

Dell EMC PowerStore

Guía de planificación

Versión 3.x

Notas, precauciones y avisos

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

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

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

Tabla de contenido

Recursos adicionales.....	5
Capítulo 1: Introducción.....	6
Introducción a PowerStore.....	6
Dispositivos.....	6
Clústeres.....	7
Visión general de la planificación y la instalación.....	8
Capítulo 2: Planificación del sitio.....	10
Pautas de espacio en el rack.....	10
Especificaciones técnicas.....	10
Dimensiones y peso del gabinete base.....	10
Dimensiones y peso del Gabinete de expansión de SAS.....	10
Dimensiones y peso del Gabinete de expansión de NVMe.....	11
Requisitos de alimentación del gabinete base.....	12
Requisitos de alimentación del Gabinete de expansión de SAS.....	13
Requisitos de alimentación del Gabinete de expansión de NVMe.....	13
Límites del entorno operativo.....	14
Requisitos de envío y almacenamiento.....	14
Capítulo 3: Requisitos de licenciamiento y de la estación de trabajo.....	17
Licenciamiento de PowerStore.....	17
Licenciamiento de VMware (para dispositivos Modelo PowerStore X).....	17
Requisitos de la estación de trabajo.....	18
Utilidad de descubrimiento de PowerStore.....	18
Capítulo 4: Conectividad de soporte.....	19
Descripción operacional de Conectividad de soporte.....	19
Conectividad de soporte y seguridad.....	19
Administración de Conectividad de soporte.....	19
Comunicación de Conectividad de soporte.....	20
Soporte remoto de Conectividad de soporte.....	20
Opciones de Conectividad de soporte.....	20
Conectividad de soporte con el uso de la opción Gateway de conexión segura.....	21
Conectividad de soporte con el uso de la opción Conectarse directamente.....	21
Requisitos para Conectividad de soporte con el uso del gateway de conexión segura.....	21
Requisitos para Conectividad de soporte con el uso de Conectarse directamente.....	22
Configuración de Conectividad de soporte.....	22
Establecer la configuración inicial de Conectividad de soporte.....	22
Administrar los ajustes de Conectividad de soporte.....	24
CloudIQ.....	25
Seguridad cibernética.....	25
Apéndice A: Uso de los puertos.....	26

Puertos de red del dispositivo.....	26
Puertos de red del dispositivo relacionados con archivos.....	28
Puertos de red relacionados con los dispositivos modelo X de PowerStore.....	32
Apéndice B: Hojas de trabajo de planificación de espacio en el rack.....	34
Ejemplo de Hoja de trabajo para la planificación de espacio en el rack.....	34
Hoja de trabajo en blanco para la planificación de espacio en el rack.....	35

 **NOTA:** PowerStore OS 3.0.0 admite únicamente los modelos PowerStore T.

 **NOTA:** Los modelos PowerStore x200 están disponibles solo como PowerStore T.

Como parte de un esfuerzo por mejorar, se lanzan periódicamente revisiones de software y hardware. Algunas funciones que se describen en este documento no son compatibles con todas las versiones del software o el hardware actualmente en uso. Las notas de la versión del producto proporcionan la información más actualizada acerca de las características del producto. Póngase en contacto con el proveedor de servicio si un producto no funciona correctamente o como se describe en este documento.

Dónde obtener ayuda

La información sobre soporte, productos y licenciamiento puede obtenerse de la siguiente manera:

- **Información de productos**

Para obtener documentación o notas de la versión de productos y funciones, vaya a la página PowerStore Documentation en <https://www.dell.com/powerstoredocs>.

- **Solución de problemas**

Para obtener información sobre productos, actualizaciones de software, licenciamiento y servicio, vaya a <https://www.dell.com/support> y busque la página de soporte del producto correspondiente.

- **Soporte técnico**

Para obtener soporte técnico y realizar solicitudes de servicio, vaya a <https://www.dell.com/support> y busque la página **Service Requests**. Para abrir una solicitud de servicio, debe contar con un acuerdo de soporte técnico válido. Póngase en contacto con el representante de ventas para recibir información sobre cómo obtener un acuerdo de soporte técnico válido o para aclarar cualquier tipo de duda en relación con su cuenta.

- **Documentación para versiones anteriores**

Para obtener documentación de las versiones anteriores de PowerStore, vaya a la página Documentación de PowerStore en <https://www.dell.com/powerstoredocs>.

Introducción

Utilice este documento para comprender mejor el proceso de instalación y preparar el sitio y la estación de trabajo para una correcta implementación de PowerStore. Este capítulo incluye los siguientes temas:

Temas:

- [Introducción a PowerStore](#)
- [Visión general de la planificación y la instalación](#)

Introducción a PowerStore

PowerStore alcanza nuevos niveles de simplicidad y agilidad operacionales con el uso de una arquitectura de microservicios basados en contenedores, tecnologías de almacenamiento avanzadas y aprendizaje automático incorporado para liberar la potencia de los datos. PowerStore es una plataforma versátil con diseño centrado en el rendimiento que ofrece una escala multidimensional, reducción de costos siempre activa y compatibilidad con medios de última generación. Aporta la simplicidad de la nube pública a la infraestructura en las instalaciones para optimizar las operaciones con un motor de aprendizaje automático incorporado y una automatización transparente, a la vez que ofrece análisis predictivo para monitorear, analizar y solucionar problemas del entorno con facilidad. PowerStore también es altamente adaptable, ya que proporciona la flexibilidad para alojar cargas de trabajo especializadas directamente en el dispositivo y modernizar la infraestructura sin interrupciones, junto con ofrecer protección de la inversión mediante soluciones de pago flexibles y actualizaciones de los datos en el lugar.

Los dispositivos PowerStore están disponibles en uno de los siguientes modelos de implementación:

- Los dispositivos Modelo PowerStore T (500T, 1000T, 1200T, 3000T, 3200T, 5000T, 5200T, 7000T, 9000T y 9200T) se centran en el almacenamiento y permiten administrar y aprovisionar almacenamiento de bloques y archivos a hosts externos. Durante la configuración inicial, puede optar por configurar un dispositivo para almacenamiento unificado (bloques y archivos) u optimizado para bloques (solo de bloques).
- Los dispositivos Modelo PowerStore X (1000X, 3000X, 5000X, 7000X y 9000X) se centran en las aplicaciones y el almacenamiento, y proporcionan una capa de hipervisor además del almacenamiento de bloques. Esta funcionalidad adicional le permite implementar y administrar máquinas virtuales y aplicaciones.

Dispositivos

Un dispositivo PowerStore es un componente preconfigurado de la infraestructura que tiene recursos de almacenamiento y computación. Un dispositivo consta de lo siguiente:

- Un gabinete base: contiene hasta 25 unidades (mínimo de seis unidades) e incluye dos nodos para alta disponibilidad con protección de datos que se implementa en los nodos.
- Un gabinete de expansión: permite agregar más unidades y aumentar la capacidad de almacenamiento del dispositivo. Puede agregar hasta tres gabinetes de expansión.
 - El PowerStore 500T admiten el Gabinete de expansión de NVMe.
 - Todos los demás modelos de PowerStore admiten el PowerStore o el Gabinete de expansión de NVMe.

NOTA: No se admite la combinación de Gabinete de expansión de NVMe y Gabinete de expansión de SAS en el mismo dispositivo.

Vaya a **Hardware > Dispositivos** para revisar el estado general de los dispositivos del clúster y recolectar materiales de soporte para los dispositivos con fines de solución de problemas.

Haga clic en el nombre del dispositivo para iniciar la página **Detalles del dispositivo**, donde puede revisar las métricas, las alertas y la información de estado del dispositivo y sus componentes. Utilice las opciones de **Más acciones** en la página de detalles para recolectar materiales de soporte para el dispositivo a fin de resolver problemas menores.

Clústeres

Un clúster de PowerStore es un grupo de entre uno y cuatro dispositivos que actúa como un único componente con fines de administración de recursos, eficiencia y disponibilidad. Un clúster puede contener hasta cuatro dispositivos. En esta versión, solamente puede haber dispositivos de la misma configuración en un clúster.

En el siguiente diagrama se muestran los componentes de un clúster.

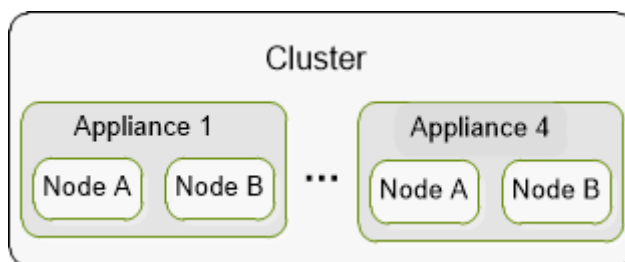


Ilustración 1. Componentes de un clúster

Un clúster proporciona los siguientes beneficios:

- Reducción de la complejidad de la administración.
- Mayor eficiencia en el rendimiento y los recursos. Los recursos de computación y almacenamiento se agrupan en pools dentro de un clúster y el uso de los recursos se equilibra entre todos los dispositivos del clúster. Los recursos se vuelven a equilibrar según sea necesario para mantener y optimizar el rendimiento y el uso de recursos del clúster. Esto se realiza en función de las tendencias de uso del espacio de almacenamiento y las evaluaciones de rendimiento del sistema que ocurren en segundo plano.
- Escalabilidad. Comience con una configuración pequeña y agregue fácilmente capacidad o rendimiento al sistema con la posterior adición de más dispositivos para satisfacer la demanda de la empresa.

Para administrar y configurar un clúster, realice las siguientes operaciones en PowerStore Manager

- Monitoree y revise las métricas agregadas para el clúster en la página **Dashboard**.
- Revise y configure diversos ajustes del clúster en la página **Settings**.
- Agregue dispositivos al clúster o quítelos de este en la página **Hardware**.

Visión general de la planificación y la instalación

En esta sección se proporciona un mapa general de los pasos que debe realizar desde la planificación hasta la instalación y, por último, el inicio de sesión en la interfaz del usuario de PowerStore Manager. Asegúrese de consultar los recursos de documentación asociados para obtener instrucciones y recomendaciones detalladas. Puede acceder a los recursos de documentación en la página PowerStore Documentation en <https://www.dell.com/powerstoredocs>.

Antes de que llegue el dispositivo:

1. Trabaje con los administradores de la infraestructura para realizar lo siguiente:
 - a. Configure la red y los switches de la parte superior del rack (ToR) en función de las recomendaciones que se proporcionan en la *Guía de redes de PowerStore para modelos PowerStore T* o *guía de redes PowerStore para modelos PowerStore X*.
 - b. Obtenga la información relacionada con la red que necesita para la configuración inicial del clúster. Use la *Guía de redes de PowerStore para modelos PowerStore T* o *guía de redes PowerStore para modelos PowerStore X* para planificar y recolectar esta información.
 - c. Configure los puertos de red para permitir que el clúster se comunique de manera segura y eficiente con los hosts y las aplicaciones pertinentes. Consulte [Uso de los puertos](#) en la página 26 para obtener más información.
2. PowerStore requiere un centro de datos o una sala de servidores que cuenten con sistemas eléctricos, ambientales, de cableado y de seguridad controlados. Planifique el sitio donde instalará los dispositivos y la ubicación de los componentes de los dispositivos (gabinetes base y gabinetes de expansión) en un rack. Consulte [Planificación del sitio](#) en la página 10 para obtener más información.
3. Configure una estación de trabajo que utilizará para descubrir los dispositivos y configurar el clúster. Es posible que también necesite descargar Discovery Utility desde el sitio web de soporte e instalarla en esta estación de trabajo. Consulte [Requisitos de la estación de trabajo](#) en la página 18 para obtener más información.
4. Determine el nivel de tolerancia de fallas de la unidad que desea configurar en cada dispositivo. El nivel de tolerancia a fallas de la unidad indica la cantidad de fallas simultáneas que el dispositivo puede admitir en las unidades sin causar un evento de pérdida de datos o datos no disponibles. El nivel de tolerancia a fallas de una sola unidad cumple con los requisitos de disponibilidad para todos los tipos de unidades y puntos de capacidad, pero la tolerancia a fallas de la unidad doble puede proporcionar una mayor resistencia y protección. No puede cambiar el nivel de tolerancia a fallas de la unidad después de configurarlo. Asegúrese de que el gabinete incluya el siguiente número de unidades SSD:
 - Al menos seis unidades para tolerancia a errores de una sola unidad
 - Siete unidades para tolerancia a fallas de dos unidades

Cuando llegue el dispositivo:

Consulte la *Guía de inicio rápido de PowerStore* que viene en la caja y realice lo siguiente:

1. Desembale e instale el dispositivo (gabinete base y gabinetes de expansión).
2. Conecte los gabinetes a la red y enciéndalos.
3. Inicie el proceso de configuración inicial. Para obtener más información, consulte la *Guía de redes de PowerStore para modelos PowerStore T* o *guía de redes PowerStore para modelos PowerStore X*.

En *Guía de instalación y servicio para modelos PowerStore* también se incluyen instrucciones de instalación para referencia posterior.

 **NOTA:** Tanto durante el proceso de configuración inicial como una vez que inicie sesión en PowerStore Manager, se recomienda enfáticamente habilitar la función Conectividad de soporte para agilizar el diagnóstico de problemas, realizar tareas de solución de problemas y acelerar el tiempo de resolución. Para obtener más información, consulte [Conectividad de soporte](#) en la página 19.

Una vez que haya completado la configuración inicial:

1. Inicie sesión en PowerStore Manager con las credenciales de administrador que estableció durante la configuración inicial.
2. Configure los ajustes del clúster y comience a aprovisionar cuentas de usuario, recursos de almacenamiento y políticas de PowerStore Manager. Consulte la *Guía de configuración de PowerStore Manager* para obtener más información sobre los pasos recomendados cuando inicie sesión en PowerStore Manager por primera vez.

Planificación del sitio

Este capítulo contiene los siguientes temas:

Temas:

- [Pautas de espacio en el rack](#)
- [Especificaciones técnicas](#)

Pautas de espacio en el rack

Cuando planifique la ubicación de los componentes de los dispositivos, tenga en cuenta las siguientes pautas de espacio en el rack:

- Deje 2U en la parte inferior del rack con fines de facilidad de reparación y manejo de cables de alimentación.
- Apile el gabinete base sin gabinete de expansión desde la parte inferior a partir de la marca 3U.
- Apile el gabinete base en orden de los gabinete de expansión menos conectados a los más conectados y, a continuación, de la mayor a la menor cantidad de unidades.
- Apile el gabinete de expansión conectado al primer gabinete base directamente sobre el gabinete base.
- Los gabinete base posteriores se apilan volteados de manera alternada.

Consulte [Hojas de trabajo de planificación de espacio en el rack](#) en la página 34 para ver un ejemplo de plan de espacio en el rack y, a continuación, utilice la hoja de trabajo en blanco para planificar los dispositivos del clúster.

Especificaciones técnicas

Revise las especificaciones técnicas para planificar y preparar el sitio en el que instalará el clúster de PowerStore.

Dimensiones y peso del gabinete base

Tabla 1. Dimensiones y peso del Gabinete base

Dimensión	Valor
Peso (totalmente completado)	41,7 kg (92 lb)
Tamaño vertical	2 unidades NEMA
Altura	8,64 cm (3,4 in)
Ancho	44,45 cm (17,5 in)
Profundidad	79,5 cm (31,3 in)

Dimensiones y peso del Gabinete de expansión de SAS

Tabla 2. Dimensiones y peso del Gabinete de expansión de SAS

Dimensión	Valor
Peso (totalmente completado)	34,98 kg (77,11 lb)
Tamaño vertical	2 unidades NEMA
Altura	8,64 cm (3,4 in)

Tabla 2. Dimensiones y peso del Gabinete de expansión de SAS (continuación)

Dimensión	Valor
Ancho	44,45 cm (17,5 in)
Profundidad	34,29 cm (13,5 in)

Dimensiones y peso del Gabinete de expansión de NVMe

Tabla 3. Dimensiones y peso del Gabinete de expansión de NVMe

Dimensión	Valor
Peso (totalmente completado)	26,08 kg (57,5 lb) (sin incluir brazos de administración de cables ni rieles de montaje)
Tamaño vertical	2 unidades NEMA
Altura	8,89 cm (3,5 in)
Ancho	43,18 cm (17 in)
Profundidad	65,30 cm (25,71 in)
Profundidad con brazos de administración de cables	84,86 cm (33,41 in)

Requisitos de alimentación del gabinete base

Los requisitos de alimentación variarán en función de la configuración del sistema, la carga y las condiciones ambientales. En la tabla a continuación, se describe el consumo de energía máximo previsto. Para calcular los valores de consumo de energía de un entorno específico, visite <https://powercalculator.dell EMC.com/>.

Tabla 4. Requisitos de alimentación

Requisito	1000T/1000X/ 1200T	3000T/3000X/ 3200T	5000T/5200T	5000X	7000T/7000X	9000T/9000X/ 9200T
Alimentación de entrada máxima	240 V CA ± 10 %, monofásica De 100 a 120 V, se requiere un transformador de paso activo suministrado por el cliente					
Corriente de línea de CA (máximo operativo a 200 V CA)	6,7 A	8,1 A	9,0 A	9,0 A	9,3 A	10,4 A
Consumo de energía (máximo operativo a 200 V CA)	1385 VA (1316 W)	1629,6 VA (1597 W)	1792,9 VA (1757 W)	1792,9 VA (1757 W)	1868,4 VA (1831 W)	2088,8 VA (2047 W)
Disipación de calor (máximo operativo)	4,73 x 10 ⁶ J/h, (4490 Btu/h)	5,74 x 10 ⁶ J/h, (5449 Btu/h)	6,32 x 10 ⁶ J/h, (5995 Btu/h)	6,32 x 10 ⁶ J/h, (5995 Btu/h)	6,59 x 10 ⁶ J/h, (6248 Btu/h)	7,37 x 10 ⁶ J/h, (6985 Btu/h)
Tipo de entrada de CA	Conector de dispositivo IEC320-C14 o IEC320-C20 por zona de alimentación			Conector de dispositivo IEC320-C20 por zona de alimentación		
Frecuencia de entrada normal	De 47 Hz a 63 Hz					
Corriente de irrupción máxima	Pico de 45 A inactivos por cable de alimentación en cualquier voltaje de línea					
Protección CA	Fusible de 20 A en cada fuente de alimentación, una sola línea					
Tiempo de transferencia	10 ms mínimo					
Distribución de corriente	± 5 % de carga completa entre las fuentes de alimentación					
Corriente de sobrecarga al arranque	Pico de 120 A “activos” por fuente de alimentación, en cualquier voltaje de línea					

Tabla 5. Apagado a temperatura ambiental alta

Temperatura ambiente	Falla de hardware	Consecuencia
Por encima de 45 °C (113 °F)	Ninguna	Se genera una advertencia no crítica.
Por encima de 50 °C (122 °F)	Ninguna	Se genera una alerta crítica. El sistema se apaga una vez que expira el temporizador de cinco minutos. Si la temperatura vuelve a menos de 45 °C (113 °F), el sistema se enciende.
Cualquiera	Las tres unidades más calientes tienen una temperatura promedio de 50 °C (122 °F)	El sistema se apaga una vez que expira el temporizador de cinco minutos.
Cualquiera	Falla de dos ventiladores	El sistema se apaga una vez que expira el temporizador de cinco minutos.

Requisitos de alimentación del Gabinete de expansión de SAS

Los requisitos de alimentación variarán en función de la configuración del sistema, la carga y las condiciones ambientales. En la tabla a continuación, se describe el consumo de energía máximo previsto. Para calcular los valores de consumo de energía de un entorno específico, visite <https://powercalculator.dellemc.com/>.

Tabla 6. Requisitos de alimentación

Requisito	Descripción
Voltaje de línea de CA	De 100 a 240 V CA $\pm$ 10 %, monofásico, de 47 a 63 Hz
Corriente de línea de CA (máximo operativo)	3,32 A máx. a 100 V CA
	1,66 A máx. a 200 V CA
Consumo de energía (máximo operativo)	308 VA (319 W) máx. a 100 V CA
	332 VA (315 W) máx. a 200 V CA
Factor de energía	0,95 mínimo a 100 V/200 V con carga completa
Disipación de calor (máximo operativo)	$1,11 \times 10^6$ J/h (1088 BTU/h) máx. a 100 V CA
	$1,20 \times 10^6$ J/h, (1075 BTU/h) máx. a 200 V CA
Corriente de irrupción	30 A máx. para medio ciclo de línea por cable de línea a 240 V CA
Corriente de sobrecarga al arranque	Pico máx. de 40 A por cable de línea, en cualquier línea de voltaje.
Protección CA	Fusible de 15 A en cada fuente de alimentación, línea y neutral
Tipo de entrada de CA	Conector de dispositivo IEC320-C14 por zona de alimentación
Tiempo de transferencia	Mínimo de 12 milisegundos
Distribución de corriente	± 5 % de carga completa entre las fuentes de alimentación

Requisitos de alimentación del Gabinete de expansión de NVMe

Los requisitos de alimentación variarán en función de la configuración del sistema, la carga y las condiciones ambientales. En la tabla a continuación, se describe el consumo de energía máximo previsto. Para calcular los valores de consumo de energía de un entorno específico, visite <https://powercalculator.dellemc.com/>.

Tabla 7. Requisitos de alimentación

Requisito	Descripción
Voltaje de línea de CA	De 100 a 240 V CA $\pm$ 10 %, monofásico, de 47 a 63 Hz
Corriente de línea de CA (máximo operativo)	6,49 A máx. a 100 V CA
	3,31 A máx. a 200 V CA
Consumo de energía (máximo operativo)	670 VA (636 W) máx. a 100 V CA
	663 VA (630 W) máx. a 200 V CA
Factor de energía	0,95 mínimo a 100 V/200 V con carga completa
Disipación de calor (máximo operativo)	$2,29 \times 10^6$ J/h (2170 Btu/h) máx. a 100 V CA
	$2,27 \times 10^6$ J/h (2150 Btu/h) máx. a 200 V CA
Corriente de irrupción	82 A máx. para medio ciclo de línea por cable de línea a 200 V CA
Corriente de sobrecarga al arranque	100 A máx. para un máximo de 125 μ Sec
Protección CA	Fusible de 15 A en cada fuente de alimentación, línea y neutral
Tipo de entrada de CA	Conector de dispositivo IEC320-C14 por zona de alimentación

Tabla 7. Requisitos de alimentación (continuación)

Requisito	Descripción
Tiempo de transferencia	10 milisegundos mínimo
Distribución de corriente	+/- 5 % de carga completa entre las fuentes de alimentación

Límites del entorno operativo

Tabla 8. Límites del entorno operativo

Descripción	Límite
Temperatura	De 5 °C a 35 °C normal; de 35 °C a 40 °C durante un 10 % del tiempo
Humedad	-12 °C DP y de un 8 % a un 85 % RH (sin condensación)
Gradiente de temperatura (disco)	20 °C/h
Compensación de altitud	Normal: temp. mínima 1 °C por 300 m sobre 950 m
	Improbable: temp. más baja 1 °C por 175 m sobre 950 m

Requisitos de envío y almacenamiento

 **PRECAUCIÓN:** Los sistemas y componentes no deben experimentar cambios de temperatura y humedad, lo cual puede causar la condensación sobre o dentro de ese sistema o componente. No supere el gradiente de temperatura de envío y almacenamiento de 25 °C/h (45 °F/h).

Tabla 9. Requisitos de envío y almacenamiento

Requisito	Descripción
Temperatura ambiente	De -40 a +65 °C (de -40 a +149 °F)
Gradiente de temperatura	25 °C/h (45 °F/h)
Humedad relativa	entre el 10 % y el 90 %, sin condensación
Altitud	De -16 a 10 600 m (de -50 a 35 000 pies)
Recomendación de hora de almacenamiento (sin alimentación)	No supere 6 meses consecutivos de almacenamiento sin alimentación.

Gabinete base Flujo de aire

El gabinete base usa un algoritmo de enfriamiento adaptable que aumenta o disminuye la velocidad de los ventiladores a medida que la unidad nota cambios en la temperatura ambiente externa. La salida aumenta con la temperatura ambiente y la velocidad del ventilador, pero se mantiene casi constante dentro de los parámetros operativos recomendados. Tenga en cuenta que la información de la tabla siguiente muestra datos representativos, medidos sin las puertas delantera ni trasera del gabinete, las cuales se supone que reducen el flujo de aire de la parte frontal a la posterior.

Tabla 10. Gabinete base Flujo de aire

Flujo de aire máximo (pies cúbicos por minuto)	Flujo de aire mínimo (pies cúbicos por minuto)	Uso máximo de alimentación (vatios)
165 pies cúbicos por minuto	50 pies cúbicos por minuto	850

Recuperación ambiental

Si el sistema supera la temperatura ambiente máxima en unos 10 °C (18 °F), sus nodos comienzan un apagado metódico que guarda los datos almacenados en caché y, luego, se apagan a sí mismos. Las tarjetas de control de enlace (LCC) de cada gabinete de expansión del sistema apagan las unidades, pero permanecen encendidas.

Si el sistema detecta un descenso de la temperatura a niveles aceptables, restaura la alimentación a los gabinetes base y las tarjetas LCC hacen lo propio con sus unidades.

Requisitos de calidad del aire

Los productos están diseñados conforme a los requisitos del manual de estándares ambientales de la ASHRAE (Asociación Estadounidense de Ingenieros en Calefacción, Enfriamiento y Aire Acondicionado) y de la versión más reciente de ASHRAE 2009b, la segunda edición de las reglas térmicas para los ambientes de procesamiento de datos.

Los gabinetes están diseñados para los ambientes de redes de datos de clase 1, los que se caracterizan por parámetros ambientales sometidos a un riguroso control, incluidas las características de temperatura, punto de condensación, humedad relativa y calidad del aire. Estas instalaciones albergan equipamiento de misión crítica y suelen tolerar fallas (incluidos los acondicionadores de aire).

En el centro de datos se debe mantener un nivel de limpieza de acuerdo con lo que se indica en ISO 14664-1, clase 8, en relación con el control de la contaminación y de las partículas de polvo. El aire que ingresa en el centro de datos se debe filtrar con un filtro MERV 11 u otro de calidad superior. El aire dentro del centro de datos se debe filtrar continuamente con un sistema de filtración MERV 8 u otro de calidad superior. Además, se debe hacer lo posible para evitar que partículas conductoras, como fibras de zinc, ingresen en la instalación.

Aunque se admite una humedad relativa de entre el 20 y el 80 % sin condensación, el rango recomendable para el ambiente operativo es de entre el 40 y el 55 %. En el caso de centros de datos que posean contaminación gaseosa (p. ej.: altos niveles de azufre), se recomiendan niveles más bajos de temperatura y humedad, a fin de minimizar el riesgo de corrosión y degradación del hardware. En general, se deben minimizar las fluctuaciones de la humedad dentro del centro de datos. Además, se recomienda que el centro de datos esté presurizado positivamente y que tenga cortinas de aire en las vías de entrada, a fin de evitar que la humedad y los contaminantes del aire del exterior entren en la instalación.

En las instalaciones con una humedad relativa inferior al 40 %, se recomienda utilizar cintas conectadas a tierra al tocar el equipo a fin de evitar descargas electrostáticas (ESD), ya que pueden dañar los equipos electrónicos.

Como parte del proceso constante de monitoreo de la propensión a la corrosión del ambiente, se recomienda colocar láminas de cobre y plata (de acuerdo con la sección 6.1 sobre reactividad de ISA 71.04-1985) en las corrientes de aire representativas del centro de datos. La tasa de reactividad mensual de las láminas debe ser inferior a 300 angstroms. Cuando se excede la tasa de reactividad monitoreada, se debe analizar la lámina para buscar especies materiales y se debe implementar un proceso correctivo de mitigación.

Recomendación de hora de almacenamiento (sin alimentación): no supere 6 meses consecutivos de almacenamiento apagado.

Exención de responsabilidades en relación con la inhibición de incendios

Como medida de seguridad adicional, siempre se deben instalar equipos de prevención de incendios en la sala de computación. Es responsabilidad del cliente contar con un sistema de contención de incendios. Seleccione con cuidado los agentes y el equipo de extinción de incendios para el centro de datos. Se debe consultar al asegurador, al jefe de bomberos local y al inspector local del edificio para seleccionar un sistema de contención de incendios que proporcione el nivel correcto de cobertura y protección.

El equipo está diseñado y fabricado para cumplir con los estándares internos y externos que requieren ciertos ambientes para funcionar de manera confiable. No realizamos afirmaciones de compatibilidad de ningún tipo ni proporcionamos recomendaciones relacionadas con sistemas de contención de incendios. No se recomienda que los equipos de almacenamiento se ubiquen directamente frente a descargas de gas de alta presión ni a fuertes sirenas de incendios a fin de minimizar las fuerzas y las vibraciones que pueden ser perjudiciales para la integridad del sistema.

NOTA: La información anterior se proporciona "tal como está" y no representa ningún tipo de responsabilidad, garantía ni obligación de parte de nuestra empresa. Esta información no modifica el alcance de ninguna garantía que se haya establecido en los términos y condiciones del acuerdo de compra básico entre el cliente y el fabricante.

Impacto y vibración

Los productos se someten a pruebas de resistencia contra impactos y niveles de vibración aleatorios. Los niveles se aplican a los tres ejes y se deben medir con un acelerómetro en los gabinetes del equipo dentro del gabinete; además, no deben exceder ninguno de los valores siguientes.

Condición de la plataforma	Nivel de respuesta medido
Impacto no operacional	25 G, 3 ms de duración
Impacto operacional	6 G, 11 ms de duración
Vibración aleatoria no operacional	0.40 Grms, entre 5 y 500 Hz, 30 minutos
Vibración aleatoria operacional	0.21 Grms, entre 5 y 500 Hz, 10 minutos

Los sistemas montados en paquetes aprobados se someten a pruebas de transporte para comprobar la tolerancia a los impactos y a las vibraciones siguientes solo en orientación vertical. No pueden superar los siguientes valores:

Condición del sistema empaquetado	Nivel de respuesta medido
Impacto en el transporte	10 G, 12 ms de duración
Vibración aleatoria en el transporte	• 0,28 GRMS • Rango de frecuencia de 4 horas: entre 1 y 100 Hz

Requisitos de licenciamiento y de la estación de trabajo

Este capítulo incluye los siguientes temas:

Temas:

- [Licenciamiento de PowerStore](#)
- [Licenciamiento de VMware \(para dispositivos Modelo PowerStore X\)](#)
- [Requisitos de la estación de trabajo](#)

Licenciamiento de PowerStore

La licencia de PowerStore se obtiene y se instala automáticamente en todos los dispositivos del clúster durante la configuración inicial. Incluye acceso a todas las funciones disponibles con PowerStore.

NOTA: La licencia de PowerStore no incluye la licencia de VMware vSphere. Para el licenciamiento del clúster de Modelo PowerStore X, también debe obtener o utilizar una licencia de VMware vSphere independiente. Para obtener más información, consulte [Licenciamiento de VMware \(para dispositivos Modelo PowerStore X\)](#) en la página 17.

Para obtener licencias automáticamente durante y después de la configuración inicial, asegúrese de que el puerto 443 esté abierto. El clúster se comunica con el sistema de administración de licenciamiento de Dell EMC (ELMS) mediante el puerto 443 para obtener el archivo de licencia. Si hay un problema para obtener el archivo de licencia, el clúster funcionará en un período de prueba de 30 días. El sistema intentará obtener una licencia automáticamente cada 24 horas. Para revisar el estado de la licencia, en PowerStore Manager, vaya a **Settings > Licensing**. Un estado **Active** indica que todos los dispositivos del clúster tienen una licencia válida.

Si aún no tiene una licencia activa, puede hacer clic en **Refresh** en la página **PowerStore Licensing** para intentar obtener la licencia automáticamente. O bien, haga clic en **Install License** para instalar la licencia manualmente.

NOTA: No necesita una licencia de PowerStore por separado cuando instala el software del entorno operativo y las actualizaciones de firmware de PowerStore.

Licenciamiento de VMware (para dispositivos Modelo PowerStore X)

Modelo PowerStore X requiere que cuente con una licencia de vSphere Enterprise Plus o superior. Los dispositivos Modelo PowerStore X incluyen una instancia integrada de VMware vSphere Enterprise 6.7. Puede aplicar una licencia de un ELA de VMware existente o comprar licencias de vSphere a VMware o a un partner.

PowerStore también es compatible con VMware vSphere las licencias de oficinas remotas de sucursales (ROBO) tanto para ROBO Enterprise como para ROBO Advanced.

NOTA: ROBO Advanced no es compatible con DRS. Antes de aplicar una licencia de ROBO Advanced a un clúster de Modelo PowerStore X, primero debe deshabilitar DRS.

Modelo PowerStore X requiere un servidor de vCenter externo. El servidor vCenter necesario debe tener una licencia de edición Standard con Modelo PowerStore X.

NOTA: De manera opcional, puede usar una licencia de edición vCenter Server Foundation, que se limita a cuatro hosts que administra el servidor de vCenter. Esta licencia de la edición Foundation limita las implementaciones de Modelo PowerStore X a:

- Dos clústeres Modelo PowerStore X de un único dispositivo
- Un clúster de Modelo PowerStore X de un único dispositivo y 2 hosts ESXi externos

Requisitos de la estación de trabajo

Una vez que realice el proceso de instalación física, disponga de una estación de trabajo o una máquina virtual basados en Windows para descubrir los dispositivos y comenzar la configuración inicial. Asegúrese de que la estación de trabajo o la máquina virtual cumplan con los siguientes requisitos:

- Ejecución del sistema operativo Microsoft® Windows® 10.
- Incluye al menos un puerto de red Ethernet/RJ-45.
- Incluye la versión más reciente de uno de los siguientes navegadores web:
 - Google Chrome
 - Mozilla Firefox
 - Microsoft Edge
 - Apple Safari

Utilidad de descubrimiento de PowerStore

Si no tiene acceso al gabinete base que desea configurar, debe descargar y ejecutar la utilidad de descubrimiento de PowerStore. La utilidad de descubrimiento de PowerStore le permite buscar dispositivos Modelo PowerStore T y Modelo PowerStore X no configurados en la red e iniciar el proceso de configuración inicial para configurar un clúster. Descargue esta utilidad desde el sitio de soporte de Dell en <https://www.dell.com/support>.

Para obtener más información sobre los requisitos y el proceso de descubrimiento, consulte *Guía de redes de PowerStore para modelos PowerStore T* o *guía de redes PowerStore para modelos PowerStore X*.

Conectividad de soporte

Este capítulo incluye los siguientes temas:

Temas:

- Descripción operacional de Conectividad de soporte
- Opciones de Conectividad de soporte
- Conectividad de soporte con el uso de la opción Gateway de conexión segura
- Conectividad de soporte con el uso de la opción Conectarse directamente
- Requisitos para Conectividad de soporte con el uso del gateway de conexión segura
- Requisitos para Conectividad de soporte con el uso de Conectarse directamente
- Configuración de Conectividad de soporte
- Establecer la configuración inicial de Conectividad de soporte
- Administrar los ajustes de Conectividad de soporte
- CloudIQ
- Seguridad cibernética

Descripción operacional de Conectividad de soporte

Las siguientes características están disponibles con una garantía o cobertura de ProSupport Enterprise Suite:

NOTA: Las funcionalidades Secure Remote Services y SupportAssist Enterprise ahora son parte del gateway de conexión segura.

- Detección de problemas, creación de casos y notificación proactivas y automatizadas
- Resolución acelerada de problemas con soporte remoto y comunicación bidireccional segura entre el proveedor de servicio y el entorno de almacenamiento
- Recomendaciones basadas en análisis para el soporte y los servicios

NOTA: Se recomienda habilitar Conectividad de soporte para agilizar el diagnóstico de problemas, realizar tareas de solución de problemas y acelerar el tiempo de resolución. Si no habilita Conectividad de soporte, es posible que deba recolectar manualmente la información del dispositivo para ayudar al proveedor de servicio a solucionar problemas del dispositivo. Además, Conectividad de soporte se debe habilitar en el dispositivo para que los datos se envíen a CloudIQ y para permitir el uso de la aplicación Cybersecurity.

Conectividad de soporte y seguridad

Conectividad de soporte emplea varias capas de seguridad en cada paso del proceso de conectividad remota para asegurarse de que usted y el proveedor de servicio puedan usar la solución con confianza:

- Todas las notificaciones enviadas al proveedor de servicio se originan desde su sitio, nunca desde un origen externo, y se mantienen seguras gracias al uso del cifrado Advanced Encryption Standard (AES) de 256 bits.
- La arquitectura basada en IP se integra a la infraestructura existente y mantiene la seguridad de su ambiente.
- Las comunicaciones entre un sitio y el proveedor de servicio se autentican de manera bilateral mediante certificados digitales de RSA®.
- Es compatible con TLS 1.2
- Solo los proveedores de servicios autorizados y verificados mediante autenticación de doble factor pueden descargar los certificados digitales necesarios para ver una notificación de su sitio.

Administración de Conectividad de soporte

Puede administrar Conectividad de soporte mediante PowerStore Manager o la API REST. Puede habilitar o deshabilitar el servicio y proporcionar la información pertinente necesaria para la opción de Conectividad de soporte que seleccione.

Comunicación de Conectividad de soporte

Conectividad de soporte no se puede habilitar en los modelos de PowerStore configurados con IPv6 para la red de administración. Conectividad de soporte no se admite a través de IPv6. Además, no se permite la reconfiguración de la red de administración de IPv4 a IPv6 cuando Conectividad de soporte está configurada en un clúster.

 **NOTA:** Para que Conectividad de soporte funcione, es necesario el acceso a un servidor de DNS.

El estado de conexión de Conectividad de soporte indica el estado de la conexión entre PowerStore y los servicios de soporte de back-end del proveedor de servicio y la calidad de servicio de la conexión. El estado de la conexión se determina en periodos de cinco minutos y la calidad de servicio de la conexión, en periodos de 24 horas. El estado de la conexión puede aparecer como uno de los siguientes valores en función de cualquiera de los dispositivos del clúster:

- **Unavailable** : los datos de conectividad no están disponibles. Es posible que haya perdido contacto con un dispositivo o que Conectividad de soporte se haya habilitado y que no haya datos suficientes para determinar el estado.
- **Disabled** : Conectividad de soporte no se ha habilitado.
- **Not connected** : la conectividad se perdió. Se detectaron cinco fallas consecutivas de Keepalive.
- **Reconnecting** : PowerStore está intentando volver a conectarse después de la pérdida de conectividad. Se necesitan cinco solicitudes correctas consecutivas de Keepalive para realizar la transición nuevamente a un estado conectado.

El estado de la conexión puede aparecer como uno de los siguientes valores en función del promedio de todos los dispositivos del clúster cuando PowerStore está conectado a los servicios de soporte de back-end del proveedor de servicio:

- **Good** : el 80 % o más de las solicitudes Keepalive consecutivas se realizó correctamente.
- **Fair** : entre el 50 % y el 80 % de las solicitudes Keepalive consecutivas se realizó correctamente.
- **Poor** : menos del 50 % de las solicitudes Keepalive consecutivas se realizó correctamente.

Soporte remoto de Conectividad de soporte

Conectividad de soporte y su característica de soporte remoto están deshabilitadas de manera predeterminada. Como parte de la habilitación de Conectividad de soporte y para utilizar sus servicios de soporte remoto, debe aceptar el Acuerdo de licencia para el usuario final (EULA). De lo contrario, Conectividad de soporte no se puede habilitar y su característica de soporte remoto no se puede usar. Una vez que se acepta el EULA de Conectividad de soporte, es posible configurar Conectividad de soporte y su característica de soporte remoto.

La habilitación de la característica de soporte remoto permite que los ingenieros de soporte autorizados por el proveedor de servicio accedan y solucionen problemas del sistema de manera segura. Esta característica permite que el personal de soporte del proveedor de servicio inicie sesión de manera remota en el sistema para abordar los problemas que pueden ocurrir. El personal de soporte puede iniciar sesión en el sistema de manera remota a través de SSH o PowerStore Manager. Su contrato de soporte determina lo que el personal de soporte tiene permitido hacer y cuándo hacerlo. Al habilitar esta función, debe otorgar acceso al sistema para que se produzcan problemas de solución de problemas y solución de problemas a medida que se producen. Por ejemplo, si se presenta una situación de Call Home, falta de disponibilidad de datos, pérdida de datos o cualquier otro evento anormal, esta característica permite que el personal de soporte del proveedor de servicio responda con mayor rapidez para corregir los problemas.

Opciones de Conectividad de soporte

Las opciones de Conectividad de soporte que están disponibles, mediante las cuales se envía información del dispositivo al proveedor de servicio para la solución de problemas remota, son las siguientes:

- **Conectarse a través del gateway de conexión segura:** esta opción es para Conectividad de soporte centralizado, donde el software del gateway de conexión segura se ejecuta en un servidor de gateway suministrado por el cliente con transferencia de archivos bidireccional, lo que incluye lo siguiente:
 - Call Home
 - Compatibilidad con CloudIQ y Cybersecurity
 - Notificaciones de software
 - Descarga del entorno operativo y el firmware desde el proveedor de servicio al clústerTambién se incluye acceso remoto para el personal de soporte del proveedor de servicio. El servidor de gateway es el punto único de entrada y salida de todas las actividades de soporte basadas en IP para los dispositivos asociados con el gateway.
- **Conectarse directamente:** esta opción es para Conectividad de soporte distribuido, donde el software del gateway de conexión segura se ejecuta en dispositivos individuales con la misma transferencia de archivos bidireccional que en la conexión a través de un servidor de gateway.

Está disponible otra opción, Deshabilitado, pero no se recomienda. Si selecciona esta opción, el proveedor de servicio no recibirá notificaciones sobre los problemas del dispositivo. Es posible que deba recolectar manualmente información del dispositivo para apoyar a los representantes de soporte en la solución de problemas.

Conectividad de soporte con el uso de la opción Gateway de conexión segura

Cuando selecciona la opción **Conectarse a través del gateway de conexión segura**, el dispositivo se agrega a otros dispositivos en un clúster de gateway de conexión segura. El clúster reside detrás de una única conexión segura común (centralizada) entre los servidores del proveedor de servicio y un servidor de gateway fuera del arreglo. El servidor de gateway es el punto único de entrada y salida de todas las actividades de soporte basadas en IP para los dispositivos asociados con el gateway.

El servidor de gateway es una aplicación de solución de soporte remoto que se instala en uno o más servidores dedicados que proporciona el cliente. La opción **Conectarse a través del gateway de conexión segura** admite hasta dos servidores de gateway, uno como principal y otro como respaldo. El servidor de gateway funciona como un agente de comunicación entre los dispositivos asociados y el proveedor de servicio.

Para configurar el dispositivo a fin de utilizar la opción **Conectarse a través del gateway de conexión segura** para Conectividad de soporte, debe proporcionar la dirección IP y el número de puerto (9443 es el valor predeterminado) para cada servidor de gateway. Además, asegúrese de que el puerto esté abierto entre el servidor de gateway y el dispositivo.

NOTA: Para usarlo, el servidor de gateway debe estar en funcionamiento antes de que se configure el dispositivo. Los dispositivos se pueden agregar al gateway solamente desde PowerStore Manager. Si el dispositivo se agrega desde el servidor de gateway, aparecerá conectado, pero no enviará correctamente la información del sistema.

Conectividad de soporte con el uso de la opción Conectarse directamente

Para la opción **Conectarse directamente**, el software de gateway de conexión segura se ejecuta directamente en el nodo primario de cada dispositivo. En un clúster, cada dispositivo establece su propia conexión al proveedor de servicio. El tráfico no se enruta a través del dispositivo primario en un clúster. Sin embargo, Conectividad de soporte se puede administrar solamente en el nivel del clúster, es decir, todos los cambios se aplican a todos los dispositivos del clúster.

Habilite y configure la opción **Conectarse directamente** desde la página **Conectividad de soporte**, a la que se puede acceder a través de **Ajustes de configuración** y que se enumera bajo **Soporte** en PowerStore Manager. Estas acciones configuran el dispositivo para usar una conexión segura entre sí y el proveedor de servicio.

Cuando selecciona la opción **Conectarse directamente** y acepta el Acuerdo de licencia para el usuario final (EULA), el dispositivo configura una conexión segura entre sí y el proveedor de servicio. Esta opción habilita la funcionalidad de conectividad del servicio de acceso remoto con el dispositivo hacia y desde el proveedor de servicio, junto con la transferencia de archivos bidireccional. Si corresponde, puede configurar la conexión desde el dispositivo a un servidor proxy asociado (opcional).

Cuando se agrega un nuevo dispositivo a un clúster existente, este detectará los ajustes de **Conectividad de soporte** del clúster y establecerá automáticamente la configuración según corresponda. Si la opción **Conectarse directamente** está habilitada, se habilitará automáticamente en el nuevo dispositivo. No es necesario realizar acciones adicionales. Si la opción **Conectarse directamente** no se puede habilitar, esto no impedirá que el proceso de adición del dispositivo finalice.

Requisitos para Conectividad de soporte con el uso del gateway de conexión segura

Los siguientes requisitos se aplican a la implementación de Conectividad de soporte con el uso de **Conectarse a través del gateway de conexión segura**:

- El tráfico de red (HTTPS) debe estar permitido en el puerto 9443 (o en el puerto que especifica el cliente, si es diferente) entre el dispositivo y el servidor del gateway de conexión segura. Además, permita el acceso a los puertos 22, 443 y 8443 entre PowerStore y el servidor del gateway de conexión segura para PowerStore Manager y el acceso SSH.
- El servidor del gateway de conexión segura debe tener la versión 5.00.06.xy o superior.
- Asegúrese de que el clúster de PowerStoreOS ejecute PowerStore versión 3.0 o superior.

 **NOTA:** Nunca agregue ni quite manualmente un dispositivo desde el servidor de gateway. Agregue o quite un dispositivo únicamente desde PowerStore Manager.

Requisitos para Conectividad de soporte con el uso de Conectarse directamente

Los siguientes requisitos se aplican a la implementación de **Connect Directly** Conectividad de soporte:

- El tráfico de red (HTTPS) debe estar permitido en los puertos 443 y 8443 (saliente) al proveedor de soporte. Cuando no se puede abrir el puerto 8443, hay un impacto considerable en el rendimiento (entre un 30 y un 45 %). Si no se abren ambos puertos, puede haber una demora en la resolución de problemas relativos al dispositivo final. Además, si la conexión utiliza un servidor proxy, el puerto 3128 es el valor predeterminado que se utiliza cuando no se especifica un puerto, **Conectividad de soporte** está habilitada con **Conectarse directamente** y se emplea un firewall entre el sistema de almacenamiento y el servidor proxy. Si el puerto predeterminado o que especifica el usuario está cerrado, la comunicación con el sistema de almacenamiento a través de este no estará disponible.

Configuración de Conectividad de soporte

Configure Conectividad de soporte para un dispositivo utilizando cualquiera de los siguientes medios:

- Asistente de configuración inicial: interfaz de usuario que lo guía a través de la configuración inicial de PowerStore Manager y que prepara el sistema para su uso.
- Conectividad de soporte: página de ajustes a la que puede acceder desde PowerStore Manager (haga clic en **Ajustes de configuración** y, en **Soporte**, seleccione **Conectividad de soporte**).
- Servidor de API REST: interfaz de aplicaciones que puede recibir solicitudes de la API REST para configurar los ajustes de la conectividad de soporte. Para obtener más información sobre la API REST, consulte *Guía de referencia de la API REST de PowerStore*.

Para determinar el estado de Conectividad de soporte, haga clic en **Ajustes de configuración** y, en **Soporte**, seleccione **Conectividad de soporte** en PowerStore Manager.

Establecer la configuración inicial de Conectividad de soporte

Requisitos previos

Al configurar Conectividad de soporte, si el firewall está configurado para inspeccionar certificados TLS con el fin de verificarlos, los archivos de certificado de la autoridad de certificación asociada se deben agregar a la lista de autoridades de confianza del firewall. Los siguientes archivos de certificado necesarios se pueden descargar mediante los enlaces correspondientes:

- DellSecureRemoteServicesRootCA.crt desde <http://esrs-crl.emc.com/DellSecureRemoteServicesRootCA.crt>
- ESRS2CA.cer desde <http://esrs-crl.emc.com/ESRS2CA.crt>

Sobre esta tarea

 **NOTA:** No utilice este procedimiento si la característica se configuró inicialmente y si se aceptó el Acuerdo de licencia para el usuario final (EULA) asociado.

Para configurar la configuración inicial de Conectividad de soporte mediante PowerStore Manager, realice lo siguiente:

 **NOTA:** Con PowerStore OS 2.1 y versiones superiores, esta característica no se puede habilitar a menos que se proporcione la información de **Contacto principal** con los valores necesarios en **Contactos de soporte**. Además, después de una actualización no disruptiva correcta, debe actualizar o cerrar y volver a abrir la pestaña del navegador para ver y utilizar la nueva funcionalidad; de lo contrario, seguirá viendo y utilizando la funcionalidad más antigua.

Pasos

1. Haga clic en **Ajustes de configuración** y, en **Soporte**, seleccione **Conectividad de soporte**.

Aparece la página Conectividad de soporte con **Contactos de soporte** seleccionado.

2. Escriba la información requerida.

NOTA: El **Nombre** y el **Apellido** del **Contacto principal** son obligatorios, así como el **Correo electrónico** o el **Teléfono** (se requiere al menos uno) del **Contacto principal**. Proporcionar información para el **Contacto secundario** es opcional. La información de contacto de Conectividad de soporte es fundamental para responder rápidamente a los problemas de soporte y debe ser precisa y actual. Además, puede ver la *Política de privacidad* y el *Aviso de telemetría* seleccionando el enlace relacionado en el texto introductorio de **Contactos de soporte**.

3. Haga clic en **Aplicar** para guardar la información.

NOTA: Debe hacer clic en **Aplicar** antes de poder navegar desde **Contactos de soporte** y seleccionar **Tipo de conexión**; de lo contrario, aparece un indicador que le pregunta si desea cancelar la transferencia de navegación o descartar la información que ha escrito.

4. Seleccione **Tipo de conexión**.

NOTA: Cuando la configuración inicial de Conectividad de soporte no se ha configurado, el estado se muestra como **Deshabilitado**.

5. Haga clic en el control **Habilitado/Deshabilitado** para comenzar a habilitar Conectividad de soporte.

Aparece el Acuerdo de licencia para el usuario final (EULA).

6. Haga clic en **Aceptar** para aceptar el EULA y habilitar Conectividad de soporte.

Aunque la función Conectividad de soporte se puede deshabilitar, esto no se recomienda. Además, si no se acepta el EULA, no se puede habilitar Conectividad de soporte.

El control **Habilitado/Deshabilitado** debe desplazarse hacia la derecha y su indicación debe cambiar a **Enabled**. Sin embargo, el estado de conexión no cambiará hasta que se ingrese la información de configuración necesaria y se haga clic en **Aplicar**.

7. Seleccione en la lista un valor **Tipo** para la opción de Conectividad de soporte que desea usar.

8. Según el tipo de opción de Conectividad de soporte que selecciona, realice una de las siguientes acciones:

- Para la opción **Conectarse a través del gateway de conexión segura**:

- Especifique la dirección IP de cada servidor de gateway, el servidor principal y, si está disponible, el servidor de respaldo.

NOTA: Cada servidor de gateway debe estar en funcionamiento antes de que se configure el dispositivo.

- Si el puerto que se utilizará para conectarse al servidor de gateway es diferente al predeterminado (9443), utilice los controles para seleccionar el número del puerto que se utilizará en la red.

- Para la opción **Conectarse directamente**:

- Si la conexión de red utiliza un servidor proxy, especifique la dirección IP del servidor proxy.

NOTA: Para usarlo, el servidor proxy debe estar en funcionamiento antes de que se configure el dispositivo.

- Utilice los controles para seleccionar el número del puerto que se utilizará para conectarse al servidor proxy en la red.

NOTA: El puerto 3128 es el valor predeterminado que se utiliza cuando no se especifica un puerto, Conectividad de soporte está habilitada con **Conectarse directamente** y se emplea un firewall entre el dispositivo y un servidor proxy. Si el puerto predeterminado o que especifica el usuario está cerrado, la comunicación con el dispositivo a través de este no estará disponible.

9. Según el tipo de opción de Conectividad de soporte que selecciona, realice una de las siguientes acciones:

- Para la opción **Conectarse directamente**, continúe con el paso siguiente.

- Para la opción **Conectarse a través del gateway de conexión segura**, seleccione **Probar conexión** para cada servidor de gateway configurado a fin de comprobar el estado de la conexión al servidor de gateway.

NOTA: Si el estado de la conectividad parece no salir de **Transitioning** y no cambia después de varios minutos (el tiempo que debe tardarse en probar la conectividad), póngase en contacto con el proveedor de servicio.

10. La casilla de verificación **Conectarse a CloudIQ** está seleccionada de manera predeterminada. Si no desea enviar archivos a CloudIQ y poder usar la aplicación Cybersecurity, deseleccione la casilla de verificación. De lo contrario, déjela seleccionada.

11. La casilla de verificación **Soporte remoto** está seleccionada de manera predeterminada. Si no desea permitir que los ingenieros de soporte autorizados por el proveedor de servicio solucionen problemas de manera segura en el sistema, deseleccione la casilla de verificación. De lo contrario, déjela seleccionada.

12. Seleccione **Enviar alerta de prueba** para enviar una alerta de prueba al proveedor de servicio con el fin de verificar la conectividad de punto a punto.

13. Seleccione **Aplicar** para conservar la información de configuración de Conectividad de soporte.

Administrar los ajustes de Conectividad de soporte

Requisitos previos

Conectividad de soporte se configuró inicialmente y el Acuerdo de licencia para el usuario final (EULA) asociado se aceptó.

Sobre esta tarea

Puede cambiar los ajustes de configuración de **Contactos de soporte** y **Tipo de conexión**, ver el estado de la característica, probar la conexión al proveedor de servicio y enviarle una alerta de prueba.

Pasos

1. En PowerStore Manager, seleccione **Ajustes de configuración** y en **Soporte**, seleccione **Conectividad de soporte**. Aparece la página Conectividad de soporte.
2. Para modificar los ajustes de configuración de Conectividad de soporte, realice una o más de las siguientes acciones según sea necesario:
 - NOTA:** Debe hacer clic en **Aplicar** antes de poder navegar desde **Contactos de soporte** o **Tipo de conexión** después de realizar los cambios en cualquiera de las pestañas; de lo contrario, aparece un indicador que le pregunta si desea cancelar la transferencia de navegación o descartar la información que ha escrito.
 - Cambie o elimine la información del **Contacto principal**, del **Contacto secundario** o de ambos.
 - NOTA:** Con PowerStore OS 2.1. y versiones posteriores, esta característica no se puede habilitar a menos que se proporcione la información de **Contacto principal** con los valores necesarios. Además, la información de **Contacto principal** solo se puede eliminar cuando la característica está deshabilitada. El **Nombre** y el **Apellido** del **Contacto principal** son obligatorios, así como el **Correo electrónico** o el **Teléfono** (se requiere al menos uno) del **Contacto principal**. Proporcionar información para el **Contacto secundario** es opcional. La información de contacto de Conectividad de soporte es fundamental para responder rápidamente a los problemas de soporte y debe ser precisa y actual. Además, puede ver la *Política de privacidad* y el *Aviso de telemetría* seleccionando el enlace relacionado en el texto introductorio de **Contactos de soporte**.
 - Haga clic en el control **Habilitado/Deshabilitado** para habilitar o deshabilitar Conectividad de soporte.
 - NOTA:** El estado de la conexión no cambiará hasta después de hacer clic en **Aplicar**.
 - Cambie la opción **Tipo de conexión** que desea utilizar y proporcione cualquier información relacionada que sea necesaria.
 - Para la opción **Conectarse a través del gateway de conexión segura**:
 - Especifique la dirección IP de cada servidor de gateway, el servidor principal y, si está disponible, el servidor de respaldo.
 - NOTA:** Cada servidor de gateway debe estar en funcionamiento antes de que se configure el dispositivo.
 - Si el puerto que se utilizará para conectarse al servidor de gateway es diferente al predeterminado (9443), utilice los controles para seleccionar el número del puerto que se utilizará en la red.
 - Para la opción **Conectarse directamente**:
 - Si la conexión de red utiliza un servidor proxy, especifique la dirección IP del servidor proxy.
 - NOTA:** Para usarlo, el servidor proxy debe estar en funcionamiento antes de que se configure el dispositivo.
 - Utilice los controles para seleccionar el número del puerto que se utilizará para conectarse al servidor proxy en la red.
 - NOTA:** El puerto 3128 es el valor predeterminado que se utiliza cuando no se especifica un puerto, Conectividad de soporte está habilitada con **Conectarse directamente** y se emplea un firewall entre el sistema de almacenamiento y un servidor proxy. Si el puerto predeterminado o que especifica el usuario está cerrado, la comunicación con el sistema de almacenamiento a través de este no estará disponible.
 - Para la opción **Conectarse a través del gateway de conexión segura**, seleccione **Probar conexión** para los servidores de gateway configurados a fin de comprobar el estado de la conexión a los servidores de gateway.
 - NOTA:** Si el estado de la conectividad parece no salir de *Transitioning* y no cambia después de varios minutos (el tiempo que debe tardarse en probar la conectividad), póngase en contacto con el proveedor de servicio.
 - Envíe una alerta de prueba al proveedor de servicio para garantizar la conectividad de punto a punto.
 - Cambie el ajuste de **Conectarse a CloudIQ**.
 - NOTA:** Para enviar archivos a CloudIQ y poder usar la aplicación Ciberseguridad, seleccione la casilla de verificación; de lo contrario, desmarque la casilla de verificación.
 - Cambie la configuración de **Soporte remoto**.

 **NOTA:** Si desea permitir que los ingenieros de soporte autorizados por el proveedor de servicio solucionen problemas de manera segura en el sistema, seleccione la casilla de verificación. De lo contrario, deselectionela.

3. Seleccione **Aplicar** para conservar la información de configuración de Conectividad de soporte.

CloudIQ

 **NOTA:** Conectividad de soporte debe estar habilitado en el dispositivo para conectarse y enviar datos a CloudIQ.

CloudIQ es un servicio alojado por Dell EMC que utiliza datos (registros, configuración del sistema, alertas, métricas de rendimiento, métricas de capacidad y datos de previsión de capacidad) que se recolectan a través de Conectividad de soporte para permitir a los usuarios monitorear el rendimiento casi en tiempo real, así como la utilización y el estado en varios clústeres de PowerStore, además de realizar acciones de servicio básicas. Se accede a la interfaz de CloudIQ a través de un navegador web en cualquier momento y desde cualquier ubicación. En CloudIQ se proporcionan vistas de tablero de todos los clústeres conectados en las que se muestra información clave, como tendencias y predicciones respecto del rendimiento y la capacidad. También brinda una facilidad de reparación proactiva que informa al usuario acerca de los problemas antes de que se produzcan y le ofrece corrección guiada simple.

Los usuarios pueden habilitar CloudIQ durante el proceso de configuración para la implementación de Conectividad de soporte. El soporte de CloudIQ se habilita de manera predeterminada cuando se habilita cualquier opción de Conectividad de soporte. Cuando Conectividad de soporte y CloudIQ están habilitados, CloudIQ se puede iniciar desde cualquier página de PowerStore Manager y está visible de manera constante. Los usuarios pueden iniciar sesión en [CloudIQ.emc.com](https://cloudiq.emc.com) con sus credenciales de servicio válidas para ver sus clústeres de PowerStore en CloudIQ.

 **NOTA:** Una vez que CloudIQ está habilitado, es posible deshabilitar Conectividad de soporte sin cambiar los ajustes de CloudIQ. Sin Conectividad de soporte, los datos no se recolectan ni se envían a CloudIQ, pero si se vuelve a habilitar Conectividad de soporte, el sistema recuerda los ajustes de CloudIQ y reanuda de inmediato el envío de datos. La deshabilitación de la compatibilidad con CloudIQ no deshabilita la transferencia de telemetría relacionada con el servicio, es decir, Call Home y recopilaciones proactivas de datos que se proporcionan a través de la conectividad de soporte.

Seguridad cibernética

 **NOTA:** Conectividad de soporte y CloudIQ deben estar habilitados en el sistema de almacenamiento para permitir el uso de la aplicación Cybersecurity.

Cybersecurity una aplicación de software como servicio de análisis de seguridad de almacenamiento basada en la nube que brinda evaluación de la seguridad y mide el nivel general de riesgo de seguridad cibernética de dispositivos mediante análisis inteligente, integral y predictivo. Cybersecurity usa Conectividad de soporte para recolectar registros del sistema, configuraciones del sistema, configuraciones y ajustes de seguridad, alertas y métricas de rendimiento de un sistema PowerStore.

Uso de los puertos

En las siguientes secciones se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en el dispositivo. El dispositivo funciona como un cliente de red en diversas circunstancias, por ejemplo, en la comunicación con una instancia de vCenter Server. En estos casos, el dispositivo inicia la comunicación y la infraestructura de red deberá admitir estas conexiones.

NOTA: Para obtener información adicional sobre los puertos, consulte el artículo de la base de conocimientos 000022861, *PowerStore: Herramienta Reglas de firewall de la red del usuario: puertos TCP/UDP* (en inglés). La herramienta permite filtrar y revisar la lista de puertos y reglas de firewall que son pertinentes a la implementación de PowerStore.

Temas:

- [Puertos de red del dispositivo](#)
- [Puertos de red del dispositivo relacionados con archivos](#)
- [Puertos de red relacionados con los dispositivos modelo X de PowerStore](#)

Puertos de red del dispositivo

En la siguiente tabla se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en el dispositivo.

Tabla 11. Puertos de red del dispositivo

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
22	Cliente SSH, Conectividad de soporte Connect Home	TCP	Bidireccional	• Permite el acceso mediante el protocolo SSH (si está habilitado). • Se requiere para Conectividad de soporte Connect Home. Si está cerrado, las conexiones de administración por medio de SSH no estarán disponibles.
25 o 587	SMTP	TCP	Saliente	Permite que el dispositivo envíe un correo electrónico. Si está cerrado, las notificaciones por correo electrónico no estarán disponibles.
26	Cliente SSH	TCP	Bidireccional	El acceso mediante SSH al puerto 22 se redirige a este puerto. Si está cerrado, las conexiones de administración por medio de SSH no estarán disponibles.
53	DNS	TCP/UDP	Saliente	Se utiliza para transmitir consultas de DNS al servidor DNS. Si está cerrado, la resolución de nombres de DNS no funcionará.
80, 8080 y 3128	Conectividad de soporte	TCP	Saliente	Se utiliza para la conexión del proxy de Conectividad de soporte.
123	NTP	TCP/UDP	Saliente	Sincronización horaria de NTP. Si está cerrado, la hora no se sincronizará entre los dispositivos.
162 o entre 1024 y 49 151	SNMP	UDP	Saliente	Comunicaciones de SNMP. Si está cerrado, los mecanismos de alerta del sistema de almacenamiento que se basan en SNMP no se enviarán. El número de puerto predeterminado para SNMP es 162.

Tabla 11. Puertos de red del dispositivo (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
443	HTTPS	TCP	Bidireccional	Tráfico HTTP seguro a PowerStore Manager. Si está cerrado, la comunicación con el dispositivo no estará disponible.
500	IPsec (IKEv2)	UDP	Bidireccional	Para hacer que IPsec funcione a través de los firewalls, abra el puerto UDP 500 y permita los números de protocolo IP 50 y 51 en los filtros de firewall entrantes y salientes. El puerto UDP 500 se debe abrir para permitir que el tráfico de Internet Security Association and Key Management Protocol (ISAKMP) se reenvíe a través de los firewalls. El ID de protocolo IP 50 se debe configurar para permitir el reenvío del tráfico de IPsec Encapsulating Security Protocol (ESP). El ID de protocolo IP 51 se debe configurar para permitir el reenvío del tráfico del encabezado de autenticación (AH). Si está cerrado, la conexión IPsec entre los dispositivos PowerStore no estará disponible.
514	Registro remoto	UDP	Saliente	Permite al dispositivo enviar mensajes de registro a los servidores de registro del sistema remoto. Si está cerrado, no se pueden enviar mensajes de registro a los servidores de registro del sistema remoto.
1468	Registro remoto	TCP	Saliente	Permite al dispositivo enviar mensajes de registro a los servidores de registro del sistema remoto. Si está cerrado, no se pueden enviar mensajes de registro a los servidores de registro del sistema remoto.
3033	Importar	TCP/UDP	Saliente	Se requiere para la importación del almacenamiento desde los sistemas EqualLogic Peer Storage y Compellent Storage Center heredados.
3260	iSCSI	TCP	- Entrante para acceso de host y host ESXi - Bidireccional para replicación - Saliente para la importación del almacenamiento	Se requiere para proporcionar el siguiente acceso a servicios de iSCSI: - Acceso iSCSI a host externo - Acceso iSCSI a host ESXi externo o integrado en PowerStore - Acceso entre clústeres para replicación - Acceso a la importación del almacenamiento desde los sistemas EqualLogic Peer Storage, Compellent Storage Center, Unity y VNX2 heredados Si está cerrado, los servicios iSCSI no estarán disponibles. Lo utiliza la movilidad de datos para admitir un rendimiento de replicación razonable en una conexión de baja latencia.
3261	Movilidad de datos	TCP	Bidireccional	Lo utiliza la movilidad de datos para admitir un rendimiento de replicación razonable en una conexión de alta latencia.
4420	Controladora de I/O	TCP	- Entrante para acceso de host y host ESXi - Bidireccional para replicación	Se requiere para proporcionar el siguiente acceso a servicios de la controladora de I/O NVMe/TCP: Acceso NVMe/TCP a host externo

Tabla 11. Puertos de red del dispositivo (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
			Saliente para la importación del almacenamiento	- Acceso NVMe/TCP a host ESXi externo o integrado en PowerStore - Acceso entre clústeres para replicación - Acceso a la importación del almacenamiento desde los sistemas EqualLogic Peer Storage, Compellent Storage Center, Unity y VNX2 heredados Si está cerrado, los servicios de la controladora de I/O NVMe/TCP no estarán disponibles.
5353	DNS de multidifusión (mDNS)	UDP	Bidireccional	Consulta DNS de multidifusión. Si está cerrado, la resolución de nombres de mDNS no funcionará.
8009	Controladora de descubrimiento	TCP	Bidireccional	Lo utiliza la movilidad de datos para admitir un rendimiento de replicación razonable en una conexión de alta latencia. Si está cerrado, los servicios de descubrimiento NVMe/TCP no estarán disponibles.
8443	VASA, Conectividad de soporte	TCP	- Entrante para VASA - Saliente para Conectividad de soporte	- Se requiere para el proveedor de VASA para VASA 3.0. - Se requiere para las funciones de Conectividad de soporte Connect Home relacionadas.
8443, 50443, 55443 o 60443	Agente de host de importación de Windows, agente de host de importación de Linux o agente de host de importación de VMware	TCP	Saliente	Uno de estos puertos debe estar abierto cuando se importa almacenamiento de datos desde sistemas de almacenamiento heredado.
9443	Conectividad de soporte	TCP	Saliente	Se requiere para la API REST de Conectividad de soporte relacionada con Connect Home.

Puertos de red del dispositivo relacionados con archivos

En la siguiente tabla se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en el dispositivo en relación con archivos.

 **NOTA:** Los puertos salientes son efímeros.

Tabla 12. Puertos de red del dispositivo relacionados con archivos

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
20	FTP	TCP	Saliente	Es el puerto utilizado para las transferencias de datos por FTP. Este puerto se puede abrir mediante la habilitación de FTP. La autenticación se ejecuta en el puerto 21 y está definida por el protocolo FTP.
21	FTP	TCP	Entrante	El puerto 21 es el puerto de control en el que el servicio FTP escucha para las solicitudes entrantes de FTP.

Tabla 12. Puertos de red del dispositivo relacionados con archivos (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
22	SFTP	TCP	Entrante	Permite notificaciones de alerta mediante SFTP (FTP por medio de SSH). SFTP es un protocolo de cliente/servidor. Los usuarios pueden usar SFTP para realizar transferencias de archivos en un dispositivo en la subred local. También proporciona control de la conexión del FTP saliente. Si está cerrado, el FTP no estará disponible.
53	DNS	TCP/UDP	Saliente	Se utiliza para transmitir consultas de DNS al servidor DNS. Si está cerrado, la resolución de nombres de DNS no funcionará. Se requiere para SMB v1.
88	Kerberos	TCP/UDP	Saliente	Se requiere para los servicios de autenticación de Kerberos.
111	Enlace RPC (para espacios de nombres de SDNAS; de lo contrario, servicio de host)	TCP/UDP	Bidireccional	Lo abre el servicio portmapper o rpcbind estándar, y es un servicio de red auxiliar del dispositivo. No puede detenerse. Por definición, si un sistema cliente cuenta con conectividad de red al puerto, puede consultarlo. No se realiza ninguna acción de autenticación.
123	NTP	UDP	Saliente	Sincronización horaria de NTP. Si está cerrado, la hora no se sincronizará entre los dispositivos.
135	RPC de Microsoft	TCP	Entrante	Múltiples usos para cliente de Microsoft.
137	WINS para NetBIOS de Microsoft	UDP; TCP/UDP	Entrante; saliente	El servicio de nombres de NetBIOS está asociado a los servicios de uso compartido de archivos SMB del dispositivo y es un componente principal de esa función (Wins). Si está deshabilitado, este puerto deshabilita todos los servicios relacionados con SMB.
138	BROWSE de Microsoft para NetBIOS	UDP	Saliente	El servicio de datagramas de NetBIOS está asociado a los servicios de uso compartido de archivos SMB del dispositivo y es un componente principal de esa función. Solo se usa el servicio de navegación. Si está deshabilitado, el puerto deshabilita la funcionalidad de navegación.
139	SMB de Microsoft	TCP	Bidireccional	El servicio de sesiones de NetBIOS está asociado a los servicios de uso compartido de archivos SMB del dispositivo y es un componente principal de esa funcionalidad. Si están habilitados los servicios de SMB, este puerto está abierto. Se requiere específicamente para SMB v1.
162 o entre 1024 y 49 151	SNMP	UDP	Saliente	Comunicaciones de SNMP. Si está cerrado, los mecanismos de alerta del sistema de almacenamiento que se basan en SNMP no se enviarán. El número de puerto predeterminado para SNMP es 162.
389	LDAP	TCP/UDP	Saliente	Consultas de LDAP no seguras. Si está cerrado, no estarán disponibles las consultas de autenticación LDAP no seguras. El

Tabla 12. Puertos de red del dispositivo relacionados con archivos (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
				protocolo LDAP seguro es configurable como alternativa.
445	SMB de Microsoft	TCP	Entrante	Se ofrece SMB (en controladoras de dominio) y puerto de conectividad SMB para clientes con Windows 2000 o posteriores. Los clientes con acceso legítimo a los servicios de SMB del dispositivo deben contar con conectividad de red al puerto para su funcionamiento continuo. La deshabilitación de este puerto deshabilita todos los servicios relacionados con SMB. Si el puerto 139 también está deshabilitado, se deshabilita el uso compartido de archivos SMB.
464	Kerberos	TCP/UDP	Saliente	Se requiere para los servicios de autenticación de Kerberos y SMB.
500	IPsec (IKEv2)	UDP	Bidireccional	Para hacer que IPsec funcione a través de los firewalls, abra el puerto UDP 500 y permita los números de protocolo IP 50 y 51 en los filtros de firewall entrantes y salientes. El puerto UDP 500 se debe abrir para permitir que el tráfico de Internet Security Association and Key Management Protocol (ISAKMP) se reenvíe a través de los firewalls. El ID de protocolo IP 50 se debe configurar para permitir el reenvío del tráfico de IPsec Encapsulating Security Protocol (ESP). El ID de protocolo IP 51 se debe configurar para permitir el reenvío del tráfico del encabezado de autenticación (AH). Si está cerrado, la conexión IPsec entre los dispositivos PowerStore no estará disponible.
514	Registro remoto	UDP	Saliente	Permite al dispositivo enviar mensajes de registro a los servidores de registro del sistema remoto. Si está cerrado, no se pueden enviar mensajes de registro a los servidores de registro del sistema remoto.
636	LDAPS	TCP/UDP	Saliente	Consultas de LDAP seguras. Si está cerrado, no estará disponible la autenticación LDAP segura.
1234	mountd de NFS	TCP/UDP	Bidireccional	Se utiliza para el servicio de montaje, que es un componente principal del servicio de NFS (versiones 2, 3 y 4).
1468	Registro remoto	TCP	Saliente	Permite al dispositivo enviar mensajes de registro a los servidores de registro del sistema remoto. Si está cerrado, no se pueden enviar mensajes de registro a los servidores de registro del sistema remoto.
2000	SSHD	TCP	Entrante	SSHD para facilidad de reparación (opcional)
2049	I/O de NFS	TCP/UDP	Bidireccional	Se utiliza para proporcionar servicios NFS.
3268	LDAP	UDP	Saliente	Consultas de LDAP no seguras. Si está cerrado, no estarán disponibles las consultas de autenticación LDAP no seguras.

Tabla 12. Puertos de red del dispositivo relacionados con archivos (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
3269	LDAPS	UDP	Saliente	Consultas de LDAP seguras. Si está cerrado, no estarán disponibles las consultas de autenticación LDAP seguras.
4000	STATD para NFSv3	TCP/UDP	Bidireccional	Se utiliza para proporcionar servicios statd de NFS. statd es el monitor de estado de bloqueo de archivos NFS y funciona junto con lockd para proporcionar funciones de falla y recuperación para NFS. Si está cerrado, no están disponibles los servicios statd de NAS.
4001	NLMD para NFSv3	TCP/UDP	Bidireccional	Se utiliza para proporcionar servicios lockd de NFS. lockd es el demonio de bloqueo de archivos NFS. Procesa solicitudes de bloqueo de clientes de NFS y funciona junto con el demonio statd. Si está cerrado, no están disponibles los servicios lockd de NAS.
4002	RQUOTAD para NFSv3	TCP/UDP; UDP	Entrante; saliente	Se utiliza para proporcionar servicios rquotad de NFS. El demonio rquotad proporciona información de cuotas a los clientes de NFS que han montado un sistema de archivos. Si está cerrado, no están disponibles los servicios rquotad de NAS.
4003	XATTRPD (atributo de archivo extendido)	TCP/UDP	Entrante	Se requiere para la administración de atributos de archivos en un entorno multiprotocolo.
4658	PAX (archivo del servidor NAS)	TCP	Entrante	PAX es un protocolo de archivos de dispositivo que funciona con formatos de cinta UNIX estándares.
8888	RCPD (ruta de datos de replicación)	TCP	Entrante	Lo utiliza el replicador (en el lado secundario). El replicador lo mantiene abierto tan pronto como advierte la existencia de datos que deben replicarse. Una vez que se inicia, no hay manera de detener el servicio.
10 000	NDMP	TCP	Entrante	• Permite controlar el respaldo y la recuperación de un servidor Network Data Management Protocol (NDMP) por medio de una aplicación de respaldo en red, sin instalar software de otros fabricantes en el servidor. En un dispositivo, el servidor NAS funciona como servidor NDMP. • El servicio NDMP puede deshabilitarse si no se utiliza el respaldo en cinta de NDMP. • El servicio NDMP se autentica con un nombre de usuario y una contraseña. El nombre de usuario puede configurarse. La documentación de NDMP describe cómo configurar la contraseña para distintos ambientes.
[10 500,10 531]	Rango reservado de NDMP para puertos dinámicos de NDMP	TCP	Entrante	En las sesiones de respaldo o restauración de tres vías, los servidores NAS utilizan del puerto 10 500 al puerto 10 531.

Tabla 12. Puertos de red del dispositivo relacionados con archivos (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
12 228	Servicio del programa antivirus	TCP	Saliente	Se requiere para el servicio del programa antivirus.

Puertos de red relacionados con los dispositivos modelo X de PowerStore

En la siguiente tabla se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en dispositivos Modelo PowerStore X.

Tabla 13. Puertos de red relacionados con los dispositivos Modelo PowerStore X

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
22	Servidor de SSH	TCP	Entrante	Permite el acceso mediante el protocolo SSH (si está habilitado). Si está cerrado, las conexiones de administración por medio de SSH no estarán disponibles.
80 y 9000	vSphere Web Access	TCP	Entrante	Acceso para el plug-in de vSphere Update Manager Web Client para vSphere Web Client.
162 o entre 1024 y 49151	SNMP	UDP	Saliente	Comunicaciones de SNMP. Si está cerrado, los mecanismos de alerta del sistema de almacenamiento que se basan en SNMP no se enviarán. El número de puerto predeterminado para SNMP es 162.
427	Protocolo de ubicación de servicios (SLP) de CIM	TCP/UDP	Bidireccional	El cliente de CIM utiliza el protocolo de ubicación de servicios versión 2 (SLPv2) para buscar servidores de CIM.
443	vSphere Web Client	TCP	Entrante	Se utiliza para las conexiones de clientes.
514	Registro remoto	UDP	Saliente	Permite al dispositivo enviar mensajes de registro a los servidores de syslog remoto. Si está cerrado, no se pueden enviar mensajes de registro a los servidores de syslog remoto.
902	Copia de archivos de red (NFC), VMware vCenter y vSphere Web Client	TCP	• Bidireccional para NFC • Saliente para VMware vCenter • Entrante para vSphere Web Client	• NFC proporciona un servicio FTP con reconocimiento del tipo de archivo para componentes de vSphere. De manera predeterminada, ESXi utiliza NFC para operaciones como copia y transferencia de datos entre almacenes de datos. • Agente de VMware vCenter • Para vSphere Web Client, se utiliza para las conexiones de clientes.
1468	Registro remoto	TCP	Saliente	Permite al dispositivo enviar mensajes de registro a los servidores de syslog remoto. Si está cerrado, no se pueden enviar mensajes de registro a los servidores de syslog remoto.
5900, 5901, 5902, 5903 y 5904	Protocolo RFB	TCP	Entrante	Acceso remoto a interfaces gráficas de usuario, como VNC.

Tabla 13. Puertos de red relacionados con los dispositivos Modelo PowerStore X (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
5988	Servidor de Common Information Model (CIM)	TCP	Entrante	Servidor para CIM.
5989	Servidor de CIM seguro	TCP	Entrante	Servidor para CIM.
6999	Enrutador lógico distribuido virtual de NSX, rabbitmqproxy	UDP	• Bidireccional para el servicio de enrutador distribuido virtual de NSX • Saliente para rabbitmqproxy	• Para el servicio de enrutador distribuido virtual de NSX, el puerto del firewall asociado a este servicio se abre cuando se instalan VIB de NSX y se crea el módulo VDR. Si no hay ninguna instancia de VDR asociada al host, no es necesario que el puerto esté abierto. • Para rabbitmqproxy, un proxy que se ejecuta en el host ESXi. Este proxy permite que las aplicaciones que se ejecutan dentro de máquinas virtuales se comuniquen con los intermediadores de AMQP que se ejecutan en el dominio de red de vCenter. No es necesario que la máquina virtual esté en la red, es decir, no se requiere ninguna NIC. Asegúrese de que las direcciones IP de la conexión saliente incluyan al menos los intermediadores en uso o futuros. Puede agregar intermediadores más adelante para realizar un escalamiento vertical.
8000	vMotion	TCP	Bidireccional	Se requiere para la migración de máquinas virtuales con vMotion. Los hosts ESXi escuchan en el puerto 8000 las conexiones TCP desde hosts ESXi remotos para el tráfico de vMotion.
8100, 8200 y 8300	Tolerancia a fallas	TCP/UDP	Bidireccional	Se utiliza para el tráfico entre hosts para vSphere Fault Tolerance (FT).
8301 y 8302	DVSSync	UDP	Bidireccional	Los puertos DVSSync se utilizan para sincronizar los estados de los puertos virtuales distribuidos entre los hosts que tienen habilitada la grabación/reproducción de VMware FT. Solamente los hosts en los que se ejecutan máquinas virtuales principales o de respaldo deben tener estos puertos abiertos. En los hosts que no usan VMware FT, no es necesario que estos puertos estén abiertos.
9080	Filtro de I/O	TCP	Saliente	Lo utiliza la función de almacenamiento de filtros de I/O.
31031	vSphere Replication y VMware Site Recovery Manager	TCP	Saliente	vSphere Replication y VMware Site Recovery Manager lo utilizan para el tráfico de replicación continuo.
44046	vSphere Replication y VMware Site Recovery Manager	TCP	Saliente	vSphere Replication y VMware Site Recovery Manager lo utilizan para el tráfico de replicación continuo.

Hojas de trabajo de planificación de espacio en el rack

En este apéndice se incluyen las siguientes hojas de trabajo:

Temas:

- [Ejemplo de Hoja de trabajo para la planificación de espacio en el rack](#)
- [Hoja de trabajo en blanco para la planificación de espacio en el rack](#)

Ejemplo de Hoja de trabajo para la planificación de espacio en el rack

40 (1U)	Switch de administración (solo modelo PowerStore T)	
39 (1U)	Switch Ethernet 2	
38 (1U)	Switch Ethernet 1	
35/36 (2U)		
33/34 (2U)		
31/32 (2U)		
29/30 (2U)		
27/28 (2U)		
25/26 (2U)		
23/24 (2U)	Gabinete base 5 (BE5) Dirección IP de administración: xxx.xx.xxx	Dispositivo 5 (2 gabinetes de expansión en la pila, orden alterno)
21/22 (2U)	Gabinete de expansión (BE5-EE1)	
19/20 (2U)	Gabinete de expansión (BE5-EE2)	
17/18 (2U)	Gabinete de expansión (BE4-EE2)	Dispositivo 4 (2 gabinetes de expansión en la pila, orden alterno)
15/16 (2U)	Gabinete de expansión (BE4-EE1)	
13/14 (2U)	Gabinete base 4 (BE4) Dirección IP de administración: xxx.xx.xxx	
11/12 (2U)	Gabinete base 3 (BE3) Dirección IP de administración: xxx.xx.xxx	Dispositivo 3 (1 gabinete de expansión en la pila)
09/10 (2U)	Gabinete de expansión (BE3-EE1)	
07/08 (2U)	Gabinete de expansión (BE2-EE1)	Dispositivo 2 (1 gabinete de expansión en la pila)
05/06 (2U)	Gabinete base 2 (BE2) Dirección IP de administración: xxx.xx.xxx	
03/04 (2U)	Gabinete base 1 (BE1)	Dispositivo 1

	Dirección IP de administración: xxx.xx.xxx	(Sin gabinete de expansión en la pila)
01/02 (2U)	Reservado con fines de facilidad de reparación	

Hoja de trabajo en blanco para la planificación de espacio en el rack

40 (1U)	Switch de administración (solo modelo PowerStore T)	
39 (1U)	Switch Ethernet 2	
38 (1U)	Switch Ethernet 1	
35/36 (2U)		
33/34 (2U)		
31/32 (2U)		
29/30 (2U)		
27/28 (2U)		
25/26 (2U)		
23/24 (2U)		
21/22 (2U)		
19/20 (2U)		
17/18 (2U)		
15/16 (2U)		
13/14 (2U)		
11/12 (2U)		
09/10 (2U)		
07/08 (2U)		
05/06 (2U)		
03/04 (2U)		
01/02 (2U)	Reservado con fines de facilidad de reparación	