Dell EMC PowerProtect DP Series Appliance

2.7.1

Notas de la versión para DP4400, DP5900, DP8400 y DP8900

Rev. 01
Diciembre de 2021
Estas notas de la versión incluyen información adicional acerca de PowerProtect DP Series Appliance.

DELL EMC

Historial de revisiones

En esta sección, se describen las actualizaciones que se realizan para cada revisión de la versión de PowerProtect DP Series Appliance.

Tabla 1. Historial de revisiones

Revisión	Fecha	Descripción
01	Diciembre de 2021	Primera versión de este documento para PowerProtect DP Series Appliance 2.7.1

Convenciones de denominación de productos y cambios de terminología

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

Tabla 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	Search
CDRA (VM)	Cloud DR (Service)
CDRS	Cloud DR Server
Cyber Recovery (VM)	Cyber Recovery (Service)
Integrated Dell Remote Access Controller (iDRAC)	iDRAC
iDRAC Service Module (iSM)/iSM service	iDRAC Service Module

Descripción del producto

PowerProtect DP Series Appliance combina varias soluciones de hardware y software en un solo producto.

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

Otros modelos de PowerProtect DP Series Appliance (DP5900, DP8400 y DP8900) se envían como una unidad completa, con todos los componentes de hardware en rack y cableados en la fábrica. El servicio al cliente de Dell EMC completa la instalación y la configuración inicial. La solución incluye un servidor de Protection Software como el nodo de servidor de respaldo con NDMP Accelerators opcionales, un sistema Protection Storage como el nodo de almacenamiento con protección, nodos de computación para componentes virtuales y software, un switch de red para mejorar la velocidad de configuración, y Cloud DR.

El software del sistema para cada componente se instala y se configura en la mayor medida posible antes de enviar el dispositivo. Una aplicación de respaldo, Protection Storage, Reporting & Analytics, Search, Cloud DR, Data Protection Central y Appliance Configuration Manager (ACM) vienen integrados en el dispositivo.

Search, Reporting & Analytics y Cloud DR se pueden configurar de manera opcional y sus funciones se pueden ejecutar mediante la implementación corporativa central de estas funciones.

Nuevas características

En esta versión, se incluyen las siguientes funciones.

Número de versión 2.7.1

Hay un nuevo número de versión 2.7.1.

Actualización del dispositivo

Puede actualizar el dispositivo a la versión 2.7.1. Asegúrese de seguir la ruta de actualización y el procedimiento correctos que se mencionan en los siguientes documentos:

- Para DP4400 y DP5900, consulte la *Guía de instalación y actualización de PowerProtect DP Series Appliance*.
- Para DP8400 y DP8900, consulte la *Guía de implementación de servicios profesionales y de campo de PowerProtect DP Series Appliance para DP5900, DP8400 y DP8900*.

Problemas resueltos

En esta sección, se enumeran los problemas que se corrigieron en esta versión.

Tabla 3. Problemas resueltos

Número de problema	Descripción del problema
IDPA-9269	PowerProtect DP Series Appliance 2.7.1 aborda la vulnerabilidad CVE-2021-44228 (vulnerabilidad log4Shell en el paquete Apache log4j) mediante el paquete log4j versión 2.16 o posterior en sus componentes, y la modera completamente para la funcionalidad DP Search.
IDPA-8635	Las vulnerabilidades de seguridad se corrigen en Protection Software.
IDPA-8592	Las vulnerabilidades de seguridad se corrigen en Data Protection Central.
IDPA-8693	Las vulnerabilidades de seguridad se corrigen en Search.
IDPA-9016	Las vulnerabilidades de seguridad se corrigen en Hypervisor y Hypervisor Manager.
IDPA-8797	Las vulnerabilidades de seguridad se corrigen en Cyber Recovery. Consulte el artículo de la base de conocimientos 000194309 para actualizar manualmente Cyber Recovery y aplicar los parches de seguridad.

Problemas conocidos

En esta sección, se describen los problemas conocidos de PowerProtect DP Series Appliance.

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones

Número de problema	Descripción del problema	Solución alternativa/resolución
IDPA-8960	Durante las validaciones de actualización, la validación de la versión del SO de DPC falla si el SO ejecuta SLES 12 SP2 en vez de SLES 12 SP5.	Póngase en contacto con el servicio de soporte para obtener asistencia.
DPC-6312	Mientras se actualizaba el dispositivo de la versión 2.6.1 a la versión 2.7, la actualización de DPC falló durante la instalación del paquete acumulativo del SO. **NOTA:** Este problema se relaciona solo con los sistemas 2.6.1 que se actualizan de versiones inferiores del dispositivo a 2.6.1.	Póngase en contacto con el servicio de soporte para obtener asistencia.
IDPA-8032	Durante la implementación de ACM, en la página **License**, cuando hace clic en **Check online for Licenses**, recibe el siguiente mensaje y el botón **Next** aparece activo: `Licenses were downloaded successfully`	Este problema se produce cuando la conexión con ELMS se realiza correctamente, pero las licencias válidas no están disponibles para su descarga. Obtenga manualmente las licencias correctas para su sistema y haga clic en **Browse** para seleccionar manualmente las licencias. Consulte la sección *Activación de licencia* en la *Guía de instalación y actualización de PowerProtect DP Series Appliance* y la *Guía de implementación de PowerProtect DP Series Appliance*.
IDPA-9456	Se produce un error en la actualización del firmware de Hypervisor y Server de 2.6.1 a 2.7.1.	Póngase en contacto con el servicio de soporte para obtener asistencia.
Avamar-23345	La actualización de Protection Software falla cuando se actualiza PowerProtect DP Series de la versión 2.6.1 a la versión 2.7.1.	Póngase en contacto con el servicio de soporte para obtener asistencia.
Avamar-22044	Se muestra el siguiente error cuando se intenta ver un resumen del cliente Protection Software desde la página **Asset Management**. `Failed to get DR copies` Este error se produce a pesar de que nunca se realizó un respaldo local ni una copia en la nube para el cliente.	Ignore el error, a menos que haya configurado explícitamente las copias de nube que se crearán para el cliente.
Avamar-21807	En la interfaz del usuario de Protection Software, en la página **Restore** > **Destination Location** de la sección **Restore everything to a different location**, si ingresa manualmente la ubicación de restauración en un formato incorrecto, por ejemplo, ***/<nombre_de_carpeta>/<nombre_de_archivo>*** en vez de ***/<nombre de directorio o de carpeta>***, Protection Software no comprueba para verificar la sintaxis de la ubicación de restauración y continúa con la restauración, lo que genera un error.	Cuando ingresa manualmente la ubicación de restauración, debe asegurarse de que la sintaxis de la ubicación de restauración sea correcta para evitar fallas de restauración.
Avamar-22108	Cuando se implementan varios proxies al mismo tiempo, una o más operaciones de implementación de proxy pueden fallar.	Vuelva a intentar la implementación del proxy fallido.
Avamar-22206	Protection Software no le permite deshabilitar la opción getter/setter de SNMP en la página de configuración **Edit DataDomain**.	No se permite deshabilitar la configuración de SNMP mientras se edita la configuración de Protection Storage en Protection Software, a pesar de que la casilla de verificación de SNMP parece estar habilitada.
Avamar-22207	Cuando se habilita FIPS en el tablero de ACM, la habilitación de FIPS falla en Protection Storage (Data Domain) con el siguiente error:	Póngase en contacto con el servicio de soporte para restablecer la contraseña de DDBoost y habilitar FIPS en el dispositivo.

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
	`[Error] Integrating Protection Storage DDBoost password into Backup Server. [Error] Failed to enable FIPS.` Este mensaje de error indica que la contraseña de DDBoost no es compatible con Protection Software (Avamar). Por ejemplo, es posible que la contraseña de DDBoost sea una contraseña MD5 y que Protection Software no sea compatible con las contraseñas MD5.	
Avamar-22213	En la página **Event Management** de la interfaz de Protection Software, se muestra la siguiente advertencia: `Data Domain system not responsive to requests.`	Esta advertencia se muestra cuando Protection Software no puede obtener una respuesta del sistema Protection Storage. Este problema puede ocurrir debido a diversas razones. Asegúrese de que la conexión de red entre Protection Software y Protection Storage esté activa. Si el problema persiste, póngase en contacto con el servicio de soporte de Dell para obtener asistencia.
Avamar-22218	Después de una instalación o actualización, la página **Event Management** en la interfaz del usuario de Protection Software muestra errores de kernel durante el inicio.	Puede ignorar estos eventos de manera segura.
Avamar-22223	Hypervisor Manager no aparece en la pestaña **Administration** > **System** de la interfaz del usuario de Protection Software, lo que impide que el usuario registre o anule el registro de Hypervisor Manager.	Este problema se produce cuando hay una conexión dañada entre una de las instancias de Hypervisor Manager y el dispositivo. Si las conexiones de Hypervisor Manager están inactivas debido a un cambio de contraseña, actualice la contraseña de Hypervisor Manager. Si Hypervisor Manager se desactiva y ya no es necesario, elimine el dominio de Hypervisor Manager en la interfaz del usuario de Protection Software.
Avamar-22228	En la interfaz del usuario de Protection Software, cuando selecciona **Asset Management** > **Clients** > ***<seleccionar cliente>*** > **View More**, es posible que aparezca el siguiente mensaje de error: `Get cloud copy failure Caused by: CDRAOperationException occurred due to: 500, {"message":"","status":null,"code":500}` Este es un mensaje de error interno del servidor que indica que la configuración del dispositivo no está completa porque Cloud DR Server no se ha configurado en Cloud DR.	Póngase en contacto con el servicio de soporte para configurar correctamente Cloud DR Server en su entorno.
Avamar-22232	En la página **Event Management** de la interfaz del usuario de Protection Software, se muestran los siguientes eventos durante la actualización: `RabbitMQ has no connection configured to the Backup & Recovery Manager server.` Durante la actualización del dispositivo, se reinician el componente de Data Protection Central (DPC) y sus servicios. Durante este tiempo, el servicio *Avamar RabbitMQ* no se puede conectar al DPC, lo que provoca que se generen los eventos.	Puede ignorar estos eventos de manera segura. Estos eventos se detienen automáticamente cuando el componente de DPC está disponible después de la actualización. Si los eventos persisten incluso después de que la actualización se completa correctamente, póngase en contacto con el servicio de soporte para obtener asistencia.
Avamar-22239	Después de una interrupción de la alimentación, en la interfaz del usuario de Protection Software, es posible	Debe revertir al último punto de control validado de Protection Software manualmente y verificar que los datos de configuración de Hypervisor Manager, los

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
	que los datos de configuración de vCenter, VM, proxies y políticas de respaldo no aparezcan.	clientes, los proxies y la política de respaldo se muestran en la interfaz del usuario de Protection Software. Si ese no es el caso, póngase en contacto con el servicio de soporte para obtener asistencia.
Avamar-22255	Instant Access falla con el error `Can't find VM Instant Access Agent.`	Reintente el trabajo de acceso instantáneo.
Avamar-22299, IDPA-7634	Como parte de las tareas posteriores a la actualización, ACM crea un punto de control de Protection Software para protegerse contra la pérdida de datos que puede ocurrir debido a un apagado brusco o una interrupción similar. ACM reemplaza al programador de mantenimiento de Protection Software para crear el punto de control en Protection Software. Las actividades de mantenimiento de Protection Software que están en curso en ese momento fallan debido al reemplazo.	La falla de las actividades de mantenimiento activadas por Protection Software es un comportamiento esperado. Puede ignorar la falla de las actividades de mantenimiento porque los datos están protegidos por el punto de control que crea ACM. Asegúrese de conectarse a la interfaz del usuario de Protection Software y confirmar las alertas generadas para la falla. Además, verifique que las siguientes actividades de mantenimiento programadas (dentro de las próximas 24 horas) se realicen correctamente. Póngase en contacto con el servicio de soporte si las actividades de mantenimiento posteriores continúan fallando. Para obtener más información, consulte el *artículo de la base de conocimientos 000191190*.
Avamar-32759	La política de respaldo de Avamar permite agregar un cliente no existente o no válido en **Asset Management** sin autenticación ni validación.	Ninguno
IDPA-5619	Se generan varias alertas dinámicas y se envían por correo electrónico desde ACM, incluso después de deshabilitar el servicio VMware Update Manager.	Ninguno.
IDPA-7477	Después de actualizar el dispositivo, el panel **Appliance** no aparece en el tablero de ACM y se muestra la siguiente advertencia aun cuando la actualización de la infraestructura se haya completado: `Appliance infrastructure components upgrade is pending. Upgrade the infrastructure components to the version bundled in PowerProtect DP series appliance (Build ) to ensure the appliance is on the recommended software and infrastructure version.`	Borre la caché y abra ACM en una nueva ventana del navegador.
IDPA-7730	Cuando configura el entorno LDAP externo en el tablero de ACM, LDAP no se configura correctamente si el nombre de dominio contiene un punto. Por ejemplo, un nombre de dominio como `dc=xyz.ams` produce un error de configuración.	Póngase en contacto con el servicio de soporte para configurar correctamente los nombres de dominio de LDAP que incluyen un punto en los componentes de Search y DPC. Para Search, consulte el capítulo *Administración de funciones y usuarios* de la *Guía de administración e implementación de Dell EMC Search*. Para DPC, consulte el capítulo *Opciones de administración de Data Protection Central* de la *Guía de administración de Dell EMC Data Protection Central*.
IDPA-7798, IDPA-7799	Durante una actualización del dispositivo, es posible que en el entorno de Hypervisor Manager se vean alertas relacionadas con una alta utilización de CPU en los servicios o con el cambio de nombre o la eliminación de servicios como parte de la actualización del dispositivo.	Estas alertas son benignas y se pueden ignorar. **NOTA:** Si hay alertas críticas relacionadas con el hardware, póngase en contacto con el servicio de soporte para obtener asistencia.

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
IDPA-7801	Después de la configuración de red correcta del dispositivo, el proceso de descarga automática de licencia podría tardar horas en completarse. Esto sucede si el puerto 443 está bloqueado en el entorno de red del cliente.	Para resolver este problema, debe desbloquear el puerto de red 443 en el entorno de red.
DDOS-52580	Los registros de Protection Storage muestran muchos mensajes que indican `"sshd" core file generation is disabled`. Estos mensajes de registro se crean cuando FIPS está habilitado en el dispositivo y usted intenta acceder a Protection Storage a través de SSH.	Ninguno
DDOS-108187	Si el sistema Protection Storage tiene millones de archivos en un directorio, es posible que DDFS se reinicie intentando leer el directorio.	A fin de evitar el reinicio de DDFS, se recomienda reestructurar el diseño del directorio para reducir la cantidad de archivos en un solo directorio.
DPC-5869, DPC-5900	Después de una falla de alimentación, cuando el dispositivo DP4400 vuelve a estar en línea, es posible que no pueda acceder a la interfaz del usuario de DPC desde el tablero de ACM debido a que los servicios *elg* o *msm-ui-main* no se inician correctamente.	Póngase en contacto con el servicio de soporte para reiniciar los servicios de DPC mediante el procedimiento descrito en el *artículo de la base de conocimientos 000190695*.
IDPA-5058	Cuando el tablero de ACM se cierra automáticamente después de 15 minutos de inactividad y el usuario no cierra la pestaña/ventana del navegador, el navegador sigue intentando conectarse a ACM con el token de autenticación vencido. Esto provoca que se registren varios errores de tokenización de autenticación en el archivo server.log de ACM.	Vuelva a iniciar sesión para acceder al tablero de ACM o cierre la ventana del navegador que cerró la sesión y que no está en uso.
IDPA-7346	Durante la actualización del dispositivo, es posible que se cierre la sesión de la página **Upgrade**.	Inicie sesión en ACM y se lo dirigirá a la página **Upgrade**.
Avamar-22142	Los trabajos de respaldo pueden completarse con excepciones cuando **Encryption method to Data Domain system** se configura en un valor **Medium**.	Establezca **Encryption method to Data Domain system** en el valor **Default**.
IDPA-7534	Durante una instalación nueva, no puede continuar desde la página **General Settings** porque el cuadro desplegable **Timezone** no se completa. El campo **Timezone** no se completa cuando la configuración de idioma del navegador tiene un idioma diferente del inglés.	Consulte el *artículo de la base de conocimientos 000081518* y resuelva el problema.
IDPA-7405	Durante la nueva instalación de DP8400 y DP8900, la configuración de Protection Software falla con un error de frase de contraseña vacía. Este problema se produce cuando instala el paquete de Protection Storage y la interfaz del usuario de **Avamar Installer Manager** se mantiene abierta.	Revierta ACM y vuelva a implementar la imagen de Protection Software.
Avamar 21543	La pestaña **System** de la interfaz del usuario de Protection Software puede mostrar un error que indica **Failed to Get Private Entry** con el siguiente mensaje de error: `Http failure response for https://dp4400-19-5.datadomain.com/acm/api/keystore/web/cert: 503 Service Unavailable`	1. Inicie sesión en Avamar mediante SSH como usuario administrador. 2. Ejecute el siguiente comando para eliminar el archivo acm.pid: `rm /usr/local/acm/bin/acm.pid` 3. Ejecute el siguiente comando para iniciar acmservice: `/usr/local/acm/bin/acmservice start`

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
Avamar-22221	La restauración a nivel de archivos (FLR) no es posible para ningún respaldo almacenado en la nube. Si intenta restaurar un respaldo en la nube, es posible que aparezca un mensaje de error en la ventana **Restore Cloud Backup**, tras lo cual se deselecciona la opción FLR.	Realice una restauración completa del respaldo localmente y recupere los archivos que desee.
Avamar-21993	**Asset Management** de Avamar permite la inclusión de clientes no válidos o con valor de elementos no utilizados sin realizar comprobaciones de verificación.	Ninguno
Avamar-21901	La página de políticas de Avamar le permite crear una copia de una política existente con un nombre no válido.	Ninguno
IDPA-3546	No se puede cambiar la contraseña del dispositivo cuando se ejecutan trabajos en Protection Software.	Cambie la contraseña del dispositivo durante una ventana de mantenimiento cuando no haya trabajos en ejecución en Protection Software.
Avamar-22258	Es posible que aparezca el siguiente mensaje de error después de una instalación nueva o cuando el dispositivo se actualiza a la versión 2.7: `RabbitMQ is misconfigured. The problem could not be corrected.`	Puede ignorar este error.
Avamar-22176	Es posible que el paquete acumulativo del SO de Protection Software no se instale durante una actualización.	Detenga la actualización de software en la interfaz del usuario de **Avamar Installation Manager** y vuelva a intentar la actualización de Protection Software en ACM.
IDPA-6188	Durante la actualización de software de la versión 2.6 a la versión 2.7 o versiones posteriores, ACM no se redirecciona automáticamente después de completar la comprobación de preparación para la actualización y, en su lugar, se muestra el cuadro de diálogo **Upgrade** con un enlace.	Haga clic manualmente en el enlace para continuar con la actualización. También puede intentar abrir el siguiente enlace en un navegador `https://<ACM_IP>:9443/`
IDPA-5756	Cuando se solucionan fallas de instalaciones nuevas, la configuración de Protection Storage falla con `Failed to create ifgroup` después del primer intento de reversión del dispositivo. Pero sin intervención alguna, la creación de `ifgroup` se realiza correctamente durante el siguiente intento de reversión.	Realice la reversión del dispositivo, espere 5 minutos y continúe con la implementación.
Avamar-40228	La restauración a nivel de archivos (FLR) muestra una carpeta con datos vacíos en la GUI de MC. Este problema se debe al uso de caracteres especiales.	Para resolver el problema, consulte el *artículo de la base de conocimientos 000165929*.

DDOS-90529	Cuando el tiempo se retrasa entre el DPC y los componentes configurados para Single Sign On (SSO), las operaciones de SSO pueden fallar.	1. Conéctese al servicio de DPC mediante SSH con credenciales de administrador.
		2. Verifique que el servidor NTP correcto esté configurado en el archivo ntp.conf en la siguiente ubicación:
		`more/etc/ntp.conf`
		3. Compruebe el estado del demonio NTPD mediante el siguiente comando:
		`systemctl status ntpd`
		a. Si el estado es “inactive”, inicie el servicio ntpd mediante `systemctl start ntpd`.
		b. Si el estado es “disabled”, habilite el servicio ntpd mediante `systemctl enable ntpd`.

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
DDOS-91798	La página Avamar Activity deja de responder cuando el usuario hace clic en *Completed Replication activity*.	Ninguno. Para obtener más información, consulte el *artículo de la base de conocimientos 000182250*.
DDOS-65860	Los trabajos de respaldo fallan con `avtar Error <41439>: Using invalid token:xxx` en el registro de respaldo o restauración de avtar. Aquí, *:xxx* es un marcador de posición para el token. El token en el error es un valor de hash de un token vacío que avtar obtiene del servidor de Protection Software. El error `DDR result code: 5002, desc: value exceeds upper bound` también se registra en el registro *ddrmaint*. Cuando el servicio ddrmaint solicita un token de Protection Storage para respaldos, se activa un reintento si falla la conexión de red. Después de una determinada cantidad de reintentos, el contador de reintentos en *ddboost* se pierde y la solicitud de token falla.	Reinicie el servicio **`ddrmaint`** en el servidor de Protection Software mediante el comando `ddrmaint-service restart`. Para obtener más información, consulte el *artículo de la base de conocimientos 546535*.
DDOS-69689	Data Protection Central informa que Protection Storage no está registrado para SSO.	Elimine la confianza de Data Protection Central en el sistema Protection Storage mediante el comando `adminaccess trust del host <IDPA_System_Manager_hostname>`. Después de esto, si el nombre de host de Data Protection Central no se puede resolver desde Protection Storage, agregue un mapeo de host a IP en Protection Storage mediante el comando `net hosts add {<ipaddr> | <ipv6addr>} <host-list>`.
DDOS-63142	Durante el arranque de ACM, se muestran algunos errores en la consola.	Estos mensajes pueden ignorarse. Estos errores no afectan la funcionalidad de PowerProtect DP Series Appliance.
DDOS-67878, DDOS-67789 y DDOS-67788	El registro de los componentes de PowerProtect DP Series Appliance para SRS falla en los entornos de red IPv6.	Registrarse en SRS es una tarea opcional. Puede optar por omitir el registro de los componentes para SRS. Si SRS es obligatorio, configure PowerProtect DP Series Appliance en un entorno de red IPv4.
261749	Cuando PowerProtect DP Series Appliance pierde energía bruscamente, por ejemplo, durante una interrupción de la alimentación, es posible que algunos de los servicios de Protection Software y Data Protection Central no se inicien de manera oportuna.	Realice estos pasos para resolver el problema: 1. Inicie manualmente los servicios de Protection Software con el comando: `# dpnctl start all --ignore_lock` 2. Inicie manualmente los servicios de SSO de DPC mediante el comando: `# service dpc-sso start`
257875	La implementación del servidor de VM Proxy falla si el DNS del puerto de red 53 está bloqueado.	Debe abrir temporalmente el DNS del puerto de red 53 durante la configuración.
260493	Los siguientes problemas se producen cuando el sistema de archivos en el punto de montaje `/storage/seat` del servicio de Hypervisor Manager Server carece de espacio libre suficiente: • Todas las operaciones, como implementaciones opcionales de productos puntuales desde el tablero de ACM, actualizaciones, configuración de descarga de PDF y cambio de contraseña realizados en Hypervisor Manager Server, fallan.	Póngase en contacto con el servicio de soporte para aumentar la capacidad del sistema de archivos que se monta en el punto de montaje `/storage/seat`. Para obtener más información, consulte el *artículo de la base de conocimientos 540267*.

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
	El siguiente error aparece en el archivo `server.log`: `Exception occurred while creating ViJava service instance with persisted vCenter parameters. java.lang.NullPointerException.` • Cuando se conecta a la interfaz del usuario de Hypervisor Manager Server, se muestra el siguiente error: `Could not connect to one or more vCenter Server Systems: https://vCenterFQDN:443/sdk.`	
251361	La cuenta de usuario de Protection Storage se bloquea debido a credenciales incorrectas en **Data Protection Central Issue Summary <Issue ID>**. Se recomienda cambiar la contraseña de administrador de Protection Storage a través del tablero de ACM. Si la contraseña se cambia directamente en el sistema Protection Storage, debe editar el sistema Protection Storage en Data Protection Central para actualizar la información de identificación. Si no actualiza la contraseña en Data Protection Central, el sistema Protection Storage bloquea la cuenta de usuario.	Para desbloquear la cuenta de usuario de Protection Storage, realice los siguientes pasos: • Quite el sistema Protection Storage de Data Protection Central. • Desbloquee la cuenta de usuario del sistema Protection Storage. Para obtener más información, consulte la *Guía de administración de Data Domain*. • Vuelva a agregar el sistema Protection Storage a Data Protection Central con la información de identificación actualizada.
250098	Después de realizar la expansión del disco, la alarma `Datastore usage on disk` se muestra en la pestaña **vSphere Web console** > **Summary**	Confirme la alarma. Para obtener más información, consulte el PowerProtect DP Series Appliance *artículo de la base de conocimientos 526173*.
257188	En Protection Software, cuando se realiza un respaldo de Oracle RAC, el respaldo falla con el error de Rman: `ORA-12162: TNS:net service name is incorrectly specified`.	Para resolver el problema, consulte el *artículo de la base de conocimientos 0469860*.
229047	Los servicios de Reporting & Analytics no se inician cuando los servicios de Reporting & Analytics se encienden manualmente.	Inicie los servicios de Reporting & Analytics manualmente. Para obtener instrucciones sobre cómo iniciar los servicios manualmente, consulte la sección *Solución de problemas de inicio* en la *Guía del producto PowerProtect DP Series Appliance*.
232845	Durante la implementación de DP4400, se muestran las siguientes alarmas de advertencia en la pestaña **vSphere Web console** > **Summary**: • `Datastore usage on disk` • `Registration/unregistraion of third-party IO filter storage providers fails on a host`	Confirme las alarmas. Para obtener más información, consulte los PowerProtect DP Series Appliance*artículos de la base de conocimientos 526173 y 526174*.
209463	Este problema se produce con los modelos DP5300, DP5900, DP8400 y DP8900. Surge cuando utiliza el asistente de configuración de ACM y omite la configuración de Dell EMC Secure Remote Services para PowerProtect DP Series Appliance y continúa con la configuración. El campo **Serial Number** de SRS en la página **General Settings** no se puede editar después de realizar estos pasos: 1. Ingrese el número de serie de SRS en la página **General Settings**. 2. Haga clic en **Next**.	Edite el archivo `/usr/local/dataprotection/var/configmgr/server_data/skuconfig/selskuconfig.xml` en ACM y quite el valor de *SerialID*. El campo **Serial Number** de la página **General Settings** se puede editar después de actualizar el archivo `selskuconfig.xml`.

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
	3. Haga clic en **Previous** para volver a la página **General Settings**. No puede editar el campo **Serial Number**.	
227371	PowerProtect DP Series Appliance utiliza la red *192.168.x.x* internamente para comunicarse con los diferentes componentes. Si alguna de estas direcciones IP ya está en uso, hay un conflicto de dirección IP.	Resuelva el conflicto de dirección IP e inténtelo nuevamente. Si los usuarios no pueden utilizar el rango de IP interno predeterminado (192.168.x.x), póngase en contacto con el servicio de soporte para obtener asistencia con el cambio del rango de IP interno en el dispositivo.
230468	Después de actualizar el dispositivo, se muestra una advertencia en Hypervisor Manager sobre un posible problema vulnerable que se describe en CVE-2018-3646. CVE-2018-3646 es una de las vulnerabilidades de ejecución especulativa de falla de terminal L1 (L1TF) y se determina que tiene un puntaje de vulnerabilidad medio. PowerProtect DP Series Appliance es un entorno restringido donde las máquinas virtuales no verificadas no se implementan en Hypervisor. Además, debido a graves sanciones de rendimiento, no se recomienda habilitar la corrección en el dispositivo PowerProtect DP Series Appliance.	PowerProtect DP Series Appliance utiliza la versión de Hypervisor que tiene las siguientes correcciones para esta vulnerabilidad; sin embargo, una de ellas no está habilitada de manera predeterminada, ya que tiene un impacto grave en el rendimiento: • Moderación del vector de ataque secuencial de contexto: esta corrección se aplica automáticamente tan pronto como se actualiza. • Moderación del vector de ataque de contexto simultáneo: esta corrección no está habilitada de manera predeterminada Esta corrección se puede habilitar mediante pasos simples en Hypervisor, pero tiene graves sanciones de rendimiento si se habilita. Se recomienda no habilitarla. Sin embargo, los clientes pueden habilitarla bajo su propio riesgo. Para obtener más información, consulte el *artículo de la base de conocimientos 55806* de VMware.
187844	La hora registrada en los registros del servidor de ACM no coincide con la hora del sistema operativo.	Para sincronizar las horas, reinicie el servicio dataprotection_webapp. 1. Conéctese a ACM mediante un cliente SSH para obtener acceso a su dirección IP. 2. Para detener el servicio, escriba: **`service dataprotection_webapp stop`** 3. Para volver a iniciar el servicio, escriba: **`service dataprotection_webapp start`**
192524	Las alertas que indican que se ha excedido el umbral de espacio de disco aparecen en Hypervisor Manager.	La alerta no afecta la funcionalidad y puede ignorarse.
194689, 194906	ACM no acepta caracteres no ingleses en ningún campo, incluidas las contraseñas.	Use solo caracteres en inglés.
197954	Si se seleccionan más de 4,000 eventos para exportar desde el panel **Event details** en la pestaña **Health**, ocurre un error en el trabajo de exportación. En el panel **Event details**, se muestran los 10 eventos en cada página, por lo que, si el recuento de páginas en la parte inferior de la pestaña es 401 o superior, hay más de 4,000 eventos.	No intente exportar más de 4,000 eventos a la vez. Si existen más de 400 páginas de eventos en el panel **Event details**, use los filtros para reducir la cantidad de eventos que se muestran y exporte múltiples informes si es necesario.
199598	En la pestaña **Health** de ACM, no se explica la opción **Today** en el cuadro de filtro de tiempo.	Al seleccionar **Today**, se enumeran los eventos que han ocurrido desde la medianoche hasta el presente.
203386	Si se realizan demasiados intentos fallidos para iniciar sesión en Data Protection Central con la contraseña incorrecta, Data Protection Central impide que el	Inicie sesión en la consola de Data Protection Central como usuario raíz y ejecute el siguiente comando: `# pam_tally2 --user=admin --reset`

Tabla 4. Problemas conocidos con una solución alternativa/resoluciones (continuación)

Número de problema	Descripción del problema	Solución alternativa/resolución
	usuario administrador inicie sesión. Esto puede suceder cuando se almacena la contraseña incorrecta en ACM.	
211137	La opción de olvido de contraseña en la página de inicio de sesión de Cloud DR no funciona si la cuenta de nube y el ID de correo electrónico no están establecidos en la configuración de Cloud DR.	El usuario debe configurar manualmente la cuenta de nube y el ID de correo electrónico en Cloud DR.
214645	DPC Alert detectó que la autenticación de usuario y la conexión al sistema Protection Storage fallaron, pero no hay ningún mensaje de seguimiento que indique que Protection Storage se volvió a conectar. Esto hace que sea confuso para los usuarios comprender el estado de Protection Storage.	Uso del botón **Dismiss Alert** en la parte superior de la pantalla **Alerts** para eliminar esas alertas obsoletas de DPC. **NOTA:** Para obtener más detalles, consulte la sección *Descartar alertas de estado* en la *Guía del administrador de DPC*.
215307	En AUI, la adición de dos direcciones IP del servidor DNS en la nueva configuración de AVProxy hace fallar la restricción de admitir solo una IP.	AUI permite ingresar solo una dirección DNS para crear el proxy.

Falsos positivos

En esta sección, se describen los problemas de falsos positivos de ACM y de los dispositivos en esta versión de PowerProtect DP Series Appliance.

Tabla 5. Falsos positivos

Número de problema	Descripción del problema
CVE-2021-44228	Cuando algunas herramientas de análisis de seguridad se ejecutan en los componentes de DPC y CDRA de PowerProtect DP Serie, muestran que es vulnerable para CVE-2021-44228, pero no se hace referencia a la biblioteca log4j afectada ni se carga en ningún servicio.
SLES-12-010400	No debe haber ningún archivo *.shosts* en el sistema operativo SUSE.
SLES-12-010410	No debe haber ningún archivo *shosts.equiv* en el sistema operativo SUSE.
SLES-12-010610	La secuencia de teclas Ctrl-Alt-Supr de x86 debe estar deshabilitada en el sistema operativo SUSE: • `systemctl` • `Información`
SLES-12-010611	La secuencia de teclas Ctrl-Alt-Supr de x86 debe estar deshabilitada en el sistema operativo SUSE para las interfaces gráficas de usuario.
SLES-12-010650	La cuenta raíz del sistema operativo SUSE debe ser la única que tenga acceso sin restricciones al sistema.
SLES-12-030040	SuSEfirewall2 debe protegerse contra los ataques de denegación de servicio (DoS) o limitarlos en el sistema operativo SUSE. Esto se debe realizar mediante la implementación de medidas de limitación de velocidad en las interfaces de red afectadas. ACM en PowerProtect DP Series Appliance 2.6 cuenta con el firewall y las reglas necesarios.
SLES-12-030100	Todos los sistemas operativos SUSE en red deben tener e implementar SSH. para proteger la confidencialidad y la integridad de la información transmitida y recibida, así como la información durante la preparación para la transmisión activa
SLES-12-030150	El sistema operativo SUSE no debe permitir el inicio de sesión automático mediante SSH.
SLES-12-030260	Se deben cifrar las conexiones X remotas enviadas con el demonio SSH del sistema operativo SUSE para los usuarios interactivos.
NESSUS-136808	Denegación de servicio en ISC BIND.

Tabla 5. Falsos positivos (continuación)

Número de problema	Descripción del problema
	El falso positivo como ACM en PowerProtect DP Series Appliance 2.6 utiliza SLES 12 SP4. Según la base de conocimientos (KB) de CVE de Suse para CVE-2020-8617, este problema se resolvió en la versión de BIND *9.11.2-3.17.1*. ACM en PowerProtect DP Series Appliance 2.6 utiliza la misma versión de BIND y este problema no afecta a PowerProtect DP Series Appliance 2.6.
NESSUS-20007	Detección de protocolos SSL versión 2 y 3: ACM no utiliza ningún protocolo SSLv2 o SSLv3 para ninguna conexión segura

Limitaciones

En esta versión se identificaron las siguientes limitaciones.

- La activación dentro del producto no es compatible en los siguientes casos:
  - En la red habilitada para IPv6
  - ACM se utiliza como DNS
- Cyber Recovery (CR)
  - Incompatible con la red IPV6
  - Cuando se implementa CR, no puede configurar los componentes opcionales como Data Protection Central, Reporting & Analytics, Cloud Disaster Recovery y Search en el dispositivo.
  - CR no cumple con FIPS
  - CR no es compatible con la integración de AD o LDAP
- Por lo general, el sistema PowerProtect DP Series Appliance Protection Storage con nivel de nube integrado contiene las siguientes métricas de uso de capacidad:
  - Capacidad de nivel activo
  - Capacidad de nivel de nube
  - Capacidad total

  El panel **Capacity** del tablero **Avamar Administrator** muestra las estadísticas de capacidad total de Protection Storage y no las estadísticas de capacidad de nivel activo. Para obtener más información acerca de las estadísticas de capacidad, consulte el *artículo de la base de conocimientos 542695*.

  Puede ver el uso de la capacidad de nivel activo de Protection Storage en las siguientes ubicaciones:

  - La página de inicio de ACM.
  - En la interfaz del usuario de Protection Storage, en **Data Domain UI** > **Data Management**.
  - La CLI de Protection Storage.
- Limitaciones cuando FIPS está habilitado:
  - Search y Cloud Disaster Recovery no son compatibles con FIPS. Estos componentes no están disponibles cuando FIPS está habilitado. VM Proxy está disponible para respaldos fuera de PowerProtect DP Series Appliance.
  - Sin alertas por correo electrónico.
  - Una vez que FIPS está habilitado, no puede revertir ni deshabilitar FIPS. Comuníquese con el soporte de Dell EMC para obtener ayuda.
- Una vez que la configuración de red se realiza correctamente, no puede alternar entre IPv6 e IPv4. Comuníquese con el soporte de Dell EMC para obtener ayuda.

Número de problema	Descripción
DDOS-93905	La vulnerabilidad de desbordamiento de buffer basado en memoria dinámica (CVE-2021-3156) en SUSE SLES12 se indica para Reporting & Analytics y para el SO ACM.
DDOS-67878	El registro de SRS para la cuadrícula de Protection Software no funciona en PowerProtect DP Series Appliance configurado con IPv6.
DDOS-67789	El registro de SRS para Reporting & Analytics no funciona en PowerProtect DP Series Appliance configurado con IPv6.
DDOS-67788	El registro de SRS para Protection Storage no funciona en PowerProtect DP Series Appliance configurado con IPv6.

Número de problema	Descripción
232027	Si no se puede acceder a un componente durante el proceso de actualización, dicho proceso falla para ese componente. Además, dado que no se puede acceder al componente, las operaciones de reversión y reintento también fallan. Póngase en contacto con el servicio de soporte para resolver la inaccesibilidad del componente y vuelva a intentarlo.

Requisitos del sistema y del ambiente

Para que PowerProtect DP Series Appliance funcione correctamente, asegúrese de que el entorno cumpla con estos requisitos mínimos.

Compatibilidad de software

Consulte la *Guía de compatibilidad de software de PowerProtect DP Series Appliance* para obtener información sobre compatibilidad e interoperabilidad.

Requisitos para ACM

Haga lo siguiente:

- Asegúrese de que estén disponibles las licencias requeridas para el dispositivo y los componentes. Para obtener más información sobre licenciamiento, consulte https://community.emc.com/community/labs/tes.
- Instale Google Chrome 75 y versiones posteriores, o Mozilla Firefox 50 y versiones posteriores.
- Asegúrese de que todos los nodos físicos estén accesibles.

  NOTA: Este requisito se aplica a DP5900, DP8400 y DP8900.
- De manera opcional, puede configurar Secure Remote Services VE Gateway (configuración centralizada) para Protection Storage, Protection Software, ACM y Reporting & Analytics.

  NOTA: Para obtener más información sobre Secure Remote Services, consulte el documento *Descripción técnica de Secure Remote Services*.

Documentación

En esta sección, se proporciona información acerca de documentos adicionales que puede consultar para obtener más información sobre PowerProtect DP Series Appliance y sus componentes individuales, y recursos de capacitación.

Referencias documentales para PowerProtect DP Series Appliance

La documentación de PowerProtect DP Series Appliance incluye las siguientes publicaciones:

- *Guía de instalación y actualización de PowerProtect DP Series Appliance*

  Instrucciones para instalar el hardware y el software de PowerProtect DP Series Appliance DP4400. La guía también contiene instrucciones para actualizar DP5900.
- *Guía de implementación de servicios profesionales y de campo de PowerProtect DP Series Appliance para DP5xxx y DP8xxx*

  Instrucciones para instalar y configurar PowerProtect DP Series Appliance DP5xxx y DP8xxx.
- *Guía del producto PowerProtect DP Series Appliance*

  Proporciona una visión general e información de administración del sistema PowerProtect DP Series Appliance.
- *Notas de la versión de PowerProtect DP Series Appliance*

  Información del producto acerca de la versión actual de PowerProtect DP Series Appliance.
- *Guía de configuración de seguridad de PowerProtect DP Series Appliance*

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 PowerProtect DP Series Appliance*

  Información sobre los componentes de software y las versiones que se usan en el producto PowerProtect DP Series Appliance.

- *Guía del procedimiento de reparación de PowerProtect DP Series Appliance DP4400*

  Procedimientos para reemplazar o actualizar los componentes de hardware de PowerProtect DP Series Appliance.

- *Guía de reemplazo de campo de PowerProtect DP Series Appliance para DP5xxx y DP8xx*

  Instrucciones para agregar, reemplazar y reparar componentes de hardware de DP5xxx y DP8xxx

Referencias de documentos para los componentes individuales

La documentación para estos componentes se puede obtener desde 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 Protection Software

Los siguientes documentos contienen información que se relaciona con Protection Software:

- *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 Protection Software 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 los servicios de VMware.

- *Guía del usuario de Avamar NDMP Accelerator para Oracle ZFS*

  En esta publicación, se describe cómo instalar, configurar, administrar y usar Protection Software NDMP Accelerator (acelerador) para respaldar y restaurar los dispositivos de almacenamiento Oracle ZFS compatibles.

- *Guía del usuario de Avamar NDMP Accelerator para filers de NetApp*

  En esta publicación, se describe cómo instalar, configurar, administrar y usar Protection Software NDMP Accelerator (acelerador) para respaldar y restaurar los filers de NetApp compatibles.

- *Guía del usuario de Avamar NDMP Accelerator para sistemas NAS de EMC*

  En esta publicación, se describe cómo instalar, configurar, administrar y usar Protection Software NDMP Accelerator (acelerador) para respaldar y restaurar los sistemas EMC Isilon, Unity, VNX, VNXe y Celerra compatibles.

- *Guía del usuario de Avamar para VMware*

  En esta publicación, se describen diferentes métodos y estrategias para proteger las máquinas virtuales 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 de administración 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.

Search

El siguiente documento contiene información que se relaciona con Search:

- *Guía de instalación y administración de Search*

  En esta publicación, se describe cómo instalar, mantener y configurar Search.

Cloud DR

Los siguientes documentos contienen información que se relaciona con Cloud Disaster Recovery:

- *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 Cloud Disaster Recovery*

  En este documento, se describe cómo instalar, implementar y utilizar el producto DD Cloud DR.

Cyber Recovery

Los siguientes documentos contienen información que se relaciona con Cyber Recovery:

- *Guía del producto PowerProtect Cyber Recovery*

  En esta guía, se describe cómo utilizar la solución Cyber Recovery para proteger los datos.

- *Guía de instalación de PowerProtect Cyber Recovery*

  En este documento, se describe cómo instalar, actualizar, aplicar parches y desinstalar el software Dell EMC PowerProtect Cyber Recovery.

- *Guía de configuración de seguridad de PowerProtect Cyber Recovery*

En esta guía, se proporciona una visión general de la configuración de Dell EMC PowerProtect Cyber Recovery para el control de acceso, los archivos de registro, la comunicación y la seguridad de los datos. También incluye información útil sobre las licencias y la integridad del código de Cyber Recovery, los parches de seguridad, la protección contra malware y la seguridad manual del vault.

Recursos de capacitación de PowerProtect DP Series Appliance

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

Puede obtener más información y capacitación adicional sobre PowerProtect DP Series Appliance en https://education.dellemc.com.

Solución de problemas y ayuda

La página de soporte de ofrece acceso a información de licencias, documentación de productos, asesorías, descargas e información práctica y de solución de problemas. Esta información puede permitirle resolver un problema con un producto antes de comunicarse con el servicio al cliente.

NOTA: El número de artículo se cambia para algunos de los artículos de la base de conocimientos. Sin embargo, cuando realiza una búsqueda con el número de artículo de la base de conocimientos anterior, el artículo correcto se muestra en “Possible Matches”.

Adónde recurrir para obtener soporte

El sitio web de soporte https://www.dell.com/support brinda acceso a información sobre solución de problemas, instrucciones, descargas, recomendaciones, documentación y licenciamiento de productos. Esta información puede ayudarlo a resolver un problema con un producto sin tener que comunicarse con el servicio de soporte.

Para acceder a la página específica de un producto:

1. Vaya a https://www.dell.com/support.
2. En el campo de búsqueda, escriba el nombre de un producto y luego seleccione el producto en la lista que aparezca.

Base de conocimientos

La base de conocimientos contiene soluciones aplicables que puede buscar por número de solución (por ejemplo, KB000xxxxxx) o por palabra clave.

Para buscar en la base de conocimientos:

1. Vaya a https://www.dell.com/support.
2. En la pestaña **Support**, haga clic en **Knowledge Base**.
3. En el cuadro de búsqueda, escriba el número de la solución o las palabras clave. De manera opcional, puede limitar la búsqueda a productos específicos si escribe un nombre de producto en el cuadro búsqueda y selecciona el producto en la lista que aparezca.

Chat en línea

Para participar en un chat interactivo en vivo con un agente de soporte, haga lo siguiente:

1. Vaya a https://www.dell.com/support.
2. En la pestaña **Support**, haga clic en **Contact Support**.
3. En la página **Contact Information**, haga clic en el soporte correspondiente y luego continúe.

Las solicitudes de servicio

Para que el área de licencia le brinde ayuda en profundidad, envíe una solicitud de servicio. Para enviar una solicitud de servicio, haga lo siguiente:

1. Vaya a https://www.dell.com/support.
2. En la pestaña **Support**, haga clic en **Service Requests**.

NOTA: Para crear una solicitud de servicio, debe contar con un acuerdo de soporte técnico válido. Comuníquese con un representante de ventas para obtener detalles acerca de una cuenta o de la obtención de un acuerdo de soporte válido. Para obtener los detalles de una solicitud de servicio, en el campo `Service Request Number`, ingrese el número de solicitud de servicio y haga clic en la flecha hacia la derecha.

Para revisar una solicitud de servicio abierta:

1. Vaya a https://www.dell.com/support.
2. En la pestaña **Support**, haga clic en **Service Requests**.
3. En la página **Service Requests**, en **Manage Your Service Requests**, haga clic en **View All Dell Service Requests**.

Comunidades en línea

Para acceder a contactos con colegas, a conversaciones y a contenido sobre soporte y soluciones de productos, vaya a la red de comunidad de https://community.emc.com. Participe de manera interactiva en línea con clientes, partners y profesionales calificados.

Cómo proporcionar comentarios

Sus comentarios ayudan a mejorar la exactitud, la organización y la calidad general de las publicaciones. Puede enviar comentarios a DPAD.Doc.Feedback@emc.com.

Notas, precauciones y advertencias

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

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

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