleccione los archivos de licencia requeridos para el almacenamiento adicional.
3. Haga clic en **Expand**.

Resultados

Después de varios minutos, el tablero refleja la mayor capacidad de almacenamiento

Para obtener información detallada sobre cómo expandir la capacidad de almacenamiento, consulte el capítulo Expansión de almacenamiento para DP4400 en la página 40.

.

Crear el primer usuario director de seguridad

Puede crear el primer usuario director de seguridad desde el tablero de ACM.

Requisitos previos

Criterios para el nombre de usuario:

- Mínimo de 1 carácter y máximo de 31 caracteres
- No debe contener caracteres especiales que no sean guion (-), guion bajo (_) y punto (.)
- Puede contener lo siguiente:
  - Una letra minúscula
  - Una letra mayúscula
  - Un dígito
  - Guion (-), guion bajo (_) o punto (.)
- Puede comenzar y finalizar con un guion bajo (_)
- No debe comenzar ni terminar con guion (-) y punto (.)

Criterios para la contraseña:

- Mínimo de 9 caracteres y máximo de 20 caracteres
- No debe comenzar con un guion (-)
- No debe contener caracteres especiales que no sean guion (-), guion bajo (_) y punto (.)
- Debe contener al menos una de las siguientes opciones:
  - Una letra minúscula
  - Una letra mayúscula
  - Un dígito
  - Cualquiera de los caracteres especiales; guion (-), guion bajo (_) y punto (.)
- La contraseña no debe incluir nombres comunes ni nombres de usuario como root o admin
- La contraseña no puede comenzar con un punto (.)
- La contraseña puede contener un máximo de tres caracteres repetidos consecutivos
- Asegúrese de que la contraseña no se base en su información de inicio de sesión personal. Por ejemplo, no debe haber ninguna cadena de caracteres común entre el nombre de usuario y la contraseña.

Pasos

1. En el panel **Protection Storage** , haga clic en el icono de **gear** y seleccione **Create First Security Officer User**.
   Se muestra el cuadro de diálogo **Create First Security Officer User**.
2. Ingrese el nombre de usuario en el campo **Username**.
3. Ingrese la contraseña en el campo **Password**.

   NOTA: Asegúrese de usar una contraseña diferente y no su contraseña de ACM.

4. Ingrese la misma contraseña en el campo **Confirm password**.
5. Haga clic en **Submit**.

Resultados

El usuario director de seguridad se creó correctamente.

NOTA: El cliente debe administrar por separado la contraseña del usuario director de seguridad. La funcionalidad Appliance Change Password no cambia esta contraseña.

Configuración de la característica de retención a largo plazo en la nube en Dispositivo PowerProtect serie DP

DD Cloud Tier se establece a través de la configuración de ACM. Siga los procedimientos que se indican a continuación para crear unidades de nube de Protection Storage y configurar políticas de respaldo de para la retención a largo plazo (LTR) en la nube.

Requisitos previos

NOTA: Las unidades de almacenamiento de nube de Protection Storage deben estar preconfiguradas en el sistema Protection Storage antes de configurarlas para el nivel de nube en la interfaz del usuario de Protection Software.

Consulte la *Guía de administración de Dell EMC DD OS* más reciente y la *Guía de integración del sistema Avamar Data Domain* más reciente disponibles en nuestro sitio de soporte (https://www.dell.com/support) para obtener más información sobre esto.

Pasos

1. En la pestaña de inicio de **ACM**, haga clic en el vínculo **Protection Storage System Manager**.
   Se mostrará la GUI de **Protection Storage System Manager**.
2. Siga el procedimiento Importación de certificados de CA en la *Guía de administración de Dell EMC DD OS* más reciente.
   Después de importar el certificado, cierre **Protection Storage Manager**.
3. Conéctese a la interfaz del usuario de a través de Data Protection Central.
   Se muestra la GUI **Avamar Administrator**.
4. Siga el procedimiento Agregar o editar un sistema Data Domain para admitir el nivel de nube en la *Guía de administración de Dell EMC DD OS* más reciente o en la *Guía de integración del sistema Avamar Data Domain*más reciente.

   NOTA: ACM hace que el paso que se refiere a Adición de un sistema Data Domain sea innecesario. Para obtener información sobre cómo acceder al cuadro de diálogo **Edit Protection Storage System**, consulte Edición de un sistema Data Domain.

5. Siga el procedimiento Creación de un nuevo grupo de niveles en la *Guía de integración del sistema Data Domain de Dell EMCAvamar* más reciente.
6. Para verificar su configuración, haga clic en el botón de inicio **Activity** en **Avamar Administrator** y revise la lista de sesiones en la pestaña **Activity Monitor**.

Panel Reporting & Analytics

En el panel **Reporting & Analytics**, se muestra la versión de DPA, las direcciones IP para Application Server y Datastore Server, el estado de licencia del nodo de y las alertas que requieren su acción.

Puede pasar el cursor sobre **Services** para ver la información de estado de los servicios de Data Protection Advisor.

Para cargar la consola de Reporting & Analytics, haga clic en el enlace **Reporting & Analytics Web UI**.

Si Reporting & Analytics no se configuró durante el proceso de configuración inicial, el panel muestra un mensaje que indica que Reporting & Analytics no está configurado. Para configurar el nodo de Reporting & Analytics, haga clic en el mensaje. Se muestra la pantalla

Reporting & Analytics Configuration. En la pantalla **Reporting & Analytics Configuration**, proporcione la información de licencia y las direcciones IP necesarias, y haga clic en **Configure**.

Dispositivo PowerProtect serie DP admite el uso de una implementación externa de Reporting & Analytics para analizar el sistema si está ejecutando una implementación corporativa de la instancia de . Sin embargo, el tablero de Dispositivo PowerProtect serie DP (ACM) no muestra ningún dato asociado con la instancia externa de Reporting & Analytics por separado. Dispositivo PowerProtect serie DP no es compatible con las funciones de búsqueda y análisis locales cuando se utilizan instancias externas de o Buscar. Además, si utiliza una instancia externa de , debe configurar y administrar cualquiera de estas instancias, ya que no se pueden configurar ni administrar a través de ACM.

Panel Buscar

El panel **Buscar** muestra la versión de Buscar, la dirección IP de Index Primary y las alertas que requieren de su atención. Para cargar la consola de Buscar, haga clic en el enlace de **Buscar**.

Coloque el cursor sobre **Services** para ver la información de estado de los servicios de Buscar.

Si Buscar no se configuró durante el proceso de configuración inicial, el panel muestra un mensaje que indica que Buscar no está configurado. Para configurar el nodo de Buscar, haga clic en el mensaje. Se muestra la pantalla Buscar Configuration. En la pantalla **Buscar Configuration**, proporcione la dirección IP requerida y haga clic en **Configure**.

Dispositivo PowerProtect serie DP es compatible con el uso de un nodo externo de Buscar si ejecuta una implementación corporativa de la instancia de Buscar. Sin embargo, el panel Buscar del tablero de Dispositivo PowerProtect serie DP (ACM) no muestra ningún dato asociado con la instancia de Buscar externa por separado. Dispositivo PowerProtect serie DP no es compatible con las funciones de búsqueda y análisis locales cuando se utilizan instancias externas de Buscar. Además, si utiliza una instancia externa de Buscar, debe configurar y administrar cualquiera de estas instancias, ya que no se pueden configurar ni administrar a través de ACM.

Configuración de clientes en Search

Para habilitar la indexación de los clientes de respaldo, se requiere configuración adicional en Search.

Consulte los procedimientos en el capítulo "Recopilaciones" de la *Guía de instalación y administración de Data Protection Search*. En la sección **Sources** del asistente de **Collections**, seleccione los clientes conectados al dispositivo.

Todos los dominios en se indexan automáticamente. Solo los dominios de cliente que se agregan después de la implementación de Search, se agregan manualmente.

Panel Cloud DR

El panel **Cloud DR** muestra la versión de Cloud DR y las alertas que requieren cualquier acción. Para cargar la consola de Cloud DR, haga clic en el enlace **Cloud DR Web UI**.

Dispositivo PowerProtect serie DP es compatible con el uso de una instancia externa de Cloud DR si está ejecutando una implementación corporativa de la instancia de Cloud DR. Sin embargo, el panel Cloud DR en el tablero de Dispositivo PowerProtect serie DP (ACM) no muestra eventos ni datos asociados con la instancia externa de Cloud DR por separado. Además, si utiliza una instancia externa de Cloud DR, debe configurar y administrar cualquiera de estas instancias, ya que no se pueden configurar ni administrar a través de ACM.

Si Cloud DR no se configura durante el proceso de configuración inicial, en el panel se muestra **Click here to configure Cloud DR**, lo que indica que Cloud DR no está configurado. Para configurar el nodo de Cloud DR, haga clic en el mensaje. Se muestra la pantalla Cloud DR Configuration. En la pantalla **Cloud DR Configuration**, proporcione la dirección IP requerida y haga clic en **Configure**.

NOTA:

- No cambie la contraseña de usuario raíz de Protection Software antes de configurar desde el tablero.
- No cambie la contraseña de usuario boost de Protection Storage antes de configurar Cloud DR desde el tablero.
- Si no se configura una cuenta de nube y una dirección de correo electrónico durante la configuración de Cloud DR, la página Cloud DR Login no funciona. Debe configurar manualmente una cuenta de nube y una dirección de correo electrónico en Cloud DR.

Cambiar la versión del servidor SNMP antes de configurar Cloud DR Server

Si utiliza Cloud DR Server con Dispositivo PowerProtect serie DP versión 2.7, antes de configurar Cloud DR Server, debe cambiar manualmente la versión de SNMP en Protection Software a la versión 2. De manera predeterminada, se agrega SNMP versión 3; por lo tanto, debe cambiar este SNMP versión 3 a SNMP versión 2.

Sobre esta tarea

Para cambiar la versión del servidor SNMP, realice los siguientes pasos:

Pasos

1. Inicie sesión en el tablero de ACM con credenciales raíz.
2. Desplácese hasta el panel Protection Software y haga clic en **Protection Software UI**.
   Se le redirigirá a la interfaz del usuario de **Avamar**.
3. Inicie sesión en la interfaz del usuario de Avamar con credenciales raíz.
4. Haga clic en **System** en el panel izquierdo.
5. Seleccione Data Domain en la pestaña superior.
   Se muestra el Data Domain que se agrega actualmente a Avamar.
6. Haga clic en **Edit** > **Account**.
7. Especifique las credenciales de DDBoostUser en el campo **`Password`** y vuelva a especificar la misma contraseña en el campo **`Verify Password`** para la verificación.

   NOTA: No modifique ningún otro campo en esta pantalla.

8. Una vez que haya especificado las credenciales, haga clic en **Validate**.
   Una vez que la validación de las credenciales especificadas por usted se realiza correctamente, se muestra el mensaje `Successfully retrieved Data Domain system information.`
9. Haga clic en **Next** y vaya a la pestaña **SNMP**.
10. En la página **SNMP**, cambie el valor a **`SNMPv2c`**.
11. En la opción **SNMP community string**, escriba **`SNMP`**.

    NOTA: No modifique ningún otro campo en esta pantalla.

12. Haga clic en **Next** y luego en **Finish**.

    NOTA: No modifique ningún otro campo en esta pantalla.

    Una vez que los pasos anteriores se realicen correctamente, se mostrará el mensaje `Updating Data Domain`. Es posible que la actualización de la configuración de Data Domain tarde un poco.

Conexión a la cuenta de la nube e incorporación de destinos de Cloud DR

Conecte Cloud DR a la cuenta de Amazon Web Services y agregue destinos a la cuenta.

Requisitos previos

- Ha iniciado sesión en Cloud DR como administrador.
- Tiene una cuenta de AWS que ya está configurada antes de conectarse a la cuenta de la nube.

NOTA: Dispositivo PowerProtect serie DP realiza la configuración de Cloud DR automáticamente.

Pasos

1. Haga clic en **Cloud Account** en la barra de menú.
   Se abre la página **Connect to Cloud Account**.
2. Haga clic en **Add Cloud Account**.
3. En el cuadro de diálogo **Connecting to AWS Cloud account**, ingrese la clave de acceso y la clave secreta para la cuenta de AWS. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys proporciona información sobre cómo obtener el acceso y las claves secretas.
4. Para copiar la política de administración de identidades y de acceso (IAM), haga clic en **Copy IAM Policy**.

   Esta acción copia en el búfer una versión JSON de los permisos mínimos de cuenta de usuario de AWS que se requieren para la implementación de Cloud DR, que luego se pueden aplicar a AWS para establecer la política de permisos para el usuario de AWS.
5. Para ver la política de administración de identidades y de acceso (IAM) que representa los permisos mínimos de cuenta de usuario de AWS que se requieren para la implementación de recuperación de Cloud DR, haga clic en **Show IAM Policy**.
6. Para guardar la cuenta de la nube de AWS, haga clic en **Verify & Save**.

Cloud DR verifica la existencia de la cuenta antes de guardar la información de la cuenta de nube y cerrar el cuadro de diálogo **Connecting to AWS Cloud account**.

NOTA: Cuando haya proporcionado credenciales para una cuenta de AWS, no podrá cambiar a otra cuenta de AWS.

Cómo agregar destinos de nube

Puede agregar uno o más destinos a la cuenta de nube que incluye la selección de un depósito de Amazon S3 y un método de cifrado.

Pasos

1. Haga clic en **Cloud Account** en la barra de menú.
   Se abre la página **Connect to Cloud Account**.
2. Haga clic en **Add Cloud DR Target** para configurar uno o más destinos de Cloud DR.
   El destino de Cloud DR es el depósito S3 en AWS donde se escriben los datos cuando los servicios se respaldan en la nube. El servidor de Cloud DR se implementa en uno de los destinos.
   Se abre el cuadro de diálogo **Add Cloud DR Target**.
3. Escriba un nombre para el destino Cloud DR.
   El nombre ingresado aquí aparece en Protection Software al crear una política de respaldo de Cloud DR.
4. Seleccione un depósito de Amazon S3 para el destino Cloud DR.
5. Haga clic en **Advance security option** y seleccione un método de cifrado:

Opción	Descripción
SSE-S3	Cifrado predeterminado (sin costo)
SSE-KMS	Cifrado de servicio de administración de claves (incurre en un costo)

   NOTA: Si selecciona el método de cifrado SSE-KMS, solo se admite la clave predeterminada administrada por el cliente. El cambio de la clave de cifrado podría causar errores con los archivos en el depósito S3 de Amazon.

   Para obtener más información sobre estos métodos de cifrado, consulte:
   - SSE-S3: https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption
   - SSE-KMS: https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption
6. Haga clic en **Add**.

Implementar Cloud DR Server

Implemente Cloud DR Server en un destino de Cloud DR específico.

Requisitos previos

- Los destinos de Cloud DR son obligatorios en la cuenta de AWS antes de realizar esta tarea. Conectarse a la cuenta de nube y agregar Nube contiene información sobre cómo agregar destinos de Cloud DR en la nube a la cuenta de AWS.
- Se deben aceptar los términos de AWS Marketplace antes de implementar el servidor de 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

Cuando se implementa Cloud DR Server, conéctese a Cloud DR Server haciendo clic en el nombre de host de Cloud DR Server.

Creación de imágenes de recuperación rápida para servicios protegidos

Puede acelerar el proceso de recuperación con anticipación mediante la creación de imágenes de recuperación rápida para los servicios protegidos.

Sobre esta tarea

La creación de una imagen de recuperación rápida inicia el proceso de rehidratación y convierte los archivos VMDK en una imagen de máquina de Amazon (AMI). A continuación, el proceso de recuperación inicia la instancia recuperada desde la AMI.

Realice este procedimiento cuando haya una nueva copia de respaldo disponible en el depósito de Amazon S3.

Pasos

1. En la interfaz del usuario de Cloud DR Server, seleccione **Protection > VM Protection** en el panel de navegación.

   El servicio protegido existente aparece en el panel derecho. En la columna **Rapid recovery image**, se indica si el servicio está habilitado para una recuperación rápida.
2. Seleccione uno o más servicios y haga clic en **Create Rapid Recovery Image**.

Resultados

- Cloud DR Server crea la AMI y elimina cualquier AMI previa para una copia anterior.
- Puede verificar los resultados mediante el análisis de la columna **Rapid recovery image**.
- Puede deshabilitar la recuperación rápida para un servicio mediante la selección de dicho servicio y haciendo clic en **Disable Rapid Recovery Image**.

- Puede monitorear el estado de protección y su progreso mediante el análisis de la columna **Protection status**.

NOTA: Cuando configure la recuperación ante desastres para los servicios del cliente que se deben restaurar en la nube mediante Cloud DR Server, AWS debe admitir la versión del SO en los servicios del cliente en el momento de la restauración. Mientras se realiza una recuperación en AWS, si la versión del kernel del SO en los servicios del cliente no es una versión de kernel compatible con AWS, las actividades de recuperación fallan con un mensaje de error.

Realizar una prueba de DR o conmutación por error en un solo servicios

En este procedimiento, se describe cómo realizar una prueba de DR o conmutación por error en un solo servicio a través de la interfaz de Cloud DR Server.

Requisitos previos

Para realizar una prueba de DR o conmutación por error de un servicio mediante la interfaz de Cloud DR Server, debe tener instancias de servicios que cuenten con el software de respaldo en las instalaciones y con la copia en la nube.

Sobre esta tarea

Para garantizar una conmutación por error exitosa y prepararse mejor para un desastre, las mejores prácticas recomiendan probar varios escenarios de recuperación ante desastres. Después de realizar una prueba de DR, puede promover la prueba a una conmutación por error.

Cuando ocurre un error operacional o un desastre en las instalaciones, puede conmutar un servicio a la nube pública. Cuando se resuelve el problema en las instalaciones, puede conmutar por recuperación el servicio al entorno en las instalaciones.

NOTA: Al realizar conmutaciones por error, debe conmutar por error los servicios en el orden correcto para garantizar el funcionamiento continuo de los servidores y las aplicaciones.

Pasos

1. En la interfaz del usuario de servidor de Cloud DR, seleccione **Recovery > VM Recovery**.

   También puede abrir la página **VM Recovery** desde el tablero al hacer clic en **See All** en el panel **Recovery**.

   Se abre la página **VM Recovery**.
2. Seleccione el servicio que desee recuperar y haga clic en **DR Test** o **Failover**.

   Si hace clic en **Failover** y nunca se ha probado el servicio, un mensaje le pregunta acerca de esta condición. Se recomienda ejecutar una prueba de DR antes de implementar una conmutación por error. El mensaje también recomienda que cierre el servicio de producción para evitar una posible pérdida de datos causada por el acceso accidental del usuario.

   Haga clic en **Select Copy** para continuar.
3. En la ventana **Copy and Network**, seleccione la copia del servicio y la red donde desea iniciar la instancia de EC2.

   En la sección **Advanced Options**, en la parte inferior de la ventana, se indica el tipo de instancia de EC2 autoseleccionada y el grupo de seguridad que se usará para el proceso de recuperación.
4. Si no desea utilizar el tipo de instancia de EC2 autoseleccionada o el grupo de seguridad,, expanda **Advanced Options** y seleccione un tipo de instancia de EC2 alternativa y uno o más grupos de seguridad.
5. Haga clic en **Start DR Test** o **Start Failover**.

Resultados

Comienza el proceso de recuperación y es posible monitorear el progreso en la página **DR Activities**. Durante el proceso de recuperación:

1. Si el servicio no está habilitado para la recuperación rápida, se inicia una instancia de servicio de restauración temporal en cada región donde se necesita recuperación. Esta instancia realiza la hidratación durante la recuperación y finaliza automáticamente después de 10 minutos de tiempo de inactividad.
2. El servidor de Cloud DR, a continuación, convierte el VMDK en AMI y se inicia una instancia de EC2 que se basa en AMI.
3. Cuando se ejecuta la instancia de EC2, el servidor de Cloud DR elimina el VMDK y AMI.

Panel Cyber Recovery

El panel **Cyber Recovery** muestra la dirección IP o el nombre de host, la versión, el tipo de bloqueo de retención, el estado de la licencia y el estado de Cyber Recovery.

Puede pasar el cursor sobre **Services** para ver la información de estado de los servicios de Cyber Recovery. Haga clic en **Cyber Recovery Web UI** para iniciar la interfaz de Cyber Recovery. Para obtener más información acerca de Cyber Recovery, consulte la *Guía del producto PowerProtect Cyber Recovery*.

Si Cyber Recovery no está configurado, el panel muestra **Click here to configure Cyber Recovery**, lo que indica que no está configurado. Para configurar Cyber Recovery, haga clic en el mensaje. Se muestra la ventana **Cyber Recovery Configuration**.

> ⚠ 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.

Panel Appliance

El panel **Appliance** muestra información acerca de la versión del dispositivo y del hardware que está utilizando.

Pase el cursor sobre la versión de hardware para ver los detalles de la versión de hardware, como la dirección IP y la versión de Hypervisor, la dirección IP y la versión de Hypervisor Manager, y la versión de firmware del dispositivo.

Panel Customer Information

El panel **Customer Information** muestra la información de contacto del administrador. También muestra la ubicación o la información del sitio. También puede modificar la dirección de correo electrónico y la dirección del servidor SMTP para enviar alertas por correo electrónico cuando el sistema encuentra un error irrecuperable o crítico.

Sobre esta tarea

Para ver el valor completo de un elemento, pase el cursor sobre él. Realice las siguientes acciones para cambiar la información del cliente:

Pasos

1. Haga clic en el icono **Edit** junto al valor que desea modificar.
   a. Ingrese el nombre del administrador en el campo **Admin name** y haga clic en **Save**.
   b. Ingrese el número de contacto del administrador en el campo **Admin contact number** y haga clic en **Save**.
   c. Ingrese el nombre de la empresa en el campo **Company Name** y haga clic en **Save**.
   d. Ingrese la ubicación de Dispositivo PowerProtect serie DP en el campo **Location** y haga clic en **Save**.
   e. Ingrese el ID de sitio de Dispositivo PowerProtect serie DP en el campo **Site ID** y haga clic en **Save**.
2. Haga clic en el icono de **Gear** y seleccione **Email Configuration**.
   Aparecerá el cuadro de diálogo **Email Configuration**.
   a. Ingrese la dirección IP del servidor SMTP en el campo **SMTP server**.
   b. El campo **Port** se completa automáticamente y especifica el puerto SMTP predeterminado.
   c. Ingrese la dirección de correo electrónico en el campo **Administrator email**.
      El sistema envía una alerta por correo electrónico a esta dirección de correo electrónico cuando el sistema encuentra un error crítico o irrecuperable.
   d. Haga clic en **Test Email** para enviar un correo electrónico a la dirección que especificó.
   e. Haga clic en **Configure**.
      El sistema guarda los cambios realizados en las configuraciones de correo electrónico.

Verificar el ID de sitio

Puede verificar su número de ID de sitio en el sitio web de Soporte en línea.

Sobre esta tarea

Para verificar el ID de sitio, realice las siguientes acciones:

Pasos

1. Inicie sesión en el sitio web de Soporte en línea con sus credenciales.
2. Seleccione **Centro de servicios**.
3. En la página centro de servicios, debajo del área de sites y contratos, haga clic en **Administer un site**.
4. Asegúrese de que el sitio donde esté instalado el sistema de almacenamiento figure en el área **My Sites**.

   NOTA: También puede buscar un sitio y agregarlo a la lista **My Sites** list. 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.

Panel General Settings

El panel **General Settings** muestra los ajustes básicos, incluidos zona horaria, LDAP externo, NTP, Secure Remote Services (SRS), DNS, gateway y modo FIPS.

Sobre esta tarea

Para ver el valor completo de un elemento, pase el cursor sobre él. Realice las siguientes acciones para cambiar la información de configuración general:

Pasos

1. En el panel **General Settings**, haga clic en el icono de engranaje y seleccione la configuración que desea cambiar.
2. Seleccione o escriba un nuevo valor:
   - **Time zone**: seleccione la zona horaria de la lista y haga clic en **Save**. Se actualiza la zona horaria para Protection Software, Protection Storage, los nodos de Reporting & Analytics y Search, ACM y el servidor del host de Hypervisor.

     NOTA: Si se cambia esta configuración, el nodo de Protection Storage se reinicia automáticamente.
   - **External LDAP**: consulte Configurar el ambiente LDAP externo para obtener más información.
   - **Secure Remote Services**: ingrese el valor de **SRS gateway IP address** y sus credenciales de **RSA Secure ID** y, a continuación, haga clic en **Configure**.
   - **NTP server IP address**: para cambiar la dirección IP del gateway, consulte Cambiar la dirección IP del servidor NTP en la página 27.

     NOTA: No utilice un nombre de servidor en este campo.
   - **Configure DNS**: para cambiar la dirección IP del servidor DNS primario y secundario, consulte Cambiar el servidor DNS en la página 28.
   - **Configure Gateway**: para cambiar la dirección IP de la puerta de enlace, consulte Cambiar la dirección IP del gateway en la página 28.
   - **FIPS Mode**: los Estándares Federales de Procesamiento de la Información (FIPS) se pueden habilitar en Dispositivo PowerProtect serie DP. FIPS está desactivado de forma predeterminada. Consulte la *Guía de configuración de seguridad de Dispositivo PowerProtect serie DP* para obtener más información sobre cómo habilitar el modo FIPS.

Configurar el entorno de LDAP externo

La opción **Configure external LDAP** está disponible en el tablero de ACM, en el panel **General Settings** del menú del icono de engranaje. La opción **Configure external LDAP** en el tablero de ACM se utiliza para configurar los ajustes de LDAP.

Sobre esta tarea

De manera predeterminada, Dispositivo PowerProtect serie DP está configurado para utilizar la configuración de LDAP interno. Sin embargo, la opción **Configure external LDAP** le permite cambiar esta configuración predeterminada a una configuración de LDAP externo.

NOTA: Cyber Recovery no es compatible con la integración de LDAP/AD.

Puede usar el nombre de usuario y la contraseña de LDAP para iniciar sesión en los componentes Protection Storage, Protection Software, Data Protection Central (DPC), Reporting & Analytics (DPA) y Buscar del dispositivo. Para configurar los ajustes de LDAP de

otros componentes del dispositivo, como Hypervisor y Hypervisor Manager, consulte la documentación del componente correspondiente. También puede consultar el capítulo Seguridad del producto y del subsistema en la *Guía de configuración de seguridad de Dell EMC Dispositivo PowerProtect serie DP* para obtener más información.

Tenga en cuenta que no puede ver los ajustes existentes de LDAP en el cuadro de diálogo **Configure external LDAP**. Si desea ver la configuración de LDAP, haga clic en el icono de PDF **Download current configuration** en el área superior derecha del tablero de ACM. Dispositivo PowerProtect serie DP genera un archivo PDF con información de configuración del dispositivo, incluidos los ajustes actuales de LDAP.

Para configurar los ajustes de LDAP, realice los siguientes pasos.

Pasos

1. En el tablero de ACM, en la esquina superior derecha del panel **General Settings**, seleccione la opción **Configure external LDAP** en el menú desplegable del icono de engranaje.

   Aparece el cuadro de diálogo **LDAP settings**.
2. En el cuadro de diálogo **LDAP settings**, realice lo siguiente:
   a. En el campo **LDAP type**, seleccione **AD** u **OPENLDAP**.
   b. Seleccione la casilla de verificación **Secure LDAP** para verificar que el LDAP sea seguro.
   c. En el campo **Server hostname**, ingrese el nombre del servidor LDAP.
   d. En el campo **Domain name**, ingrese el nombre de dominio.
      - El dominio al que pertenece **Server hostname** debe ser el mismo que el **Domain name** especificado.
      - El nombre de dominio puede tener caracteres alfanuméricos y caracteres especiales.
   e. En el campo **Query username**, ingrese el nombre de usuario de consulta.

      El nombre de usuario de consulta puede tener caracteres alfanuméricos y caracteres especiales (`-`, `_`, `.`, `,` y `=`).
   f. En el campo **Query password**, ingrese la contraseña del usuario.

      La contraseña de consulta debe contener un mínimo de 9 a 20 caracteres, al menos una letra minúscula, una letra mayúscula, un dígito y cualquiera de los caracteres especiales admitidos (`-`, `_`, y `.`).
   g. En **Admin group name**, ingrese el nombre del grupo de administradores.

      Admin group name distingue mayúsculas de minúsculas y debe ser idéntico al nombre del grupo ingresado en el servidor de LDAP. Si hay una incompatibilidad en los nombres, la configuración fallará.

      Ya debe tener agregados los usuarios necesarios y haber proporcionado los privilegios adecuados a aquellos usuarios que necesitan acceso a DPC, ya que DPC se utiliza para acceder a las interfaces del usuario de los componentes del dispositivo o conectarse a ellas. Para obtener más información, consulte la sección Orígenes de identidad en Data Protection Central de la *Guía de administración de Dell EMC Data Protection Central versión 19.5*, que está disponible en el sitio web de soporte en línea en https://www.dell.com/support/home.
   h. Ingrese el número de puerto en el campo **Port number**.
   i. Haga clic en **Validate** para comprobar la validación de la configuración de LDAP.
   j. Haga clic en **Submit** y luego en **Close**.
      La configuración se actualiza al entorno de LDAP externo.
   k. Haga clic en **Close**.

Actualizar la contraseña de LDAP externo

Sobre esta tarea

En esta sección, se describe cómo cambiar la contraseña de todos los componentes de Dispositivo PowerProtect serie DP que están configurados con LDAP.

Pasos

1. En el tablero de ACM, vaya al panel **General Settings** y haga clic en la opción **Configure external LDAP** en el menú desplegable del icono de engranaje.
2. Seleccione **Update External LDAP password**.

   Solo se puede acceder al campo **Query password** después de seleccionar este campo.
3. Ingrese la nueva contraseña para el usuario de consulta de LDAP y haga clic en **Validate**.
4. Haga clic en **Save** para guardar la contraseña nueva.
   La contraseña se cambia para todos los componentes del dispositivo configurados con LDAP.

Revertir al entorno de LDAP interno

De manera predeterminada, Dispositivo PowerProtect serie DP utiliza la configuración de LDAP interno. Sin embargo, si cambió esta configuración predeterminada a una configuración de LDAP externo y necesita revertirla a una configuración de LDAP interno, realice los siguientes pasos:

Sobre esta tarea

Considere un escenario en el que haya cambiado la contraseña común del dispositivo después de configurar LDAP externo. En tales casos, la cuenta de LDAP interno sigue asociada con la contraseña común anterior del dispositivo que estaba en uso antes de que se configurara LDAP externo.

Para crear o verificar una contraseña de LDAP interno, consulte la sección Solución de problemas de LDAP.

Pasos

1. Actualice la configuración de LDAP desde el tablero de ACM mediante los siguientes valores:
   - LDAP type: *OPENLDAP*
   - Secure LDAP: *marcado/seleccionado*
   - Server hostname: *<ACM_NOMBREDEHOST_FQDN>*
   - Domain name: *dc=idpa,dc=local*
   - Query username: *uid=idpauser,ou=People,dc=idpa,dc=local*
   - Query password: *<Contraseña de la cuenta de usuario de LDAP interno>*
   - Admin groupname: *dp_admin*
   - Port number: *636*
2. Conéctese a ACM mediante un cliente SSH.
3. Modifique los siguientes ajustes en el archivo `/usr/local/dataprotection/var/configmgr/server_data/config/commonconfig.xml file:`

   `<useExternalLdapSettings>true</useExternalLdapSettings>` para `<useExternalLdapSettings>false</useExternalLdapSettings>`

Cambiar la dirección IP del servidor NTP

En esta sección, se describen los pasos para cambiar la dirección IP del servidor NTP desde el tablero de ACM.

Requisitos previos

Asegúrese de verificar lo siguiente antes de cambiar la dirección IP del servidor NTP:

- La nueva IP es válida y es accesible desde todos los componentes del dispositivo.
- La IP de red privada se utiliza para conectarse a la interfaz del usuario del tablero de ACM.
- La dirección IP está en la misma red o máscara de subred.

PRECAUCIÓN: El cambio del servidor NTP en ACM no se refleja en ninguno de los proxies externos. Debe actualizar manualmente los proxies externos; si no los actualiza, se producirá una falla en el respaldo.

Sobre esta tarea

Para cambiar la dirección IP del servidor NTP, realice uno de los siguientes pasos:

Pasos

1. En el panel **General Settings**, haga clic en el icono de **engranaje** y seleccione **Configure NTP**.
   Se muestra la ventana **Update NTP**.
2. Ingrese la dirección IP en el campo **NTP server IP address**.
3. Haga clic en **Guardar**.

   El sistema valida la dirección IP del servidor NTP y la ventana **Update NTP** muestra la barra de progreso con el estado de actualización de NTP.
   - Si las validaciones se realizan correctamente, el estado se muestra como **Completed**.
   - Si las validaciones fallan, el estado se muestra como **Failed**.
4. Haga clic en **Finalizar**.

Si las validaciones fallan o si hay algún error, consulte la sección de requisitos previos para resolver los errores e inicie el procedimiento nuevamente.

NOTA: Si falla la actualización de NTP para un componente, los otros componentes restantes en los que se configura el nuevo NTP también se revierten al NTP anterior.

El panel **General settings** muestra la nueva dirección IP del servidor NTP y también se actualiza correctamente en todos los componentes.

Cambiar el servidor DNS

En esta sección, se describen los pasos para cambiar la dirección IP del servidor DNS desde el tablero de ACM.

Requisitos previos

Asegúrese de verificar lo siguiente antes de cambiar la dirección IP del servidor DNS:

- Búsqueda directa e inversa para la nueva dirección IP del servidor DNS
- FQDN del SO para la nueva dirección IP del servidor DNS
- El nuevo servidor DNS debe tener el mismo mapeo de IP-FQDN que en el servidor DNS antiguo existente para todas las direcciones IP utilizadas por los componentes del dispositivo.
- No hay componentes con error de desincronización

PRECAUCIÓN: El cambio del servidor DNS en ACM no se refleja en ninguno de los proxies externos. Debe actualizar manualmente los proxies externos; si no los actualiza, se producirá una falla en el respaldo.

Sobre esta tarea

Para cambiar el servidor DNS, realice las siguientes acciones:

Pasos

1. En el panel **General Settings** haga clic en el icono de **Gear** y seleccione **Configure DNS**.
   Se muestra la ventana **Update DNS server**.
2. Ingrese la dirección IP en los campos **Primary DNS server IP address** y **Secondary DNS server IP address**.

   NOTA: Secondary DNS server IP address es un campo opcional.

3. Haga clic en **Save**.

   El sistema valida la dirección IP de DNS y la ventana **Update DNS server** muestra la barra de progreso con el estado de actualización de DNS.
   - Si las validaciones se realizan correctamente, el estado se muestra como **Completed**.
   - Si las validaciones fallan, el estado se muestra como **Failed**.
4. Haga clic en **Finish**.

   Si las validaciones fallan o si hay algún error, consulte la sección de requisitos previos para resolver los errores e inicie el procedimiento nuevamente.

   El panel **General settings** muestra la nueva dirección IP de DNS y también se actualiza correctamente en todos los componentes.

Cambiar la dirección IP del gateway

En esta sección, se describen los pasos para cambiar la dirección IP del gateway desde el tablero de ACM.

Requisitos previos

Asegúrese de verificar lo siguiente antes de cambiar la dirección IP del gateway:

- Se puede acceder a DNS, NTP, SMTP, LDAP y todos los componentes a través de este gateway.
- La IP de red privada se utiliza para conectarse a la interfaz del usuario del tablero de ACM.
- La IP del gateway está en la misma red o máscara de subred.
- Para el modelo DP5xxx, si se requieren cambios de VLAN, se debe actualizar en el switch TOR, los nodos de hipervisor y alfmacenamiento con protección antes de cambiar el gateway.

PRECAUCIÓN: El cambio de la dirección IP del gateway en ACM no se refleja en ninguno de los proxies externos. Debe actualizar manualmente los proxies externos; si no los actualiza, se producirá una falla en el respaldo.

Sobre esta tarea

Para cambiar el gateway, realice las siguientes acciones:

Pasos

1. En el panel **General Settings** , haga clic en el icono de **Gear** y seleccione **Configure Gateway**.
   Se muestra la ventana **Update Gateway**.
2. Ingrese la dirección IP en el campo **Gateway IP address**.
3. Haga clic en **Save**.
   El sistema valida la dirección IP del gateway y la ventana **Update Gateway** muestra la barra de progreso con el estado de actualización del gateway.
   - Si las validaciones se realizan correctamente, el estado se muestra como **Completed**.
   - Si las validaciones fallan, el estado se muestra como **Failed**.
4. Haga clic en **Finish**.
   Si las validaciones fallan o si hay algún error, consulte la sección de requisitos previos para resolver los errores e inicie el procedimiento nuevamente.
   El panel **General settings** muestra la nueva dirección IP del gateway y también se actualiza correctamente en todos los componentes.

Eliminar componentes opcionales

En esta sección, se describen los pasos para eliminar los componentes opcionales que están configurados en el dispositivo.

Requisitos previos

- Asegúrese de que no haya operaciones del tablero de ACM en curso, como un cambio de contraseña, una actualización de NTP, etc.
- La funcionalidad de eliminación solo está disponible si el dispositivo tiene componentes opcionales configurados.

Sobre esta tarea

Los componentes opcionales, como Data Protection Central (DPC), Data Protection Advisor, Buscar, Reporting & Analytics y Cloud DR se pueden eliminar mediante la funcionalidad **Delete** disponible en el icono de engranaje.

AVISO: Después de quitar el DPC del dispositivo, no puede reinstalarlo.

Realice los siguientes pasos para eliminar los componentes opcionales:

Pasos

1. Vaya al tablero de ACM.
2. Seleccione cualquiera de los siguientes componentes opcionales:
   - **Data Protection Central**
   - **Reporting & Analytics**
   - **Buscar**
   - **Cloud DR**
3. Haga clic en el icono de engranaje del componente opcional correspondiente.
   Cada panel de componente tiene el icono de engranaje en la parte superior derecha.
4. Seleccione la opción **Delete**.
   Por ejemplo, para eliminar Data Protection Central, seleccione **Delete DPC**
   AVISO: Una vez que elimine estos componentes opcionales, los datos asociados se eliminarán permanentemente. Además, una vez que los elimine, no podrá aprovechar ni utilizar las características o funcionalidades proporcionadas por ellos.
   .
5. Haga clic en **Yes** en la ventana de confirmación.

La operación de eliminación elimina correctamente el componente opcional correspondiente.

6. Haga clic en **OK**.

Apagar Dispositivo PowerProtect serie DP

Puede apagar Dispositivo PowerProtect serie DP desde la consola de ACM.

Requisitos previos

- Asegúrese de que no haya trabajos de respaldo en ejecución en Protection Software Backup Server.
  - Si hay trabajos de respaldo en ejecución en Protection Software Backup Server cuando la operación de apagado de Dispositivo PowerProtect serie DP está en curso, dicha operación espera a que los trabajos de Protection Software se completen con el estado `Waiting for shutdown of Backup Server`.
  - Se recomienda esperar a que se completen los trabajos de respaldo. Sin embargo, si debe apagar el dispositivo inmediatamente, tendrá que iniciar sesión en la interfaz del usuario de Protection Software y cancelar los trabajos de respaldo que están en curso.
- Apagar Dispositivo PowerProtect serie DP requiere la intervención física o el uso de iDRAC para reiniciar el sistema. Si está apagando de forma remota los dispositivos Dispositivo PowerProtect serie DP, asegúrese de tener acceso físico al sistema o de haber configurado iDRAC en el sistema.

Sobre esta tarea

Para apagar Dispositivo PowerProtect serie DP, realice las siguientes acciones:

Pasos

1. En el tablero de ACM, pestaña **Home**, haga clic en el icono **Shutdown Appliance**.
2. Ingrese la contraseña raíz de ACM y haga clic en **Yes**.
   Se muestra el progreso de apagado del dispositivo. Dispositivo PowerProtect serie DP apaga los componentes en el siguiente orden:
   - Protection Software
   - Buscar
   - Reporting & Analytics
   - Data Protection Central
   - Agente de Recuperación ante desastres en la nube
   - Protection Storage
   - Appliance Configuration Manager
   - Hypervisor Server
   - Nodo de computación

   Si el apagado iniciado por ACM no puede apagar **Backup Server** y **Protection Storage**, o ambos, ACM muestra un mensaje en el que se enumeran los componentes que no se pudieron apagar. Posteriormente, ACM continúa apagando los demás componentes.

   Para DP4400, después de apagar todos los productos puntuales, el hipervisor necesita 15 minutos para entrar en modo de mantenimiento y apagarse. Si el hipervisor no se apaga, debe apagar manualmente el hipervisor. El apagado de DP4400 tarda más de 30 minutos. Para obtener más información sobre cómo apagar el hipervisor de forma manual, consulte Apagado manual del hipervisor

   Si alguno de los componentes no se puede apagar, debe apagarlo manualmente. Para obtener más información sobre el apagado manual de los componentes de Dispositivo PowerProtect serie DP, consulte Solución de problemas de apagado

Iniciar Dispositivo PowerProtect serie DP

El siguiente procedimiento se aplica solo al modelo DP5900. Dispositivo PowerProtect serie DP El modelo DP4400 solo tiene un servidor de Hypervisor y el encendido de ese servidor de Hypervisor garantiza el encendido de todos los productos puntuales de Dispositivo PowerProtect serie DP en la secuencia requerida.

Sobre esta tarea

Encender Dispositivo PowerProtect serie DP requiere el inicio de los componentes individuales en el orden correcto.

Pasos

1. Encienda el sistema Protection Storage.
2. Encienda las instancias de NDMP Accelerator si están incluidas en la configuración.

NOTA: No continúe hasta que Protection Storage y todas las instancias de NDMP Accelerator se hayan inicializado completamente. Para verificar que el sistema Protection Storage esté completamente inicializado, inicie sesión en el sistema Protection Storage con **`sysadmin`** como el *nombre de usuario* y, para la *contraseña*, utilice la contraseña común de Dispositivo PowerProtect serie DP. Compruebe el estado del sistema de archivos mediante el comando `filesys status`. El sistema de archivos debe estar en funcionamiento. Para verificar que las instancias de NDMP Accelerator estén completamente inicializadas, conéctese al nodo acelerador mediante **SSH**.

3. Para configuraciones con implementación física de Protection Software, encienda el nodo de utilidad y los nodos de almacenamiento. Este paso no es necesario para las configuraciones con Protection Software virtual.
4. Inicie sesión en la GUI de administrador de Protection Software para asegurarse de que el dispositivo esté encendido y que Protection Software esté completamente inicializado.
5. En el modelo Dispositivo PowerProtect serie DP DP5900, encienda cada una de las instancias de los ESXi servers, desde el servidor de hipervisor inferior hacia arriba.

Resultados

El proceso restante finaliza automáticamente. Una vez que se encienden los servidores de Hypervisor, Dispositivo PowerProtect serie DP inicia automáticamente todos los demás componentes.

Para conocer los problemas durante el inicio, consulte Solución de problemas para el inicio.

NOTA: Después de que Dispositivo PowerProtect serie DP se inicia correctamente, puede conectarse al tablero de ACM y monitorear el progreso del inicio. Si hay una falla en el inicio, la aplicación muestra un mensaje de error con una opción para acceder a la página del tablero de ACM.

Acceder a componentes con un navegador

Además de hacer clic en los enlaces del panel ACM, puede acceder a la interfaz del usuario para los componentes individuales; para ello, navegue hasta la ubicación de red correspondiente y escriba el nombre de usuario y la contraseña.

En cada una de las siguientes secciones, *<component_ip>* se refiere a la dirección IP del componente. Las credenciales de Buscar y Data Protection Central están determinadas por su configuración de LDAP. Data Protection Central se utiliza para acceder o conectarse a las interfaces de usuario de los productos puntuales respectivos. Data Protection Central utiliza Single Sign On cuando intenta acceder a la interfaz del usuario de un producto puntual específico.

Las referencias de LDAP de la siguiente tabla se aplican solo a los componentes Data Protection Central y Buscar. El dispositivo y otros componentes no utilizan los ajustes de LDAP configurados desde ACM.

NOTA: Asegúrese de utilizar Flash versión 27.0.0.183 o posterior para acceder al cliente web de Hypervisor.

Tabla 11. Acceso a los componentes

Componente	Ubicación	SSO desde Data Protection Central	Nombre de usuario
Administrador del cliente Protection Software	**`https://<component_ip>/aam`**	Sí	**`MCUser`**
Interfaz del usuario de Protection Software	**`https://<component_ip>/mcui`**	Sí	**`MCUser`**
Interfaz del usuario de Protection Storage	**`https://<component_ip>`**	Sí, puede configurar esto manualmente. Consulte las secciones Habilitación y deshabilitación de SSO y Configuración de grupos de Single Sign On (SSO) del tema Configuración de autenticación de SSO en la *Guía de administración de Dell EMC DD OS versión 7.2* para	**`Administrador de sistema`**

Tabla 11. Acceso a los componentes (continuación)

Componente	Ubicación	SSO desde Data Protection Central	Nombre de usuario
		configurar SSO desde Data Protection Central.	
Interfaz del usuario de DPC	**https://<component_ip>**	No se aplica	**<username>@<domain>** **NOTA:** Si LDAP externo no se ha configurado, entonces el nombre de usuario predeterminado es **idpauser**.
Interfaz del usuario de DPA	**https://<component_ip>:9002/dpaui/jsp**	Sí	**administrador**
Interfaz del usuario de Buscar	**https://<component_ip>/admin/#/login**	Sí	**<username>@<domain>** **NOTA:** Si LDAP externo no se ha configurado, entonces el nombre de usuario predeterminado es **idpauser**.
Cliente web de Hypervisor	**https://<component_ip>**	No	**idpauser**
Recuperación ante desastres en la nube	**https://<component_ip>**	No	El nombre de usuario es **admin**
Cyber Recovery	**https://<component_ip>:14777No**	No	**crso**

Cuentas de usuario para los componentes

La configuración de Dispositivo PowerProtect serie DP utiliza las cuentas de usuario en Componente y asignación de la cuenta de usuario en la página 32. De manera predeterminada, estas cuentas utilizan la contraseña común Dispositivo PowerProtect serie DP que se establece en el panel **General Settings** de la interfaz del usuario de ACM.

Tabla 12. Componente y asignación de la cuenta de usuario

Componente	Nombre de usuario	Password
ACM	root	Contraseña común proporcionada durante la configuración del dispositivo.
ACM (LDAP interno)	idpauser	Contraseña común proporcionada durante la configuración del dispositivo.
ACM (si LDAP externo está configurado)	Credenciales de LDAP correspondientes	Contraseña de LDAP externo, según corresponda.
DPC (si no está configurado LDAP externo)	idpauser	Contraseña común proporcionada durante la configuración del dispositivo.
DPC (si LDAP externo está configurado)	Credenciales de LDAP correspondientes	Contraseña de LDAP externo, según corresponda.
DPC (como usuario local desde la interfaz del usuario de DPC)	administrator@dpc.local	Contraseña común proporcionada durante la configuración del dispositivo.
Protection Software (si no está configurado LDAP externo)	admin	Contraseña común proporcionada durante la configuración del dispositivo.
Protection Software (si está configurado LDAP externo)	Credenciales de LDAP correspondientes	Contraseña de LDAP externo, según corresponda.

Tabla 12. Componente y asignación de la cuenta de usuario (continuación)

Componente	Nombre de usuario	Password
Protection Storage (si no está configurado LDAP externo)	sysadmin e idpauser	Contraseña común proporcionada durante la configuración del dispositivo.
Protection Storage (si está configurado LDAP externo)	Credenciales de LDAP correspondientes	Contraseña de LDAP externo, según corresponda.
Reporting & Analytics (si no está configurado LDAP externo)	administrador	Contraseña común proporcionada durante la configuración del dispositivo.
Reporting & Analytics (si está configurado LDAP externo)	Credenciales de LDAP correspondientes	Contraseña de LDAP externo, según corresponda.
Buscar	Credenciales de LDAP correspondientes. Si LDAP externo no está configurado, use idpauser	Contraseña común proporcionada durante la configuración del dispositivo.
Buscar (como usuario local en la interfaz del usuario de Search)	admin	Contraseña común proporcionada durante la configuración del dispositivo.
Cloud DR	admin	Contraseña común proporcionada durante la configuración del dispositivo.
CDRS	admin o monitor	Contraseña configurada durante la implementación de Cloud DR Server.
Hypervisor Manager (Service)	idpauser	Contraseña común proporcionada durante la configuración del dispositivo.
Hypervisor	idpauser	Contraseña común proporcionada durante la configuración del dispositivo.
Cyber Recovery	Inicio de sesión en la interfaz del usuario: CRSO `OS user: admin`	Contraseña común proporcionada durante la configuración del dispositivo.

Cambio de contraseñas y sincronización de los componentes

El cambio de contraseña de usuario con un solo clic es una característica que simplifica el mantenimiento de la contraseña de Dispositivo PowerProtect serie DP. Con la función de cambio de contraseña de usuario con un solo clic, puede cambiar la contraseña de todos los componentes del dispositivo que se muestran en el tablero de ACM al mismo tiempo.

Sobre esta tarea

Realice los siguientes pasos para cambiar la contraseña de todos los componentes del dispositivo al mismo tiempo.

Pasos

1. Inicie de sesión en el tablero de ACM.
2. En la esquina superior derecha del tablero de ACM, haga clic en **Change Appliance Password** (icono de clave).
3. Especifique las credenciales necesarias.

Cambiar la contraseña de LDAP externo para los componentes del dispositivo

Puede cambiar la contraseña de LDAP externo para los componentes Protection Storage, Protection Software, DPC, DPA y Buscar del dispositivo al mismo tiempo desde el tablero de ACM.

Sobre esta tarea

Realice los siguientes pasos para cambiar la contraseña de LDAP de los componentes Protection Storage, Protection Software, DPC, DPA y Buscar del dispositivo.

Pasos

1. Inicie de sesión en el tablero de ACM.
2. En el tablero de ACM, en la esquina superior derecha del panel **General Settings**, seleccione la opción **Configure external LDAP** en el menú desplegable del icono de engranaje.

   Aparece el cuadro de diálogo **LDAP settings**.
3. En el campo **Query password**, cambie la contraseña de consulta.

   La contraseña de consulta debe contener un mínimo de 9 a 20 caracteres, al menos una letra minúscula, una letra mayúscula, un dígito y cualquiera de los caracteres especiales admitidos (`-`, `_`, y `.`).

Cambiar contraseñas de componentes individuales

Si bien puede cambiar la contraseña de todos los componentes que se muestran en ACM de una sola vez, si decide cambiar las contraseñas de cada componente individualmente, puede hacerlo siguiendo los procedimientos mencionados a continuación. Si decide cambiar la contraseña de cada componente individualmente, asegúrese de actualizar también la misma contraseña en Dispositivo PowerProtect serie DP.

- Todas las contraseñas de componentes individuales deben cumplir con los requisitos de Dispositivo PowerProtect serie DP, aun cuando se cambian en componentes individuales.
- Si modifica la contraseña manualmente en el servidor de Protection Software y no utiliza la opción de cambio de contraseña en Dispositivo PowerProtect serie DP, el sistema muestra un mensaje de error cuando intenta actualizar la contraseña mediante el tablero de ACM. Para obtener más información sobre cómo resolver la contraseña de Protection Software que no está sincronizada, consulte la sección Discrepancia de credenciales.
- Asegúrese de que todos los servicios de productos puntuales estén en funcionamiento antes de cambiar la contraseña.
- Asegúrese de que el tablero de Dispositivo PowerProtect serie DP esté en verde antes de cambiar la contraseña.

AVISO: No se recomienda cambiar las contraseñas de los componentes individuales. Debido a cualquier circunstancia imprevista, si tiene que cambiar las contraseñas de los componentes individuales, consulte las siguientes secciones:

Configuración de Protection Storage

Actualización de la contraseña de Protection Storage

Para obtener más información sobre cómo cambiar la contraseña de la cuenta `sysadmin` de Protection Storage, consulte la *Guía de administración del sistema operativo de Data Domain*. Después de cambiar la contraseña de la cuenta `sysadmin`, inicie sesión en Data Protection Advisor y actualice las credenciales de SSH de Protection Storage con la misma contraseña que utilizó para la cuenta `sysadmin`.

Las seis contraseñas anteriores para la cuenta de usuario sysadmin se registran en Protection Storage. Si intenta establecer una de estas seis contraseñas anteriores una vez más, debe deshabilitar la política del historial de contraseñas y establecer una contraseña anterior o cambiarla seis veces más para volver a establecer la contraseña anterior.

NOTA: Actualice las credenciales de SSH de Protection Storage en Data Protection Advisor inmediatamente. No hacerlo puede provocar el bloqueo de cuenta cuando Protection Storage intenta conectarse repetidamente con la contraseña anterior.

Después de actualizar la contraseña en Protection Storage, inicie sesión en ACM y actualice la contraseña de **Protection Storage** con la misma contraseña que utilizó para la cuenta sysadmin.

NOTA: No cambie la contraseña de usuario boost de Protection Storage antes de configurar Cloud DR desde el tablero.

Configuración de Protection Software

Protection Software utiliza varias cuentas de usuario, incluidas `MCUser`, `viewuser`, `root` del servidor, `admin` del SO y `root` del SO.

Actualización de contraseñas de Protection Software

Dispositivo PowerProtect serie DP requiere que las cuentas de `admin` del SO y de `root` del SO utilicen la misma contraseña. Las cuentas de `MCUser`, `viewuser` y `root` del servidor también deben compartir una contraseña, que puede ser diferente de la contraseña de `admin` del SO y de `root` del SO. Para obtener más información sobre cómo cambiar la contraseña de Protection Software, consulte la *Guía de administración de Avamar*.

Después de cambiar la contraseña de cualquier cuenta de Protection Software, inicie sesión en ACM y actualice la contraseña de **Backup Server** con la misma contraseña que utilizó para la cuenta de Protection Software.

Si cambia la contraseña de la cuenta de `MCUser`, actualícela en la interfaz del usuario de administrador de Buscar. Para obtener más información sobre cómo cambiar la contraseña de Protection Software para Buscar, consulte la *Guía de instalación y administración de Search*.

Si cambia la contraseña de la cuenta de `viewuser`, actualícela en la interfaz del usuario de Data Protection Advisor. Para obtener más información sobre cómo cambiar la contraseña de Protection Software en Data Protection Advisor, consulte la *Guía de instalación y administración de Data Protection Advisor*.

Actualización de la contraseña del usuario de DD Boost

Después de cambiar la contraseña para la cuenta `DDBoostUser` de Protection Storage, inicie sesión en la GUI de **Avamar Administrator**. Edite la configuración del sistema Protection Storage y actualice la contraseña de usuario de DD Boost con la misma contraseña que utilizó para la cuenta `DDBoostUser` de Protection Storage. Para obtener más información, consulte el procedimiento "Edición de un sistema Data Domain" en la *Guía de administración de Avamar*.

NOTA: Actualice la contraseña de usuario boost de Protection Storage solo después de configurar CDR desde el tablero.

Configuración de Data Protection Advisor

Para cambiar la contraseña de la cuenta `administrator` o la contraseña de `root` de Data Protection Advisor, debe iniciar sesión y cambiar esa contraseña para cada nodo de Data Protection Advisor.

Actualización de contraseñas de Data Protection Advisor

Para obtener más información sobre cómo cambiar una contraseña en Data Protection Advisor, consulte la *Guía de instalación y administración de Data Protection Advisor*.

Después de cambiar la contraseña en todos los nodos, inicie sesión en ACM y actualice la contraseña de Reporting & Analytics con la misma contraseña que utilizó para la cuenta `administrator` o la cuenta `root` de Data Protection Advisor.

Actualización de la cadena de comunidad SNMP de Protection Storage

Si se cambia el valor predeterminado de *public* de la cadena de comunidad, Protection Storage debe actualizarse para reflejar el cambio.

1. Inicie sesión en Protection Storage y cambie la cadena de comunidad con el siguiente comando, donde *<community_string>* es la nueva cadena y *<Dpa_DC_Agent_IP>* es la dirección IP del servicio de Data Collection Agent.

   ```
   snmp add rw-community
   Hosts de <community_string>
   <Dpa_DC_Agent_IP>
   ```
2. En el panel **Reporting & Analytics** de ACM, haga clic en el enlace **Reporting & Analytics Web UI**.
3. Haga clic en **Manage Credentials** en la página **Admin** > **System**.
4. Seleccione **EMC Data Domain Credential** y actualice la cadena de comunidad con la misma contraseña que utilizó para la cadena de comunidad.

Configuración de Search

Para cambiar la contraseña de `root` del SO Search, debe iniciar sesión y cambiar la contraseña de `root` del SO para cada nodo de Search.

Actualización de la contraseña de Search

Para obtener más información sobre cómo cambiar la contraseña de `root` del SO, consulte la *Guía de instalación y administración de Search*.

Después de cambiar la contraseña de la cuenta `root` del SO de Search, inicie sesión en ACM y actualice la contraseña de **Search** con la misma contraseña que utilizó para la cuenta `root` del SO de Search.

NOTA: **#**, **?**, **/** y **** son caracteres no permitidos para las contraseñas nuevas.

Actualización de la configuración de LDAP para Search

Si se cambia la contraseña del usuario de consulta de LDAP, es posible que no se pueda iniciar sesión en la interfaz del usuario del administrador de Search. Para actualizar esta contraseña, consulte los procedimientos a los que se hace referencia en la *Guía de instalación y administración de Search*.

1. La primera vez que inicie sesión en un nodo de Search con SSH, deberá aceptar el EULA. Para obtener más información, consulte el procedimiento "Inicialización del entorno de Data Protection Search" en la *Guía de instalación y administración de Search*.
2. Después de aceptar el EULA, seleccione la opción `[2] Configure Network Settings` y presione **F9** para salir.
3. Cuando el sistema muestre `Do you want to reboot now? y(es) or n(o):`, escriba **no**.
4. Para actualizar la configuración de LDAP, complete el procedimiento "Actualización de la configuración de LDAP en el script de instalación del administrador de Data Protection Search" en *Guía de instalación y administración de Search*.
5. Repita los pasos del 1 al 4 para cada nodo de Search.
6. Inicie sesión en cada nodo de datos de índice de Search con SSH y ejecute el comando **`service unicorn restart`**.
7. Inicie sesión en el nodo primario de índice de Search con SSH y ejecute el comando **`service unicorn restart`**.

Configuración de Hypervisor Manager (Service)

Para obtener información sobre cómo cambiar la contraseña de `root` de Hypervisor Manager (Service), consulte la documentación en el sitio web de soporte de Hypervisor Manager (Service).

Actualización de la contraseña de Hypervisor Manager (Service) para ACM

Después de cambiar la contraseña:

NOTA: Si va a cambiar manualmente la contraseña del servidor de Hypervisor Manager (Service), la contraseña que configuró para las cuentas `vsphere.local\Administrator` y `root user` debe ser la misma.

1. Inicie sesión en ACM con SSH.
2. Cambie el directorio a `/usr/local/dataprotection/customscripts/tools`
3. Ejecute el script. `sync_vcenter_password.sh`
4. Modifique los permisos en el script mediante la ejecución del comando `chmod +x sync_vcenter_password.sh`

Para obtener más información sobre el script `sync_vcenter_passwords.sh`, ejecute `sync_vcenter_passwords.sh -h`

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 Hypervisor Manager (Service). Esta cuenta de usuario tiene privilegios limitados, pero tiene acceso a información que puede ayudar a identificar y solucionar problemas.

Actualización de la contraseña de Hypervisor Manager (Service) para Protection Software

1. Conéctese a la interfaz del usuario de Protection Software con un cliente SSH como usuario con la función de administrador. Se muestra la GUI **Avamar Administrator**.
2. Ubique el cliente Hypervisor Manager (Service) en el dominio de Hypervisor Manager (Service).
3. Edite el cliente Hypervisor Manager (Service) y actualice la contraseña de `root` con la misma contraseña que utilizó para la cuenta raíz.

Actualización de contraseña vsphere.local\Administrator

Para obtener información sobre cómo cambiar la contraseña de `vsphere.local\Administrator`, consulte la documentación en el sitio web de soporte de Hypervisor Manager (Service). El dominio es `vsphere.local`.

Configurar la política de vencimiento de la contraseña raíz

Si bien la contraseña raíz de Hypervisor Manager sigue siendo válida o no ha caducado, y si desea que la contraseña raíz de Hypervisor Manager nunca caduque para el usuario raíz de Hypervisor Manager, realice los siguientes pasos:

Pasos

1. Inicie sesión en **VMware vSphere Appliance Management UI** yendo a **`https://`***<nombre de host o IP de VCSA>*:**`5480`** mediante las credenciales **`root`**/*<contraseña común de IDPA>*.
2. En **vCenter Server Appliance Management UI**, haga clic en **Administration**.
3. En el panel **Password Expiration Settings**, seleccione **`No`** para el campo **Root password expires**.

4. Haga clic en **Submit**.

Cambiar la contraseña vencida de la cuenta de usuario raíz

Si la actualización falla, debe realizar los siguientes pasos para cambiar la contraseña vencida de la cuenta de usuario raíz:

Pasos

1. Inicie sesión en **VMware vSphere Appliance Management UI** yendo a **`https://`***<nombre de host o IP de VCSA>*:**`5480`** mediante las credenciales **`root`**/*<contraseña común de IDPA>*.
2. En **vCenter Server Appliance Management UI**, haga clic en **Administration**.
3. En el panel **Change root password**, especifique todos los campos obligatorios y haga clic en **Submit**.
4. Escriba una contraseña nueva cinco veces para borrar la restricción y restablecer la misma contraseña que se estableció antes del vencimiento de la contraseña.
5. Inicie el proceso de actualización mediante la opción **RETRY**.

Configuración de Hypervisor

Para obtener información sobre cómo cambiar la contraseña de Hypervisor, consulte la documentación en el sitio web de soporte de Hypervisor.

Actualización de la contraseña de Hypervisor

Después de cambiar la contraseña:

1. Inicie sesión en ACM con SSH.
2. Cambie el directorio a `/usr/local/dataprotection/customscripts/tools`
3. Ejecute el script. `sync_Switch_Server_ESX_Passwords.sh`
4. Modifique los permisos en el script mediante la ejecución del comando:

```
chmod +x sync_Switch_Server_ESX_Passwords.sh
```

Para obtener más información sobre el script `sync_Switch_Server_ESX_Passwords.sh`, ejecute `sync_Switch_Server_ESX_Passwords.sh -h`

Requisitos de la contraseña de LDAP

La contraseña de LDAP debe cumplir con lo siguiente:

- Use solo los siguientes caracteres:
  - Letras (**`A`**-**`Z`**, **`a`**-**`z`**)
  - Números (**`0`**-**`9`**)
  - Punto (**`.`**)
  - Guion (**`-`**)
  - Guion bajo (**`_`**)
- Debe tener al menos un carácter especial compatible.
- No debe tener más de 20 caracteres.

Monitorear el clúster de Storage Pool

El clúster Almacén de datos de Storage Pool se aplica únicamente al modelo DP5900. PowerProtect DP Series Appliance aloja los servicios de los componentes en un clúster de Almacén de datos de Storage Pool de tres nodos. El clúster tolera la falla de un nodo único o un disco único.

Para asegurarse de que el clúster de Almacén de datos de Storage Pool funcione sin problemas, monitoree los nodos del clúster diariamente mediante Hypervisor Manager. Si se produce un error en uno de los nodos, se muestra un círculo rojo con un signo de exclamación en su icono. Su estado se marca como **Not responding** y su grupo de discos no está montado. Para obtener información sobre cómo conectarse a Hypervisor Manager, consulte Acceso a componentes con un navegador y la documentación en el sitio web de soporte de Hypervisor Manager.

NOTA: Si falla uno de los servidores del clúster de PowerProtect DP Series Appliance , debe iniciar sesión inmediatamente en la GUI de **Avamar Administrator** y deshabilitar los trabajos de respaldo en Autoprotección del sistema. Para obtener más información sobre la deshabilitación de trabajos de respaldo de Protection Software, consulte la *Guía de administración de Avamar*. Para continuar el trabajo de PowerProtect DP Series Appliance con dos servidores, comuníquese con Servicio al cliente.

NOTA: Los trabajos de respaldo se relacionan con los servicios alojados en Dispositivo PowerProtect serie DP. Si falla uno de los servidores del clúster, puede que no sea posible tomar una instantánea del servicio, lo que provoca una falla de respaldo. Una vez que los tres servidores del clúster estén en funcionamiento, debe volver a habilitar los trabajos de respaldo desde la interfaz del usuario de Protection Software. Para obtener más información sobre cómo volver a habilitar los trabajos de respaldo a través de la interfaz del usuario de Protection Software, consulte la *Guía de administración de Avamar*.

Configurar Dispositivo PowerProtect serie DP para utilizar interfaces específicas para la replicación

Un trabajo de replicación copia los datos de respaldo del cliente desde Dispositivo PowerProtect serie DP de origen a otro Dispositivo PowerProtect serie DP, por ejemplo, un sistema Protection Storage. El propósito de la replicación es evitar la pérdida de datos si falla el sistema Dispositivo PowerProtect serie DP de origen.

Sobre esta tarea

Realice los siguientes pasos para configurar la replicación de los datos de respaldo:

Después de realizar los siguientes pasos, debe seguir los pasos que se mencionan en:

- Sección Replicación de la *Guía de administración de Dell EMC Avamar* para configurar la replicación.
- Si desea obtener más información sobre ifgroups para el tráfico de replicación, consulte la *Guía de administración de Dell EMC Data Domain Boost for Partner Integration*.

NOTA: Los pasos adicionales que se enumeran a continuación son para configurar Dispositivo PowerProtect serie DP y utilizar conexiones 10G en lugar de la conexión 1G predeterminada para la replicación.

Pasos

1. Inicie sesión en el sistema Protection Storage mediante SSH.
2. Ejecute el siguiente comando para enumerar los *mtree* (mtree de Protection Software) disponibles en el sistema Protection Storage:
   ```
   sysadmin@ddhostname # mtree list
   ```
   Se muestra una salida similar a la siguiente:
   ```
   Name                            Pre-Comp (GiB)    Status
   ----------------------------    --------------    ------
   /data/col1/avamar-1542004352            3999.3         RW
   /data/col1/backup                          0.0         RW
   /data/col1/esx1-logs                       0.0         RW/Q
   ----------------------------    --------------    -----
   ```
   Anote los detalles del mtree de Protection Software.
3. Ejecute el siguiente comando para asignar el mtree de Protection Software al *ifgroup* y también para agregar el servidor de Protection Storage de destino:
   ```
   ifgroup replication assign <IFGROUP_NAME> mtree <MTREE_PATH> remote
   <TARGET_DD_MANAGEMENT_HOSTNAME>
   ```
   Se muestra una salida similar a la siguiente:
   ```
   ifgroup replication assign vlan280 mtree /data/col1/avamar-1542004352 remote
   vdppunvm126.vdp.emc.com
   ```
4. Ejecute el siguiente comando para ver el resumen del *ifgroup*:
   ```
   sysadmin@ddhostname # ifgroup show config <IFGROUP_NAME> all
   ```

Se muestra una salida similar a la siguiente:

```
Group-name   Status    Interface   Clients   Replication
----------   -------   ---------   -------   -----------
vlan280      enabled           2         1             1
----------   -------   ---------   -------   -----------

Group-name   Status        Interfaces
----------   -------   --------------
vlan280      enabled   10.118.136.110
vlan280      enabled   10.118.136.111
----------   -------   --------------
Group-name   Status    DD Boost Clients
----------   -------   ----------------
vlan280      enabled   10.118.136.0/22
----------   -------   ----------------

Group-name   Status    Replication Mtree              Replication
Remote Host
----------   -------   ----------------------------   -----------
------------
vlan280      enabled   /data/col1/avamar-1542004352
vdppunvm126.vdp.emc.com
----------   -------   ----------------------------   -----------
------------
File replication is allowed on ifgroup.
Client may use any interface.
```

5. De manera similar, cree el *ifgroup* en el sistema Protection Storage de destino y agregue las interfaces, los clientes y la ruta del *mtree* de Protection Software como se mencionó en los pasos anteriores.

   Una vez que haya creado correctamente el *ifgroup*, se muestra una salida similar a la siguiente:

```
ifgroup replication assign <IFGROUP_NAME> mtree <MTREE_PATH> remote
<SOURCE_DD_MANAGEMENT_HOSTNAME>
```

6. Ejecute la replicación desde la interfaz del usuario de Protection Software, y desde el sistema Protection Storage, verifique si el tráfico de replicación utiliza las interfaces en el *ifgroup* de replicación mediante la ejecución del siguiente comando:

   ```
   ifgroup show connections
   ```

7. Una vez que los pasos anteriores se ejecuten correctamente, puede continuar configurando las políticas de replicación. Para obtener más información, consulte la *Guía de administración de Dell EMC Avamar*.

3

Expansión de almacenamiento para DP4400

Puede actualizar la capacidad de almacenamiento del dispositivo DP4400 a 96 TB. Puede expandir la capacidad de almacenamiento en múltiplos de 4 TB (para el dispositivo con capacidad de 8 TB a 24 TB) hasta 24 TB y en múltiplos de 12 TB (para el dispositivo con capacidad de 24 TB o más) hasta un máximo de 96 TB.

Temas:

Extracción del bisel frontal para acceder a los discos duros del panel frontal

El procedimiento para extraer el bisel frontal con el panel LCD es el mismo que se usa para extraer el bisel frontal sin el panel LCD.

Pasos

1. Desbloquee el bisel usando la llave de bisel.
2. Presione el botón de liberación y tire del extremo izquierdo del bisel.
3. Desenganche el extremo derecho y extraiga el bisel.

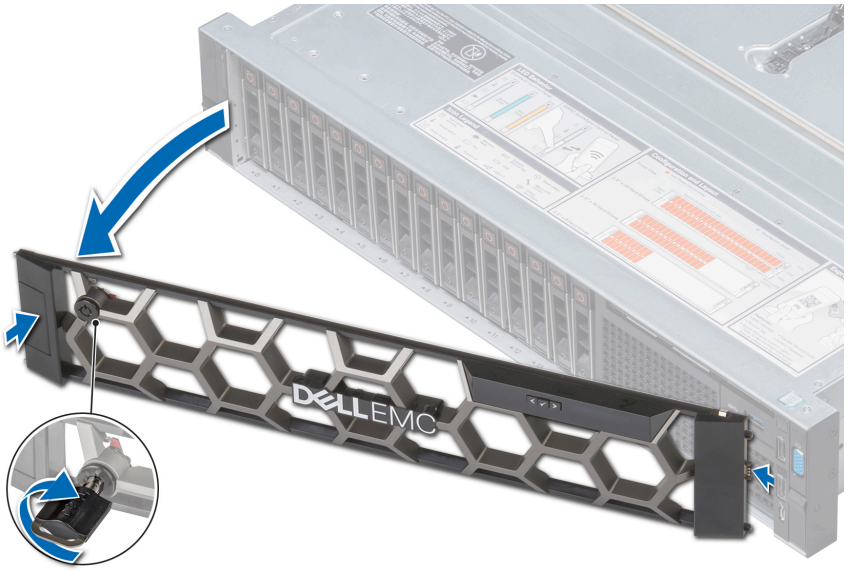

Ilustración 1. Quitar el bisel frontal

Instalar discos duros de expansión

Sobre esta tarea

Instale los discos duros de expansión en las ranuras 4-11 de la parte frontal del sistema.

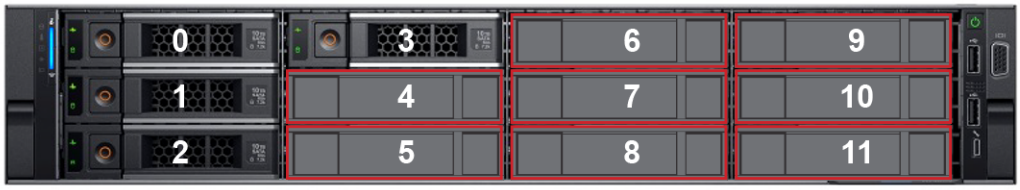

Ilustración 2. Ranuras de disco duro

NOTA: Dell recomienda instalar solo los discos duros proporcionados por Dell en el kit de expansión de disco.

Pasos

1. Extraiga el disco duro de relleno.

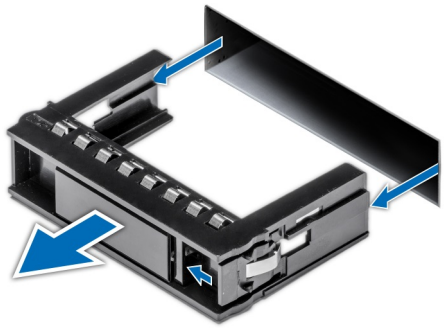

Ilustración 3. Extracción de una unidad de relleno

2. Presione el botón de liberación en la parte frontal del disco duro para abrir la palanca de liberación.

Ilustración 4. Apertura del asa de liberación

3. Inserte el disco duro en la ranura del disco duro y deslícelo hasta que se conecte con el backplane.
4. Cierre el asa de liberación del disco duro para bloquear el disco duro en su lugar.

Ilustración 5. Instalación de un disco duro

Instale el bisel frontal

El procedimiento para instalar el bisel frontal con el panel LCD es el mismo que se usa para instalar el bisel frontal sin el panel LCD.

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.

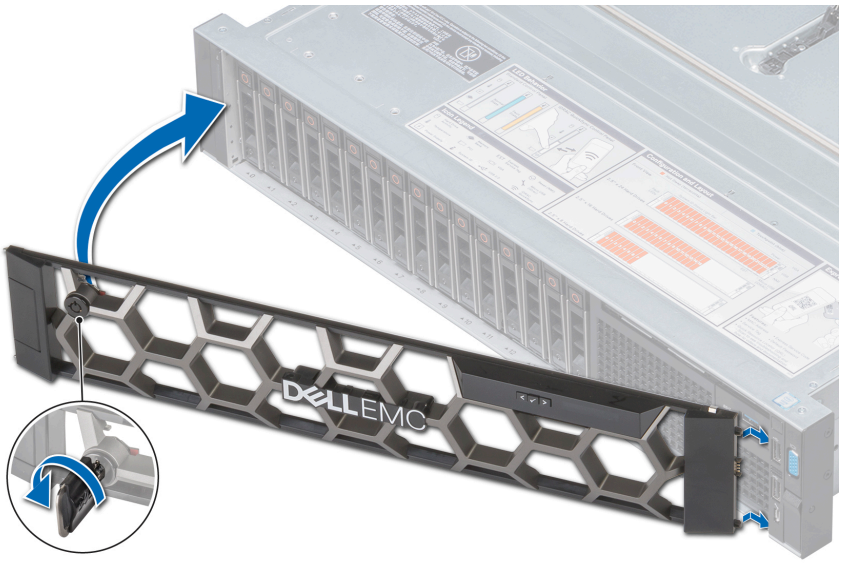

Ilustración 6. Instalación del bisel frontal

Expansión y actualización de almacenamiento

Puede ampliar la capacidad de almacenamiento mediante la obtención de las licencias adicionales necesarias a través del servidor de licenciamiento de Dell. La capacidad de almacenamiento del dispositivo DP4400 con una capacidad de 8 TB a 24 TB se puede expandir más allá de 24 TB agregando unidades de disco al dispositivo mediante el kit de expansión de discos. Puede actualizar el dispositivo mediante ACM e instalar las unidades de disco. Si tiene un dispositivo con capacidad de 8 TB a 24 TB, puede expandir la capacidad de almacenamiento mediante el kit de expansión de discos.

Requisitos previos

Se requieren los siguientes requisitos previos cuando se expande el modelo DP4400 (de 8 TB a 24 TB) más allá de 24 TB mediante el kit de expansión de discos:

- Asegúrese de tener la versión 2.6 de Dispositivo PowerProtect serie DP.
- Asegúrese de que la capacidad de almacenamiento en la nueva licencia no sea menor que la capacidad de la licencia actual.
- Asegúrese de borrar la caché del navegador.
- Si la licencia original de Protection Storage incluye la licencia para el nivel de nube, la nueva licencia de expansión de almacenamiento debe incluir la licencia para el nivel de nube.

Sobre esta tarea

Para expandir la capacidad de almacenamiento del dispositivo, realice las siguientes acciones.

Pasos

1. Inicie sesión en la UI de ACM.
   Se muestra la página de **Home** del tablero ACM.
2. Haga clic en el icono de **Gear** y seleccione **Expand Storage** en el panel **Protection Storage**.
   Se muestra la ventana **Storage expansion**.
3. Haga clic en **Browse** en el campo **License file** en la sección **Protection Storage**.
   Aparece el cuadro de diálogo **Open**.
4. Seleccione el archivo de licencia de para la expansión de discos que descargó.

   NOTA: Si la licencia es válida, se muestra una marca verde.

5. Seleccione la casilla de verificación **I agree that the expansion operation overwrites data on the additional 8 drives** para sobrescribir los datos existentes en las unidades nuevas.

   NOTA: Esta casilla de verificación solo está disponible cuando expande la capacidad de almacenamiento del dispositivo de 8 TB a 24 TB más allá de 24 TB.

6. Seleccione la casilla de verificación **I agree to restart Protection Storage server** o **I agree to restart Protection Storage file system** para reiniciar el servidor de Protection Storage a fin de agregar la controladora SCSI y reiniciar el servicio del sistema de archivos para habilitar la función de nube durante la expansión del almacenamiento.

   NOTA: Esta opción solo se aplica cuando expande su capacidad de almacenamiento del dispositivo de 8 TB a 24 TB más allá de 24 TB.

   NOTA: Las casillas de verificación **I agree to restart Protection Storage server** o **I agree to restart Protection Storage file system** no se muestran cuando la controladora SCSI se agregó anteriormente y si no hay ningún cambio en el estado habilitado del nivel de nube.

   NOTA: La casilla de verificación **I agree to restart Protection Storage file system** habilita la función de nube en el servidor de Protection Storage durante la expansión del almacenamiento.

   NOTA: La casilla de verificación **I agree to restart Protection Storage server** agrega la controladora SCSI al servidor de Protection Storage y cambia el estado habilitado del nivel de nube (si corresponde) durante la expansión del almacenamiento.

   NOTA: Asegúrese de que no haya ninguna operación de I/O activa en ejecución en el servidor de **Protection Storage**.

7. Haga clic en **Expand**.
   La ventana **Storage expansion** muestra la barra de progreso. Puede ver los detalles de la expansión del almacenamiento.
8. Haga clic en **Finish**.

Se muestra la página de **Home** del tablero ACM.

Resultados

Las capacidades de almacenamiento se actualizan en los campos **Total backup storage**, **Available backup storage** y los campos **Cloud Storage** en el panel **Protection Storage**.

NOTA: El campo **Cloud Storage** se actualiza si agregó la función de nube durante la expansión del almacenamiento.

NOTA: Se muestran las casillas de verificación en `Step 5` y `Step 6` si expande la capacidad de almacenamiento del dispositivo más allá de 24 TB.

4

Solución de problemas

Este capítulo contiene información sobre la solución de problemas básica para ayudar a resolver los posibles problemas.

Se abordarán los siguientes temas:

Temas:

Archivos de registro del sistema

Para ayudar a solucionar problemas, descargue los archivos de registro agrupados para PowerProtect DP Series Appliance directamente desde la página de la pestaña **Home**. Seleccione la opción **Download log bundle** desde el icono de paquete de registro disponible en la página de la pestaña **Home** para descargar los archivos de registro. Los archivos de registro para los componentes especificados se guardan en la carpeta `/Downloads/` en el sistema en un formato comprimido.

Durante una actualización, se generan archivos de registro adicionales en una ubicación diferente.

NOTA: El usuario no debe crear ni copiar sus registros en la carpeta `/data01/log_bundle`, ya que esta funcionalidad elimina todos los registros existentes mientras se crea el paquete de registros.

También puede usar Appliance Configuration Manager (ACM) para crear el paquete de registros de dispositivos. Para crear los registros, ejecute el comando `acmlogbundle -p`, seguido de la contraseña raíz de ACM. Asegúrese de que el servicio dataprotection_webapp esté en ejecución a fin de que pueda crear el paquete de registros para el dispositivo. Si el servicio no está en ejecución, el paquete de registros se crea solo para ACM.

Solucionar problemas de apagado

Durante el proceso de apagado, si el dispositivo o cualquiera de los componentes no se apaga automáticamente, puede apagar manualmente Dispositivo PowerProtect serie DP y sus componentes individuales.

Si los sistemas Protection Software o Protection Storage no se apagan, aparte de realizar un apagado manual de estos componentes, también debe apagar los componentes de la infraestructura, que incluyen los servidores de Hypervisor Manager y Hypervisor.

Errores de validación de apagado del dispositivo

Cuando el apagado del dispositivo falla, el dispositivo muestra los errores pertinentes y le solicita que tome medidas correctivas para completar el proceso de apagado. En la siguiente tabla, se detalla el mensaje de error y la acción correctiva asociada que debe realizar.

Tabla 13. Fallas de validación de apagado del dispositivo

Componente	Mensaje de error	Acción correctiva
Hypervisor Manager	`Hypervisor Manager password is out of sync.`	Actualice la contraseña de Hypervisor Manager desde el tablero de ACM.

Tabla 13. Fallas de validación de apagado del dispositivo (continuación)

Componente	Mensaje de error	Acción correctiva
Hypervisor	`Hypervisor password out of sync`	Actualice la contraseña de Hypervisor desde el tablero de ACM. Si hay máquinas virtuales no estándares presentes en ESXi, debe apagarlas manualmente.
Protection Storage	`Protection Storage sysadmin user out of sync.`	Actualice la contraseña desde el tablero de ACM.
Protection Software	• `Protection Software admin, root, mcuser are out of sync` • `Failed to stop scheduler service on Protection Software` • `Jobs are running` • `Protection Software shutdown precheck failed` • `Failed to start scheduler service after validation`	La falla de validación de apagado de Protection Software produce este mensaje de error en la interfaz del usuario. Según el mensaje de error, se debe tomar la acción adecuada de la siguiente lista: • Actualice los usuarios de Protection Software que no están sincronizados desde el tablero de ACM. • Detenga manualmente el servicio del programador en Protection Software mediante el comando `dpnctl scheduler stop`. • En la interfaz del usuario de Protection Software, finalice los trabajos o espere a que se completen. • Ejecute el comando `avosshutdown precheck` en el nodo de utilidad. • Inicie el servicio del programador de Protection Software manualmente mediante el comando `dpnctl scheduler start`. Consulte la documentación de Avamar para obtener más información. Póngase en contacto con el servicio de soporte técnico para obtener asistencia.
Reporting & Analytics	`DPA Server , DPA agent or DPA datastore passwords are out of sync`	Actualice las contraseñas en el panel DPA desde el tablero de ACM.
Buscar	`DPS master or data index nodes are out of sync`	Actualice las contraseñas en el panel DPS desde el tablero de ACM.
Cyber Recovery	• `Cyber Recovery password out of sync` • `Jobs are running on Cyber Recovery`	• Actualice la contraseña de Cyber Recovery desde el tablero de ACM. • En la interfaz del usuario de Cyber Recovery, finalice los trabajos o espere a que se completen.

Tabla 14. Fallas de apagado del dispositivo

Componente	Mensaje de error	Acción correctiva
Protection Storage	`Failed to do Protection Software (Service) OS Shutdown`	Recopile los registros de Protection Software para mediante la creación de un paquete de registros desde el tablero de ACM. Además, consulte con el soporte de Avamar.

Buscar	`Failed to shutdown DPS Data Index node`	Compruebe el siguiente estado de servicio y deténgalo si aún no se ha detenido:
		`service puppet status`
		`service search-worker status`
		`service search-networker-worker status`
		`service search-avamar-worker status`
		`service search-api status`
		`service search-adminapi status`
		`service search-cis-schedule status`

Tabla 14. Fallas de apagado del dispositivo (continuación)

Componente	Mensaje de error	Acción correctiva

		`service search-cis-core status`
		`service nginx status`
		`service elasticsearch status`

Buscar	`Failed to shutdown DPS Data Master node`	Compruebe el siguiente estado de servicio y deténgalo si aún no se ha detenido:
		`service puppet status`
		`service puppetmaster status`
		`service search-worker status`
		`service search-networker-worker status`
		`service search-avamar-worker status`
		`service search-api status`
		`service search-adminapi status`
		`service search-cis-schedule status`
		`service search-cis-core status`
		`service nginx status`
		`service elasticsearch status`

Protection Storage	`Failed to shutdown`	Ejecute el comando `system poweroff` desde la consola de Protection Storage. Póngase en contacto con el servicio de soporte técnico para obtener asistencia.
Data Protection Central	`Failed to shutdown`	Compruebe el estado del servicio `/usr/local/dpc/bin/dpc status` y deténgalo si aún no está detenido.
Hypervisor Manager	`Failed to shutdown`	Compruebe si hay VM en ejecución en VCSA. Si es así, realice acciones correctivas de la tabla anterior para la VM correspondiente. • Apague las VM manualmente. • Apague Hypervisor Manager (Service).
Hypervisor	`Failed to shutdown`	Compruebe si hay VM en ejecución en Hypervisor. Si es así, realice acciones correctivas de la tabla anterior para la VM correspondiente. • Apague las VM manualmente. • Asegúrese de que todas las VM estén apagadas. • Ponga Hypervisor en modo de mantenimiento. • Apague Hypervisor desde la consola de Hypervisor.

Errores de validación de apagado de Protection Software

La siguiente es una lista completa de errores de validación de apagado de Protection Software que puede encontrar antes de apagar el servidor de Protection Software.

Si encuentra alguno de estos errores, debe realizar la acción sugerida para el error que encuentra. Después de realizar la acción de sugerencia sobre el error de validación, puede iniciar el apagado del dispositivo una vez más.

Tabla 15. Errores de validación de apagado de

Mensaje de error de validación	Acción sugerida
`One of the Avamar OS user is out of sync`	En el tablero de ACM, haga clic en la ventana emergente del mensaje de error e ingrese la contraseña para ese usuario de Protection Software en particular que no está sincronizado.
`Avamar MC user is out of sync`	En el tablero de ACM, haga clic en la ventana emergente del mensaje de error e ingrese la contraseña para ese usuario de Protection Software en particular que no está sincronizado.
`Accelerators found to be out of sync`	En el tablero de ACM, haga clic en la ventana emergente del mensaje de error e ingrese la contraseña para el nodo acelerador que no está sincronizado.
`Failed to stop scheduler service of Avamar`	Para detener manualmente los servicios del programador en Protection Software: 1. Inicie sesión en Protection Software Utility Node. 2. Ejecute el comando `dpnctl stop scheduler .` 3. Apague el dispositivo.
`One or more of the services are down/disabled so cannot shutdown`	Asegúrese de que los servicios de Avamar Server, MCS y EMT en Protection Software estén en ejecución. Para comprobar el estado de los servicios, inicie sesión en Protection Software Utility Node y ejecute el comando `dpnctl status all`.
`Found running jobs on Avamar, will not proceed for appliance shutdown`	Asegúrese de que no haya trabajos de respaldo en ejecución en el servidor de Protection Software. Consulte Apagar el dispositivo PowerProtect serie DP para obtener más información. Consulte también la sección Habilitación y deshabilitación de una política de respaldo en la *Guía de administración de Dell EMC Avamar* para deshabilitar todas las políticas de respaldo mediante la interfaz del usuario de Protection Software.
`Backup Server MCS flush not done within last 12 hours`	1. Inicie sesión en Protection Software Utility Node. 2. Respalde los datos de MCS mediante la ejecución del comando `mcserver.sh –flush`. 3. Apague el dispositivo.

Apagar Protection Software manualmente

Puede apagar el componente de Protection Software manualmente para las diversas instancias de Dispositivo PowerProtect serie DP.

Apagar Protection Storage manualmente

En esta sección, se proporciona información sobre cómo apagar el componente Protection Storage manualmente.

Sobre esta tarea

Para apagar manualmente el componente Protection Storage, realice las siguientes acciones.

NOTA: El apagado manual del sistema Protection Storage se aplica al dispositivo DP5900.

NOTA: El apagado manual de Protection Storage se aplica al dispositivo DP4400.

Pasos

1. Abra una nueva sesión de SSH para iniciar sesión en el sistema Protection Storage y en Protection Storage.
2. Ejecute este comando para apagar el sistema Protection Storage.

   `system poweroff`

NOTA: Si tiene el dispositivo DP4400, debe apagar Hypervisor. Para obtener más información sobre el apagado manual de Hypervisor, consulte Apagado manual del hipervisor.

DP5900 y DP4400

En esta sección, se proporciona información sobre cómo apagar manualmente el componente en los dispositivos DP5900 y DP4400.

Sobre esta tarea

Para apagar manualmente el componente Protection Software en su edición virtual, realice las siguientes acciones:

Pasos

Inicie sesión en Protection Software Server con SSH mediante la dirección IP de .

a. Ejecute el siguiente comando para crear un punto de control.
   ```
   mccli checkpoint create --override_maintenance_scheduler
   ```
b. Respalde los datos de MCS mediante la ejecución del siguiente comando:
   ```
   mcserver.sh --flush
   ```
c. Para detener todos los servicios de , ejecute el siguiente comando.
   ```
   dpnctl stop all
   ```
d. Apague Protection Software desde Hypervisor Manager.

NOTA: Si tiene el dispositivo DP4400, debe apagar Hypervisor. Para obtener más información sobre el apagado manual de Hypervisor, consulte Apagar Hypervisor manualmente en la página 49.

Apagar Hypervisor Manager manualmente

En esta sección, se proporciona información sobre cómo apagar Hypervisor Manager manualmente.

Sobre esta tarea

Este procedimiento para apagar Hypervisor Manager manualmente se aplica a todos los modelos de Dispositivo PowerProtect serie DP. Para apagar Hypervisor Manager manualmente, realice las siguientes acciones.

Pasos

1. Abra un navegador e ingrese la dirección IP para acceder a Hypervisor Manager.
   Se mostrará la página de inicio de sesión.
2. Ingrese su nombre de usuario y contraseña en la página de inicio de sesión de Hypervisor Manager.
3. Apague la aplicación virtual de Data Protection.

   NOTA: Todos los servicios y las aplicaciones virtuales en la aplicación virtual de Data Protection se apagan automáticamente.

4. Apague el sistema operativo huésped de la máquina virtual de Dispositivo PowerProtect serie DP y el servicio.

Apagar Hypervisor manualmente

En esta sección, se proporciona información sobre cómo apagar Hypervisor manualmente.

Sobre esta tarea

Este procedimiento para apagar Hypervisor manualmente se aplica a todos los modelos de Dispositivo PowerProtect serie DP. Para apagar Hypervisor manualmente, realice las siguientes acciones.

Pasos

1. Inicie sesión en el servidor de Hypervisor en el que está instalado Hypervisor Manager.

2. Inicie sesión en cada host de Hypervisor.
3. Configure todos los hosts de Hypervisor en modo de mantenimiento mediante la ejecución del siguiente comando en cada host
   `esxcli system maintenanceMode set -e true -m noAction`
4. Apague todos los hosts de Hypervisor mediante el cliente de plataforma de Hypervisor o el host de Hypervisor.

Solución de problemas del inicio

Si una parte del proceso de inicio no se completa automáticamente, se puede resolver el problema manualmente para permitir que el inicio continúe.

El sistema Protection Software no se inicia

Si Protection Software no completa el inicio, conéctese a Avamar Server. Si Protection Software informa que Avamar Server no se ha apagado correctamente, seleccione la opción de revertir al último punto de control.

Si los servicios de Protection Software no se inician, conéctese a Avamar Server mediante SSH e inicie los servicios de Protection Software manualmente con el comando: `# dpnctl start all --ignore_lock`

Los nodos individuales no se inician

Si el servicio de nodo individual no se inicia en un plazo de 2 horas y 15 minutos desde el encendido del dispositivo, uno o varios de los siguientes componentes no están encendidos o no son accesibles en la red:

- Protection Storage
- Protection Software

1. Verifique que estén encendidos los componentes que se requieren para la configuración.
2. Verifique que los componentes necesarios sean accesibles en la red. Resuelva cualquier problema de conectividad que encuentre.
   - Si el software de nodo individual se carga correctamente, omita el resto de este procedimiento. Los nodos de Buscar, los nodos de Data Protection Advisor, Data Protection Central, Protection Software (Service) y Proxy de Protection Storage se inician automáticamente.
   - Si todos los componentes necesarios se encendieron y son accesibles, pero ACM no se carga, reinicie el servicio de ACM:
3. Detener el servicio `dataprotection_webapp`: **`service dataprotection_webapp stop`**
4. Iniciar el servicio `dataprotection_webapp`: **`service dataprotection_webapp start`**

Hypervisor Manager (Service) no se inicia

Presione el botón de encendido que se encuentra en el servidor de Dell. ACM inicia internamente `local.sh (/etc/init.d/local.sh)` y Hypervisor Manager (Service) se inicia automáticamente. Para iniciar manualmente Hypervisor Manager (Service):

1. Saque a Hypervisor del modo de mantenimiento de forma manual.
   NOTA: Para ello, inicie sesión en Hypervisor con las credenciales de **`idpauser`** y seleccione **Exit maintenance mode**.
2. Inicie DataProtection-Hypervisor Manager mediante la ejecución del script `/etc/init.d/local.sh` en Hypervisor o encienda Hypervisor Manager (Service). El servicio de DataProtection-ACM comienza cinco minutos después de que se inicia Hypervisor Manager (Service).
3. Si Protection Storage Hypervisor Manager (Service) no está activo, haga clic en el botón **Power on** para iniciar Protection Storage Hypervisor Manager (Service). El sistema espera hasta que Protection Storage Hypervisor Manager (Service) esté en funcionamiento.
4. Si Protection Storage no se inicia, inicie el servicio de Protection Storage desde la interfaz del usuario de ESXi.
5. Inicie sesión en Protection Storage con credenciales de administrador. ACM ejecuta los comandos `dpnctl status all`, `dpnctl start all` y `dpnctl start maint`.
6. Si algo sale mal, ejecute lo siguiente en secuencia y haga clic en el botón **Power on**:
   - DataProtectionSearch Vapp
   - Servicio de DPADatastoreServer
   - Servicio de DPAApplicationServer
   - VApp DataDomainCloudDR
   - VApp DataProtectionCentral
   - Proxy de Protection Storage Hypervisor Manager (Service).

7. Si la vApp de DPS no se inicia, inicie la vApp.
8. Inicie los servicios de Search iniciando sesión en la dirección IP primaria del índice mediante las credenciales raíz del sistema operativo y ejecute los siguientes comandos:
   a. `service elasticsearch start`
   b. `service search-cis-core start`
   c. `service search-cis-schedule start`
   d. `service search-networker-worker start`
   e. `service search-networker-action start`
   f. `service search-avamar-worker start`
   g. `service search-avamar-action start`
   h. `service search-worker start`
   i. `service search-adminapi start`
   j. `service search-api start`
9. Inicie sesión en el servicio de Application Server mediante SSH.
10. Detenga todos los servicios de aplicaciones mediante la ejecución del siguiente comando: `/opt/emc/dpa/services/bin/dpa.sh service stop` Si hay errores, puede continuar omitiéndolos.
11. Inicie sesión en el servicio de Application Server mediante SSH.
12. Para detener todos los servicios de Datastore Server, ejecute el siguiente comando: `/opt/emc/dpa/services/bin/dpa.sh service stop`
13. Ejecute el siguiente comando para verificar si todos los servicios se detienen en Application Server y en Datastore Server: `/opt/emc/dpa/services/bin/dpa.sh service status`
14. Una vez que se detengan todos los servicios en Application Server y Datastore Server, reinicie los servicios en DPA Datastore Server mediante la ejecución del siguiente comando: `/opt/emc/dpa/services/bin/dpa.sh service start`
15. Una vez que se inician todos los servicios en Datastore Server, reinicie los servicios en Application Server mediante la ejecución del siguiente comando: `/opt/emc/dpa/services/bin/dpa.sh service start`
16. Debe esperar unos minutos hasta que todos los servicios se inicien en Datastore Server. Puede verificar el estado mediante la ejecución del siguiente comando: `/opt/emc/dpa/services/bin/dpa.sh service status`
17. Debe esperar un momento hasta que todos los servicios se inicien en Application Server. Puede verificar el estado mediante la ejecución del siguiente comando: `/opt/emc/dpa/services/bin/dpa.sh service status`
18. Inicie sesión en Hypervisor con las credenciales de **`idpauser`**, seleccione el servicio de **AVProxy** y haga clic en el botón **Power on**.
19. Después del inicio de Dispositivo PowerProtect serie DP, inicie dos servicios de Protection Software mediante el comando `dpnctl start emt`.

Solución de problemas de LDAP

En este tema, se proporciona información sobre cómo solucionar problemas de configuraciones de LDAP.

Solucionar problemas de configuración de LDAP seguro

Durante la configuración de LDAP seguro, es posible que aparezca el mensaje de error `Unable to connect to secure LDAP/AD. Please verify whether the LDAP/AD Server provided is present as alternate name in LDAPS Certificate`.

Sobre esta tarea

Java SE Development Kit 8, actualización 181 está causando este problema relacionado con la identificación de terminales de LDAP. Para obtener más información sobre este problema, consulte las Notas de la versión de Java SE Development Kit 8, actualización 181.

Realice los siguientes pasos para deshabilitar la identificación de terminales de LDAP a fin de solucionar este problema.

Pasos

1. Conéctese a ACM mediante a un cliente SSH.
2. Mediante un editor de texto, abra el archivo *catalina.sh* que se encuentra en el directorio `/usr/local/dataprotection/tomcat/bin/`.

3. En el archivo *catalina.sh*, busque la siguiente línea:

```
JAVA_OPTS="$JAVA_OPTS -Dorg.apache.catalina.security.SecurityListener.UMASK=`umask`"
```

4. Modifique esta línea según los valores que se proporcionan a continuación:

```
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
-Dorg.apache.catalina.security.SecurityListener.UMASK=`umask`"
```

5. Guarde los cambios realizados en el archivo *catalina.sh*.
6. Reinicie el servicio de protección de datos en ACM mediante el siguiente comando:

```
service dataprotection_webapp restart
```

Verificar la contraseña de LDAP interno

Si ya conoce la contraseña de LDAP interno, realice los siguientes pasos para verificar la contraseña:

Requisitos previos

Si conoce su contraseña de LDAP interno, anótela y téngala a mano.

Pasos

1. Conéctese a ACM mediante un cliente SSH.
2. Para validar su contraseña existente, ejecute el comando `ldapsearch` con su contraseña. A continuación se muestra un ejemplo.

```
# ldapsearch -h ldaps:/<ACM_IP> -p 636 -D uid=idpauser,ou=People,dc=idpa,dc=local -b
dc=idpa,dc=local -w <IDPAUSER_PWD>
```

Crear contraseña de LDAP interno

Si no recuerda la contraseña de LDAP interno, primero debe configurar la contraseña de LDAP interno mediante los siguientes pasos:

Pasos

1. Conéctese a ACM mediante un cliente SSH.
2. Genere un `hash` para la nueva contraseña. A continuación, se muestra un ejemplo de entrada.

```
#/etc/openldap/slappasswd -s <NEW_PASSWORD>
```

3. Cree un archivo con el archivo `hash` modificado. A continuación se muestra un ejemplo.

```
# vi /etc/openldap/update_idpauserpwd.ldif

dn: uid=idpauser,ou=People,dc=idpa,dc=local
changetype: modify
replace: userPassword
userPassword: <COMMAND_OUPUT_IN_FIRSTSTEP>
```

4. Ejecute el siguiente comando para actualizar la contraseña mediante la contraseña raíz de LDAP.

```
# ldapmodify -x -D cn=Manager,dc=idpa,dc=local -w "<LDAP_ROOT_PASSWORD>" -f /etc/openldap/
update_idpauserpwd.ldif
```

Donde *<LDAP_ROOT_PASSWORD>* es la misma que la contraseña común del dispositivo.

5. Ejecute el comando `ldapsearch` en ACM con la nueva contraseña para validar. A continuación se muestra un ejemplo.

```
# ldapsearch -h ldaps:/<ACM_IP> -p 636 -D uid=idpauser,ou=People,dc=idpa,dc=local -b
dc=idpa,dc=local -w <NEW_IDPAUSER_PWD>
```

Cambiar el DNS de ACM

Para cambiar la configuración de Domain Name Server (DNS) de Appliance Configuration Manager (ACM), realice los siguientes pasos:

Pasos

1. Conéctese a ACM mediante un cliente SSH.
2. Edite el archivo `/etc/resolv.conf` y especifique la dirección IP del servidor DNS del cliente y el nombre de dominio.
   Por ejemplo, cuando el entorno del cliente tiene un servidor DNS público con la dirección IP 10.254.66.23 y el nombre de dominio es mycompany.com, el archivo `/etc/resolv.conf` contiene las siguientes entradas:

   NOTA: El siguiente resultado es un ejemplo, no contiene el nombre de dominio real ni las direcciones de nameserver. El cliente debe proporcionar los detalles necesarios.

   ```
   search mycompany.com
   nameserver 10.254.66.23
   nameserver 192.168.100.100
   ```

   NOTA: Asegúrese de que la entrada para el servidor DNS público aparezca antes que el servidor DNS privado. Si el servidor DNS privado aparece primero, se producirá un error en la integración de DPA con el sistema Protection Storage.

3. Cambie la línea `allow-recursion { <old_primary_dns>; <old_secondary_dns>; };` del archivo /etc/named.conf a `allow-recursion { <new_primary_dns>; <new_secondary_dns>; };`
4. Reinicie el servicio named mediante el comando `service named restart`.

Las credenciales no coinciden

En esta sección, se proporciona información sobre cómo resolver el escenario de incompatibilidad de contraseña para los productos puntuales de Dispositivo PowerProtect serie DP. Si modifica manualmente la contraseña en los productos puntuales y no utiliza la opción de cambiar contraseña en , el sistema muestra un mensaje de error cuando intenta actualizar la contraseña mediante el tablero de ACM.

Sobre esta tarea

Además, si encuentra el mensaje de error `Failed to validate connection`, podría haber una incompatibilidad de credenciales entre los productos puntuales o los servicios de esos productos asociados.

Para resolver una incompatibilidad de contraseña, realice las siguientes acciones:

Pasos

1. Haga clic en el mensaje de advertencia que aparece en el panel de productos puntuales e ingrese una nueva contraseña.
2. Haga clic en **Update Password** en el panel de productos puntuales e ingrese una nueva contraseña.
3. Haga clic en el botón **Refresh** del tablero de ACM.
   El sistema actualiza la contraseña nueva para todas las cuentas pertinentes.

Solución de problemas de Protection Software

Si hay un problema con Protection Software, el panel **Protection Software** en el tablero de ACM muestra el siguiente estado:

`Backup Agents Installation in progress...`

Las posibles causas posibles para este problema incluyen:

- El servicio de Protection Software y Protection Software están inactivos.
- No se puede hacer ping a Protection Software.
- Hay un error de coincidencia entre la contraseña de administrador de Protection Software y la contraseña almacenada en ACM.

Protection Software (Service) está inactivo

Para iniciar Protection Software (Service):

1. Mediante un cliente SSH, conéctese a Protection Software Utility Node como el usuario **admin**.
2. Ejecute el comando .

Protection Software o Protection Software (Service) están inactivos

Encienda Protection Software o el servidor de Protection Software (Service).

No se puede hacer un ping a Protection Software

Si no se puede hacer un ping a Protection Software, encuentre y resuelva el origen del problema. Las causas posibles incluyen:

- Protection Software Server está inactivo.
- Hay un problema de conectividad de red.
- Protection Software Server tiene un problema de hardware.

Solución de problemas del monitoreo de estado

Si hay un problema con SNMP o uno de los procesos de monitoreo de estado, la pestaña **Health** no puede mostrar datos.

Errores de validación de SNMP

De forma predeterminada, ACM valida la configuración de SNMP del servidor de Dell cada 4 horas. Si ACM detecta que la configuración de SNMP para un componente está desactivada o ausente, corrige automáticamente la configuración.

Si ACM no puede conectarse con uno de los componentes en su IP interna, se muestra el siguiente mensaje en la pestaña **Health**: `Failed to validate SNMP configuration on component(s) <unreachable-component>`

Para resolver este problema:

1. Verifique que las direcciones IP internas del servidor de Dispositivo PowerProtect serie DP sean accesibles en la red.
2. Si el componente es accesible en la red, verifique la conectividad del protocolo SSH al intentar conectarse con la contraseña predeterminada del protocolo SSH. Si no se puede establecer una conexión de protocolo SSH, revierta la contraseña del protocolo SSH en el componente a la contraseña predeterminada.

Errores de los procesos del monitor de estado

Si el puerto del receptor de SNMP, el servicio de Message Broker o el servicio de base de datos están inactivos, se muestra el siguiente mensaje en la pestaña **Health**: `Health monitor processes are down : <process>`

Para resolver este problema, conéctese a ACM mediante SSH y siga el procedimiento que corresponda al mensaje de error:

- Si el puerto del receptor de SNMP está inactivo, verifique que esté activado el puerto 161. Si el puerto está activado y el problema continúa, reinicie el servicio Tomcat con el siguiente comando:

  ```
  service dataprotection_webapp restart
  ```

- Si el servicio de Message Broker está inactivo, verifique que el servicio RabbitMQ esté en ejecución con el siguiente comando:

  ```
  service rabbitmq-server status
  ```

  Si el servicio no está en ejecución, inícielo con el siguiente comando:

  ```
  service rabbitmq-server start
  ```

- Si el servicio de base de datos está inactivo, verifique que el servicio PostgreSQL esté en ejecución con el siguiente comando:

  ```
  service dataprotection_database status
  ```

Si el servicio no está en ejecución, inícielo con el siguiente comando:

```
service dataprotection_database start
```

5

Recuperación de dispositivos con Cyber Recovery

Cuando Cyber Recovery está configurado en el dispositivo, puede realizar los siguientes pasos para la recuperación después de un desastre.

Temas:

Respaldo de recuperación ante desastres

Cuando Cyber Recovery está configurado, PowerProtect DP Series Appliance crea un paquete de recuperación ante desastres (DR) de los servicios. Los paquetes de DR se deben usar para restaurar los servicios del dispositivo.

El paquete de DR se crea para ACM, Hypervisor Manager y Cyber Recovery, y se almacena en `DataDomain MTree./data/col1/DP-drbackups`. Los paquetes de DR se crean diariamente para ACM, Hypervisor Manager y Cyber Recovery. Consulte Modificar la frecuencia del paquete de DR en la página 56 a fin de conocer los pasos para modificar la frecuencia.

El límite de retención predeterminado para los paquetes de DR se establece en **7**. Consulte Modificar el límite de retención del paquete de DR en la página 57 para conocer los pasos para modificar el límite de retención.

Modificar la frecuencia del paquete de DR

En esta sección, se describen los pasos para modificar la frecuencia del paquete de DR de ACM, Hypervisor Manager y Cyber Recovery.

Cyber Recovery

Realice estos pasos para modificar la frecuencia del paquete de DR.

Sobre esta tarea

Inicie sesión en la interfaz del usuario de **PowerProtect Cyber Recovery** y realice estos pasos:

Pasos

1. En la navegación de cabecera, haga clic en el ícono de engranaje para acceder a la lista de **Configuraciones del sistema**.
2. Seleccione **Respaldos de recuperación ante desastres**.
   Aparece el cuadro de diálogo **Respaldos de recuperación ante desastres**.
3. Modifique el campo **Frequency**.

ACM y Hypervisor Manager

Realice estos pasos para modificar la frecuencia del paquete de DR.

Pasos

1. Detenga el servicio web de ACM: `acmstop`
2. Modifique el campo *dr_backup_frequency_in_hours* en el archivo `/usr/local/dataprotection/customscripts/customConfig.properties`.

3. Inicie el servicio web de ACM: `acmstart`

Modificar el límite de retención del paquete de DR

En esta sección, se describen los pasos para modificar el límite de retención del paquete de DR de ACM, Hypervisor Manager y Cyber Recovery.

Cyber Recovery

Realice estos pasos para modificar el límite de retención del paquete de DR.

Sobre esta tarea

Inicie sesión en la interfaz del usuario de **PowerProtect Cyber Recovery** y realice estos pasos:

Pasos

1. En la navegación de cabecera, haga clic en el ícono de engranaje para acceder a la lista de **System Settings** .
2. Seleccione **Maintenance**.
   Aparece el cuadro de diálogo **Maintenance**.
3. Modifique el campo **Delete DR Backups older than**.

ACM y Hypervisor Manager

Realice estos pasos para modificar el límite de retención del paquete de DR.

Pasos

1. Detenga el servicio web de ACM: `acmstop`
2. Modifique el campo *max_dr_backup_count* en el archivo `/usr/local/dataprotection/customscripts/customConfig.properties`.
3. Inicie el servicio web de ACM: `acmstart`

Restaurar los servicios

En esta sección, se describen los pasos para restaurar los servicios de ACM, Hypervisor Manager y Cyber Recovery mediante los paquetes de DR.

Restaurar archivos de configuración de ACM

Realice estos pasos para restaurar los archivos de configuración de ACM.

Pasos

1. Inicie sesión en ACM con SSH mediante las credenciales raíz.
2. Detenga el servicio web de ACM: `acmstop`
3. Cree un punto de montaje en ACM:
   ```
   mkdir -p /mnt/drbackup
   ```
4. Monte el MTree de Protection Storage:
   ```
   sudo -S mount -t nfs 192.168.100.109:/data/col1/DP-drbackups /mnt/drbackup
   ```
5. Inicie sesión como idpauser:
   ```
   su idpauser
   ```
6. Vaya al directorio de respaldo de ACM:

```
cd /mnt/drbackup/acm
```

7. Enumere todos los archivos tar de respaldo de ACM:
   ```
   ls -lrt
   ```
8. Copie el archivo tar requerido en `/tmp`:
   ```
   cp <tar-name.tar.gz> /tmp/
   ```
9. Salga de idpauser:
   ```
   exit
   ```
10. Vaya al directorio `/tmp`:
    ```
    cd /tmp
    ```
11. Cambie el nombre del archivo tar a configuration.tar:
    ```
    mv <tar-name.tar.gz> configuration.tar
    ```
12. Ejecute el script de restauración:
    ```
    sh /usr/local/dataprotection/customscripts/configure.sh
    ```
13. Desmonte el MTree de Protection Storage:
    ```
    sudo -S umount /mnt/drbackup
    ```
14. Inicie el servicio de ACM: `acmstart`

Restaurar archivos de configuración de Cyber Recovery

En esta sección, se describen los pasos para restaurar los archivos de configuración de Cyber Recovery.

Requisitos previos

El paquete tar de respaldo de Cyber Recovery creado antes del desastre es necesario para completar el procedimiento.

Pasos

1. Obtenga el archivo tar de respaldo de CR desde el mtree de Protection Storage.
   a. Inicie sesión en ACM con SSH mediante las credenciales raíz.
   b. Cree el directorio de montaje:
      ```
      mkdir /mnt/drbackup
      ```
   c. Ejecute el comando en ACM para montar Protection Storage:
      ```
      mtree "/data/col1/DP-drbackups"
      sudo -S mount -t nfs 192.168.100.109:/data/col1/DP-drbackups /mnt/drbackup
      ```
      Ejemplo de salida:
      ```
      # sudo -S mount -t nfs 192.168.100.109:/data/col1/DP-drbackups /mnt/drbackup
      # cd /mnt/drbackup/
      :/mnt/drbackup # ls
      .snapshot acm cr.19.8.0.2-149.2021-05-19.17_04_51.tar.gz staging vcsa
      ```
   d. Copie el archivo tar de respaldo de CR `cr.<CR-version>.<date>.17_04_51.tar.gz` en el servicio de CR.
      Por ejemplo:
      ```
      /tmp/cr_backups/cr.19.8.0.2-149.2021-05-19.17_04_51.tar.gz
      ```
2. Inicie sesión en el servicio de Cyber Recovery con SSH mediante el usuario administrador y ejecute el siguiente comando para cambiar al usuario raíz:
   ```
   su root
   ```
   Ejecute los siguientes comandos en el servicio de CR:
   a. Vaya al directorio `/tmp` y convierta el archivo `cyber-recovery-installer.bin` en un archivo ejecutable:
      ```
      # cd tmp
      # chmod +x ./cyber-recovery-installer.bin
      ```
   b. Ejecute el archivo `cyber-recovery-installer.bin`:
      ```
      # ./cyber-recovery-installer.bin
      ```

El sistema vuelve al estado en que se encontraba después de implementar el dispositivo virtual de Cyber Recovery.

c. Inicie la restauración del software Cyber Recovery:

i. Ejecute el script de instalación `crsetup.sh`:

```
crsetup.sh --recover
```

ii. Escriba `y` para continuar:

```
Do you want to continue [y/n]:
```

iii. Escriba `y` para confirmar y continuar:

```
Are you REALLY sure you want to continue [y/n]:
```

iv. Escriba la ruta completa a la ubicación del paquete tar de respaldo de Cyber Recovery, por ejemplo:

```
/tmp/cr_backups/cr.19.2.1.0-3.2019-09-19.08_02_09.tar.gz
```

El sistema solicita la contraseña de MongoDB recién instalado. Proporcione la contraseña anterior de MongoDB antes de la recuperación (contraseña guardada en el dispositivo). La operación de restauración de Cyber Recovery continúa y muestra un mensaje de ejecución satisfactoria:

```
05.24 12_51_35 :
05.24 12_51_35 : Cyber Recovery has been successfully recovered onto this system
05.24 12_51_35 :
```

d. Inicie sesión en la interfaz del usuario o la CLI de Cyber Recovery y valide que se restaure la instalación anterior.

e. Realice la limpieza:

i. Elimine el archivo tar de respaldo copiado en el servicio de CR, por ejemplo:

```
rm /tmp/cr_backups/cr.19.8.0.2-149.2021-05-19.17_04_51.tar.gz
```

ii. Desmonte el punto de montaje creado en ACM:

```
sudo -S umount /mnt/drbackup
```

Restaurar la configuración de Hypervisor Manager mediante el respaldo de DR

En esta sección, se describen los pasos para restaurar la configuración de Hypervisor Manager mediante el respaldo de DR.

Pasos

1. Ejecute el comando en ACM para detener el servicio de ACM:
   ```
   acmstop
   ```
2. Ejecute los comandos en ACM para montar el directorio de respaldo de DR en ACM:
   ```
   mkdir -p /mnt/drbackup
   sudo -S mount -t nfs 192.168.100.109:/data/col1/DP-drbackups /mnt/drbackup
   ```
3. Ejecute los comandos en ACM para copiar el respaldo de Hypervisor Manager en ACM:
   ```
   su idpauser
   cd /mnt/drbackup/vcsa/
   cp <vcsa_tar_file_name>.tar.gz /tmp/
   ```
4. Ejecute los comandos en ACM para extraer el respaldo de Hypervisor Manager:
   ```
   cd /tmp
   tar zxvf <vcsa_tar_file_name>.tar.gz
   ```

   NOTA: Tome nota del nombre de la subcarpeta en la carpeta extraída `vcsaBackup`.

5. Ejecute el comando en ACM para iniciar la restauración de Hypervisor Manager:

   ```
   python /usr/local/dataprotection/customscripts/vcenter_restore.py -s <acm_ip> -d <vCenter_ip>
   -f /tmp/vcsaBackup -b <backup_subfolder_name> -u root -p <vCenter_password> -c <acm_password>
   ```

   NOTA: En caso de que falle la restauración de Hypervisor Manager, vuelva a implementar el OVA de Hypervisor Manager y ejecute el script de restauración nuevamente.

6. Inicie sesión en la interfaz del usuario de Hypervisor Manager y verifique si la restauración se realizó correctamente.
7. Ejecute el comando en ACM para iniciar el servicio de ACM: `acmstart`
8. Realice la limpieza:
   a. Elimine los archivos de respaldo en ACM mediante la ejecución de los siguientes comandos:

      ```
      rm -rf /tmp/vcsaBackup
      rm -rf <vcsa_tar_file_name>.tar.gz
      ```

   b. Desmonte el punto de montaje creado en ACM:

      ```
      sudo -S umount /mnt/drbackup
      ```

6

Recursos adicionales

En este capítulo, se proporcionan referencias a otros materiales relacionados con Dispositivo PowerProtect serie DP y los componentes individuales.

Temas:

Referencias de documentos para Dispositivo PowerProtect serie DP

La documentación de Dispositivo PowerProtect serie DP incluye las siguientes publicaciones:

Guía de instalación y actualización de dispositivo de Dell EMC PowerProtect DP series.	Instrucciones para instalar el hardware y el software de Dispositivo PowerProtect serie DP DP4400.
Guía de implementación de servicios profesionales y de campo de Dispositivo PowerProtect serie DP para DP5xxx.	Instrucciones para instalar y configurar Dispositivo PowerProtect serie DP DP5xxx.
Guía del producto de Dispositivo PowerProtect serie DP.	Proporciona una visión general e información de administración del sistema Dispositivo PowerProtect serie DP.
Notas de la versión de Dispositivo PowerProtect serie DP.	Información del producto sobre la versión actual de Dispositivo PowerProtect serie DP.
Guía de configuración de seguridad de Dispositivo PowerProtect serie DP.	Información sobre las funciones de seguridad que se usan para controlar el acceso de red y de los usuarios, monitorear el acceso al sistema y su uso, y permitir la transmisión de datos de almacenamiento.
Guía de compatibilidad de software de Dispositivo PowerProtect serie DP	Información sobre los componentes de software y las versiones que se usan en el producto Dispositivo PowerProtect serie DP.

Guía del procedimiento de reparación de Dispositivo PowerProtect serie DP DP4400.	Procedimientos para reemplazar o actualizar los componentes de hardware de Dispositivo PowerProtect serie DP.
Guía de reemplazo en campo de Dispositivo PowerProtect serie DP para DP5xxx.	Instrucciones para agregar, reemplazar y reparar componentes de hardware de DP5xxx.

Referencias de documentos para los componentes individuales

Se puede obtener la documentación para estos componentes de Soporte en línea en la siguiente ubicación.

https://www.dell.com/support.

Nodo Protection Storage

El siguiente documento contiene información que se relaciona con Protection Storage:

- *Guía de administración del sistema operativo de Data Domain*

En esta publicación, se explica cómo administrar sistemas Protection Storage con un énfasis en los procedimientos que usan Protection Storage Data Protection Central.

Nodo de Backup Server

Los siguientes documentos contienen información que se relaciona con :

Guía de administración de Avamar	En esta publicación, se describe cómo configurar, administrar, monitorear y mantener un servidor de Protection Software.
Guía de integración de Avamar y sistemas Data Domain	En esta guía, se incluyen procedimientos para configurar el servidor de a fin de ejecutar las operaciones de nivel de nube en el sistema Protection Storage.
Guía del usuario de Avamar para VMware	En esta publicación, se describen diferentes métodos y estrategias para proteger el servicio de VMware.
Guía del usuario de Avamar NDMP Accelerator para Oracle ZFS	En esta publicación, se describe cómo instalar, configurar, administrar y usar NDMP Accelerator (acelerador) a fin de respaldar y restaurar los dispositivos de almacenamiento Oracle ZFS admitidos.
Guía del usuario de Avamar NDMP Accelerator para filers de NetApp	En esta publicación, se describe cómo instalar, configurar, administrar y usar NDMP Accelerator (acelerador) a fin de respaldar y restaurar los filers de NetApp admitidos.
Guía del usuario de Avamar NDMP Accelerator para sistemas NAS de EMC	En esta publicación, se describe cómo instalar, configurar, administrar y usar s NDMP Accelerator (acelerador) a fin de respaldar y restaurar los sistemas EMC Isilon, Unity, VNX, VNXe y Celerra admitidos.

Guía del usuario de Avamar para VMware	En esta publicación, se describen diferentes métodos y estrategias para proteger el servicio de VMware.

Nodo Data Protection Central

Los siguientes documentos contienen información que se relaciona con Data Protection Central:

Notas de la versión de Data Protection Central	Contiene la información más actualizada sobre la versión actual.
Guía de introducción a Data Protection Central	En este documento, se incluye información sobre cómo implementar Data Protection Central y comenzar a usar la administración de Data Protection Central.
Guía del administrador de Data Protection Central	En este documento, se incluye información sobre cómo administrar Data Protection Central.
Guía de configuración de seguridad de Data Protection Central	En este documento, se incluye información sobre las características de seguridad y las funcionalidades de Data Protection Central.

Nodo Reporting & Analytics

Los siguientes documentos contienen información que se relaciona con Reporting & Analytics:

Guía de instalación y administración de Data Protection Advisor	En esta publicación, se describe cómo instalar, mantener y configurar Reporting & Analytics.
Guía del producto Data Protection Advisor	En este documento, se brinda información sobre cómo usar la consola web de Reporting & Analytics para ejecutar y crear informes, visualizar alertas y ver el estado de las operaciones de replicación.

Buscar

El siguiente documento contiene información que se relaciona con Buscar:

Guía de instalación y administración de Search	En esta publicación, se describe cómo instalar, mantener y configurar Buscar.

Cloud DR

Los siguientes documentos contienen información que se relaciona con DD Cloud DR y Cloud DR:

Notas de la versión de Data Domain Cloud Disaster Recovery	Contiene información complementaria sobre DD Cloud DR y la información más actualizada sobre la versión actual.
Guía de instalación y administración de Data Domain	En este documento, se describe cómo instalar, implementar y utilizar el producto DD Cloud DR.

Cloud Disaster Recovery

Recursos de capacitación de Dispositivo PowerProtect serie DP

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

Puede obtener más información y capacitación de Dispositivo PowerProtect serie DP en https://education.dellemc.com/content/emc/home.