Documentación de ASA r2

ASA r2

NetApp
September 26, 2024

Tabla de contenidos

Documentación de ASA r2

Notas de la versión

Novedades de ONTAP 9.16,0 para los sistemas ASA R2

Descubra las nuevas funcionalidades disponibles en ONTAP 9.16,0 para los sistemas ASA R2.

Plataformas

Actualizar	Descripción
Nuevas plataformas	Están disponibles los siguientes sistemas R2 de NetApp ASA. Estas plataformas ofrecen una solución de hardware y software unificada que crea una experiencia simplificada específica para las necesidades de los clientes de SAN solo. • ASA A1K • ASA A70 • ASA A90

System Manager

Actualizar	Descripción
"Soporte optimizado para clientes de SAN únicamente"	System Manager se ha optimizado para ofrecer compatibilidad con la funcionalidad SAN esencial, al tiempo que elimina la visibilidad de las características y funciones que no se admiten en los entornos SAN.

Gestión del almacenamiento

Actualizar	Descripción
"Gestión de almacenamiento simplificada"	Los sistemas R2 de ASA presentan el uso de unidades de almacenamiento con grupos de consistencia para simplificar la gestión del almacenamiento. • A *storage unit* hace que el espacio de almacenamiento esté disponible para los hosts SAN para realizar operaciones de datos. Una unidad de almacenamiento hace referencia a un LUN para hosts SCSI o un espacio de nombres NVMe para los hosts NVMe. • *Un grupo de consistencia* es una colección de unidades de almacenamiento que se gestionan como una sola unidad.

Seguridad de datos

Actualizar	Descripción
"Gestor de claves incorporado y cifrado de doble capa"	Los sistemas R2 de ASA admiten un gestor de claves incorporado y cifrado de doble capa (hardware y software).

Manos a la obra

Obtenga información sobre los sistemas de almacenamiento R2 de ASA

Los nuevos sistemas NetApp ASA R2 (ASA A1K, ASA A70 y ASA A90) ofrecen una solución de hardware y software unificada que crea una experiencia simplificada específica de las necesidades de clientes exclusivos de SAN.

Los sistemas R2 de ASA son compatibles con todos los protocolos SAN (iSCSI, FC, NVMe/FC, NVMe/TCP) en una puesta en marcha de par de alta disponibilidad único. Los protocolos SCSI (iSCSI y FC) utilizan una arquitectura activo-activo simétrica para la multivía, de modo que todas las rutas entre los hosts y el almacenamiento estén activas/optimizadas. Los protocolos NVMe admiten rutas directas entre los hosts y el almacenamiento.

En un sistema ASA R2, se han optimizado el software ONTAP y System Manager para proporcionar compatibilidad con las funciones SAN esenciales mientras se quitan características y funciones que no se admiten en los entornos SAN.

Los sistemas R2 de ASA introducen el uso de unidades de almacenamiento con grupos de coherencia:

- A *storage unit* hace que el espacio de almacenamiento esté disponible para los hosts SAN para realizar operaciones de datos. Una unidad de almacenamiento hace referencia a un LUN para hosts SCSI o un espacio de nombres NVMe para los hosts NVMe.
- *Un grupo de consistencia* es una colección de unidades de almacenamiento que se gestionan como una sola unidad.

Los sistemas R2 de ASA utilizan unidades de almacenamiento y grupos de consistencia para simplificar la administración del almacenamiento y la protección de datos. Por ejemplo, suponga que tiene una base de datos que consta de 10 unidades de almacenamiento en un grupo de coherencia y necesita realizar un backup de toda la base de datos. En lugar de realizar un backup de cada unidad de almacenamiento de forma individual, puede proteger toda la base de datos mediante un backup del grupo de coherencia.

Para ayudar a proteger sus datos contra ataques maliciosos como el robo o ransomware, los sistemas ASA R2 admiten un administrador de claves integrado, cifrado de doble capa, copias Snapshot a prueba de manipulaciones, autenticación multifactor y verificación multiadministrador.

Los sistemas R2 de ASA no admiten la combinación de clústeres con los sistemas ASA, AFF o FAS actuales.

Si quiere más información

- Obtenga más información sobre la compatibilidad con los sistemas ASA R2 y las limitaciones en la "NetApp Hardware Universe".
- Más información sobre "Los nuevos sistemas R2 de ASA en comparación con los sistemas ASA".
- Obtenga más información sobre el "ASA de NetApp".

Inicio rápido para los sistemas de almacenamiento ASA R2

Para ponerse en funcionamiento con su sistema ASA R2, instale los componentes de hardware, configure el clúster, configure el acceso a datos desde los hosts al sistema de

almacenamiento y aprovisione el almacenamiento.

1. **Instale y configure el hardware**

"Instalar y configurar" Su sistema ASA R2 e implantarlo como pareja de alta disponibilidad en su entorno de ONTAP.

2. **Configure su clúster**

Use System Manager para guiarle a través de un proceso rápido y fácil para "Configure su clúster de ONTAP".

3. **Configure el acceso a los datos**

"Conecte su sistema R2 de ASA a sus clientes SAN".

4. **Aprovisione su almacenamiento**

"Aprovisionar almacenamiento" Empezar a servir datos a sus clientes SAN.

El futuro

Ahora puede usar System Manager para proteger sus datos por "creación de snapshots".

Instale su sistema ASA R2

Flujo de trabajo de instalación y configuración de sistemas de almacenamiento R2 de ASA

Para instalar y configurar su sistema ASA R2, revise los requisitos de hardware, prepare su sitio, instale y cablee los componentes de hardware, encienda el sistema y configure el clúster de ONTAP.

1. **"Revise los requisitos de instalación de hardware"**

Revise los requisitos de hardware para instalar su sistema de almacenamiento R2 de ASA.

2. **"Prepárese para instalar el sistema de almacenamiento R2 de ASA"**

Para preparar la instalación del sistema ASA R2, debe preparar el sitio, comprobar los requisitos ambientales y eléctricos y asegurarse de que hay suficiente espacio en el rack. A continuación, desembale el equipo, compare su contenido con la hoja de embalaje y registre el hardware para acceder a los beneficios de soporte.

3. **"Instale el hardware del sistema de almacenamiento R2 de ASA"**

Para instalar el hardware, instale los kits de rieles para el sistema de almacenamiento y las bandejas, y, a continuación, instale y asegure el sistema de almacenamiento en el armario o el rack de telecomunicaciones.

A continuación, deslice los estantes sobre los rieles. Por último, conecte los dispositivos de gestión de cables a la parte posterior del sistema de almacenamiento para organizar el enrutamiento de los cables.

4 **"Conecte los cables de las controladoras y las bandejas de almacenamiento para el sistema de almacenamiento ASA R2"**

Para conectar el hardware, primero conecte las controladoras de almacenamiento a la red y, a continuación, conecte las controladoras a las bandejas de almacenamiento.

5 **"Encienda el sistema de almacenamiento R2 de ASA"**

Antes de encender las controladoras, encienda cada bandeja NS224 y asigne un ID de bandeja exclusivo para comprobar que cada bandeja se identifique de forma única en la configuración.

Requisitos de instalación para los sistemas de almacenamiento ASA R2

Revise el equipo necesario y las precauciones de elevación para el sistema de almacenamiento R2 de ASA y las bandejas de almacenamiento.

Equipo necesario para la instalación

Para instalar el sistema de almacenamiento R2 de ASA, necesita los siguientes equipos y herramientas.

- Acceso a un explorador web para configurar el sistema de almacenamiento
- Correa de descarga electrostática (ESD)
- Linterna
- Portátil o consola con conexión USB/serie
- Clip de papel o bolígrafo con punta estrecha para fijar NS224 ID de estante de almacenamiento
- Destornillador Phillips número 2

Precauciones de elevación

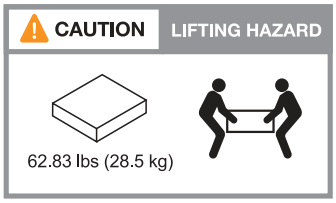
Los sistemas de almacenamiento R2 y las bandejas de almacenamiento NS224 de ASA son pesados. Tenga cuidado al levantar y mover estos elementos.

Pesos del sistema de almacenamiento

Tome las precauciones necesarias al mover o levantar su sistema de almacenamiento ASA R2.

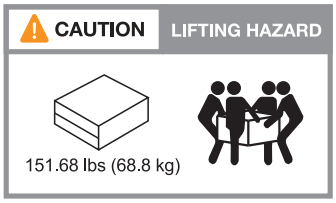
ASA A1K

Un sistema de almacenamiento ASA A1K puede pesar hasta 28,5 kg (62,83 lbs). Para levantar el sistema, se necesitan dos personas o un elevador hidráulico.



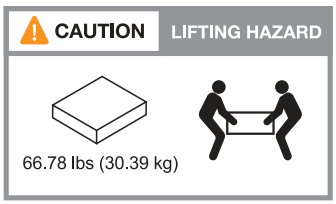
ASA A70 y ASA A90

Un sistema de almacenamiento A70 de ASA o un sistema de almacenamiento A90 de ASA pueden pesar hasta 68,8 kg (151,68 libras). Para levantar el sistema, se necesitan cuatro personas o un elevador hidráulico.



Peso del estante de almacenamiento

Un estante de almacenamiento NS224 puede pesar hasta 66,78 lbs (30,29 kg). Para levantar el estante de almacenamiento, se necesitan dos personas o un elevador hidráulico. Conserve todos los componentes en la bandeja de almacenamiento (tanto delantera como trasera) para evitar que se desequilibre el peso de bandeja.



Información relacionada

- "Información sobre seguridad y avisos normativos"

El futuro

Después de haber revisado los requisitos de hardware, usted "Prepare la instalación del sistema de almacenamiento R2 de ASA".

Prepárese para instalar un sistema de almacenamiento R2 de ASA

Prepárese para instalar su sistema de almacenamiento ASA R2 preparando el sitio, desempaquetando las cajas y comparando el contenido de las cajas con la hoja de embalaje, y registrando el sistema para acceder a los beneficios de soporte.

Paso 1: Preparar el sitio

Para instalar el sistema de almacenamiento ASA R2, asegúrese de que el sitio y el armario o rack que planea utilizar cumplan las especificaciones de su configuración.

Pasos

1. Utilice "NetApp Hardware Universe" esta herramienta para confirmar que su centro cumple los requisitos ambientales y eléctricos del sistema de almacenamiento ASA R2.
2. Asegúrese de que dispone de espacio de rack adecuado:
   - 4U en una configuración de alta disponibilidad para el sistema de almacenamiento
   - 2U por cada bandeja de almacenamiento NS224
3. Instale los switches de red necesarios.

   Consulte la "Documentación de los switches" para obtener instrucciones de instalación y "NetApp Hardware Universe" para obtener información sobre compatibilidad.

Paso 2: Desempaquetar las cajas

Después de asegurarse de que el sitio y el gabinete o rack que planea utilizar para su sistema de almacenamiento ASA R2 cumplen con las especificaciones requeridas, desembale todas las cajas y compare el contenido con los artículos en la hoja de embalaje.

Pasos

1. Abra cuidadosamente todas las cajas y coloque el contenido de una manera organizada.
2. Compara el contenido que has desempaquetado con la lista de la hoja de embalaje.

   Usted puede obtener su lista de embalaje escaneando el código QR en el lado de la caja de envío.

   Los siguientes elementos son algunos de los contenidos que puede ver en las cajas.

   Asegúrese de que todo lo que hay en las cajas coincide con la lista de la hoja de embalaje. Si hay alguna discrepancia, anótelas para realizar otras acciones.

Hardware	Cables	
• Frontal • Dispositivo de gestión de cables • Sistema de almacenamiento • Kits de rieles con instrucciones (opcional) • Bandeja de almacenamiento	• Cables Ethernet de gestión (cables RJ-45) • Cables de red • Cables de alimentación • Cables de almacenamiento (si ha pedido almacenamiento adicional) • Cable de puerto serie USB-C.	

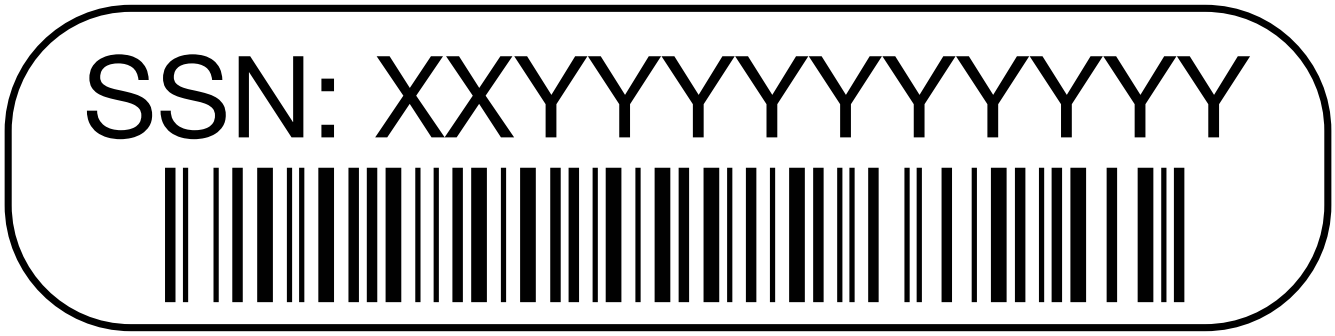
Paso 3: Registre el sistema de almacenamiento

Una vez que se asegura de que su sitio cumple los requisitos de las especificaciones de su sistema de almacenamiento R2 de ASA y que cuenta con todas las piezas solicitadas, debe registrar su sistema.

Pasos

1. Busque el número de serie del sistema de almacenamiento.

   Puede encontrar el número en la hoja de embalaje, en el correo electrónico de confirmación o en el módulo de gestión del sistema del controlador después de desempaquetarlo.



2. Vaya a la "Sitio de soporte de NetApp".
3. Determine si necesita registrar el sistema de almacenamiento:

Si usted es un…	Siga estos pasos…
Cliente existente de NetApp	a. Inicie sesión con su nombre de usuario y contraseña. b. Selecciona **Sistemas** > **Mis sistemas**. c. Confirme que el nuevo número de serie aparece en la lista. d. De lo contrario, siga las instrucciones para nuevos clientes de NetApp.
Nuevo cliente de NetApp	a. Haga clic en **Registrar ahora** y cree una cuenta. b. Selecciona **Sistemas** > **Registrar sistemas**. c. Introduzca el número de serie del sistema de almacenamiento y los detalles solicitados. Una vez aprobado el registro, puede descargar el software necesario. El proceso de aprobación puede llevar hasta 24 horas.

El futuro

Después de haber preparado para instalar su hardware ASA R2, usted "Instale el hardware del sistema de almacenamiento ASA R2".

Instale su sistema de almacenamiento R2 de ASA

Después de preparar la instalación del sistema de almacenamiento ASA R2, instale el hardware para el sistema. En primer lugar, instale los kits de guías. A continuación, instale y proteja su sistema de almacenamiento en un armario o rack de

telecomunicaciones.

Antes de empezar

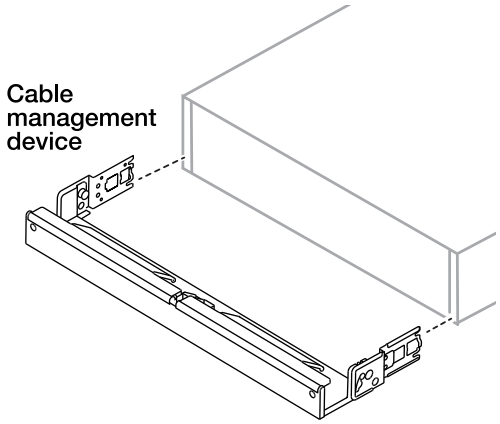
- Asegúrese de tener las instrucciones incluidas en el kit de guías.
- Tenga en cuenta los problemas de seguridad asociados con el peso del sistema de almacenamiento y la bandeja de almacenamiento.
- Comprenda que el flujo de aire a través del sistema de almacenamiento entra desde la parte frontal donde se instalan las tapas de la cubierta protectora o de los extremos y sale de la parte posterior donde se encuentran los puertos.

Pasos

1. Instale los kits de rieles para el sistema de almacenamiento y las bandejas de almacenamiento, según sea necesario, siguiendo las instrucciones incluidas en los kits.
2. Instale y proteja su sistema de almacenamiento en el armario o el rack de telecomunicaciones:
   a. Coloque el sistema de almacenamiento en los rieles situados en el centro del armario o rack de telecomunicaciones, y luego apoye el sistema de almacenamiento desde la parte inferior y deslícelo en su lugar.
   b. Fije el sistema de almacenamiento al armario o al rack de telecomunicaciones con los tornillos de montaje incluidos.
3. Instale la bandeja de almacenamiento:
   a. Coloque la parte posterior de la bandeja de almacenamiento en los raíles, apoye la bandeja desde la parte inferior y deslícela en el armario o el rack de telecomunicaciones.

      Si va a instalar varias bandejas de almacenamiento, coloque la primera bandeja de almacenamiento directamente encima de las controladoras. Coloque la segunda bandeja de almacenamiento directamente debajo de las controladoras. Repita este patrón para todas las bandejas de almacenamiento adicionales.

   b. Fije la bandeja de almacenamiento al armario o al rack Telco con los tornillos de montaje incluidos.
4. Conecte los dispositivos de gestión de cables a la parte posterior del sistema de almacenamiento.



5. Conecte el panel frontal a la parte frontal del sistema de almacenamiento.

El futuro

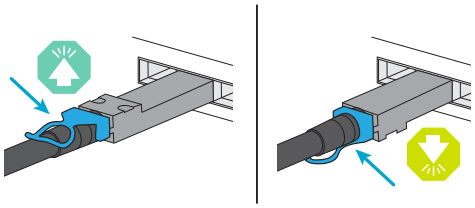
Después de instalar el hardware de su sistema ASA R2, usted"Conecte los cables de las controladoras y las bandejas de almacenamiento para el sistema ASA R2".

Conecte el hardware del sistema de almacenamiento ASA R2

Después de instalar el hardware de rack para el sistema de almacenamiento ASA R2, instale los cables de red para las controladoras y conecte los cables entre las controladoras y las bandejas de almacenamiento.

Antes de empezar

Compruebe que la flecha de la ilustración en los diagramas de cableado tiene la orientación correcta de la lengüeta de extracción del conector de cable.



- Al insertar el conector, debe sentir que encaja en su sitio; si no siente que hace clic, quítelo, gire el cabezal del cable y vuelva a intentarlo.
- Si se conecta a un switch óptico, inserte el transceptor de factor de forma pequeño conectable (SFP) en el puerto de la controladora antes de cablear al puerto.

Paso 1: Conecte las controladoras de almacenamiento a la red

Conecte las controladoras directamente entre sí y a su red host.

Antes de empezar

Póngase en contacto con el administrador de red para obtener información sobre cómo conectar el sistema de almacenamiento a los switches de red host.

Acerca de esta tarea

Estos procedimientos muestran configuraciones comunes. El cableado específico depende de los componentes solicitados del sistema de almacenamiento. Para obtener información completa sobre la configuración y la prioridad de las ranuras, consulte "NetApp Hardware Universe".

ASA A1K

Conecte las controladoras de almacenamiento entre sí para crear las conexiones del clúster de ONTAP y luego conecte los puertos Ethernet de cada controladora a la red de host.

Pasos

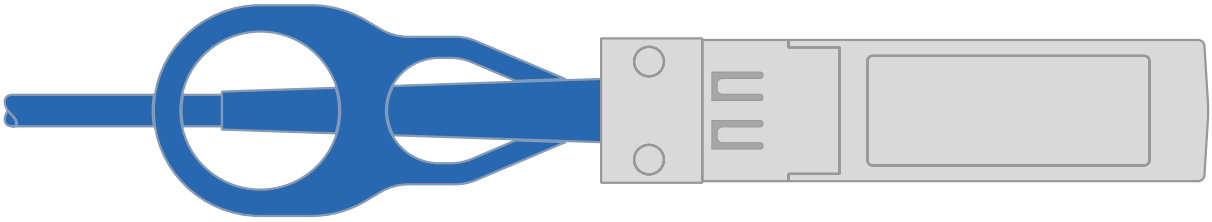
1. Use el cable de interconexión de clúster/alta disponibilidad para conectar los puertos e1a a e1a y los puertos e7a a e7a.

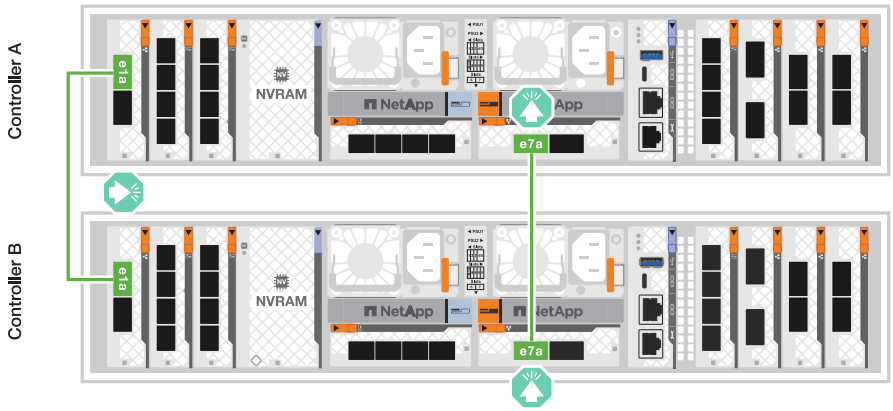
   El tráfico de interconexión de clúster y el tráfico de alta disponibilidad comparten los mismos puertos físicos.

   a. Conecte el puerto e1a de la Controladora A al puerto E1A de la Controladora B.

   b. Conecte el puerto e7a de la Controladora A al puerto E1A de la Controladora B.

      - Cables de interconexión Cluster/HA*





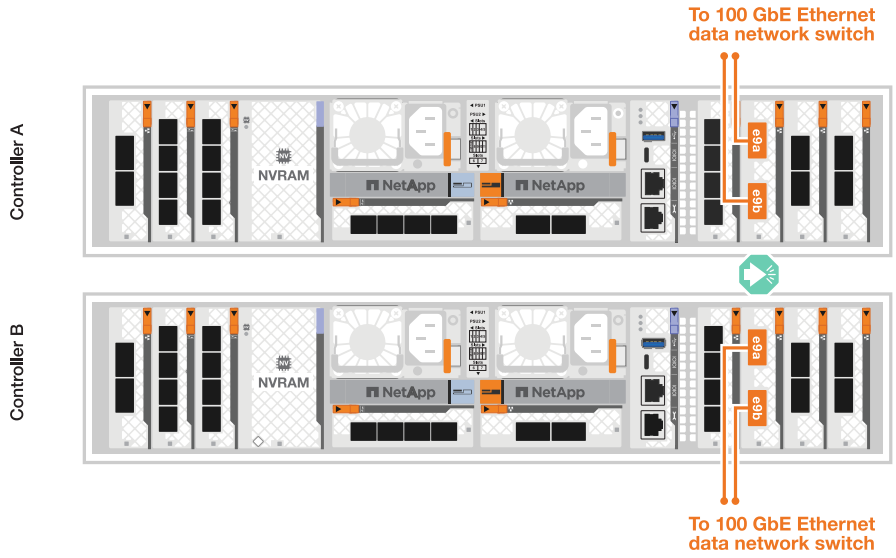
2. Conecte los puertos del módulo Ethernet a la red host.

   A continuación se muestran algunos ejemplos típicos de cableado de red host. Consulte "NetApp Hardware Universe" para obtener información sobre la configuración específica del sistema.

   a. Conecte los puertos e9a y e9b al switch de red de datos Ethernet como se muestra.

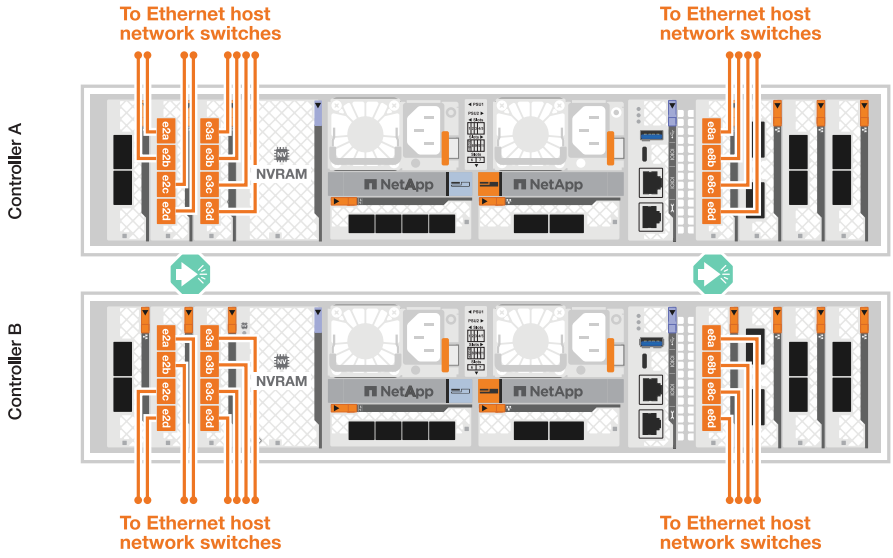
      Para obtener el rendimiento máximo del sistema para el tráfico de alta disponibilidad y clúster, no utilice los puertos e1b y e7b para las conexiones de red de host. Utilice una tarjeta de host independiente para maximizar el rendimiento.

      Cable de 100 GbE



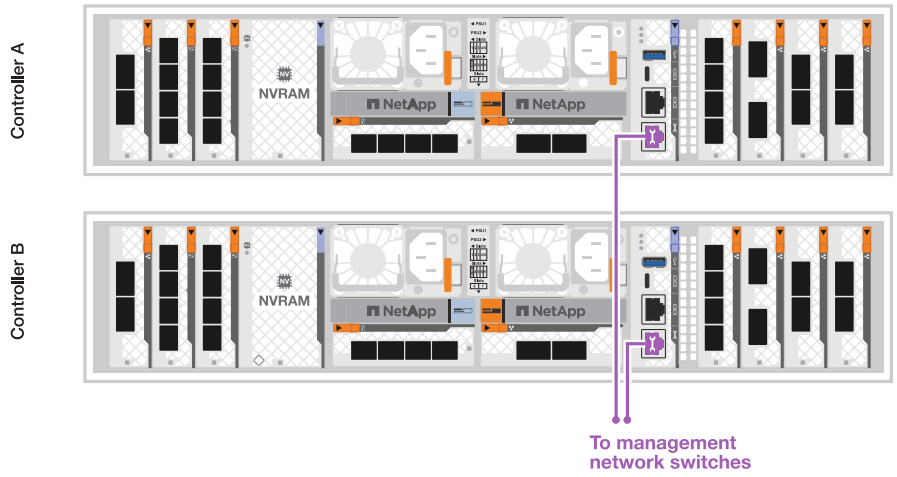
b. Conecte los switches de red host de 10/25 GbE.

Host de 10/25 GbE



3. Use los cables 1000BASE-T RJ-45 para conectar los puertos de gestión de controladoras (llave) a los switches de red de gestión.

◦ 1000BASE-T CABLES RJ-45*



No enchufe los cables de alimentación todavía.

ASA A70 y ASA A90

Conecte las controladoras de almacenamiento entre sí para crear las conexiones del clúster de ONTAP y luego conecte los puertos Ethernet de cada controladora a la red de host.

Pasos

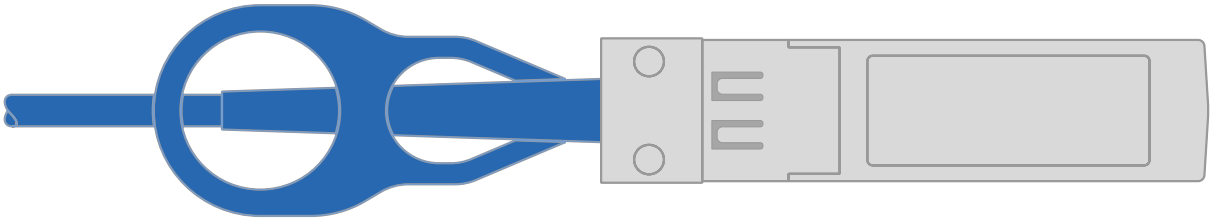
1. Use el cable de interconexión de clúster/alta disponibilidad para conectar los puertos e1a a e1a y los puertos e7a a e7a.

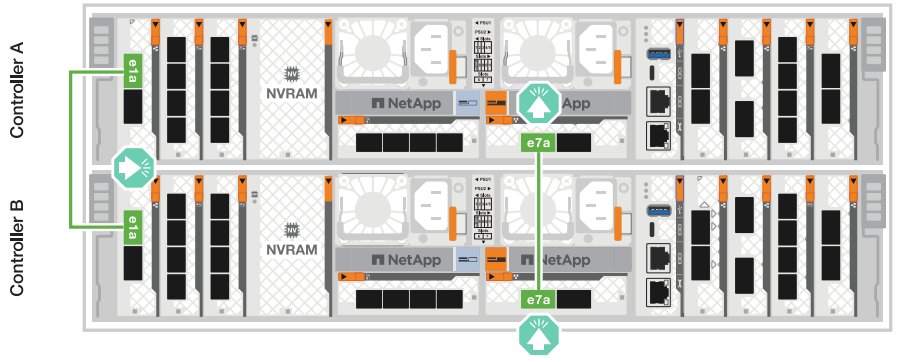
   El tráfico de interconexión de clúster y el tráfico de alta disponibilidad comparten los mismos puertos físicos.

   a. Conecte el puerto e1a de la Controladora A al puerto E1A de la Controladora B.

   b. Conecte el puerto e7a de la Controladora A al puerto E1A de la Controladora B.

      - Cables de interconexión Cluster/HA*





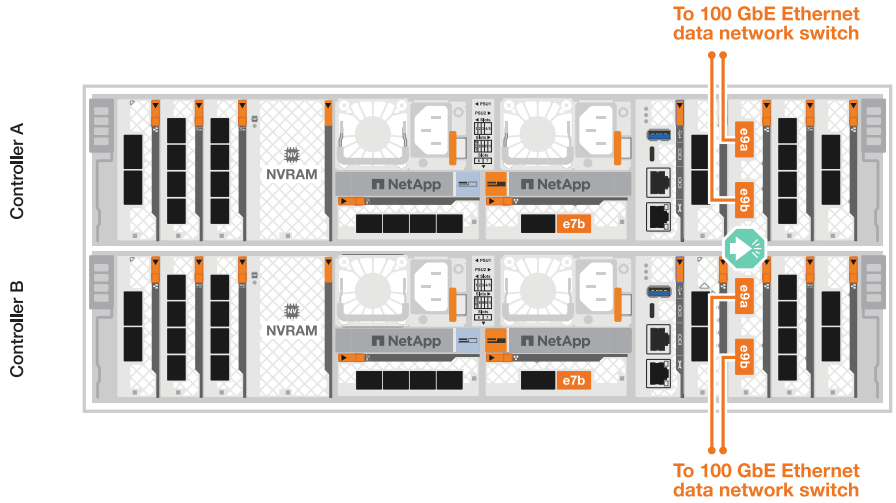
2. Conecte los puertos del módulo Ethernet a la red host.

A continuación se muestran algunos ejemplos típicos de cableado de red host. Consulte "NetApp Hardware Universe" para obtener información sobre la configuración específica del sistema.

a. Conecte los puertos e9a y e9b al switch de red de datos Ethernet como se muestra.

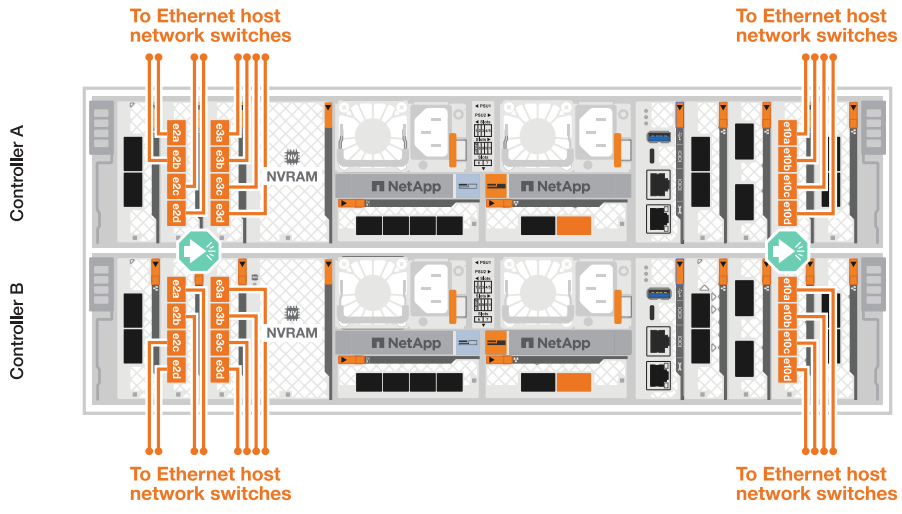
> Para obtener el rendimiento máximo del sistema para el tráfico de alta disponibilidad y clúster, no utilice los puertos e1b y e7b para las conexiones de red de host. Utilice una tarjeta de host independiente para maximizar el rendimiento.

Cable de 100 GbE



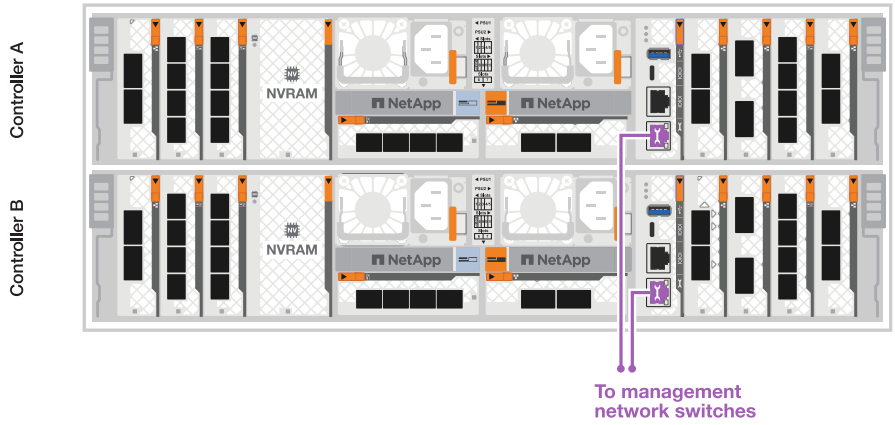
b. Conecte los switches de red host de 10/25 GbE.

4 puertos, 10/25 GbE Host



3. Use los cables 1000BASE-T RJ-45 para conectar los puertos de gestión de controladoras (llave) a los switches de red de gestión.

- 1000BASE-T CABLES RJ-45*



No enchufe los cables de alimentación todavía.

Paso 2: Conecte las controladoras de almacenamiento a las bandejas de almacenamiento

Los siguientes procedimientos de cableado muestran cómo conectar las controladoras a una bandeja y a dos bandejas. Puede conectar directamente hasta cuatro bandejas a las controladoras.

ASA A1K

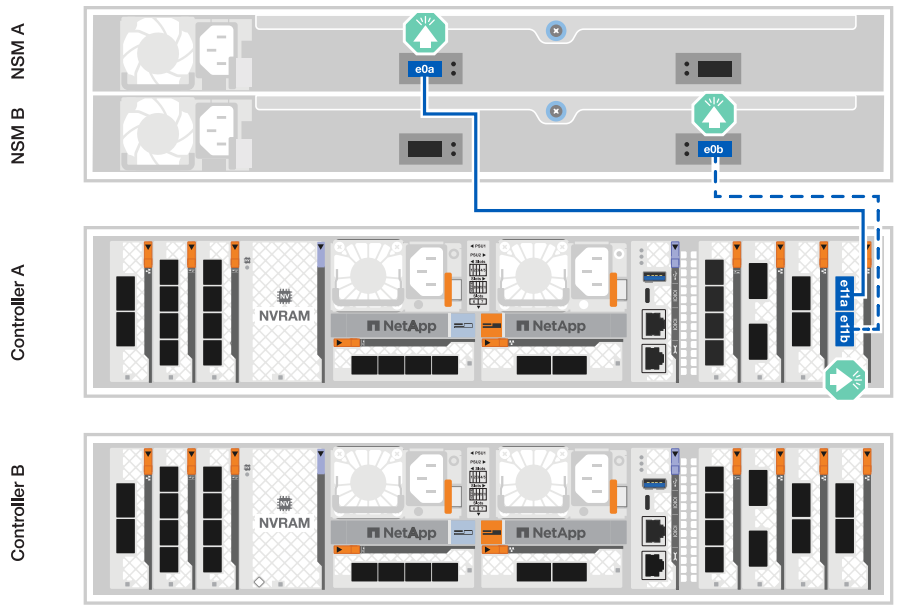
Elija una de las siguientes opciones de cableado que coincidan con su configuración.

Opción 1: Conecte las controladoras a una bandeja de almacenamiento NS224

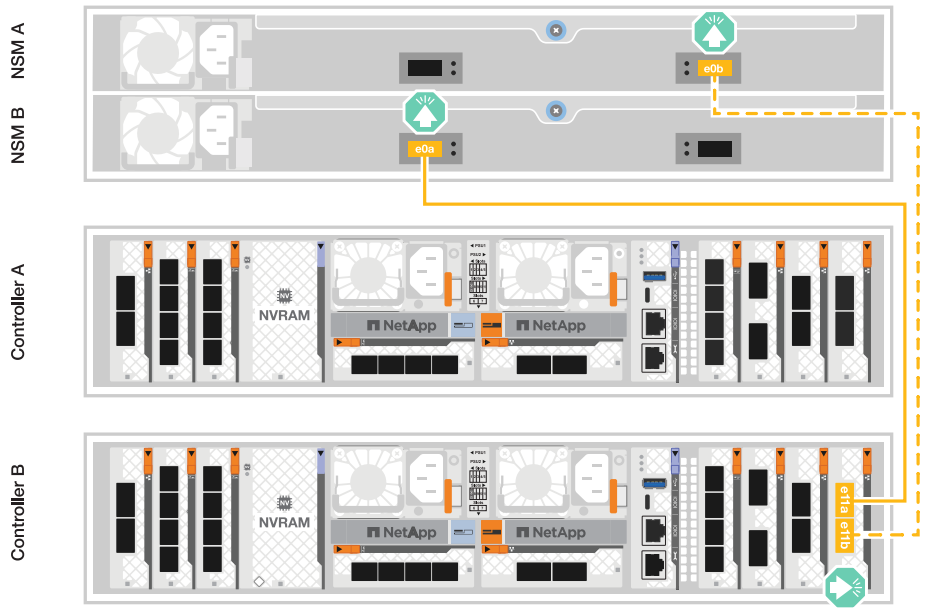
Conecte cada controladora a los módulos NSM de la bandeja NS224. Los gráficos muestran el cableado de cada una de las controladoras: El cableado de la controladora A se muestra en azul y el cableado de la controladora B se muestra en amarillo.

Pasos

1. En la controladora A, conecte los siguientes puertos:
   a. Conecte el puerto e11a al puerto NSM A e0a.
   b. Conecte el puerto e11b al puerto NSM B e0b.



2. En la controladora B, conecte los siguientes puertos:
   a. Conecte el puerto e11a al puerto NSM B e0a.
   b. Conecte el puerto e11b al puerto NSM A e0b.

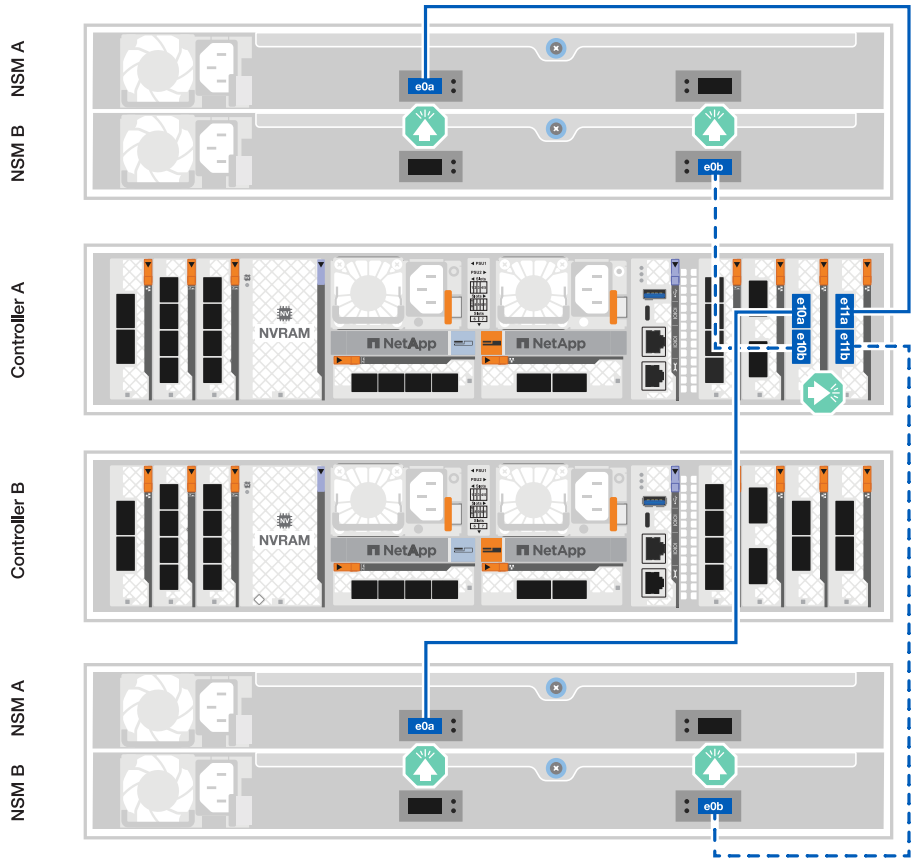


Opción 2: Conecte las controladoras a dos bandejas de almacenamiento NS224

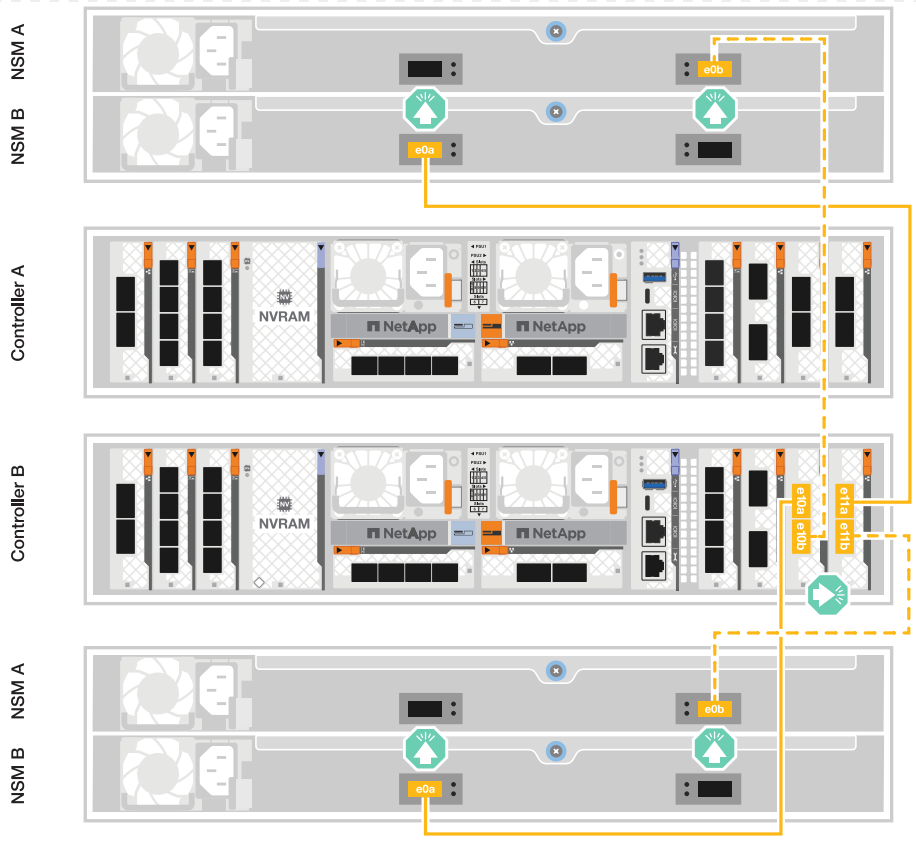
Conecte cada controladora a los módulos NSM de ambas bandejas NS224. Los gráficos muestran el cableado de cada una de las controladoras: El cableado de la controladora A se muestra en azul y el cableado de la controladora B se muestra en amarillo.

Pasos

1. En la controladora A, conecte los siguientes puertos:
   a. Conecte el puerto e11a a el puerto e0a de NSM A de la bandeja 1.
   b. Conecte el puerto e11b al puerto e0b NSM B de la bandeja 2.
   c. Conecte el puerto E10A a el puerto e0a de NSM A de la bandeja 2.
   d. Conecte el puerto e10b a el puerto e0b de NSM A de la bandeja 1.



2. En la controladora B, conecte los siguientes puertos:
   a. Conecte el puerto e11a al puerto e0a NSM B de la bandeja 1.
   b. Conecte el puerto e11b a el puerto e0b de NSM A de la bandeja 2.
   c. Conecte el puerto E10A al puerto e0a NSM B de la bandeja 2.
   d. Conecte el puerto e10b a el puerto e0b de NSM A de la bandeja 1.



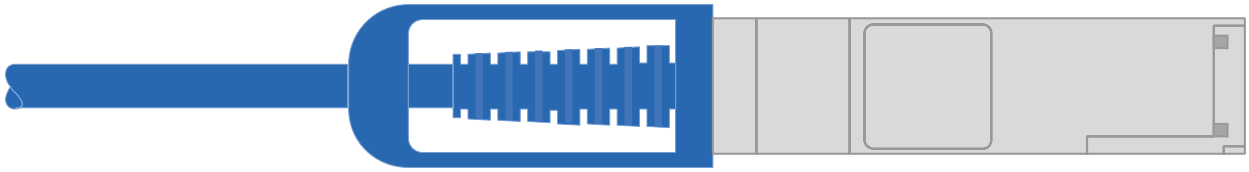
ASA A70 y ASA A90

Elija una de las siguientes opciones de cableado que coincidan con su configuración.

Opción 1: Conecte las controladoras a una bandeja de almacenamiento NS224

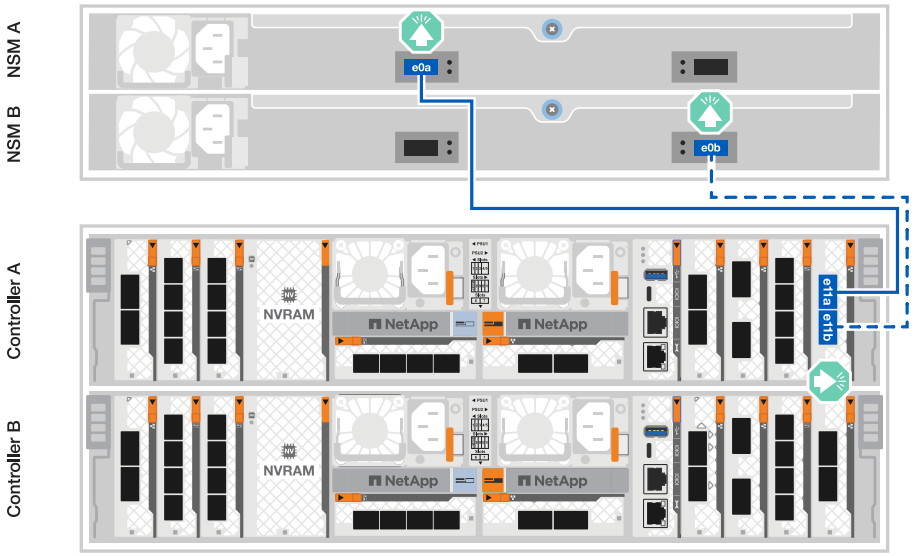
Conecte cada controladora a los módulos NSM de la bandeja NS224. Los gráficos muestran el cableado de cada una de las controladoras: El cableado de la controladora A se muestra en azul y el cableado de la controladora B se muestra en amarillo.

100 GbE QSFP28 cables de cobre

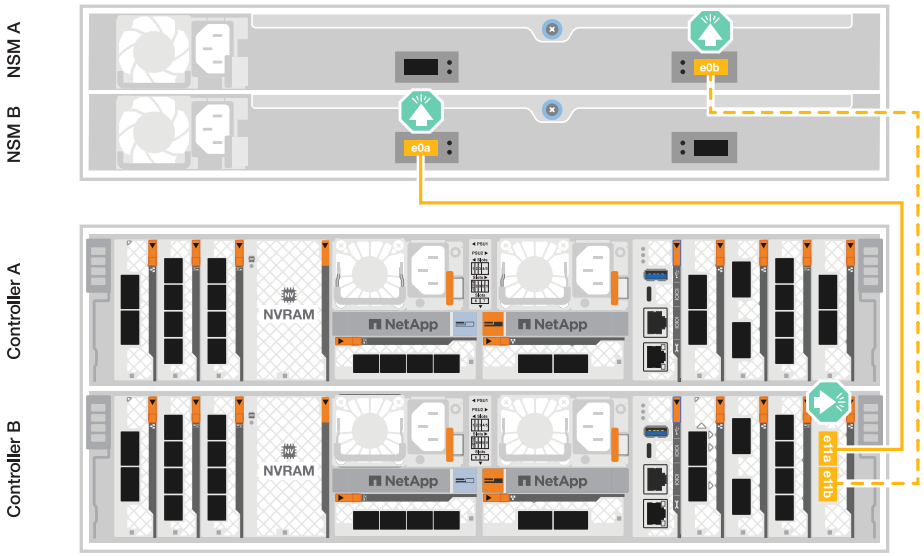


Pasos

1. Conecte el puerto e11a de la controladora A al puerto NSM A e0a.
2. Conecte la controladora A del puerto e11b al puerto NSM B e0b.



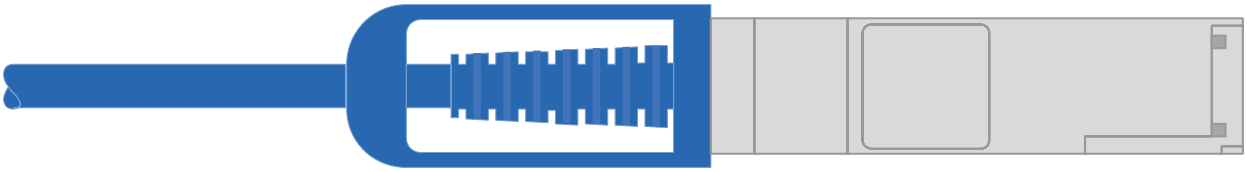
3. Conecte el puerto e11a de la controladora B al puerto NSM B e0a.
4. Conecte el puerto e11b de la controladora B al puerto NSM A e0b.


NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NVRAM
NetApp
e11a
e11b

Opción 2: Conecte las controladoras a dos bandejas de almacenamiento NS224

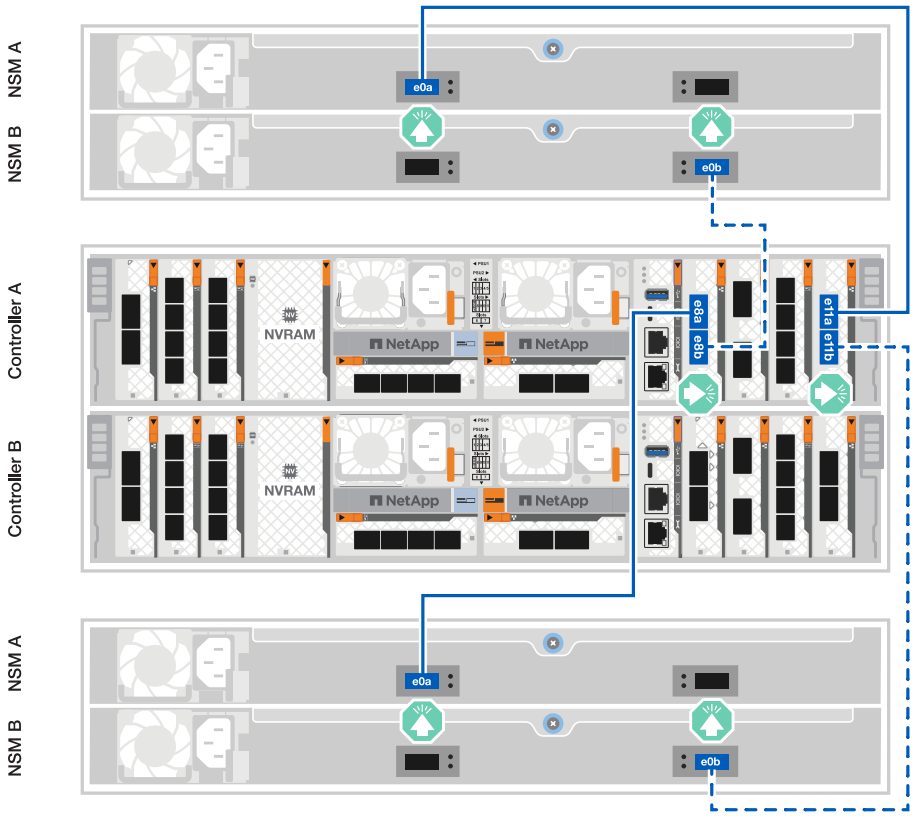
Conecte cada controladora a los módulos NSM de ambas bandejas NS224. Los gráficos muestran el cableado de cada una de las controladoras: El cableado de la controladora A se muestra en azul y el cableado de la controladora B se muestra en amarillo.

100 GbE QSFP28 cables de cobre



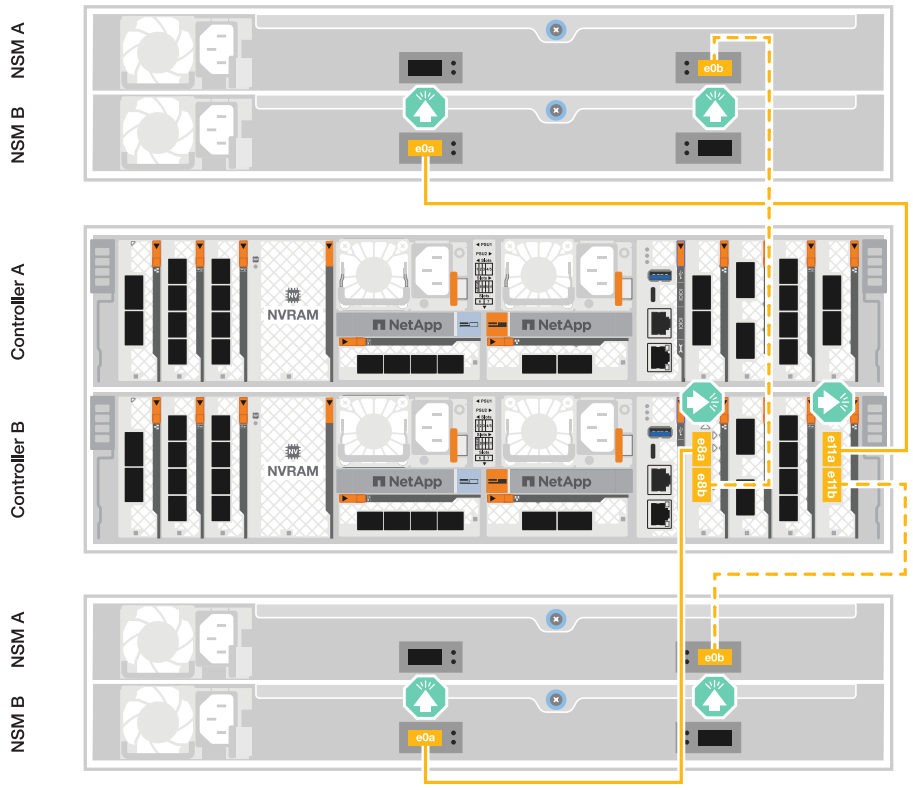
Pasos

1. En la controladora A, conecte los siguientes puertos:
   a. Conecte el puerto e11a a la bandeja 1, NSM A, puerto e0a.
   b. Conecte el puerto e11b a la bandeja 2, puerto NSM B e0b.
   c. Conecte el puerto E8a a la bandeja 2, NSM A, puerto e0a.
   d. Conecte el puerto e8b a la bandeja 1, puerto NSM B e0b.



2. En la controladora B, conecte los siguientes puertos:
   a. Conecte el puerto e11a a la bandeja 1, puerto NSM B e0a.
   b. Conecte el puerto e11b a la bandeja 2, NSM A, puerto e0b.
   c. Conecte el puerto E8a a la bandeja 2, puerto NSM B e0a.

d. Conecte el puerto e8b a la bandeja 1, NSM A, puerto e0b.



El futuro

Después de conectar las controladoras de almacenamiento a la red y luego conectar las controladoras a las bandejas de almacenamiento, usted"Encienda el sistema de almacenamiento R2 de ASA".

Encienda el sistema de almacenamiento R2 de ASA

Después de instalar el hardware de rack para el sistema de almacenamiento ASA R2 e instalar los cables para las controladoras y las bandejas de almacenamiento, debe encender las bandejas de almacenamiento y las controladoras.

Paso 1: Encienda la bandeja y asigne el ID de bandeja

Cada bandeja NS224 se distingue por un ID de bandeja único. Este ID garantiza que la bandeja sea distinta dentro de la configuración del sistema de almacenamiento. De manera predeterminada, los ID de bandeja se asignan como «00» y «01», pero es posible que deba ajustar estos ID para mantener la singularidad en todo su sistema de almacenamiento.

Acerca de esta tarea

- Un ID de bandeja válido tiene un valor de 00 a 99.
- Se debe apagar y encender la bandeja (desconecte los dos cables de alimentación, espere la cantidad de tiempo correspondiente y vuelva a conectarlos) para que el ID de bandeja surta efecto.

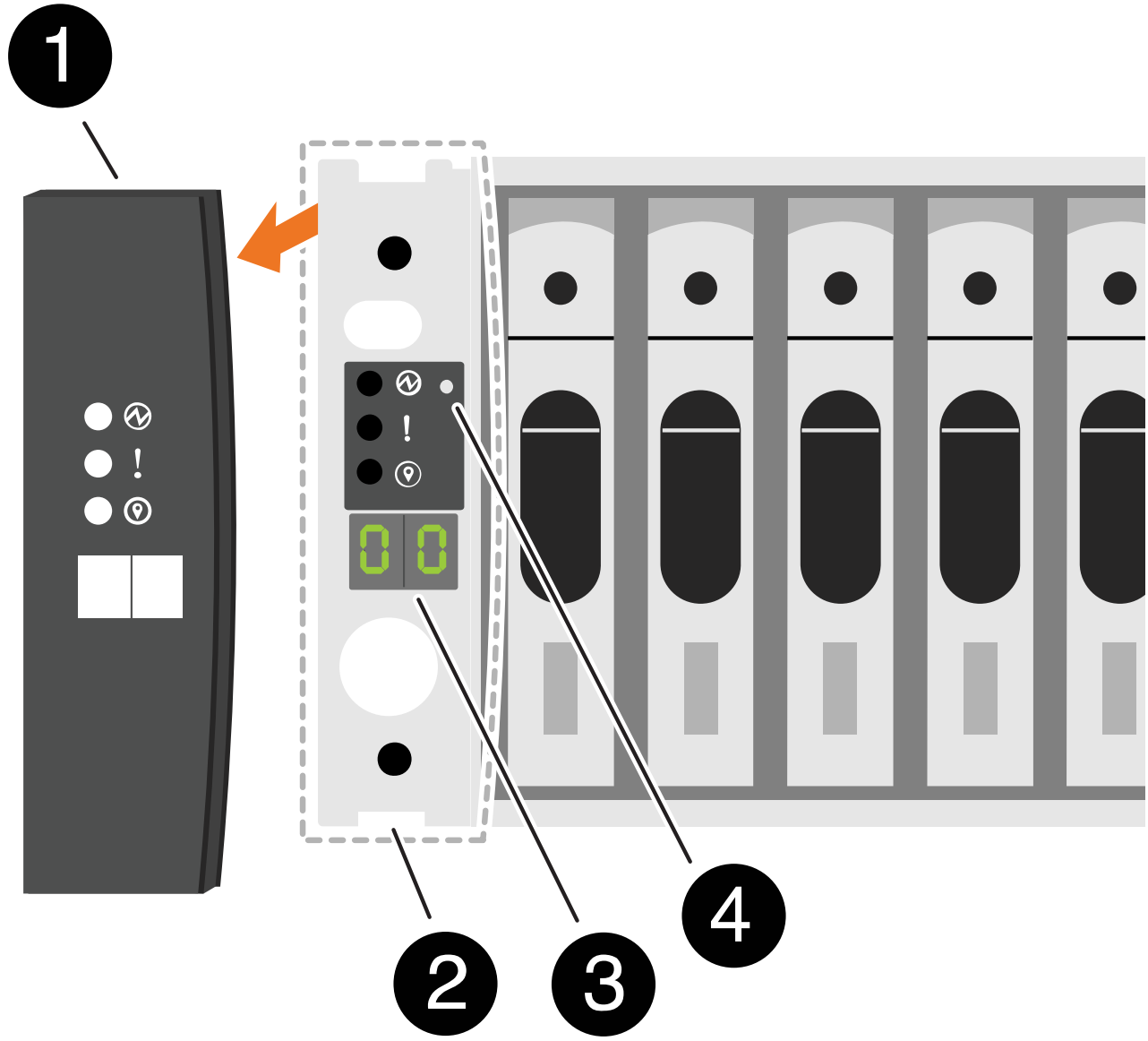
Pasos

1. Para encender la bandeja, conecte primero los cables de alimentación a la bandeja, fíjelos en su sitio con

el retén del cable de alimentación y, a continuación, conecte los cables de alimentación a las fuentes de alimentación en diferentes circuitos.

La bandeja se enciende y arranca automáticamente cuando se conecta a la fuente de alimentación.

2. Quite la tapa del extremo izquierdo para acceder al botón de ID de bandeja detrás de la placa frontal.



1	Tapa final de estante

2	Placa frontal de la bandeja
3	Número de ID de la bandeja
4	Botón de ID de bandeja

3. Cambie la primera cantidad de ID de bandeja:

   a. Inserte el extremo enderezado de un clip de papel o un bolígrafo con punta estrecha en el orificio pequeño para presionar el botón de identificación de la bandeja.

   b. Mantenga presionado el botón de ID de la bandeja hasta que el primer número de la pantalla digital parpadee y, a continuación, suelte el botón.

      Este número puede tardar hasta 15 segundos en parpadear. De este modo se activa el modo de programación del identificador de bandeja.

      > Si el ID tarda más de 15 segundos en parpadear, mantenga presionado el botón de ID de bandeja otra vez, asegurándose de presionarlo por completo.

   c. Presione y suelte el botón de ID de la bandeja para avanzar el número hasta que alcance el número deseado de 0 a 9.

      Cada duración de la prensa y la liberación puede ser de un segundo.

   El primer número continúa parpadeando.

4. Cambie el segundo número de ID de bandeja:

   a. Mantenga presionado el botón hasta que el primer número de la pantalla digital parpadee.

      Este número puede tardar hasta tres segundos en parpadear.

   El primer número de la pantalla digital deja de parpadear.

a. Presione y suelte el botón de ID de la bandeja para avanzar el número hasta que alcance el número deseado de 0 a 9.

   El segundo número continúa parpadeando.

5. Bloquee el número deseado y salga del modo de programación manteniendo presionado el botón de ID de la bandeja hasta que el segundo número deje de parpadear.

   El número puede tardar hasta tres segundos en dejar de parpadear.

   Ambos números de la pantalla digital comienzan a parpadear y el LED ámbar se enciende después de unos cinco segundos, para alertarle de que el ID de bandeja pendiente aún no ha aplicado.

6. Apague y encienda la bandeja durante al menos 10 segundos para que el ID de bandeja quede registrado.
   a. Desconecte el cable de alimentación de ambas fuentes de alimentación de la bandeja.
   b. Espere 10 segundos.
   c. Vuelva a conectar los cables de alimentación a los suministros de alimentación de la bandeja para completar el ciclo de alimentación.

      Una fuente de alimentación se enciende tan pronto como se conecta el cable de alimentación. Su LED bicolor debe iluminarse en verde.

7. Vuelva a colocar la tapa del extremo izquierdo.

Paso 2: Encienda los controladores

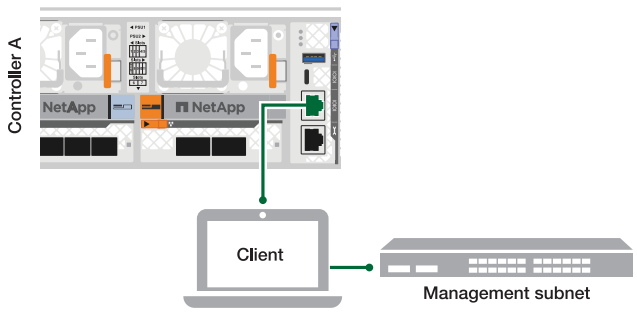
Después de encender las bandejas de almacenamiento y asignarles ID únicos, encienda la alimentación de las controladoras de almacenamiento.

Pasos

1. Conecte el portátil al puerto de la consola de serie. Esto le permitirá supervisar la secuencia de arranque cuando se encienden las controladoras.
   a. Configure el puerto de consola serie del portátil a 115.200 baudios con N-8-1.

      Consulte la ayuda en línea de su portátil para obtener instrucciones sobre cómo configurar el puerto de la consola de serie.

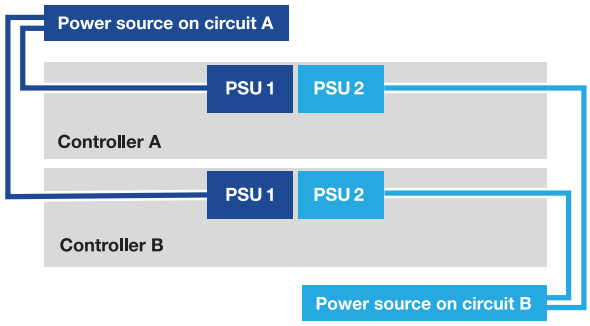
   b. Conecte el cable de consola al portátil y conecte el puerto de consola serie de la controladora mediante el cable de consola que se incluía con el sistema de almacenamiento.
   c. Conecte el portátil al interruptor de la subred de administración.



   d. Asigne una dirección TCP/IP al equipo portátil, utilizando una que se encuentre en la subred de

administración.

2. Enchufe los cables de alimentación a las fuentes de alimentación de la controladora y luego conéctelos a fuentes de alimentación de diferentes circuitos.



   - El sistema de almacenamiento comienza a arrancar. El arranque inicial puede tardar hasta ocho minutos.
   - Los LED parpadean y los ventiladores se inician, lo que indica que las controladoras se están encendiendo.
   - Los ventiladores pueden ser muy ruidosos cuando se ponen en marcha por primera vez. El ruido del ventilador durante el arranque es normal.

3. Asegure los cables de alimentación con el dispositivo de seguridad de cada fuente de alimentación.

El futuro

Después de encender su sistema de almacenamiento ASA R2,"Configure un clúster R2 de ONTAP ASA"

Configure su sistema ASA R2

Configure un clúster de ONTAP en su sistema de almacenamiento ASA R2

System Manager de ONTAP le guía a través de un flujo de trabajo rápido y sencillo para configurar un clúster de ONTAP ASA R2.

Durante la configuración del clúster, se crea la máquina virtual de almacenamiento de datos predeterminada. De manera opcional, puede habilitar el sistema de nombres de dominio (DNS) para resolver los nombres de host, configurar el clúster para que utilice el protocolo de tiempo de redes (NTP) para la sincronización de hora y habilitar el cifrado de datos en reposo.

Antes de empezar

Recopile la siguiente información:

- Dirección IP de gestión del clúster

  La dirección IP de administración del clúster es una dirección IPv4 exclusiva para la interfaz de gestión de clústeres que usa el administrador del clúster para acceder a la máquina virtual de almacenamiento de administrador y gestionar el clúster. Puede pedirle esta dirección IP al administrador responsable de la asignación de direcciones IP en la organización.

- Máscara de subred de red

  Durante la configuración del clúster, ONTAP recomienda un conjunto de interfaces de red adecuadas para la configuración. Puede ajustar la recomendación si es necesario.

- Dirección IP de puerta de enlace de red
- Dirección IP del nodo asociado
- Nombres de dominio DNS
- Direcciones IP del servidor de nombres DNS
- Direcciones IP del servidor NTP
- Máscara de subred de datos

Pasos

1. Detecte la red del clúster
   a. Conecte su portátil al switch de administración y acceda a los equipos y dispositivos de red.
   b. Abra el Explorador de archivos.
   c. Seleccione **Red**; luego haga clic con el botón derecho y seleccione **Actualizar**.
   d. Seleccione el icono de ONTAP y luego acepte los certificados que se muestran en la pantalla.

      Se abrirá System Manager.

2. En **Contraseña**, crea una contraseña segura para la cuenta de administrador.

   La contraseña debe tener al menos ocho caracteres y debe contener al menos una letra y un número.

3. Vuelva a introducir la contraseña para confirmar y luego seleccione **Continuar**.
4. En **Direcciones de red**, ingrese un nombre de sistema de almacenamiento o acepte el nombre predeterminado.

   Si cambia el nombre del sistema de almacenamiento predeterminado, el nuevo nombre debe comenzar por una letra y debe tener menos de 44 caracteres. Puede utilizar un punto (.), un guión (-) o un guión bajo (_) en el nombre.

5. Introduzca la dirección IP de administración del clúster, la máscara de subred, la dirección IP de la puerta de enlace y la dirección IP del nodo asociado; a continuación, seleccione * Continuar *.
6. En **Servicios de red**, seleccione las opciones deseadas para **Usar el Sistema de nombres de dominio (DNS) para resolver nombres de host** y **Usar el Protocolo de hora de red (NTP) para mantener los tiempos sincronizados**.

   Si decide utilizar el DNS, introduzca el dominio DNS y los servidores de nombres. Si elige usar NTP, ingrese los servidores NTP; luego seleccione **Continuar**.

7. En **Cifrado**, ingrese una frase de contraseña para Onboard Key Manager (OKM).

   El cifrado de los datos en reposo mediante un gestor de claves incorporado (OKM) se selecciona de forma predeterminada. Si desea usar un gestor de claves externo, actualice las selecciones.

   De manera opcional, puede configurar el clúster para el cifrado tras completar la configuración del clúster.

8. Selecciona **Inicializar**.

   Una vez completada la configuración, se le redirigirá a la dirección IP de administración del clúster.

9. En **Red**, selecciona **Configurar protocolos**.

Para configurar IP (iSCSI y NVMe/TCP), haga lo siguiente…	Para configurar FC y NVMe/FC, haga esto…
a. Seleccione **IP**; luego seleccione **Configurar interfaces IP**. b. Seleccione **Añadir una subred**. c. Escriba un nombre para la subred y, a continuación, introduzca las direcciones IP de la subred. d. Introduzca la máscara de subred y, opcionalmente, introduzca una puerta de enlace; a continuación, seleccione **Agregar**. e. Selecciona la subred que acabas de crear y, a continuación, selecciona **Guardar**. f. Seleccione **Guardar**.	a. Seleccione **FC**; luego seleccione **Configurar interfaces FC** y/o **Configurar interfaces NVMe/FC**. b. Seleccione los puertos FC y/o NVMe/FC; a continuación, seleccione **Guardar**.

10. Opcionalmente, descargue y ejecute "Config Advisor de ActiveIQ" para confirmar la configuración.

    ActiveIQ Config Advisor es una herramienta para sistemas NetApp que comprueba errores de configuración comunes.

El futuro

Está listo para "configure el acceso a los datos" pasar de sus clientes SAN a su sistema ASA R2.

Habilite el acceso a datos desde hosts SAN a su sistema de almacenamiento ASA R2

Para configurar el acceso a los datos, debe asegurarse de que los parámetros y los ajustes específicos del cliente SAN que sean críticos para el funcionamiento correcto con ONTAP se hayan configurado correctamente. Si utiliza VMware, debe migrar las máquinas virtuales.

Configure el acceso a datos desde hosts SAN

La configuración necesaria para configurar el acceso a los datos al sistema ASA R2 desde los hosts SAN varía en función del sistema operativo del host y del protocolo. La configuración correcta es importante para obtener el mejor rendimiento y una correcta recuperación tras fallos.

Consulte la documentación del host SAN de ONTAP para "Clientes SCSI VMware vSphere" "Clientes NVMe VMware vSphere"y "Otros clientes SAN" para configurar correctamente los hosts para conectarse al sistema ASA R2.

Migrar los equipos virtuales de VMware

Si necesita migrar la carga de trabajo de sus máquinas virtuales desde un sistema de almacenamiento de ASA a un sistema de almacenamiento R2 de ASA, NetApp recomienda utilizar "VSphere vMotion de VMware" para realizar una migración activa y sin interrupciones de los datos.

El futuro

Está preparado para "aprovisionar almacenamiento"habilitar los hosts SAN para leer y escribir datos en unidades de almacenamiento.

Use ONTAP para gestionar sus datos

Demostraciones en vídeo del sistema de almacenamiento R2 de ASA

Vea vídeos breves que muestran cómo utilizar System Manager de ONTAP para realizar tareas comunes de forma rápida y sencilla en sus sistemas de almacenamiento R2 de ASA.

Configure los protocolos SAN en su sistema ASA R2

"Transcripción de vídeo"

Aprovisionar almacenamiento SAN en su sistema ASA R2

"Transcripción de vídeo"

Replique datos en un clúster remoto de un sistema ASA R2

"Transcripción de vídeo"

Gestione su almacenamiento

Aprovisione el almacenamiento SAN de ONTAP en los sistemas ASA R2

Al aprovisionar almacenamiento, permite que los hosts de SAN lean y escriban datos en sistemas de almacenamiento ASA R2. Para aprovisionar almacenamiento, se debe usar ONTAP System Manager para crear unidades de almacenamiento, añadir iniciadores de host y asignar el host a una unidad de almacenamiento. También debe realizar los pasos en el host para habilitar las operaciones de lectura/escritura.

Cree unidades de almacenamiento

En el sistema R2 de ASA, una unidad de almacenamiento pone el espacio de almacenamiento a disposición de los hosts SAN para realizar operaciones de datos. Una unidad de almacenamiento hace referencia a un LUN para hosts SCSI o un espacio de nombres NVMe para los hosts NVMe. Si el clúster está configurado para admitir hosts SCSI, se le pedirá que cree un LUN. Si el clúster se configuró para admitir hosts NVMe, se le solicitará que cree un espacio de nombres de NVMe. Una unidad de almacenamiento ASA R2 tiene una capacidad máxima de 128TB TB.

Consulte los "NetApp Hardware Universe"límites más actuales del almacenamiento para los sistemas ASA R2.

Los iniciadores de host se añaden y se asignan a la unidad de almacenamiento como parte del proceso de creación de la unidad de almacenamiento. También puede "añada iniciadores de host"acceder a "asignar"las unidades de almacenamiento después de crear las unidades de almacenamiento.

Pasos

1. En el Administrador del sistema, seleccione **Almacenamiento** y, a continuación, seleccione + Add.
2. Introduzca un nombre para la nueva unidad de almacenamiento.

3. Introduzca el número de unidades que desea crear.

   Si se crea más de una unidad de almacenamiento, cada unidad se crea con la misma capacidad, sistema operativo de host y asignación de hosts.

4. Introduzca la capacidad de la unidad de almacenamiento y seleccione el sistema operativo del host.
5. Acepte el **mapeo de host** seleccionado automáticamente o seleccione un grupo de host diferente para la unidad de almacenamiento a la que se asignará.

   Asignación de host se refiere al grupo host al que se asignará la nueva unidad de almacenamiento. Si existe un grupo de hosts preexistente para el tipo de host seleccionado para la nueva unidad de almacenamiento, el grupo de hosts existente se selecciona automáticamente para la asignación de host. Puede aceptar el grupo de hosts que se selecciona automáticamente para la asignación de host o puede seleccionar un grupo de hosts diferente.

   Si no existe un grupo de hosts preexistente para los hosts que se ejecutan en el sistema operativo especificado, ONTAP crea automáticamente un nuevo grupo de hosts.

6. Si desea hacer alguna de las siguientes acciones, seleccione **Más opciones** y complete los pasos requeridos.

Opción	Pasos
Cambie la política de calidad de servicio (QoS) predeterminada Si la política de calidad de servicio predeterminada no se configuró anteriormente en la máquina virtual de almacenamiento (VM) donde se está creando la unidad de almacenamiento, esta opción no está disponible.	a. En **Almacenamiento y optimización**, junto a **Calidad de servicio (QoS)**, selecciona . b. Seleccione una política de calidad de servicio existente.

Opción	Pasos
Cree una nueva política de calidad de servicio	a. En **Almacenamiento y optimización**, junto a **Calidad de servicio (QoS)**, selecciona . b. Seleccione **Definir nueva política**. c. Introduzca un nombre para la nueva política de calidad de servicio. d. Establezca un límite de calidad de servicio, una garantía de calidad de servicio o ambos. i. Opcionalmente, en **Límite**, introduzca un límite máximo de rendimiento, un límite máximo de IOPS o ambos. Al establecer un rendimiento máximo e IOPS para una unidad de almacenamiento, se restringe el impacto en los recursos del sistema, de modo que no se reduce el rendimiento de las cargas de trabajo críticas. ii. Opcionalmente, en **Guarantee**, introduzca un rendimiento mínimo, un IOPS mínimo o ambos. Establecer un rendimiento mínimo e IOPS para una unidad de almacenamiento, garantiza que se cumplen los objetivos de rendimiento mínimos sin importar la demanda de otras cargas de trabajo en competencia. e. Seleccione **Agregar**.
Añada un nuevo host SCSI	a. En **Información del host**, seleccione **SCSI** para el protocolo de conexión. b. Seleccione el sistema operativo del host. c. En **Asignación de host**, selecciona **Nuevos hosts**. d. Seleccione **FC** o **iSCSI**. e. Seleccione iniciadores de host existentes o seleccione **Añadir iniciador** para añadir un nuevo iniciador de host. Un ejemplo de un WWPN de FC válido es «01:02:03:04:0A:0b:0C:0d». Algunos ejemplos de nombres de iniciadores iSCSI válidos son «iqn.1995-08.com.example:string" y «eui.0123456789abcdef».
Cree un nuevo grupo de hosts SCSI	a. En **Información del host**, seleccione **SCSI** para el protocolo de conexión. b. Seleccione el sistema operativo del host. c. En **Asignación de host**, selecciona **Nuevo grupo de hosts**. d. Introduzca un nombre para el grupo de hosts y, a continuación, seleccione los hosts que desea agregar al grupo.

Opción	Pasos
Añada un nuevo subsistema NVMe	a. En **Información del host**, selecciona **NVMe** para el protocolo de conexión. b. Seleccione el sistema operativo del host. c. En **Asignación de host**, selecciona **Nuevo subsistema NVMe**. d. Introduzca un nombre para el subsistema o acepte el nombre predeterminado. e. Escriba un nombre para el iniciador. f. Si desea habilitar la autenticación en banda o la seguridad de la capa de transporte (TLS), seleccione ; y, a continuación, seleccione sus opciones. La autenticación en banda permite una autenticación bidireccional y unidireccional segura entre sus hosts NVMe y su sistema ASA R2. TLS cifra todos los datos enviados a través de la red entre los hosts NVMe/TCP y el sistema ASA R2. g. Seleccione **Agregar iniciador** para agregar más iniciadores. El NQN host debe formatearse como <nqn.yyyy-mm> seguido de un nombre de dominio completo. El año debe ser igual o posterior a 1970. La longitud máxima total debe ser 223. Un ejemplo de un iniciador NVMe válido es nqn.2014-08.com.example:string

7. Seleccione **Agregar**.

El futuro

Las unidades de almacenamiento se crean y se asignan a los hosts. Ahora puede "crear snapshots"proteger los datos en su sistema ASA R2.

Si quiere más información

Más información sobre "Cómo utilizan los sistemas R2 de ASA las máquinas virtuales de almacenamiento".

Añada iniciadores de host

Puede añadir nuevos iniciadores de host al sistema ASA R2 en cualquier momento. Los iniciadores hacen que los hosts sean elegibles para acceder a las unidades de almacenamiento y realizar operaciones de datos.

Antes de empezar

Si desea replicar la configuración del host en un clúster de destino durante el proceso de añadir iniciadores de host, el clúster debe estar en una relación de replicación. De manera opcional, puede "cree una relación de replicación" después de añadir el host.

Añada iniciadores de host para los hosts SCSI o NVMe.

Hosts SCSI

Pasos

1. Seleccione **Host**.
2. Seleccione **SCSI** y, a continuación, seleccione + Add.
3. Introduzca el nombre del host, seleccione el sistema operativo del host e introduzca una descripción.
4. Si desea replicar la configuración del host en un clúster de destino, seleccione **Replicar configuración de host** y, a continuación, seleccione el clúster de destino.

   Su clúster debe estar en una relación de replicación para replicar la configuración del host.

5. Añada hosts nuevos o existentes.

Añadir nuevos hosts	Añada hosts existentes
a. Seleccione **Nuevos hosts**. b. Seleccione **FC** o **iSCSi** y, a continuación, seleccione los iniciadores de host. c. Opcionalmente, selecciona **Configurar proximidad de host**. La configuración de la proximidad del host permite a ONTAP identificar la controladora más cercana al host para la optimización de la ruta de datos y la reducción de latencia. Esto es aplicable solo si ha replicado los datos en una ubicación remota. Si no configuró la replicación de snapshot, no es necesario seleccionar esta opción. d. Si necesita agregar nuevos iniciadores, seleccione **Agregar iniciadores**.	a. Seleccione **Hosts existentes**. b. Seleccione el host que desea añadir. c. Seleccione **Agregar**.

6. Seleccione **Agregar**.

El futuro

Los hosts SCSI se añaden al sistema ASA R2 y está listo para asignar los hosts a las unidades de almacenamiento.

Hosts NVMe

Pasos

1. Seleccione **Host**.
2. Seleccione **NVMe** y, a continuación, seleccione + Add.
3. Introduzca un nombre para el subsistema NVMe, seleccione el sistema operativo del host e introduzca una descripción.
4. Seleccione **Añadir iniciador**.

El futuro

Los hosts NVMe se añaden al sistema ASA R2 y está listo para asignar los hosts a las unidades de

almacenamiento.

Cree grupos de hosts

En un sistema ASA R2, un *grupo de hosts* es el mecanismo utilizado para dar acceso a los hosts a las unidades de almacenamiento. Un grupo de hosts hace referencia a un igroup para hosts SCSI o a un subsistema NVMe para hosts NVMe. Un host solo puede ver las unidades de almacenamiento que están asignadas a los grupos de hosts a los que pertenece. Cuando se asigna un grupo de hosts a una unidad de almacenamiento, los hosts que son miembros del grupo pueden montar (crear directorios y estructuras de archivos en) la unidad de almacenamiento.

Los grupos de hosts se crean de forma automática o manual al crear las unidades de almacenamiento. De manera opcional, es posible usar los siguientes pasos para crear grupos de hosts antes o después de la creación de la unidad de almacenamiento.

Pasos

1. En el Administrador del sistema, seleccione **Host**.
2. Seleccione los hosts que desea añadir al grupo de hosts.

   Después de seleccionar el primer host, se muestra la opción de añadir a un grupo de hosts sobre la lista de hosts.

3. Seleccione **Añadir al grupo de hosts**.
4. Busque y seleccione el grupo de hosts al que desea añadir el host.

El futuro

Creó un grupo de hosts y ahora puede asignarlo a una unidad de almacenamiento.

Asignar la unidad de almacenamiento a un host

Después de crear las unidades de almacenamiento de ASA R2 y añadir iniciadores de host, debe asignar los hosts a las unidades de almacenamiento para comenzar a servir datos. Las unidades de almacenamiento se asignan a los hosts como parte del proceso de creación de unidades de almacenamiento. También puede asignar unidades de almacenamiento existentes a hosts nuevos o existentes en cualquier momento.

Pasos

1. Selecciona **Almacenamiento**.
2. Coloque el cursor sobre el nombre de la unidad de almacenamiento que desea asignar.
3. Seleccione ⋮ ; y, a continuación, seleccione **Asignar a hosts**.
4. Seleccione los hosts que desea asignar a la unidad de almacenamiento; luego seleccione **Mapa**.

El futuro

La unidad de almacenamiento está asignada a los hosts y está preparada para completar el proceso de aprovisionamiento en los hosts.

Completar el aprovisionamiento en el lado del host

Después de crear las unidades de almacenamiento, añadir los iniciadores de host y asignar las unidades de almacenamiento, existen pasos que debe realizar en los hosts para poder leer y escribir datos en el sistema ASA R2.

Pasos

1. Para FC y FC/NVMe, divida los switches FC por WWPN.

   Use una zona por iniciador e incluya todos los puertos de destino en cada zona.

2. Descubra la nueva unidad de almacenamiento.
3. Inicialice la unidad de almacenamiento y cree un sistema de archivos.
4. Verifique que el host pueda leer y escribir datos en la unidad de almacenamiento.

El futuro

Usted ha completado el proceso de aprovisionamiento y está listo para empezar a servir datos. Ahora puede "crear snapshots"proteger los datos en su sistema ASA R2.

Si quiere más información

Para obtener más detalles sobre la configuración del lado del host, consulte la "Documentación del host SAN de ONTAP" para su host específico.

Clone datos en sistemas de almacenamiento R2 de ASA

La clonado de datos crea copias de unidades de almacenamiento y grupos de coherencia en su sistema ASA R2 mediante System Manager de ONTAP, que se pueden usar para el desarrollo de aplicaciones, pruebas, backups, migración de datos u otras funciones administrativas.

Clonar unidades de almacenamiento

Cuando se clona una unidad de almacenamiento, se crea una nueva unidad de almacenamiento en el sistema ASA R2, que es una copia editable de un momento específico de la unidad de almacenamiento que clonó.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Pase el ratón por el nombre de la unidad de almacenamiento que desea clonar.
3. Seleccione ⋮; y, a continuación, seleccione **Clonar**.
4. Acepte el nombre predeterminado para la nueva unidad de almacenamiento que se creará como clon o introduzca uno nuevo.
5. Seleccione el sistema operativo del host.

   De forma predeterminada, se crea una nueva copia de Snapshot para el clon.

6. Si desea utilizar una instantánea existente, crear un nuevo grupo de hosts o agregar un nuevo host, seleccione **Más opciones**.

Opción	Pasos
Usar una instantánea existente	a. En **Instantánea para clonar**, selecciona **Usar una instantánea existente**. b. Seleccione la copia de Snapshot que desea usar para el clon.

Opción	Pasos
Cree un nuevo grupo de hosts	a. En **Asignación de host**, selecciona **Nuevo grupo de hosts**. b. Introduzca un nombre para el nuevo grupo de hosts y, a continuación, seleccione los iniciadores de host que se incluirán en el grupo.
Añada un nuevo host	a. En **Asignación de host**, selecciona **Nuevos hosts**. b. Introduzca el nombre A para el nuevo host y seleccione **FC** o **iSCSi**. c. Seleccione los iniciadores de host de la lista de iniciadores existentes o seleccione **Añadir** para añadir iniciadores nuevos para el host.

7. Seleccione **Clonar**.

El futuro

Ha creado una nueva unidad de almacenamiento idéntica a la unidad de almacenamiento clonada. Ya está listo para utilizar la nueva unidad de almacenamiento según sea necesario.

Clonar grupos de consistencia

Cuando se clona un grupo de consistencia, se crea un nuevo grupo de consistencia que es idéntico en estructura, unidades de almacenamiento y datos al grupo de consistencia que se clona. Utilice un clon de grupo de consistencia para realizar la prueba de las aplicaciones o migrar datos. Suponga que, por ejemplo, necesita migrar una carga de trabajo de producción fuera de un grupo de consistencia. Puede clonar el grupo de consistencia para crear una copia de la carga de trabajo de producción a fin de mantener como backup hasta que se complete la migración.

El clon se crea a partir de una copia de Snapshot del grupo de coherencia que se va a clonar. La snapshot utilizada para el clon se toma en el momento específico en que el proceso de clonación se inicia de forma predeterminada. Puede modificar el comportamiento predeterminado para utilizar una instantánea preexistente.

Las asignaciones de unidades de almacenamiento se copian como parte del proceso de clonación. Las políticas de Snapshot no se copian como parte del proceso de clonación.

Puede crear clones a partir de grupos de consistencia almacenados localmente en el sistema ASA R2 o desde grupos de coherencia que se hayan replicado a ubicaciones remotas.

Clone mediante instantánea local

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón sobre el grupo de consistencia que desea clonar.
3. Seleccione y, a continuación, seleccione **Clonar**.
4. Introduzca un nombre para el clon del grupo de consistencia o acepte el nombre predeterminado.
5. Seleccione el sistema operativo del host.
6. Si desea disociar el clon del grupo de consistencia de origen y asignar espacio en disco, seleccione **Dividir clon**.
7. Si desea utilizar una instantánea existente, crear un nuevo grupo de hosts o agregar un nuevo host para el clon, seleccione **Más opciones**.

Opción	Pasos
Usar una instantánea existente	a. En **Instantánea para clonar**, selecciona **Usar una instantánea existente**. b. Seleccione la copia de Snapshot que desea usar para el clon.
Cree un nuevo grupo de hosts	a. En **Asignación de host**, selecciona **Nuevo grupo de hosts**. b. Introduzca un nombre para el nuevo grupo de hosts y, a continuación, seleccione los iniciadores de host que se incluirán en el grupo.
Añada un nuevo host	a. En **Asignación de host**, selecciona **Nuevos hosts**. b. Introduzca el nombre del nuevo host y seleccione **FC** o **iSCSi**. c. Seleccione los iniciadores de host de la lista de iniciadores existentes o seleccione **Add initiator** para añadir iniciadores nuevos para el host.

8. Seleccione **Clonar**.

Clone mediante instantánea remota

Pasos

1. En System Manager, seleccione **Protección > Replicación**.
2. Pasa el cursor sobre la **Fuente** que deseas clonar.
3. Seleccione y, a continuación, seleccione **Clonar**.
4. Seleccione el clúster de origen y la máquina virtual de almacenamiento; a continuación, introduzca un nombre para el nuevo grupo de consistencia o acepte el nombre predeterminado.

5. Seleccione la instantánea que desea clonar y luego seleccione **Clonar**.

El futuro

Clonó un grupo de consistencia desde la ubicación remota. El nuevo grupo de coherencia está disponible en el sistema ASA R2 en local para utilizarlo según sea necesario.

El futuro

Para proteger los datos, debe "crear snapshots"hacerlo del grupo de consistencia clonado.

Modifique las unidades de almacenamiento en los sistemas de almacenamiento R2 de ASA

Para optimizar el rendimiento en el sistema ASA R2, es posible que deba modificar las unidades de almacenamiento para aumentar la capacidad, actualizar las políticas de calidad de servicio o cambiar los hosts que se asignan a las unidades. Por ejemplo, si se añade una nueva carga de trabajo de una aplicación crítica a una unidad de almacenamiento existente, es posible que deba cambiar la política de calidad de servicio (QoS) aplicada a la unidad de almacenamiento para respaldar el nivel de rendimiento necesario para la nueva aplicación.

Aumente la capacidad

Aumente el tamaño de una unidad de almacenamiento antes de que alcance su capacidad completa para evitar una pérdida de acceso a los datos que puede producirse si la unidad de almacenamiento se queda sin espacio editable. La capacidad de una unidad de almacenamiento se puede aumentar a 128 TB, que es el tamaño máximo permitido por ONTAP.

Modificar las asignaciones de hosts

Modifique los hosts que están asignados a una unidad de almacenamiento para ayudar a equilibrar las cargas de trabajo o a reconfigurar los recursos del sistema.

Modifique la política de calidad de servicio

Las políticas de calidad de servicio garantizan que el rendimiento de las cargas de trabajo críticas no se ve degradado por cargas de trabajo de la competencia. Puede utilizar políticas de calidad de servicio para establecer un *limit* de rendimiento de QoS y un *guarantee* de rendimiento de QoS.

- Límite de rendimiento de calidad de servicio

  El rendimiento *limit* de calidad de servicio restringe el impacto de una carga de trabajo en los recursos del sistema al limitar el rendimiento de la carga de trabajo a un número máximo de IOPS o MBps, o IOPS y MBps.

- Garantía de rendimiento de calidad de servicio

  El rendimiento *guarantee* de QoS garantiza que las cargas de trabajo críticas cumplan los objetivos de rendimiento mínimos, sin importar la demanda de cargas de trabajo de la competencia, garantizando que el rendimiento de la carga de trabajo crucial no caiga por debajo de un número mínimo de IOPS o MB/s, ni IOPS y MBps.

Pasos

1. En System Manager, seleccione **Almacenamiento**.

2. Pase el ratón sobre el nombre de la unidad de almacenamiento que desea editar.
3. Seleccione ⋮ y, a continuación, seleccione **Editar**.
4. Actualice los parámetros de la unidad de almacenamiento según sea necesario para aumentar la capacidad, cambiar la política de calidad de servicio y actualizar la asignación del host.

El futuro

Si aumentó el tamaño de la unidad de almacenamiento, debe volver a analizar la unidad de almacenamiento en el host para que el host reconozca el cambio de tamaño.

Elimine unidades de almacenamiento en los sistemas de almacenamiento R2 de ASA

Elimine una unidad de almacenamiento si ya no necesita mantener los datos contenidos en la unidad. Eliminar unidades de almacenamiento que ya no son necesarias puede ayudar a liberar el espacio necesario para otras aplicaciones host.

Antes de empezar

Si la unidad de almacenamiento que desea eliminar se encuentra en un grupo de consistencia que está en una relación de replicación, debe "retire la unidad de almacenamiento del grupo de consistencia" antes de eliminarla.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Pase el ratón sobre el nombre de la unidad de almacenamiento que desea eliminar.
3. Seleccione ⋮ y, a continuación, seleccione **Eliminar**.
4. Confirme que la eliminación no se puede deshacer.
5. Seleccione **Eliminar**.

El futuro

Puede usar el espacio liberado de la unidad de almacenamiento eliminada hasta "aumente el tamaño" las unidades de almacenamiento que necesiten capacidad adicional.

Límites de almacenamiento de ASA R2

Para obtener un rendimiento, configuración y soporte óptimos, debe conocer sus límites de almacenamiento de ASA R2.

Los sistemas ASA R2 ofrecen lo siguiente:

N.o máx. De nodos por clúster	2
Tamaño máximo de la unidad de almacenamiento	128TB

Si quiere más información

Para obtener una lista completa de los límites de almacenamiento más actuales de ASA R2, consulte "NetApp Hardware Universe".

Proteja sus datos

Crear snapshots para realizar backup de sus datos en los sistemas de almacenamiento R2 de ASA

Para realizar un backup de los datos en su sistema ASA R2, tiene que crear una copia Snapshot. Puede usar System Manager de ONTAP para crear una Snapshot manual de una sola unidad de almacenamiento, o para crear un grupo de coherencia y programar Snapshot automáticas de varias unidades de almacenamiento al mismo tiempo.

Paso 1: Opcionalmente, cree un grupo de consistencia

Un grupo de consistencia es una colección de unidades de almacenamiento que se administran como una sola unidad. Cree grupos de coherencia para simplificar la gestión del almacenamiento y la protección de datos para cargas de trabajo de aplicaciones que abarcan varias unidades de almacenamiento. Por ejemplo, suponga que tiene una base de datos que consta de 10 unidades de almacenamiento en un grupo de coherencia y necesita realizar un backup de toda la base de datos. En lugar de realizar un backup de cada unidad de almacenamiento, puede hacer backups de toda la base de datos simplemente añadiendo la protección de datos Snapshot al grupo de coherencia.

Cree un grupo de consistencia mediante nuevas unidades de almacenamiento o cree un grupo de consistencia mediante unidades de almacenamiento existentes.

Utilice nuevas unidades de almacenamiento

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Seleccione + Add; y, a continuación, seleccione **Utilizando nuevas unidades de almacenamiento**.
3. Introduzca un nombre para la nueva unidad de almacenamiento, el número de unidades y la capacidad por unidad.

   Si se crea más de una unidad, cada unidad se crea con la misma capacidad y el mismo sistema operativo host. Para asignar una capacidad diferente a cada unidad, selecciona **Más opciones** y luego selecciona **Añadir una capacidad diferente**.
4. Seleccione el sistema operativo del host y la asignación del host.
5. Seleccione **Agregar**.

El futuro

Creó un grupo de consistencia que contiene las unidades de almacenamiento que desea proteger. Ya está listo para crear una instantánea.

Utilice las unidades de almacenamiento existentes

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Seleccione + Add; y, a continuación, seleccione **Utilizando unidades de almacenamiento existentes**.
3. Introduzca un nombre para el grupo de consistencia y seleccione las unidades de almacenamiento que desea incluir en el grupo de consistencia.
4. Seleccione **Agregar**.

El futuro

Creó un grupo de consistencia que contiene las unidades de almacenamiento que desea proteger. Ya está listo para crear una instantánea.

Paso 2: Crear una instantánea

Una copia Snapshot es una copia local de solo lectura de los datos que se puede utilizar para restaurar unidades de almacenamiento a momentos específicos.

Las instantáneas se pueden crear bajo demanda o se pueden crear automáticamente en intervalos regulares basados en un "política y programación de snapshot". La programación y la política de Snapshot especifica cuándo se crearán las snapshots, cuántas copias se retendrán, cómo se nombrarán y cómo se etiquetarán para la replicación. Por ejemplo, un sistema puede crear una copia Snapshot cada día a las 12:10 a. m., conservar las dos copias más recientes, llamarlas «diaria» (se agrega con una marca de tiempo) y etiquetarlas como «diaria» para replicación.

Tipos de Snapshot

Se puede crear una snapshot bajo demanda de una sola unidad de almacenamiento o de un grupo de coherencia. Es posible crear Snapshot automatizadas de un grupo de coherencia que contenga varias unidades de almacenamiento. No es posible crear copias Snapshot automatizadas de una sola unidad de

almacenamiento.

- Snapshots bajo demanda

  Se puede crear una copia Snapshot bajo demanda de una unidad de almacenamiento en cualquier momento. No es necesario que la unidad de almacenamiento sea miembro de un grupo de coherencia para estar protegida por una copia Snapshot bajo demanda. Si se crea una snapshot bajo demanda de una unidad de almacenamiento que es miembro de un grupo de coherencia, las otras unidades de almacenamiento del grupo de coherencia no se incluyen en la snapshot bajo demanda. Si crea una snapshot bajo demanda de un grupo de coherencia, todas las unidades de almacenamiento del grupo de coherencia se incluyen en la snapshot.

- Snapshots automatizadas

  Las Snapshot automatizadas se crean mediante políticas de Snapshot. Para aplicar una política de Snapshot a una unidad de almacenamiento para la creación automática de snapshots, la unidad de almacenamiento debe ser miembro de un grupo de coherencia. Si aplica una política Snapshot a un grupo de coherencia, todas las unidades de almacenamiento del grupo de coherencia están protegidas con Snapshot automatizadas.

Cree una snapshot de un grupo de coherencia o de una unidad de almacenamiento.

Snapshot de un grupo de coherencia

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón sobre el nombre del grupo de consistencia que desea proteger.
3. Seleccione ⋮ ; y, a continuación, seleccione **Proteger**.
4. Si desea crear una instantánea inmediata bajo demanda, en **Protección local**, seleccione **Añadir una instantánea ahora**.

   La protección local crea la instantánea en el mismo clúster que contiene la unidad de almacenamiento.

   a. Escriba un nombre para la snapshot o acepte el nombre predeterminado; a continuación, de manera opcional, introduzca una etiqueta de SnapMirror.

      El destino remoto usa la etiqueta de SnapMirror.

5. Si desea crear instantáneas automáticas utilizando una política de instantáneas, seleccione **Programar instantáneas**.

   a. Seleccione una política de Snapshot.

      Acepte la política de snapshots predeterminada, seleccione una política existente o cree una nueva.

Opción	Pasos
Seleccione una política de Snapshot existente	⌄ Seleccione junto a la política predeterminada y, a continuación, seleccione la política existente que desea utilizar.
Cree una nueva política de snapshots	i. Seleccione + Add ; a continuación, introduzca los parámetros de la política Snapshot. ii. Seleccione **Añadir política**.

6. Si desea replicar sus instantáneas en un clúster remoto, en **Protección remota**, seleccione **Replicar a un clúster remoto**.

   a. Seleccione el clúster de origen y la máquina virtual de almacenamiento; a continuación, seleccione la política de replicación.

      La transferencia inicial de datos para la replicación comienza inmediatamente de forma predeterminada.

7. Seleccione **Guardar**.

Instantánea de la unidad de almacenamiento

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Pase el ratón sobre el nombre de la unidad de almacenamiento que desea proteger.
3. Seleccione ⋮ ; y, a continuación, seleccione **Proteger**. Si desea crear una instantánea inmediata bajo demanda, en **Protección local**, seleccione **Añadir una instantánea ahora**.

La protección local crea la instantánea en el mismo clúster que contiene la unidad de almacenamiento.

4. Escriba un nombre para la snapshot o acepte el nombre predeterminado; a continuación, de manera opcional, introduzca una etiqueta de SnapMirror.

   El destino remoto usa la etiqueta de SnapMirror.

5. Si desea crear instantáneas automáticas utilizando una política de instantáneas, seleccione **Programar instantáneas**.

   a. Seleccione una política de Snapshot.

      Acepte la política de snapshots predeterminada, seleccione una política existente o cree una nueva.

Opción	Pasos
Seleccione una política de Snapshot existente	Seleccione junto a la política predeterminada y, a continuación, seleccione la política existente que desea utilizar.
Cree una nueva política de snapshots	i. Seleccione + Add ; a continuación, introduzca los parámetros de la política Snapshot. ii. Seleccione **Añadir política**.

6. Si desea replicar sus instantáneas en un clúster remoto, en **Protección remota**, seleccione **Replicar a un clúster remoto**.

   a. Seleccione el clúster de origen y la máquina virtual de almacenamiento; a continuación, seleccione la política de replicación.

      La transferencia inicial de datos para la replicación comienza inmediatamente de forma predeterminada.

7. Seleccione **Guardar**.

El futuro

Ahora que los datos están protegidos con copias snapshot, debe "configurar la replicación de snapshots"copiar sus grupos de coherencia en una ubicación geográficamente remota a efectos de backup y recuperación ante desastres.

Replique snapshots en un clúster remoto de los sistemas de almacenamiento R2 de ASA

La replicación de Snapshot es un proceso en el que los grupos de coherencia del sistema ASA R2 se copian a una ubicación geográficamente remota. Tras la replicación inicial, los cambios en los grupos de consistencia se copian en la ubicación remota basada en una política de replicación. Los grupos de consistencia replicados pueden usarse para recuperación ante desastres o migración de datos.

La replicación de snapshots desde un sistema de almacenamiento R2 de ASA se admite únicamente en otro sistema de almacenamiento R2 de ASA. No puede replicar snapshots de un sistema ASA R2 en un sistema ASA, AFF o FAS actual.

Para configurar la replicación de Snapshot, necesita establecer una relación de replicación entre su sistema ASA R2 y la ubicación remota. La relación de replicación se rige por una política de replicación. Se crea una política predeterminada para replicar todas las copias de Snapshot durante la configuración del clúster. Puede utilizar la política predeterminada o, opcionalmente, crear una nueva.

Paso 1: Crear una relación de paridad entre clústeres

Para poder proteger los datos replicándolos en un clúster remoto, tiene que crear una relación de paridad de clústeres entre el clúster local y el remoto.

Pasos

1. En el clúster local, en System Manager, seleccione **Clúster > Configuración**.
2. En **Intercluster Settings** junto a **Cluster peers**, seleccione y luego seleccione **Add a cluster peer**.
3. Selecciona **Lauch remote cluster**; esto genera una frase de contraseña que usarás para autenticarte con el cluster remoto.
4. Después de generar la frase de acceso para el clúster remoto, péguela en **Passphrase** en el clúster local.
5. Seleccione + Add ; y, a continuación, introduzca la dirección IP de la interfaz de red de interconexión de clústeres.
6. Seleccione **Iniciar interconexión de clústeres**.

El futuro

Ha establecido una relación entre iguales para el clúster R2 de ASA local con un clúster remoto. Ahora puede crear una relación de replicación.

Paso 2: Opcionalmente, cree una política de replicación

La política de replicación de Snapshot define cuándo se replican las actualizaciones realizadas en el clúster de ASA R2 en el sitio remoto.

Pasos

1. En System Manager, seleccione **Protección > Políticas**; a continuación, seleccione **Políticas de replicación**.
2. Seleccione + Add .
3. Escriba un nombre para la política de replicación o acepte el nombre predeterminado y, a continuación, introduzca una descripción.
4. Seleccione el **Policy Scope**.

   Si desea aplicar la política de replicación a todo el clúster, seleccione **Cluster**. Si desea que la política de replicación se aplique solo a las unidades de almacenamiento de una VM de almacenamiento específica, seleccione **Storage VM**.

5. Seleccione el **Tipo de política**.

Opción	Pasos
Copie datos en el sitio remoto una vez que se hayan escrito en el origen.	a. Selecciona **Asíncrono**. b. En **Transferir instantáneas desde el origen**, acepte el programa de transferencia predeterminado o seleccione uno diferente. c. Seleccione esta opción para transferir todas las instantáneas o para crear reglas para determinar qué instantáneas desea transferir. d. Opcionalmente, habilitar la compresión de red.
Escribir datos en los sitios de origen y remotos simultáneamente.	a. Selecciona **Síncrono**.

6. Seleccione **Guardar**.

El futuro

Ha creado una política de replicación y ahora está listo para crear una relación de replicación entre su sistema ASA R2 y la ubicación remota.

Si quiere más información

Más información sobre "Equipos virtuales de almacenamiento para el acceso de clientes".

Paso 3: Crear una relación de replicación

Una relación de replicación de Snapshot establece una conexión entre el sistema ASA R2 y una ubicación remota para que pueda replicar grupos de coherencia en un clúster remoto. Los grupos de consistencia replicados pueden usarse para recuperación ante desastres o para migración de datos.

Para obtener protección contra ataques de ransomware, cuando se configura la relación de replicación, puede seleccionar bloquear las copias de Snapshot de destino. Las instantáneas bloqueadas no se pueden eliminar accidentalmente ni de forma malintencionada. Puede utilizar snapshots bloqueados para recuperar datos si una unidad de almacenamiento se ve afectada por un ataque de ransomware.

Antes de empezar

Si desea bloquear las snapshots de destino, debe "Inicialice el reloj de cumplimiento de normativas de instantáneas"antes de crear la relación de replicación.

Crear una relación de replicación con o sin snapshots de destino bloqueadas.

Con instantáneas bloqueadas

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Seleccione un grupo de consistencia.
3. Seleccione ⋮; y, a continuación, seleccione **Proteger**.
4. En **Protección remota**, selecciona **Replicar a un clúster remoto**.
5. Seleccione la **Política de replicación**.

   Debe seleccionar una política de replicación *vault*.

6. Selecciona **Ajustes de destino**.
7. Seleccione **Bloquear instantáneas de destino para evitar su eliminación**
8. Introduzca el período de retención de datos máximo y mínimo.
9. Para retrasar el inicio de la transferencia de datos, anule la selección de **Iniciar transferencia inmediatamente**.

   De forma predeterminada, la transferencia de datos inicial comienza inmediatamente.

10. Opcionalmente, para anular el horario de transferencia predeterminado, seleccione **Configuración de destino** y, a continuación, seleccione **Anular horario de transferencia**.

    Su horario de transferencia debe ser de un mínimo de 30 minutos para ser admitido.

11. Seleccione **Guardar**.

Sin instantáneas bloqueadas

Pasos

1. En System Manager, seleccione **Protección > Replicación**.
2. Seleccione esta opción para crear la relación de replicación con el destino local o el origen local.

Opción	Pasos
Destinos locales	a. Seleccione **Destinos locales** y, a continuación, seleccione Replicate. b. Busque y seleccione el grupo de coherencia de origen. El grupo de consistencia *source* hace referencia al grupo de coherencia en el clúster local que desea replicar.

Opción	Pasos
Fuentes locales	a. Seleccione **Fuentes locales** y, a continuación, seleccione Replicate . b. Busque y seleccione el grupo de coherencia de origen. El grupo de consistencia *source* hace referencia al grupo de coherencia en el clúster local que desea replicar. c. En **Destino de replicación**, seleccione el clúster en el que desea replicar y, a continuación, seleccione la VM de almacenamiento.

3. Seleccione una política de replicación.
4. Para retrasar el inicio de la transferencia de datos, seleccione **Ajustes de destino**; luego anule la selección de **Iniciar transferencia inmediatamente**.

   De forma predeterminada, la transferencia de datos inicial comienza inmediatamente.

5. Opcionalmente, para anular el horario de transferencia predeterminado, seleccione **Configuración de destino** y, a continuación, seleccione **Anular horario de transferencia**.

   Su horario de transferencia debe ser de un mínimo de 30 minutos para ser admitido.

6. Seleccione **Guardar**.

El futuro

Ahora que ha creado una política y una relación de replicación, la transferencia de datos inicial comienza según se define en la política de replicación. Opcionalmente, puede probar la conmutación por error de replicación para verificar que se puede producir una conmutación por error correcta si el sistema ASA R2 se desconecta.

Paso 4: Pruebe la conmutación por error de replicación

Opcionalmente, compruebe que puede servir datos con éxito desde unidades de almacenamiento replicadas en un clúster remoto si el clúster de origen está sin conexión.

Pasos

1. En System Manager, seleccione **Protección > Replicación**.
2. Pase el ratón sobre la relación de replicación que desea probar y, a continuación, seleccione .
3. Seleccione **Test failover**.
4. Ingrese la información de failover y luego seleccione **Test failover**.

El futuro

Ahora que sus datos están protegidos con la replicación de snapshots para la recuperación ante desastres, debe "cifre sus datos en reposo" permitir que no se puedan leer si un disco de su sistema ASA R2 se reasigna, devuelve, se pierde o es robado.

Proteja sus aplicaciones de Kubernetes en los sistemas de almacenamiento R2 de ASA

Utilice Astra Control Center para proteger sus aplicaciones de Kubernetes. Astra Control Center le permite migrar aplicaciones y datos de un clúster de Kubernetes a otro, replicar aplicaciones en un sistema remoto mediante la tecnología NetApp SnapMirror y clonar aplicaciones de la configuración provisional a la producción.

Si quiere más información

"Obtén más información sobre la protección de aplicaciones de Kubernetes mediante Astra Control".

Restauración de los datos en sistemas de almacenamiento R2 de ASA

Los datos de un grupo de coherencia o unidad de almacenamiento protegidos por Snapshot se pueden restaurar si se pierden o resultan dañados.

Restaure un grupo de consistencia

Al restaurar un grupo de coherencia, se reemplazan los datos de todas las unidades de almacenamiento del grupo de coherencia con los datos de una copia Snapshot. Los cambios realizados en las unidades de almacenamiento después de crear la instantánea no se restauran.

Es posible restaurar un grupo de coherencia desde una copia de Snapshot local o remota.

Restaurar desde una instantánea local

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Haga doble clic en el grupo de consistencia que contiene los datos que necesita restaurar.

   Se abrirá la página de detalles del grupo de consistencia.
3. Seleccione **Snapshots**.
4. Seleccione la instantánea que desea restaurar y, a continuación, seleccione ⋮.
5. Seleccione **Restaurar grupo de consistencia desde esta instantánea**; luego seleccione **Restaurar**.

Restaurar desde una snapshot remota

Pasos

1. En System Manager, seleccione **Protección > Replicación**.
2. Selecciona **Destinos locales**.
3. Seleccione el **Source** que desea restaurar y, a continuación, seleccione ⋮.
4. Seleccione **Restaurar**.
5. Seleccione el clúster, la máquina virtual de almacenamiento y el grupo de consistencia en el que desea restaurar datos.
6. Seleccione la copia de Snapshot desde la que desea restaurar.
7. Cuando se le solicite, ingrese “Restaurar”; luego seleccione **Restaurar**.

Resultado

El grupo de coherencia se restaura al momento específico de la Snapshot utilizada para la restauración.

Restaurar una unidad de almacenamiento

Al restaurar una unidad de almacenamiento, se reemplazan todos los datos de la unidad de almacenamiento con los datos de una instantánea. Los cambios realizados en la unidad de almacenamiento después de crear la instantánea no se restauran.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Haga doble clic en la unidad de almacenamiento que contiene los datos que necesita restaurar.

   Se abrirá la página de detalles de la unidad de almacenamiento.

3. Seleccione **Snapshots**.
4. Seleccione la copia Snapshot que desea restaurar.
5. Seleccione ⋮; y, a continuación, seleccione **Restaurar**.
6. Seleccione **Usar esta instantánea para restaurar la unidad de almacenamiento**; luego seleccione **Restaurar**.

Resultado

La unidad de almacenamiento se restaura al punto en el tiempo de la instantánea utilizada para la restauración.

Gestionar grupos de consistencia ONTAP en sistemas de almacenamiento R2 de ASA

Un grupo de consistencia es una colección de unidades de almacenamiento que se administran como una sola unidad. Utilice grupos de coherencia para simplificar la gestión del almacenamiento. Por ejemplo, suponga que tiene una base de datos que consta de 10 unidades de almacenamiento en un grupo de coherencia y necesita realizar un backup de toda la base de datos. En lugar de realizar un backup de cada unidad de almacenamiento, puede hacer backups de toda la base de datos simplemente añadiendo la protección de datos Snapshot al grupo de coherencia. Realizar un backup de las unidades de almacenamiento como un grupo de coherencia en lugar de hacerlo individualmente también proporciona un backup coherente de todas las unidades, mientras que realizar un backup individual puede provocar incoherencias.

Añade protección de datos de snapshot a un grupo de coherencia

Cuando se añade la protección de datos Snapshot a un grupo de coherencia, las Snapshot locales del grupo de coherencia se realizan a intervalos regulares de acuerdo con una programación predefinida.

Puede usar instantáneas "restaure los datos"para que estén perdidas o dañadas.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.

2. Pase el ratón sobre el grupo de coherencia que desea proteger.
3. Seleccione ⋮; y, a continuación, seleccione **Editar**.
4. En **Protección local**, selecciona **Programar instantáneas**.
5. Seleccione una política de Snapshot.

   Acepte la política de snapshots predeterminada, seleccione una política existente o cree una nueva.

Opción	Pasos
Seleccione una política de Snapshot existente	⌄ Seleccione junto a la política predeterminada y, a continuación, seleccione la política existente que desea utilizar.
Cree una nueva política de snapshots	a. Seleccione + Add ; y, a continuación, introduzca el nuevo nombre de la política. b. Seleccione el ámbito de la política. c. En **Programaciones** seleccione + Add . d. Seleccione el nombre que aparece bajo **Nombre de horario**; a continuación, seleccione ⌄. e. Seleccione la programación de políticas. f. En **Máximo de instantáneas**, introduzca el número máximo de instantáneas que desea conservar del grupo de consistencia. g. Opcionalmente, en **Etiqueta SnapMirror**, introduzca una etiqueta SnapMirror. h. Seleccione **Guardar**.

6. Seleccione **Editar**.

El futuro

Ahora que sus datos están protegidos con copias snapshot, debe "configurar la replicación de snapshots"copiar sus grupos de coherencia a una ubicación geográficamente remota a efectos de backup y recuperación ante desastres.

Quite la protección de datos Snapshot de un grupo de coherencia

Cuando se quita la protección de datos Snapshot de un grupo de coherencia, se deshabilitan las Snapshot para todas las unidades de almacenamiento del grupo de coherencia.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón sobre el grupo de coherencia que desea dejar de proteger.
3. Seleccione ⋮; y, a continuación, seleccione **Editar**.
4. En **Protección local**, deseleccione Programar instantáneas.
5. Seleccione **Editar**.

Resultado

No se realizarán Snapshot para ninguna de las unidades de almacenamiento del grupo de consistencia.

Añada unidades de almacenamiento a un grupo de consistencia

Expanda la cantidad de almacenamiento gestionado por un grupo de consistencia añadiendo unidades de almacenamiento al grupo de consistencia.

Puede agregar unidades de almacenamiento existentes al grupo de consistencia, o bien crear nuevas unidades de almacenamiento para agregarlas al grupo de coherencia.

Agregue unidades de almacenamiento existentes

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón sobre el grupo de consistencia que desea expandir.
3. Seleccione ⋮; y, a continuación, seleccione **Expandir**.
4. Seleccione **Usando unidades de almacenamiento existentes**.
5. Seleccione las unidades de almacenamiento que desea agregar al grupo de consistencia y, a continuación, seleccione **Expandir**.

Añada nuevas unidades de almacenamiento

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón sobre el grupo de consistencia que desea expandir.
3. Seleccione ⋮; y, a continuación, seleccione **Expandir**.
4. Seleccione **Utilizando nuevas unidades de almacenamiento**.
5. Introduzca la cantidad de unidades que desea crear y la capacidad por unidad.

   Si crea más de una unidad, cada unidad se crea con la misma capacidad y el mismo sistema operativo host. Para asignar una capacidad diferente a cada unidad, selecciona **Añadir una capacidad diferente** para asignar una capacidad diferente a cada unidad.

6. Seleccione **Expandir**.

Lo siguiente

Después de crear una nueva unidad de almacenamiento, debe "añada iniciadores de host" y "asigne la unidad de almacenamiento recién creada a un host". Cuando se añaden iniciadores de host, los hosts son elegibles para acceder a las unidades de almacenamiento y realizar operaciones de datos. La asignación de una unidad de almacenamiento a un host permite que la unidad de almacenamiento comience a servir datos al host al que se asigna.

El futuro

Las copias Snapshot existentes del grupo de coherencia no incluirán las unidades de almacenamiento que se acaban de añadir. Se debe "cree una instantánea inmediata"de su grupo de coherencia para proteger las unidades de almacenamiento recién añadidas hasta que se cree automáticamente la siguiente snapshot programada.

Quitar una unidad de almacenamiento de un grupo de consistencia

Es necesario quitar una unidad de almacenamiento de un grupo de consistencia si se desea eliminar la unidad de almacenamiento, si se desea gestionarla como parte de un grupo de consistencia diferente o si ya no necesita proteger los datos que contiene. Al quitar una unidad de almacenamiento de un grupo de consistencia, se interrumpe la relación entre la unidad de almacenamiento y el grupo de consistencia, pero no se elimina la unidad de almacenamiento.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Haga doble clic en el grupo de coherencia del que desea quitar una unidad de almacenamiento.
3. En la sección **Descripción general**, en **Unidades de almacenamiento**, seleccione la unidad de almacenamiento que desea eliminar; luego seleccione **Eliminar del grupo de consistencia**.

Resultado

La unidad de almacenamiento ya no es miembro del grupo de coherencia.

El futuro

Si necesita continuar con la protección de datos para la unidad de almacenamiento, agregue la unidad de almacenamiento a otro grupo de consistencia.

Eliminar un grupo de consistencia

Si ya no es necesario administrar los miembros de un grupo de consistencia como una sola unidad, puede eliminar el grupo de consistencia. Después de eliminar un grupo de consistencia, las unidades de almacenamiento anteriormente en el grupo siguen activas en el clúster.

Antes de empezar

Si el grupo de consistencia que desea eliminar se encuentra en una relación de replicación, debe romper la relación antes de eliminar el grupo de consistencia. Después de eliminar un grupo de consistencia de replicación anterior, las unidades de almacenamiento que estaban en el grupo de consistencia permanecen activas en el clúster y las copias replicadas permanecen en el clúster remoto.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón sobre el grupo de consistencia que desea eliminar.
3. Seleccione ⋮; y, a continuación, seleccione **Eliminar**.
4. Acepte la advertencia, luego seleccione **Eliminar**.

El futuro

Después de eliminar un grupo de coherencia, las unidades de almacenamiento anteriormente en el grupo de coherencia ya no están protegidas por las Snapshot. Considere la posibilidad de añadir estas unidades de almacenamiento a otro grupo de consistencia para protegerlas contra la pérdida de datos.

Gestione las políticas y los programas de protección de datos de ONTAP en sistemas de almacenamiento R2 de ASA

Use políticas de Snapshot para proteger los datos de sus grupos de coherencia con una programación automatizada. Use los programas de políticas dentro de las políticas de Snapshot para determinar la frecuencia con la que se realizan snapshots.

Crear una nueva programación de políticas de protección

Una programación de la política de protección define la frecuencia con la que se ejecuta una política de Snapshot. Se pueden crear programaciones para que se ejecuten en intervalos regulares en función de la cantidad de días, horas o minutos. Por ejemplo, se puede crear una programación para que se ejecute cada hora o solo una vez al día. También se pueden crear programaciones para ejecutarse en momentos específicos en días concretos de la semana o del mes. Por ejemplo, puede crear una programación para que se ejecute a las 12:15am el 20th de cada mes.

La definición de diferentes programas de políticas de protección le proporciona la flexibilidad para aumentar o reducir la frecuencia de snapshots para distintas aplicaciones. Esto le permite proporcionar un mayor nivel de protección y un menor riesgo de pérdida de datos para sus cargas de trabajo cruciales del que podría necesitar para cargas de trabajo menos cruciales.

Pasos

1. Seleccione **Protección > Políticas** y, a continuación, **Programación**.
2. Seleccione + Add .
3. Introduzca un nombre para la programación y, a continuación, seleccione los parámetros.
4. Seleccione **Guardar**.

El futuro

Ahora que ha creado una nueva programación de políticas, puede usar la programación recién creada dentro de sus políticas para definir cuándo se tomarán Snapshot.

Crear una política de Snapshot

Una política de Snapshot define la frecuencia con la que se realizan las instantáneas, la cantidad máxima de instantáneas permitidas y el tiempo que se retienen.

Pasos

1. En System Manager, seleccione **Protección > Políticas**; a continuación, seleccione **Políticas de instantánea**.
2. Seleccione + Add .
3. Escriba un nombre para la política de Snapshot.
4. Seleccione **Cluster** para aplicar la política a todo el clúster. Seleccione **Storage VM** para aplicar la política a una VM de almacenamiento individual.
5. Seleccione **Agregar un horario**; luego ingrese el horario de la política de instantáneas.
6. Seleccione **Añadir política**.

El futuro

Ahora que ha creado una política Snapshot, puede aplicarla a un grupo de coherencia. Se realizarán Snapshot del grupo de coherencia en función de los parámetros configurados en la política de Snapshot.

Aplicar una política Snapshot a un grupo de coherencia

Aplique una política Snapshot a un grupo de coherencia para crear, conservar y etiquetar automáticamente copias Snapshot del grupo de coherencia.

Pasos

1. En System Manager, seleccione **Protección > Políticas**; a continuación, seleccione **Políticas de**

instantánea.

2. Pase el ratón sobre el nombre de la política de Snapshot que desea aplicar.
3. Seleccione ⋮; y, a continuación, seleccione **Aplicar**.
4. Seleccione los grupos de coherencia a los que desea aplicar la política Snapshot y, a continuación, seleccione **Aplicar**.

El futuro

Ahora que los datos están protegidos con copias snapshot, debe "configure una relación de replicación"copiar sus grupos de coherencia en una ubicación geográficamente remota a efectos de backup y recuperación ante desastres.

Editar, eliminar o deshabilitar una política de Snapshot

Edite una política de Snapshot para modificar el nombre de la política, la cantidad máxima de Snapshot o la etiqueta de SnapMirror. Elimine una política para eliminarla y sus datos de backup asociados del clúster. Deshabilite una política para detener temporalmente la creación o transferencia de snapshots especificada por la política.

Pasos

1. En System Manager, seleccione **Protección > Políticas**; a continuación, seleccione **Políticas de instantánea**.
2. Pase el ratón sobre el nombre de la política de Snapshot que quiera editar.
3. ⋮Seleccione ; y, a continuación, seleccione **Editar**, **Eliminar** o **Desactivar**.

Resultado

Ha modificado, eliminado o deshabilitado la política de snapshots.

Editar una política de replicación

Edite una política de replicación para modificar la descripción de la política, la programación de transferencia y las reglas. También puede editar la política para habilitar o deshabilitar la compresión de red.

Pasos

1. En System Manager, seleccione **Protección > Políticas**.
2. Seleccione **Políticas de replicación**.
3. Coloque el cursor sobre la política de replicación que desea editar y, a continuación, ⋮seleccione .
4. Seleccione **Editar**.
5. Actualice la política y, a continuación, seleccione **Guardar**.

Resultado

Modificó la política de replicación.

Proteja sus datos

Cifrado de datos estáticos en sistemas de almacenamiento R2 de ASA

Al cifrar datos en reposo, no se podrán leer si un medio de almacenamiento se reasigna, devuelve, se pierde o es robado. Puede usar System Manager de ONTAP para cifrar sus

datos a nivel de hardware y software para lograr una protección de doble capa.

El cifrado en almacenamiento de NetApp (NSE) admite el cifrado de hardware mediante unidades de cifrado automático (SED). SEDS cifra los datos a medida que se escriben. Cada SED contiene una clave de cifrado única. Los datos cifrados almacenados en el SED no se pueden leer sin la clave de cifrado del SED. Los nodos que intentan leer desde un SED se deben autenticar para acceder a la clave de cifrado del SED. Los nodos se autentican obteniendo una clave de autenticación de un administrador de claves y, a continuación, presentando la clave de autenticación al SED. Si la clave de autenticación es válida, el SED le dará al nodo su clave de cifrado para acceder a los datos que contiene.

Use el administrador de claves incorporado o un gestor de claves externo de ASA R2 para servir claves de autenticación a los nodos.

Además de NSE, también puede habilitar el cifrado del software para añadir otra capa de seguridad a sus datos.

Pasos

1. En el Administrador del sistema, selecciona **Clúster > Configuración**.
2. En la sección **Seguridad**, en **Cifrado**, selecciona **Configurar**.
3. Configure el gestor de claves.

Opción	Pasos
Configure el gestor de claves incorporado	a. Seleccione **Onboard Key Manager** para agregar los servidores de claves. b. Introduzca una frase de contraseña.
Configure un gestor de claves externo	a. Seleccione **Administrador de claves externo** para agregar los servidores de claves. b. + Add Seleccione para agregar los servidores de claves. c. Añada los certificados de CA del servidor KMIP. d. Añada los certificados de cliente KMIP.

4. Seleccione **Cifrado de doble capa** para habilitar el cifrado de software.
5. Seleccione **Guardar**.

El futuro

Ahora que ha cifrado sus datos en reposo, si utiliza el protocolo NVMe/TCP, puede hacerlo "cifrar todos los datos enviados a través de la red" entre su host NVMe/TCP y su sistema ASA R2.

Protéjase contra ataques de ransomware en sistemas de almacenamiento ASA R2

Para obtener una mejor protección contra ataques de ransomware, replica snapshots en un clúster remoto y, a continuación, bloquea las snapshots de destino para que estén a prueba de manipulaciones. Las instantáneas bloqueadas no se pueden eliminar accidentalmente ni de forma malintencionada. Puede utilizar snapshots bloqueados para recuperar datos si una unidad de almacenamiento se ve afectada por un ataque de

ransomware.

Inicialice el reloj de SnapLock Compliance

Para poder crear copias Snapshot a prueba de manipulaciones, debe inicializar el reloj de SnapLock Compliance en los clústeres locales y de destino.

Pasos

1. Seleccione **Cluster > Overview**.
2. En la sección **Nodos**, selecciona **Inicializar reloj SnapLock Compliance**.
3. Selecciona **Inicializar**.
4. Compruebe que se ha inicializado el reloj de conformidad.
   a. Seleccione **Cluster > Overview**.
   b. En la sección **Nodos**, seleccione ; y luego seleccione **Reloj SnapLock Compliance**.

¿Cuál es el siguiente?

Después de inicializar el reloj de SnapLock Compliance en los clústeres locales y de destino, está listo para "crear una relación de replicación con snapshots bloqueadas".

Proteja las conexiones NVMe en sus sistemas de almacenamiento ASA R2

Si utiliza el protocolo NVMe, puede configurar la autenticación en banda para mejorar la seguridad de sus datos. La autenticación en banda permite una autenticación bidireccional y unidireccional segura entre sus hosts NVMe y su sistema ASA R2. La autenticación en banda está disponible para todos los hosts NVMe. Si utiliza el protocolo NVMe/TCP, puede mejorar aún más la seguridad de datos configurando la seguridad de la capa de transporte (TLS) para cifrar todos los datos enviados a través de la red entre los hosts NVMe/TCP y el sistema ASA R2.

Pasos

1. Seleccione **HOSTS**; luego seleccione **NVMe**.
2. Seleccione + Add .
3. Introduzca el nombre de host y, a continuación, seleccione el sistema operativo del host.
4. Introduzca la descripción de un host y, a continuación, seleccione la máquina virtual de almacenamiento para conectarse al host.
5. Seleccione junto al nombre de host.
6. Seleccione **Autenticación en banda**.
7. Si está utilizando el protocolo NVMe/TCP, seleccione **Requerir seguridad de la capa de transporte (TLS)**.
8. Seleccione **Agregar**.

Resultado

La seguridad de sus datos se mejora con la autenticación en banda y/o TLS.

Administración y supervisión

Gestione el acceso de clientes a las máquinas virtuales de almacenamiento en los sistemas de almacenamiento R2 de ASA

Las unidades de almacenamiento de un sistema ASA R2 se encuentran dentro de las máquinas virtuales de almacenamiento (VM). Los equipos virtuales de almacenamiento se utilizan para suministrar datos a sus clientes SAN. Use System Manager de ONTAP para crear una LIF (interfaz de red) para los clientes de SAN con el fin de conectarse a una máquina virtual de almacenamiento y acceder a los datos de las unidades de almacenamiento. Opcionalmente, puede utilizar subredes para simplificar la creación de LIF y los espacios IP para proporcionar a las máquinas virtuales de almacenamiento su propio almacenamiento, administración y enrutamiento seguros.

Cree espacios IP

Un espacio IP es un espacio de direcciones IP distinto en el que residen las máquinas virtuales de almacenamiento. Cuando se crean espacios IP, se permite que las máquinas virtuales de almacenamiento tengan su propio almacenamiento, administración y enrutamiento seguros. También puede habilitar a los clientes en dominios de red independientes de forma administrativa para que utilicen direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

Debe crear un espacio IP para poder crear una subred.

Pasos

1. Selecciona **Red > Descripción general**.
2. En **IPspaces**, seleccione + Add .
3. Introduzca un nombre para el espacio IP o acepte el nombre predeterminado.

   Un nombre de espacio IP no puede ser “all” porque “all” es un nombre reservado por el sistema.

4. Seleccione **Guardar**.

El futuro

Ahora que ha creado un espacio IP, puede utilizarlo para crear una subred.

Crear subredes

Una subred le permite asignar bloques específicos de direcciones IPv4 o IPv6 que deben usarse al crear una LIF (interfaz de red) . Una subred simplifica la creación de LIF al permitirle especificar el nombre de subred en lugar de una dirección IP y una máscara de red específicas para cada LIF.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El "dominio de retransmisión"espacio IP y en el que desea agregar la subred debe existir.

Pasos

1. Selecciona **Red > Descripción general**.
2. Seleccione **subredes**; luego seleccione + Add.
3. Introduzca el nombre de la subred.

   Todos los nombres de subred deben ser únicos en un espacio IP.

4. Introduzca la dirección IP de subred y la máscara de subred.
5. Especifique el rango de direcciones IP para la subred.

   Cuando especifique el rango de direcciones IP para la subred, no superponga las direcciones IP con otras subredes. Se pueden producir problemas de red cuando las direcciones IP de subred se superponen y diferentes subredes o hosts intentan utilizar la misma dirección IP.

6. Seleccione el dominio de retransmisión de la subred.
7. Seleccione **Agregar**.

El futuro

Ha creado una subred que ahora puede usar para simplificar la creación de sus LIF.

Crear una LIF (interfaz de red)

Una LIF (interfaz de red) es una dirección IP asociada a un puerto físico o lógico. Cree LIF en los puertos que desee utilizar para acceder a los datos. Los equipos virtuales de almacenamiento sirven datos a los clientes a través de una o más LIF. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, de modo que la comunicación de la red no se interrumpa.

Cuando se crea una LIF de datos de IP, puede atender tanto el tráfico iSCSI como NVMe/TCP de forma predeterminada. Es necesario crear LIF de datos independientes para el tráfico FC y NVMe/FC.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El puerto de red físico o lógico subyacente debe haberse configurado en el `up` estado administrativo.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.
- Una LIF que gestiona tráfico dentro del clúster entre nodos no debe estar en la misma subred que una LIF que gestiona el tráfico de gestión o una LIF que gestiona el tráfico de datos.

Pasos

1. Selecciona **Red > Descripción general**.
2. Seleccione **Interfaces de red**; luego seleccione + Add.
3. Seleccione el tipo de interfaz y el protocolo y, a continuación, seleccione la máquina virtual de almacenamiento.
4. Escriba un nombre para la LIF o acepte el nombre predeterminado.
5. Seleccione el nodo de inicio de la interfaz de red y, a continuación, introduzca la dirección IP y la máscara de subred.
6. Seleccione **Guardar**.

Resultado

Ha creado una LIF para el acceso a los datos.

Modificar una LIF (interfaces de red)

Las LIF se pueden deshabilitar o cambiar su nombre según sea necesario. También puede cambiar la dirección IP de LIF y la máscara de subred.

Pasos

1. Seleccione **Red > Descripción general** y, a continuación, seleccione **Interfaces de red**.
2. Coloque el cursor sobre la interfaz de red que desea editar y, a continuación, seleccione .
3. Seleccione **Editar**.
4. Puede deshabilitar la interfaz de red, cambiar el nombre de la interfaz de red, cambiar la dirección IP o cambiar la máscara de subred.
5. Seleccione **Guardar**.

Resultado

Se ha modificado su LIF.

Gestione las redes de clúster en sistemas de almacenamiento R2 de ASA

Es posible usar System Manager de ONTAP para realizar administración básica de red de almacenamiento en el sistema ASA R2. Por ejemplo, puede agregar un dominio de retransmisión o reasignar puertos a un dominio de retransmisión diferente.

Añada un dominio de retransmisión

Utilice dominios de retransmisión para simplificar la gestión de la red de clúster agrupando los puertos de red que pertenecen a la misma red de capa 2. Las máquinas virtuales de almacenamiento (VM) pueden usar los puertos del grupo para el tráfico de datos o de gestión.

El dominio de retransmisión “default” y el dominio de retransmisión “Cluster” se crean durante la configuración del clúster. El dominio de difusión “predeterminado” contiene puertos que están en el espacio IP “predeterminado”. Estos puertos se utilizan principalmente para servir datos. Los puertos de gestión de clústeres y gestión de nodos también están en este dominio de retransmisión. El dominio de difusión “Cluster” contiene puertos que están en el espacio IP “Cluster”. Estos puertos se utilizan para la comunicación del clúster e incluyen todos los puertos de clúster de todos los nodos del clúster.

Puede crear dominios de retransmisión adicionales después de inicializar el clúster. Cuando se crea un dominio de retransmisión, se crea automáticamente un grupo de conmutación por error que contiene los mismos puertos.

Acerca de esta tarea

La unidad de transmisión máxima (MTU) de los puertos agregados a un dominio de retransmisión se actualiza al valor MTU establecido en el dominio de retransmisión.

Pasos

1. En System Manager, seleccione **Red > Descripción general**.
2. En Dominios **Broadcast**, seleccione + Add.

3. Escriba un nombre para el dominio de retransmisión o acepte el nombre predeterminado.

   Todos los nombres de dominio de retransmisión deben ser únicos en un espacio IP.

4. Seleccione el espacio IP del dominio de retransmisión.

   Si no especifica un nombre de espacio IP, el dominio de difusión se crea en el espacio IP "predeterminado".

5. Introduzca la unidad de transmisión máxima (MTU).

   MTU es el paquete de datos más grande que se puede aceptar en su dominio de retransmisión.

6. Seleccione los puertos deseados y luego seleccione **Guardar**.

Resultado

Ha añadido un nuevo dominio de retransmisión.

Reasigne los puertos a un dominio de retransmisión diferente

Los puertos solo pueden pertenecer a un dominio de retransmisión. Si desea cambiar el dominio de retransmisión al que pertenece un puerto, deberá reasignar el puerto del dominio de retransmisión existente a un nuevo dominio de retransmisión.

Pasos

1. En System Manager, seleccione **Red > Descripción general**.
2. En **Dominios de difusión**, seleccione ⋮ junto al nombre de dominio; luego seleccione **Editar**.
3. Anule la selección de los puertos Ethernet que desea reasignar a otro dominio.
4. Seleccione el dominio de difusión al que desea reasignar el puerto y, a continuación, seleccione **Reasignar**.
5. Seleccione **Guardar**.

Resultado

Ha reasignado los puertos a un dominio de retransmisión diferente.

Cree una VLAN

Una VLAN consta de puertos de switch agrupados en un dominio de retransmisión. Las VLAN le permiten aumentar la seguridad, aislar problemas y limitar las rutas disponibles dentro de su infraestructura de red IP.

Antes de empezar

Los switches implementados en la red deben cumplir los estándares IEEE 802.1Q o tener una implementación de VLAN específica por proveedor.

Acerca de esta tarea

- No se puede crear una VLAN en un puerto de grupo de interfaces que no contenga puertos miembro.
- Cuando se configura una VLAN por primera vez en un puerto, el puerto podría estar inactivo, lo que podría dar lugar a una desconexión temporal de la red. Las adiciones posteriores de VLAN al mismo puerto no afectan al estado del puerto.
- No debe crear una VLAN en una interfaz de red con el mismo identificador que la VLAN nativa del switch. Por ejemplo, si la interfaz de red e0b se encuentra en una VLAN 10 nativa, no se debe crear una VLAN

e0b-10 en esa interfaz.

Pasos

1. En el Administrador del sistema, seleccione **Red > Puertos Ethernet** y, a continuación, seleccione + VLAN.
2. Seleccione el nodo y el dominio de retransmisión para la VLAN.
3. Seleccione el puerto para la VLAN.

   La VLAN no se puede conectar a un puerto que aloje una LIF de clúster ni a los puertos asignados al espacio IP del clúster.

4. Introduzca un ID de VLAN.
5. Seleccione **Guardar**.

Resultado

Creó una VLAN para aumentar la seguridad, aislar problemas y limitar las rutas disponibles dentro de la infraestructura de red IP.

Supervise el uso y aumente la capacidad

Supervise el rendimiento de los clústeres y de la unidad de almacenamiento en los sistemas de almacenamiento R2 de ASA

Utilice System Manager de ONTAP para supervisar el rendimiento general de su clúster y el rendimiento de unidades de almacenamiento específicas para determinar cómo la latencia, las IOPS y el rendimiento afectan a sus aplicaciones vitales para el negocio. El rendimiento se puede supervisar en varios períodos de tiempo que van de una hora a un año.

Por ejemplo, supongamos que una aplicación crítica está experimentando alta latencia y bajo rendimiento. Cuando se observa el rendimiento del clúster de los últimos cinco días laborables, se observa una disminución del rendimiento a la misma hora cada día. Se utiliza esta información para determinar que la aplicación crucial está compitiendo por los recursos del clúster cuando un proceso no crítico comienza a ejecutarse en segundo plano. A continuación, puede modificar la política de calidad de servicio para limitar el impacto de la carga de trabajo no crítica en los recursos del sistema y garantizar que la carga de trabajo crítica cumpla con los objetivos de rendimiento mínimos.

Supervise el rendimiento del clúster

Use las métricas de rendimiento del clúster para determinar si necesita cambiar cargas de trabajo para minimizar la latencia y maximizar las IOPS y el rendimiento para sus aplicaciones críticas.

Pasos

1. En System Manager, seleccione **Panel**.
2. En **Rendimiento**, vea la latencia, IOPS y rendimiento del clúster por hora, día, semana, mes o año.
3. Seleccione para descargar los datos de rendimiento.

El futuro

Use las métricas de rendimiento del clúster para analizar si necesita modificar las políticas de calidad de

servicio o realizar otros ajustes en las cargas de trabajo de la aplicación para maximizar el rendimiento general del clúster.

Supervise el rendimiento de la unidad de almacenamiento

Utilice métricas de rendimiento de unidad de almacenamiento para determinar el impacto de aplicaciones específicas en la latencia, las operaciones de IOPS y el rendimiento.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Seleccione la unidad de almacenamiento que desea supervisar; luego seleccione **Descripción general**.
3. En **Rendimiento**, vea la latencia, IOPS y rendimiento de la unidad de almacenamiento por hora, día, semana, mes o año.
4. Seleccione para descargar los datos de rendimiento.

El futuro

Utilice las métricas de rendimiento de su unidad de almacenamiento para analizar si necesita modificar las políticas de calidad de servicio asignadas a sus unidades de almacenamiento para reducir la latencia y maximizar las IOPS y el rendimiento.

Supervise el uso del clúster y de la unidad de almacenamiento en los sistemas de almacenamiento R2 de ASA

Utilice System Manager de ONTAP para supervisar la utilización del almacenamiento y garantizar que dispone de la capacidad de almacenamiento necesaria para satisfacer las cargas de trabajo actuales y futuras.

Supervise el uso del clúster

Supervise regularmente la cantidad de almacenamiento que consume el clúster para garantizar que, si es necesario, esté preparado para expandir la capacidad del clúster antes de quedarse sin espacio.

Pasos

1. En System Manager, seleccione **Panel**.
2. En **Capacidad**, vea la cantidad de espacio físico utilizado y la cantidad de espacio disponible en su clúster.

   La proporción de reducción de datos representa la cantidad de espacio ahorrado gracias a la eficiencia del almacenamiento.

El futuro

Si su clúster se está quedando sin espacio o si no tiene capacidad para satisfacer una demanda futura, debe planificar la "añadir unidades nuevas" puesta en marcha de su sistema ASA R2 para aumentar la capacidad de almacenamiento.

Supervisar el uso de la unidad de almacenamiento

Supervisar la cantidad de almacenamiento consumido por una unidad de almacenamiento para aumentar de forma proactiva el tamaño de la unidad de almacenamiento en función de las necesidades de su negocio.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Seleccione la unidad de almacenamiento que desea supervisar; luego seleccione **Descripción general**.
3. En **Almacenamiento**, vea lo siguiente:
   - Tamaño de la unidad de almacenamiento
   - Cantidad de espacio utilizado
   - De reducción de datos

     La relación de reducción de datos representa la cantidad de espacio ahorrado gracias a la eficiencia del almacenamiento
   - Instantánea utilizada

     Snapshot utilizada representa la cantidad de almacenamiento que usan las instantáneas.

El futuro

Si la unidad de almacenamiento se está acercando a su capacidad, debe "modifique la unidad de almacenamiento"aumentar su tamaño.

Aumente la capacidad de almacenamiento en los sistemas de almacenamiento R2 de ASA

Añada unidades a un nodo o bandeja para aumentar la capacidad de almacenamiento del sistema ASA R2.

Utilice NetApp Hardware Universe para preparar la instalación de una unidad nueva

Antes de instalar una unidad nueva en un nodo o bandeja, utilice NetApp Hardware Universe para confirmar que la unidad que desea añadir es compatible con la plataforma ASA R2 y para identificar la ranura correcta para la unidad nueva. Las ranuras correctas para añadir unidades varían según el modelo de plataforma y la versión de ONTAP. En algunos casos, es necesario añadir unidades a ranuras específicas en secuencia.

Pasos

1. Vaya a la "NetApp Hardware Universe".
2. En **Productos**, selecciona tus configuraciones de hardware.
3. Seleccione su plataforma ASA R2.
4. Seleccione su versión de ONTAP; luego seleccione **Mostrar resultados**.
5. Debajo del gráfico, selecciona **Haga clic aquí para ver vistas alternativas**; luego elige la vista que coincida con tu configuración.
6. Utilice la vista de su configuración para confirmar que la unidad nueva es compatible y la ranura correcta para la instalación.

Resultado

Ha confirmado que la unidad nueva es compatible y conoce la ranura adecuada para la instalación.

Instale una nueva unidad en el ASA R2

La cantidad mínima de unidades que debe añadir en un solo procedimiento es de seis. Al añadir una sola

unidad, se puede reducir el rendimiento.

Acerca de esta tarea

Debe repetir los pasos de este procedimiento con cada unidad.

Pasos

1. Puesta a tierra apropiadamente usted mismo.
2. Retire con cuidado el bisel de la parte delantera de la plataforma.
3. Inserte la nueva unidad en la ranura correcta.
   a. Con la palanca de leva en posición abierta, utilice ambas manos para insertar la nueva transmisión.
   b. Presione hasta que la unidad se detenga.
   c. Cierre el asa de leva de forma que la unidad esté completamente asentada en el plano medio y el asa encaje en su lugar.

      Asegúrese de cerrar el mango de leva lentamente para que quede alineado correctamente con la cara de la transmisión.

4. Verifique que el LED de actividad de la unidad (verde) esté iluminado.
   - SI el LED está fijo, la unidad tiene alimentación.
   - Si el LED parpadea, la unidad se enciende y las operaciones de I/O están en curso. El LED también parpadeará si se está actualizando el firmware de la unidad.

     El firmware de la unidad se actualiza automáticamente (sin interrupciones) en las unidades nuevas que no tienen versiones de firmware actuales.

5. Si el nodo está configurado para la asignación automática de unidades, puede esperar a que ONTAP asigne automáticamente las nuevas unidades a un nodo. Si el nodo no está configurado para la asignación automática de unidades o si se prefiere, es posible asignar las unidades manualmente.

   Las unidades nuevas no se reconocen hasta que se asignan a un nodo.

¿Cuál es el siguiente?

Una vez que se reconozcan las unidades nuevas, verifique que se hayan añadido y se haya especificado correctamente su propiedad.

Actualice el firmware en los sistemas de almacenamiento R2 de ASA

ONTAP descarga y actualiza automáticamente los archivos de firmware y sistema en el sistema ASA R2 de forma predeterminada. Si desea obtener flexibilidad para visualizar las actualizaciones recomendadas antes de descargar e instalar, puede usar ONTAP System Manager para deshabilitar las actualizaciones automatizadas o para editar los parámetros de actualización para mostrar las notificaciones de las actualizaciones disponibles antes de realizar cualquier acción.

Active las actualizaciones automáticas

Las actualizaciones recomendadas para el firmware de almacenamiento, el firmware de SP/BMC y los archivos del sistema se descargan e instalan automáticamente en el sistema ASA R2 de forma predeterminada. Si se han desactivado las actualizaciones automáticas, puede habilitarlas para restablecer el comportamiento predeterminado.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** seleccione ⋮ y luego seleccione **Activar**.
3. Lea y acepte el contrato de licencia para usuario final.
4. Acepte las opciones predeterminadas para actualizar automáticamente los archivos del firmware y del sistema. Opcionalmente, seleccione para mostrar notificaciones o para descartar automáticamente las actualizaciones recomendadas.
5. Seleccione esta opción para confirmar que las modificaciones de la actualización se aplicarán a todas las actualizaciones actuales y futuras.
6. Seleccione **Guardar**.

Resultado

Las actualizaciones recomendadas se descargan e instalan automáticamente en su sistema ASA R2 según sus selecciones de actualización.

Desactive las actualizaciones automáticas

Desactive las actualizaciones automáticas si desea tener la flexibilidad de ver las actualizaciones recomendadas antes de instalarlas. Si deshabilita las actualizaciones automáticas, tendrá que realizar las actualizaciones de firmware y los archivos del sistema manualmente.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** seleccione ⋮ y luego seleccione **Desactivar**.

Resultado

Las actualizaciones automáticas están desactivadas. Debe comprobar regularmente si hay actualizaciones recomendadas y decidir si desea realizar una instalación manual.

Ver actualizaciones automáticas

Vea una lista de las actualizaciones de archivos del sistema y firmware que se han descargado en el clúster y están programadas para la instalación automática. Vea también las actualizaciones que se han instalado previamente automáticamente.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** selecciona ⋮ y luego selecciona **Ver todas las actualizaciones automáticas**.

Editar actualizaciones automáticas

Puede seleccionar que las actualizaciones recomendadas del firmware de almacenamiento, el firmware de SP/BMC y los archivos del sistema se descarguen e instalen automáticamente en el clúster, o bien puede seleccionar que se descarten automáticamente las actualizaciones recomendadas. Si desea controlar manualmente la instalación o el despido de las actualizaciones, seleccione para recibir una notificación cuando haya disponible una actualización recomendada; a continuación, puede seleccionar manualmente para instalarla o descartarla.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Actualización automática** selecciona ⋮ y luego selecciona **Editar actualizaciones automáticas**.
3. Actualice las selecciones para actualizaciones automáticas.
4. Seleccione **Guardar**.

Resultado

Las actualizaciones automáticas se modifican en función de las selecciones.

Actualice el firmware manualmente

Si desea la flexibilidad de ver las actualizaciones recomendadas antes de que se descarguen e instalen, puede deshabilitar las actualizaciones automatizadas y actualizar el firmware manualmente.

Pasos

1. Descargue el archivo de actualización de firmware en un servidor o cliente local.
2. En System Manager, seleccione **Clúster > Descripción general** y, a continuación, seleccione **Actualizar**.
3. Seleccione **Actualización de firmware**; seleccione + Update firmware.

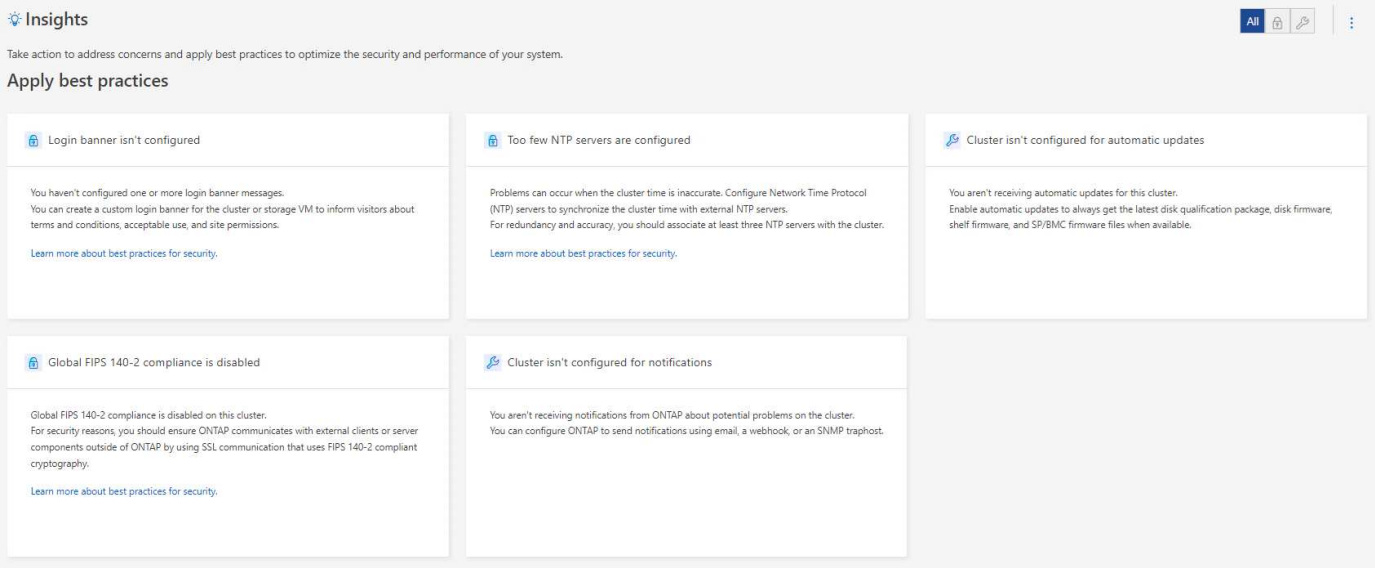
Resultado

El firmware se ha actualizado.

Optimice la seguridad y el rendimiento del clúster con las estadísticas del sistema de almacenamiento R2 de ASA

Vea *Insights* en ONTAP System Manager para identificar las prácticas recomendadas y las modificaciones de configuración que puede implementar en su sistema ASA R2 para optimizar la seguridad y el rendimiento de los clústeres.

Por ejemplo, suponga que tiene servidores de protocolo de tiempo de redes (NTP) configurados para el clúster. Sin embargo, no sabe que tiene menos de la cantidad recomendada de servidores NTP necesarios para gestionar el tiempo del clúster de forma óptima. Para ayudarle a evitar los problemas que pueden producirse cuando la hora del clúster no es precisa, Insights le notificará que tiene demasiados pocos servidores NTP configurados y le dará opciones para obtener más información acerca de este problema, solucionarlo o ignorarlo.



Pasos

1. En System Manager, selecciona **Insights**.
2. Revise las recomendaciones.

El futuro

Realice las acciones necesarias para implementar las prácticas recomendadas y optimizar la seguridad y el rendimiento del clúster.

Vea los eventos y las tareas del clúster en los sistemas de almacenamiento R2 de ASA

Utilice System Manager de ONTAP para ver una lista de errores o alertas que se han producido en el sistema junto con las acciones correctivas recomendadas. También es posible ver los registros de auditoría del sistema y una lista de los trabajos activos, completados o con errores.

Pasos

1. En System Manager, seleccione **Eventos y trabajos**.
2. Ver los eventos y los trabajos del clúster.

Para ver esto…	Realice lo siguiente…
Eventos del clúster	Selecciona **Eventos**; luego selecciona **Registro de eventos**.
Sugerencias de Active IQ	Selecciona **Eventos**; luego selecciona **Sugerencias de Active IQ**.
Alertas del sistema	a. Selecciona **Alertas del sistema**. b. Seleccione la alerta del sistema cuya acción desea realizar. c. Confirme o suprima la alerta.

Para ver esto…	Realice lo siguiente…
Trabajos del clúster	Seleccione **Jobs**.
Registros de auditoría	Seleccione **Registros de auditoría**.

Envíe notificaciones por correo electrónico de eventos del clúster y registros de auditoría

Configure su sistema para enviar una notificación a direcciones de correo electrónico específicas cuando haya un evento del clúster o una entrada del registro de auditoría.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Gestión de notificaciones** selecciona ⋮.
3. Para configurar un destino de evento, selecciona **Ver destinos de evento**; luego selecciona **Destinos de evento**. Para configurar un destino de registro de auditoría, seleccione **Ver destinos de auditoría** y, a continuación, seleccione **Destinos de registro de auditoría**.
4. Seleccione + Add.
5. Ingrese la información de destino y luego seleccione **Agregar**.

Resultado

La dirección de correo electrónico que añadió ahora recibirá las notificaciones por correo electrónico especificadas para los eventos del clúster y los registros de auditoría.

Gestione los nodos

Reinicie un nodo en un sistema de almacenamiento ASA R2

Es posible que necesite reiniciar un nodo para mantenimiento, solucionar problemas, actualizaciones de software u otros motivos administrativos. Cuando un nodo se reinicia, su compañero de alta disponibilidad ejecuta automáticamente una toma de control. A continuación, el nodo del partner realiza una devolución al control automática cuando el nodo reiniciado vuelve a conectarse.

Pasos

1. En System Manager, seleccione **Clúster > Descripción general**.
2. Seleccione ⋮ junto al nodo que desea reiniciar y, a continuación, seleccione **Reiniciar**.
3. Introduzca el motivo por el que está reiniciando el nodo; a continuación, seleccione **Reiniciar**.

   El motivo por el que se introduce el reinicio se registra en el registro de auditoría del sistema.

El futuro

Mientras el nodo se está reiniciando, su compañero de alta disponibilidad realiza una toma de control para que no haya interrupción en el servicio de datos. Cuando el reinicio se completa, el partner de alta disponibilidad realiza un retorno al nodo primario.

Cambie el nombre de un nodo en un sistema de almacenamiento ASA R2

Puede usar ONTAP System Manager para cambiar el nombre de un nodo en el sistema ASA R2. Es posible que deba cambiar el nombre de un nodo para alinearlo con las convenciones de nomenclatura de la organización o por otros motivos administrativos.

Pasos

1. En System Manager, seleccione **Clúster > Descripción general**.
2. Seleccione ⋮ junto al nodo al que desea cambiar el nombre y, a continuación, seleccione **Cambiar nombre**.
3. Introduzca el nuevo nombre para el nodo y, a continuación, seleccione **Renombrar**.

Resultado

Se aplica el nuevo nombre al nodo.

Gestione cuentas de usuario y roles en sistemas de almacenamiento R2 de ASA

Use System Manager para configurar el acceso a la controladora de dominio de Active Directory, la autenticación LDAP y SAML para sus cuentas de usuario. Cree roles de cuenta de usuario para definir funciones específicas que los usuarios asignados a los roles pueden realizar en el clúster.

Configure el acceso del controlador de dominio de Active Directory

Configurar el acceso de la controladora de dominio de Active Directory (AD) al clúster o a la máquina virtual de almacenamiento para poder habilitar el acceso de la cuenta de AD.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, en **Active Directory**, selecciona **Configurar**.

El futuro

Ahora puede habilitar el acceso a la cuenta de AD en su sistema ASA R2.

Configurar LDAP

Configure un servidor de protocolo ligero de acceso a directorios (LDAP) para mantener de forma centralizada la información de usuario para la autenticación.

Antes de empezar

Debe haber generado una solicitud de firma de certificación y añadido un certificado digital de servidor firmado por CA.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, junto a **LDAP**, selecciona ⚙.

3. Introduzca el servidor LDAP necesario y la información de enlace; a continuación, seleccione **Guardar**.

El futuro

Ahora puede usar LDAP para información y autenticación de usuario.

Configurar la autenticación SAML

La autenticación del lenguaje de marcado de aserción de seguridad (SAML) permite a los usuarios autenticarse mediante un proveedor de identidad (IdP) seguro en lugar de los proveedores de servicios directos, como Active Directory y LDAP.

Antes de empezar

- Se debe configurar el IDP que se planea usar para la autenticación remota.

  Consulte la documentación de IdP para la configuración.

- Debe tener el URI del IDP.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Autenticación SAML**, selecciona .
3. Seleccione **Habilitar autenticación SAML**.
4. Introduzca la URL del IdP y la dirección IP del sistema host; a continuación, seleccione **Guardar**.

   Una ventana de confirmación muestra la información de metadatos, que se ha copiado automáticamente en el portapapeles.

5. Vaya al sistema IdP que especificó y, a continuación, copie los metadatos desde el portapapeles para actualizar los metadatos del sistema.
6. Vuelva a la ventana de confirmación en System Manager; luego seleccione **He configurado el IdP con el URI del host o metadatos**.
7. Seleccione **Logout** para habilitar la autenticación basada en SAML.

   El sistema IDP mostrará una pantalla de autenticación.

El futuro

Ahora puede usar la autenticación SAML para las cuentas de usuario.

Crear roles de cuenta de usuario

Los roles para los administradores del clúster y los administradores de máquinas virtuales de almacenamiento se crean automáticamente cuando se inicializa el clúster. Cree roles de cuenta de usuario adicionales para definir funciones específicas que los usuarios asignados a los roles pueden realizar en el clúster.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, junto a **Usuarios y roles**, selecciona .
3. En **Roles**, seleccione + Add .
4. Seleccione los atributos de rol.

Para agregar varios atributos, seleccione + Add .

5. Seleccione **Guardar**.

Resultado

Se creará una nueva cuenta de usuario que estará disponible para usar en su sistema ASA R2.

Cree una cuenta de administrador

Cree una cuenta de usuario de administrador para permitir al usuario de la cuenta realizar acciones específicas en el clúster en función del rol asignado a la cuenta. Para mejorar la seguridad de las cuentas, configure la autenticación multifactor (MFA) al crear la cuenta.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Seguridad**, junto a **Usuarios y roles**, selecciona →.
3. En **Usuarios**, seleccione + Add .
4. Introduzca un nombre de usuario y, a continuación, seleccione un rol para asignarlo al usuario.
5. Seleccione el método de inicio de sesión de usuario y el método de autenticación.
6. Para habilitar MFA, seleccione + Add ; y, a continuación, seleccione un método de inicio de sesión secundario y un método de autenticación
7. Introduzca una contraseña para el usuario.
8. Seleccione **Guardar**.

Resultado

Se creará una nueva cuenta de administrador y estará disponible para usar en el clúster de ASA R2.

Gestione certificados de seguridad en sistemas de almacenamiento R2 de ASA

Utilice certificados de seguridad digital para verificar la identidad de los servidores remotos.

El protocolo de estado de certificados en línea (OCSP) valida el estado de las solicitudes de certificados digitales de los servicios de ONTAP mediante conexiones SSL y de seguridad de la capa de transporte (TLS).

Genere una solicitud de firma de certificación

Genere una solicitud de firma de certificación (CSR) para crear una clave privada que se pueda utilizar para generar un certificado público.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, selecciona →; y luego selecciona + Generate CSR.
3. Introduzca el nombre común del asunto y, a continuación, seleccione el país.
4. Si desea cambiar los valores predeterminados de GSR, seleccionar el uso de clave ampliada o agregar nombres alternativos de asunto, seleccione ↙↗ More options; y, a continuación, realice las

actualizaciones deseadas.

5. Seleccione **generar**.

Resultado

Ha generado una CSR en la que se puede utilizar para generar un certificado público.

Agregue una autoridad de certificación de confianza

ONTAP proporciona un conjunto predeterminado de certificados raíz de confianza para aplicaciones que utilizan Seguridad de la capa de transporte (TLS). Puede agregar autoridades de certificación de confianza adicionales según sea necesario.

Pasos

1. Seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, selecciona →.
3. Seleccione **Autoridades de certificación de confianza**.
4. Introduzca o importe los detalles del certificado y, a continuación, seleccione + Add.

Resultado

Añadió una nueva entidad de certificación de confianza al sistema ASA R2.

Renueve o elimine una entidad de certificación de confianza

Las autoridades certificadoras de confianza deben renovarse anualmente. Si no desea renovar un certificado caducado, debe eliminarlo.

Pasos

1. Seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, selecciona →.
3. Seleccione **Autoridades de certificación de confianza**.
4. Seleccione la autoridad de certificación de confianza que desea renovar o eliminar.
5. Renueve o elimine la entidad de certificación.

Para renovar la autoridad de certificación, haga lo siguiente…	Para eliminar la autoridad del certificado, haga lo siguiente…
a. ⋮ Seleccione ; y, a continuación, seleccione **Renovar**. b. Ingrese o importe la información del certificado; luego seleccione **Renovar**.	a. ⋮ Seleccione ; y, a continuación, seleccione **Eliminar**. b. Confirme que desea eliminar y, a continuación, seleccione * Eliminar *.

Resultado

Renovó o eliminó una entidad de certificación de confianza existente en el sistema ASA R2.

Agregue un certificado de cliente/servidor o autoridades de certificación locales

Agregue un certificado de cliente/servidor o autoridades de certificación locales para habilitar servicios web

seguros.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a **Certificados**, selecciona →.
3. Seleccione **Certificados de cliente/servidor** o **Autoridades de certificación locales**.
4. Agregue la información del certificado y, a continuación, seleccione + Add.

Resultado

Ha agregado un nuevo certificado de cliente/servidor o autoridades locales al sistema ASA R2.

Renovar o eliminar un certificado de cliente/servidor o autoridades de certificación locales

Los certificados de cliente/servidor y las autoridades de certificación locales deben renovarse anualmente. Si no desea renovar un certificado caducado o autoridades de certificación locales, debe eliminarlos.

Pasos

1. Seleccione **Cluster > Settings**.
2. En **Seguridad**, junto a Certificados, seleccione →.
3. Seleccione **Certificados de cliente/servidor** o **Autoridades de certificación locales**.
4. Seleccione el certificado que desea renovar o eliminar.
5. Renueve o elimine la entidad de certificación.

Para renovar la autoridad de certificación, haga lo siguiente…	Para eliminar la autoridad del certificado, haga lo siguiente…
a. ⋮ Seleccione ; y, a continuación, seleccione **Renovar**. b. Ingrese o importe la información del certificado; luego seleccione **Renovar**.	⋮ Seleccione ; y, a continuación, seleccione **Eliminar**.

Resultado

Ha renovado o eliminado un certificado de cliente/servidor o una autoridad de certificación local existente en el sistema ASA R2.

Verifique la conectividad de host en el sistema de almacenamiento R2 de ASA

Si existe un problema con las operaciones de datos del host, puede usar ONTAP System Manager para verificar que la conexión del host al sistema de almacenamiento ASA R2 esté activa.

Pasos

1. En System Manager, seleccione **Host**.

El estado de conectividad de host se indica junto al nombre del grupo de hosts de la siguiente manera:

- **OK**: Indica que todos los iniciadores están conectados a ambos nodos.
- **Parcialmente conectado**: Indica que algunos de los iniciadores no están conectados ambos nodos.
- **Ninguno conectado**: Indica que no hay iniciadores conectados.

El futuro

Realice actualizaciones en el host para corregir los problemas de conectividad. ONTAP volverá a comprobar el estado de la conexión cada quince minutos.

Mantenga su sistema de almacenamiento R2 de ASA

Vaya al "ASA R2 mantiene la documentación" para obtener más información sobre cómo realizar procedimientos de mantenimiento en los componentes del sistema ASA R2.

Leer más

ASA R2 para usuarios avanzados de ONTAP

Compare los sistemas R2 de ASA con otros sistemas ONTAP

Los sistemas R2 de ASA ofrecen una solución unificada de hardware y software para entornos SAN basados en plataformas all-flash. Los sistemas ASA R2 varían con respecto a otros sistemas de ONTAP (ASA, AFF y FAS) en la implantación de su capa de almacenamiento, los protocolos compatibles y la personalidad de ONTAP.

En un sistema ASA R2, se ha optimizado el software ONTAP para admitir las funciones SAN esenciales, a la vez que se limita la visibilidad y la disponibilidad de las funciones y funciones que no son de SAN. Por ejemplo, System Manager que se ejecuta en un sistema ASA R2 no muestra opciones para crear directorios iniciales para clientes NAS. Esta versión optimizada de ONTAP se identifica como *ASA R2 Personality*. ONTAP que se ejecuta en todos los demás sistemas ONTAP (ASA, AFF, FAS) se identifica como *Unified ONTAP Personality*. Las diferencias entre las personalidades de la ONTAP se mencionan en la referencia de comandos de ONTAP (páginas de manual), la especificación de la API de REST y los mensajes de EMS donde corresponda.

Puede verificar la personalidad de su almacenamiento de ONTAP desde System Manager o desde la CLI de ONTAP.

- En el menú Administrador del sistema, seleccione **Clúster > Descripción general**.
- En la CLI, introduzca: `san config show`

La personalidad de su sistema de almacenamiento de ONTAP no puede cambiarse.

La capa de almacenamiento de sistemas ONTAP que ejecutan la personalidad unificada de ONTAP utiliza agregados como unidad de almacenamiento base. Un agregado posee un conjunto específico de discos disponibles en un sistema de almacenamiento. El agregado asigna espacio en los discos que posee a volúmenes para LUN y espacios de nombres. Un usuario de ONTAP unificado puede usar la interfaz de línea de comandos (CLI) para crear y modificar agregados, volúmenes, LUN y espacios de nombres.

La capa de almacenamiento de los sistemas ASA R2 utiliza una zona de disponibilidad de almacenamiento en lugar de agrupaciones. Una zona de disponibilidad de almacenamiento es un conjunto común de almacenamiento que tiene acceso a todos los discos disponibles en el sistema de almacenamiento. La zona de disponibilidad de almacenamiento está visible para ambos nodos de un par de alta disponibilidad ASA R2. Cuando se crea una unidad de almacenamiento (basada en un LUN o en un espacio de nombres NVMe), ONTAP crea automáticamente un volumen que contiene una máquina virtual de almacenamiento (VM) en la zona de disponibilidad de almacenamiento para alojar la unidad de almacenamiento. Debido a este enfoque automatizado y simplificado de la gestión del almacenamiento, ciertas opciones de System Manager, los comandos de la ONTAP y los extremos de la API de REST no están disponibles o su uso es limitado en un sistema ASA R2. Por ejemplo, debido a que la creación y gestión de volúmenes están automatizadas para los sistemas ASA R2, el menú **Volúmenes** no aparece en el Administrador del sistema y el `volume create` comando no es compatible.

El almacenamiento R2 de ASA se compara con otros sistemas de almacenamiento de ONTAP de las siguientes formas:

	ASA r2	ASA	AFF	FAS
Personalidad ONTAP	ASA r2	ASA	Unificado	Unificado
Soporte de protocolo SAN	Sí	Sí	Sí	Sí
• Compatibilidad con protocolo NAS*	No	No	Sí	Sí
• Soporte de capa de almacenamiento*	Zona de disponibilidad del almacenamiento	Agregados	Agregados	Agregados

Las siguientes plataformas de ASA se clasifican como sistemas ASA R2:

- ASA A1K
- ASA A70
- ASA A90

Si quiere más información

- Más información sobre "Sistemas de hardware de ONTAP".
- Vea todas las limitaciones y compatibilidad de la configuración de los sistemas ASA y ASA R2 en "NetApp Hardware Universe".
- Obtenga más información sobre el "ASA de NetApp".

Resumen de las diferencias del sistema ASA R2

A continuación, se describen las principales diferencias entre los sistemas de ASA R2 y los sistemas FAS, AFF y ASA, relevantes para la interfaz de línea de comandos (CLI) y la API REST DE ONTAP.

Creación predeterminada de SVM con servicios de protocolo

Los clústeres nuevos contienen automáticamente una SVM de datos predeterminada con los protocolos SAN habilitados. Los LIF de datos de IP admiten los protocolos iSCSI y NVMe/TCP y utilizan `default-data-blocks` la política de servicio de forma predeterminada.

Creación de volúmenes automática

La creación de una unidad de almacenamiento (LUN o espacio de nombres) crea automáticamente un volumen desde la zona de disponibilidad de almacenamiento. El resultado es un espacio de nombres común y simplificado. Al eliminar una unidad de almacenamiento, se elimina automáticamente el volumen asociado.

Cambios en el aprovisionamiento ligero y grueso

Las unidades de almacenamiento de están siempre aprovisionadas con thin provisioning en los sistemas de almacenamiento R2 de ASA. No se admite el aprovisionamiento grueso.

Compatibilidad del software ONTAP y limitaciones para los sistemas de almacenamiento R2 de ASA

Aunque los sistemas ASA R2 ofrecen una amplia gama de compatibilidad para las soluciones SAN, ciertas funciones de software ONTAP no son compatibles.

Los sistemas ASA R2 no son compatibles con lo siguiente:

- Recuperación tras fallos de LIF de iSCSI
- FabricPool
- Aprovisionamiento grueso de LUN
- MetroCluster
- Protocolos de objetos
- ONTAP S3 SnapMirror y API S3
- SnapMirror al cloud
- De SnapMirror a sistemas R2 que no sean de ASA
- Asignación de LUN selectiva (SLM)

Los sistemas ASA R2 ofrecen lo siguiente:

- SnapLock
- Cifrado de doble capa

Si quiere más información

- Consulte la "NetApp Hardware Universe" para obtener más información acerca de las limitaciones y la compatibilidad del hardware de ASA R2.
- "Aprenda a bloquear instantáneas" En su sistema ASA R2.
- "Aprenda a aplicar el cifrado de doble capa" A los datos de su sistema ASA R2.

Compatibilidad con la interfaz de línea de comandos de ONTAP para los sistemas de almacenamiento R2 de ASA

En lugar de agregados tradicionales, que poseen un conjunto específico de discos disponibles en un sistema de almacenamiento, los sistemas ASA R2 utilizan una *storage availability zone*. Una zona de disponibilidad de almacenamiento es un conjunto común de almacenamiento que tiene acceso a todos los discos disponibles en el sistema de almacenamiento. La zona de disponibilidad de almacenamiento está visible para ambos nodos de un par de alta disponibilidad ASA R2. Cuando se crea una unidad de almacenamiento (LUN o espacio de nombres NVMe), ONTAP crea automáticamente un

volumen que contiene una máquina virtual de almacenamiento (VM) en la zona de disponibilidad de almacenamiento para alojar la unidad de almacenamiento.

Debido a este método simplificado de gestión del almacenamiento, `storage aggregate` los comandos no son compatibles con los sistemas ASA R2. La compatibilidad con ciertos `lun` `volume` comandos y parámetros de AND también está limitada.

ASA R2 no admite los siguientes comandos y conjuntos de comandos:

Comandos <code>lun</code> no admitidos

- `lun copy`
- `lun geometry`
- `lun import`
- `lun mapping add-reportng-nodes`
- `lun mapping-remove-reporting-nodes`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  Este comando se reemplaza con lun rename/vserver nvme namespace rename.

- `lun transition`

Comandos y parámetros <code>volume</code> no admitidos

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  Este comando no está disponible cuando se usa junto con los siguientes parámetros:

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`
- `volume mount`

- volume move
- volume offline
- volume rehost
- volume rename
- volume restrict
- volume transition-prepare-to-downgrade
- volume unmount

Comandos <code>volume clone</code> no compatibles

- volume clone create
- volume clone split

Comandos <code>volume SnapLock </code> no compatibles

- volume snaplock modify

Comandos Snapshot de volumen <code>volume no compatibles </code>

- volume snapshot
- volume snapshot autodelete modify
- volume snapshot policy modify

Conjuntos de comandos <code>volume</code> no admitidos

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

Comandos <code>storage</code> no compatibles

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

Si quiere más información

Consulte la "Referencia de comandos del ONTAP"para obtener una lista completa de comandos admitidos

Configure un clúster de ONTAP ASA R2 mediante la interfaz de línea de comandos

Se recomienda que usted "Utilice System Manager para configurar su clúster de ONTAP ASA R2". System Manager ofrece un flujo de trabajo guiado rápido y sencillo para poner el clúster en funcionamiento. Sin embargo, si está acostumbrado a trabajar con comandos de la ONTAP, opcionalmente se puede utilizar la interfaz de línea de comandos de la ONTAP para la configuración del clúster. La configuración del clúster mediante CLI no ofrece opciones ni ventajas adicionales a la configuración del clúster con System Manager.

Durante la configuración del clúster, se crea la máquina virtual de almacenamiento de datos (VM) predeterminada, se crea una unidad de almacenamiento inicial y se detectan las LIF de datos automáticamente. Opcionalmente, puede habilitar el Sistema de nombres de dominio (DNS) para resolver nombres de host, configurar el clúster para que utilice el Protocolo de hora de red (NTS) para la sincronización

de tiempo y habilitar el cifrado de datos en reposo.

Antes de empezar

Recopile la siguiente información:

- Dirección IP de gestión del clúster

  La dirección IP de administración del clúster es una dirección IPv4 exclusiva para la interfaz de gestión de clústeres que usa el administrador del clúster para acceder a la máquina virtual de almacenamiento de administrador y gestionar el clúster. Puede pedirle esta dirección IP al administrador responsable de la asignación de direcciones IP en la organización.

- Máscara de subred de red

  Durante la configuración del clúster, ONTAP recomienda un conjunto de interfaces de red adecuadas para la configuración. Puede ajustar la recomendación si es necesario.

- Dirección IP de puerta de enlace de red
- Dirección IP del nodo asociado
- Nombres de dominio DNS
- Direcciones IP del servidor de nombres DNS
- Direcciones IP del servidor NTP
- Máscara de subred de datos

Pasos

1. Encienda ambos nodos del par de alta disponibilidad.
2. Muestre los nodos detectados en la red local:

   ```
   system node show-discovered -is-in-cluster false
   ```

3. Inicie el asistente de configuración del clúster:

   ```
   cluster setup
   ```

4. Reconozca la declaración de AutoSupport.
5. Introduzca los valores para el puerto de la interfaz de gestión de nodos, la dirección IP, la máscara de red y la pasarela predeterminada.
6. Presione **Enter** para continuar con la configuración usando la interfaz de línea de comandos; luego ingrese **create** para crear un nuevo clúster.
7. Acepte los valores predeterminados del sistema o introduzca sus propios valores.
8. Después de completar la configuración en el primer nodo, inicie sesión en el clúster.
9. Compruebe que el clúster esté activo y que el primer nodo esté en buen estado:

   ```
   system node show-discovered
   ```

10. Añada el segundo nodo al clúster:

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. De manera opcional, sincronice la hora del sistema en todo el clúster

Sincronice sin autenticación simétrica	`cluster time-service ntp server create -server <server_name>`
Sincronice con autenticación simétrica	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

    a. Compruebe que el clúster esté asociado con un servidor NTP:

```
Cluster time-service ntp show
```

12. Opcionalmente, descargue y ejecute "Config Advisor de ActiveIQ" para confirmar la configuración.

El futuro

Está preparado para "configure el acceso a los datos" pasar de sus clientes SAN a su sistema.

Soporte para la API de REST para ASA R2

La API REST DE ASA R2 se basa en la API REST proporcionada con la personalidad unificada de ONTAP, con una serie de cambios adaptados a las características y funcionalidades únicas de la personalidad de ASA R2.

Tipos de cambios de API

Existen varios tipos de diferencias entre la API de REST del sistema ASA R2 y la API DE REST unificada de ONTAP disponible en sistemas FAS, AFF y ASA. Comprender los tipos de cambios le ayudará a utilizar mejor la documentación de referencia de la API en línea.

No se admiten nuevos extremos de ASA R2 en Unified ONTAP

Se han añadido varios extremos a la API de REST DE ASA R2 que no están disponibles con Unified ONTAP.

Por ejemplo, se ha agregado un nuevo extremo de volumen de bloque a la API DE REST para los sistemas ASA R2. El extremo de volumen de bloques proporciona acceso a los objetos de espacio de nombres LUN y NVMe, lo que permite una vista agregada de los recursos. Solo está disponible en la API de REST.

Como otro ejemplo, los puntos finales **storage-units** proporcionan una vista agregada de los LUN y los espacios de nombres NVMe. Hay varios puntos finales y todos se basan en o se derivan de

`/api/storage/storage-units`. También debe revisar `/api/storage/luns` y `/api/storage/namespaces`.

Restricciones en los métodos HTTP utilizados para algunos puntos finales

Varios puntos finales disponibles con ASA R2 tienen restricciones sobre los métodos HTTP que se pueden utilizar en comparación con el ONTAP unificado. Por ejemplo, POST y DELETE no se permiten cuando se utiliza el punto final `/api/protocols/nvme/services` con sistemas ASA R2.

Cambios de propiedad para un punto final y método HTTP

Algunas combinaciones de métodos y puntos finales del sistema ASA R2 no admiten todas las propiedades definidas disponibles en la personalidad unificada de ONTAP. Por ejemplo, al utilizar EL PARCHE con el punto final `/api/storage/volumes/{uuid}`, no se admiten varias propiedades con ASA R2, entre las que se incluyen:

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

Cambios en el procesamiento interno

Hay varios cambios en la forma en que ASA R2 procesa ciertas solicitudes de API de REST. Por ejemplo, una solicitud DE SUPRESIÓN con el punto final `/api/storage/luns/{uuid}` se procesa de forma asíncrona.

Seguridad mejorada con OAuth 2,0

OAuth 2,0 es el marco de autorización estándar de la industria. Se utiliza para restringir y controlar el acceso a recursos protegidos basados en tokens de acceso firmados. Puede configurar OAuth 2,0 mediante System Manager para proteger los recursos del sistema ASA R2.

Una vez configurado OAuth 2,0 con System Manager, se puede controlar el acceso a los clientes API de REST. Primero debe obtener un token de acceso desde un servidor de autorización. A continuación, el cliente REST pasa el token al clúster de ASA R2 como un token portador mediante el encabezado de solicitud de autorización HTTP. Consulte "Autenticación y autorización mediante OAuth 2,0" para obtener más información.

Acceda a la documentación de referencia de API de ASA R2 a través de la interfaz de usuario de Swagger

Puede acceder a la documentación de referencia de la API de REST a través de la interfaz de usuario de Swagger en el sistema ASA R2.

Acerca de esta tarea

Debe acceder a la página de documentación de referencia de ASA R2 para obtener más detalles sobre la API DE REST. Como parte de esto, puede buscar la cadena **Especialidades de la plataforma** para encontrar detalles sobre el soporte del sistema ASA R2 para las llamadas y propiedades de la API.

Antes de empezar

Debe tener lo siguiente:

- La dirección IP o el nombre de host de la LIF de gestión del clúster del sistema ASA R2
- El nombre de usuario y la contraseña de una cuenta con autoridad para acceder a la API DE REST

Pasos

1. Escribe la URL en tu navegador y presiona **Enter**:
   `https://<ip_address>/docs/api`
2. Inicie sesión con su cuenta de administrador.

   La página de documentación de API de ASA R2 se muestra con las llamadas API organizadas en las principales categorías de recursos.

3. Para ver un ejemplo de una llamada a la API que es específicamente aplicable solo a los sistemas ASA R2, desplácese hacia abajo hasta la categoría **SAN** y haga clic en **OBTENER /storage/storage-units**.

Obtenga ayuda

Gestione AutoSupport en sistemas de almacenamiento R2 de ASA

AutoSupport es un mecanismo que supervisa de forma proactiva el estado del sistema y envía automáticamente mensajes al soporte técnico de NetApp, su organización de soporte interno y un partner de soporte.

Los mensajes de AutoSupport para el soporte técnico se habilitan de forma predeterminada cuando configura el clúster. Debe configurar las opciones correctas y contar con un host de correo válido para que se envíen mensajes a la organización de soporte interno. ONTAP comienza a enviar mensajes de AutoSupport 24 horas después de que se ha habilitado.

Antes de empezar

Debe ser un administrador de clústeres para gestionar AutoSupport.

Probar la conectividad AutoSupport

Después de configurar el clúster, debe probar su conectividad AutoSupport para verificar que el soporte técnico recibirá mensajes generados por AutoSupport.

Pasos

1. En el administrador del sistema, selecciona **Cluster >Settings**.
2. Junto a **AutoSupport** selecciona ⋮; y luego selecciona **Probar conectividad**.
3. Ingrese un asunto para el mensaje AutoSupport y luego seleccione **Enviar mensaje AutoSupport de prueba**.

El futuro

Ha verificado que el soporte técnico puede recibir mensajes de AutoSupport de su sistema ASA R2 y dispondrá de los datos necesarios para ayudarle en caso de que experimente un problema.

Agregar destinatarios de AutoSupport

Añada miembros de la organización de soporte interno a la lista de direcciones de correo electrónico que reciben mensajes de AutoSupport.

Pasos

1. En el administrador del sistema, selecciona **Cluster >Settings**.
2. Junto a **AutoSupport** selecciona ⋮; y luego selecciona **Más opciones**.
3. Junto a **Correo electrónico**, seleccione ✎; y, a continuación, seleccione + Add .
4. Introduzca la dirección de correo electrónico del destinatario y, a continuación, la categoría del destinatario.

   Para los socios, seleccione **Partner** para la categoría de destinatarios. Seleccione **General** para los miembros de su organización de apoyo interno.

5. Seleccione GUARDAR.

El futuro

Las direcciones de correo electrónico que haya añadido recibirán nuevos mensajes de AutoSupport para su categoría de destinatario específica.

Enviar datos AutoSupport

Si se produce algún problema en el sistema ASA R2, los datos de AutoSupport pueden reducir considerablemente el tiempo necesario para identificar y resolver los problemas.

Pasos

1. En el administrador del sistema, selecciona **Cluster >Settings**.
2. Junto a **AutoSupport** selecciona ⋮; y luego selecciona **Generar y enviar**.
3. Introduzca un asunto para el mensaje AutoSupport y, a continuación, seleccione **Enviar**.

El futuro

Los datos de AutoSupport se envían al soporte técnico.

Suprimir la generación de casos de soporte

Si realiza una actualización o un mantenimiento en el sistema ASA R2, podría suprimir la generación de casos de soporte de AutoSupport hasta que se complete la actualización o el mantenimiento.

Pasos

1. En el administrador del sistema, selecciona **Cluster >Settings**.
2. Junto a **AutoSupport** seleccione ⋮; y luego seleccione **Suprimir generación de casos de soporte**.
3. Especifique la cantidad de horas para suprimir la generación de casos de soporte y, a continuación, seleccione los nodos para los que no desea que se generen los casos.
4. Seleccione **Enviar**.

El futuro

Los casos AutoSupport no se generarán durante el tiempo especificado. Si completa la actualización o el mantenimiento antes de que caduque el tiempo especificado, deberá reanudar la generación de casos de soporte de inmediato.

Reanudar la generación de casos de soporte

Si ha suprimido la generación de casos de soporte durante una ventana de actualización o mantenimiento, debería reanudar la generación de caso de soporte inmediatamente una vez que finalice la actualización o el mantenimiento.

Pasos

1. En el administrador del sistema, selecciona **Cluster >Settings**.
2. Junto a **AutoSupport** seleccione ⋮; y luego seleccione **Reanudar generación de casos de soporte**.
3. Seleccione los nodos para los que desea reanudar los casos de AutoSupport generados.
4. Seleccione **Enviar**.

Resultado

Los casos AutoSupport se generan automáticamente para el sistema ASA R2 según sea necesario.

Envíe y consulte casos de soporte de los sistemas de almacenamiento R2 de ASA

Si tiene un problema que requiere ayuda, puede usar System Manager de ONTAP para enviar un caso al soporte técnico. También puede usar ONTAP System Manager para ver casos que se han cerrado o en curso.

Debe "Registrado con Active IQ"ser ver los casos de soporte de su sistema ASA R2.

Pasos

1. Para enviar un caso de soporte, en el Administrador del sistema, seleccione * Clúster > Soporte *; a continuación, seleccione * Ir a Soporte de NetApp *.
2. Para ver un caso enviado anteriormente, en System Manager, seleccione **Cluster >Support**; luego seleccione **Ver mis casos**.

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.