Use ONTAP para gestionar sus datos

ASA r2

NetApp
February 11, 2026

Tabla de contenidos

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 un sistema ASA r2, una unidad de almacenamiento pone a disposición de sus hosts SAN espacio de almacenamiento para operaciones de datos. Una unidad de almacenamiento se refiere a una LUN para hosts SCSI o a un espacio de nombres NVMe para hosts NVMe. Si su clúster está configurado para admitir hosts SCSI, se le solicitará que cree un LUN. Si su clúster está configurado para admitir hosts NVMe, se le solicitará que cree un espacio de nombres NVMe.

Una unidad de almacenamiento ASA r2 tiene una capacidad máxima de 128 TB. Ver el"NetApp Hardware Universe" para conocer los límites de almacenamiento más actuales para los sistemas ASA r2.

Usted agrega y asigna iniciadores de host a la unidad de almacenamiento como parte del proceso de creación de la unidad de almacenamiento. También puedes"agregar" y"asignar" iniciadores de host después de crear las unidades de almacenamiento.

A partir de ONTAP 9.18.1, puede modificar la reserva de instantáneas y habilitar la eliminación automática de instantáneas al crear una unidad de almacenamiento. La reserva de instantáneas es la cantidad de espacio en la unidad de almacenamiento reservada específicamente para instantáneas. Cuando la reserva de instantáneas está configurada con eliminación automática de instantáneas, las instantáneas más antiguas se

eliminan automáticamente cuando el espacio utilizado por las instantáneas supera la reserva de instantáneas.

"Obtenga más información sobre la reserva de instantáneas en los sistemas ASA r2.".

Las unidades de almacenamiento se aprovisionan de forma ligera de manera predeterminada. El aprovisionamiento fino permite que la unidad de almacenamiento crezca hasta el tamaño asignado, pero no reserva el espacio por adelantado. El espacio se asigna dinámicamente a partir del espacio libre disponible según sea necesario. Esto le permite lograr una mayor eficiencia de almacenamiento al sobreaprovisionar su espacio disponible. Por ejemplo, supongamos que tiene 1 TB de espacio libre y necesita crear cuatro unidades de almacenamiento de 1 TB. En lugar de agregar inmediatamente 3 TB de capacidad de almacenamiento adicional a su sistema, puede crear unidades de almacenamiento, monitorear la utilización del espacio y aumentar su capacidad de almacenamiento a medida que las unidades de almacenamiento consumen espacio real. Obtenga más información sobre"aprovisionamiento fino" .

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.

   Para optimizar el equilibrio de carga de trabajo en la zona de disponibilidad de almacenamiento, cree una cantidad par de unidades de almacenamiento.

4. Introduzca la capacidad de la unidad de almacenamiento y seleccione el sistema operativo del host.

   Si está creando más de una unidad de almacenamiento, cada unidad se crea con la misma capacidad. Multiplique la cantidad de unidades de almacenamiento que está creando por la capacidad deseada para asegurarse de tener suficiente espacio utilizable. Si no dispone de suficiente espacio libre y decide sobreaprovisionar, supervise de cerca la utilización para evitar quedarse sin espacio y perder datos.

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.

   Mapeo de host se refiere al grupo de host al que se asignará la nueva unidad de almacenamiento. Si hay un grupo de host preexistente para el tipo de host que seleccionó para su nueva unidad de almacenamiento, el grupo de host preexistente se selecciona automáticamente para su asignación de host. Puede aceptar el grupo de host que se selecciona automáticamente o puede seleccionar un grupo de host diferente.

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

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.
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 QoS, una garantía de QoS 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**.
Cambie el nivel de servicio de rendimiento predeterminado.	a. En **Almacenamiento y optimización**, junto al **Nivel de servicio de rendimiento**, selecciona . b. Selecciona **Rendimiento**. Los sistemas ASA r2 ofrecen dos niveles de rendimiento. El nivel de rendimiento predeterminado es **Extremo**, que es el nivel más alto disponible. Puedes bajar el nivel a **Rendimiento**.

Opción	Pasos
Modifique la reserva de instantáneas predeterminada y habilite la eliminación automática de instantáneas.	a. En **Porcentaje de reserva de instantáneas**, introduzca el valor numérico del porcentaje del espacio de la unidad de almacenamiento que desea asignar a las instantáneas. b. Seleccione **Eliminar automáticamente las instantáneas antiguas**.
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. Formatee el NQN del host 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.

Asignar la unidad de almacenamiento a un host

Después de crear unidades de almacenamiento ASA r2 y agregar iniciadores de host, asigne hosts a unidades de almacenamiento para comenzar a servir datos. Las unidades de almacenamiento se asignan a los hosts como parte del proceso de creación de la unidad 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.
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.

Divida el clon del grupo de consistencia

Cuando se divide un clon de un grupo de consistencia, se disocia el clon del grupo de consistencia de origen y se asigna espacio en disco al clon. El clon se convierte en un grupo de consistencia independiente que se puede usar independientemente del grupo de consistencia de origen.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón por el clon del grupo de consistencia que desea dividir.
3. Seleccione **Split clone**.
4. Selecciona **Split**.

Resultado

El clon se separa del grupo de consistencia de origen y se asigna el espacio en disco para el clon.

Administrar grupos de hosts

Cree grupos de host en su sistema ASA r2

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

Has creado un grupo de host y ahora puedes "asignarlo a una unidad de almacenamiento" .

Eliminar un grupo de hosts en su sistema ASA r2

En un sistema ASA r2, un grupo de hosts es el mecanismo que permite a los hosts acceder a las unidades de almacenamiento. Un grupo de hosts se refiere a un igroup para hosts SCSI o a un subsistema NVMe para hosts NVMe. Un host solo puede ver las unidades de almacenamiento asignadas a los grupos de hosts a los que pertenece. Es posible que desee eliminar un grupo de hosts si ya no desea que los hosts del grupo tengan acceso a las unidades de almacenamiento asignadas a él.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. En **Mapeo de host** seleccione el grupo de host que desea eliminar.
3. Seleccione **Almacenamiento mapeado**.
4. Seleccione **Más**; luego seleccione **Eliminar**.
5. Seleccione para verificar que desea continuar; luego seleccione **Eliminar**.

El futuro

Se elimina el grupo de hosts. Los hosts que lo formaban ya no tienen acceso a las unidades de almacenamiento asignadas a él.

Gestión de unidades de almacenamiento

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.

Mueva unidades de almacenamiento a los sistemas de almacenamiento R2 de ASA

Si una zona de disponibilidad de almacenamiento se está quedando sin espacio, puede mover las unidades de almacenamiento a otra zona de disponibilidad de almacenamiento para equilibrar la utilización del almacenamiento en todo el clúster.

Puede mover una unidad de almacenamiento mientras la unidad de almacenamiento está en línea y sirve datos. La operación de movimiento no es disruptiva.

Antes de empezar

- Debe ejecutar ONTAP 9.16.1 o una versión posterior.
- El clúster debe constar de cuatro o más nodos.

Pasos

1. En System Manager, seleccione **Almacenamiento** y, a continuación, seleccione la unidad de almacenamiento que desea mover.
2. Seleccione ⋮ ; y, a continuación, seleccione **Mover**.
3. Seleccione la zona de disponibilidad de almacenamiento a la que desea mover la unidad de almacenamiento y, a continuación, seleccione **Mover**.

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 está en un grupo de consistencia que está en relación de replicación, debe"retire la unidad de almacenamiento del grupo de consistencia" Antes de borrarlo.

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.

Migrar máquinas virtuales de almacenamiento

Migrar una máquina virtual de almacenamiento de un clúster ASA a un clúster ASA r2

A partir de ONTAP 9.18.1, puede migrar sin interrupciones una máquina virtual (VM) de almacenamiento desde cualquier clúster ASA a cualquier clúster ASA r2. La migración de un clúster ASA a un clúster ASA r2 le permite adoptar la arquitectura simplificada y optimizada de los sistemas ASA r2 para entornos exclusivamente SAN.

La migración de máquinas virtuales de almacenamiento entre sistemas de almacenamiento ASA y ASA r2 se admite de la siguiente manera:

Desde cualquiera de los siguientes sistemas ASA :	A cualquiera de los siguientes sistemas ASA r2:
• ASA C800 • ASA C400 • ASA C250 • ASA A900 • ASA A800 • ASA A400 • ASA A250 • ASA A150 • ASA AFF A800 • ASA AFF A700 • ASA AFF A400 • ASA AFF A250 • ASA AFF A220	• ASA A1K • ASA C30 • ASA A90 • ASA A70 • ASA A50 • ASA A30 • ASA A20

Para obtener la lista más actualizada de sistemas ASA y ASA r2, consulte"NetApp Hardware Universe" . Los sistemas ASA r2 aparecen en NetApp Hardware Universe como "ASA Serie A/Serie C (Nuevo)".

Solo se puede migrar una máquina virtual de almacenamiento a un clúster ASA r2 desde un clúster ASA . No se admite la migración desde ningún otro tipo de sistema ONTAP .

Antes de empezar

Todos los nodos del clúster ASA r2 y del clúster ASA deben estar ejecutando ONTAP 9.18.1 o posterior. Las versiones de parches de ONTAP 9.18.1 en los nodos del clúster pueden variar.

Paso 1: Verifique el estado de la máquina virtual de almacenamiento ASA.

Antes de migrar una máquina virtual de almacenamiento desde un sistema ASA , no debe haber espacios de nombres NVMe ni vVols presentes y cada volumen en la máquina virtual de almacenamiento debe contener solo un LUN. No se admite la migración de espacios de nombres NVMe ni de vVols . La arquitectura de los sistemas ASA r2 requiere que los volúmenes contengan un único LUN.

Pasos

1. Verifique que no haya espacios de nombres NVMe presentes en la máquina virtual de almacenamiento:

   ```
   vserver nvme namespace show -vserver <storage_VM>
   ```

   Si se muestran entradas, los objetos NVMe deben ser"convertido" a LUN o eliminados. Ver el `vserver nvme namespace delete` y el `vserver nvme subsystem delete` comandos en el"Referencia de comandos del ONTAP" Para obtener más información.

2. Verifique que no haya vVols presentes en la máquina virtual de almacenamiento:

```
lun show -verser <storage_VM> -class protocol-endpoint,vvol
```

Si existen vVols , deben copiarse a otra máquina virtual de almacenamiento y luego eliminarse de la máquina virtual de almacenamiento que se va a migrar. Ver el `lun copy` y `lun delete` comandos en el"Referencia de comandos del ONTAP" Para obtener más información.

3. Verifique que cada volumen en la máquina virtual de almacenamiento contenga un único LUN:

```
lun show -verser <storage_VM>
```

Si un volumen contiene más de un LUN, utilice el `volume create` y `lun move` comandos para crear una relación volumen-LUN de 1:1. Ver el"Referencia de comandos del ONTAP" Para más información.

¿Cuál es el siguiente?

Ya está listo para crear una relación de pares de clúster entre sus clústeres ASA y ASA r2.

Paso 2: Cree una relación de pares de clúster entre sus clústeres ASA y ASA r2.

Antes de poder migrar una máquina virtual de almacenamiento de un clúster ASA a un clúster ASA r2, es necesario crear una relación de pares. Una relación entre pares define las conexiones de red que permiten a los clústeres ONTAP y a las máquinas virtuales de almacenamiento intercambiar datos de forma segura.

Antes de empezar

Debe haber creado LIF intercluster en cada nodo de los clústeres que se están interconectando utilizando uno de los siguientes métodos.

- "Configure las LIF intercluster en los puertos de datos compartidos."
- "Configure las LIF intercluster en puertos de datos dedicados."
- "Configurar LIF entre clústeres en espacios IP personalizados"

Pasos

1. En el clúster ASA r2, cree una relación de pares con el clúster ASA y genere una contraseña:

```
cluster peer create -peer-addrs <ASA_cluster_LIF_IPs> -generate
-passphrase
```

El siguiente ejemplo crea una relación de pares de clúster entre el clúster 1 y el clúster 2 y crea una contraseña generada por el sistema:

```
cluster1::> cluster peer create -peer-addrs 10.98.191.193 -generate
-passphrase
Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
            Peer Cluster Name: cluster2
            Initial Allowed Vserver Peers: -
            Expiration Time: 6/7/2017 09:16:10 +5:30
            Intercluster LIF IP: 10.140.106.185
Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Copie la frase de contraseña generada.
3. En el clúster ASA , cree una relación de pares con el clúster ASA r2:

```
cluster peer create -peer-addrs <ASA_r2_LIF_IPs>
```

4. Introduzca la contraseña generada en el clúster ASA r2.
5. Verifique que se haya creado la relación de pares del clúster:

```
cluster peer show
```

El siguiente ejemplo muestra el resultado esperado para clústeres emparejados correctamente.

```
cluster1::> cluster peer show

Peer Cluster Name   Cluster Serial Number   Availability
Authentication
-----------------   ---------------------   --------------
--------------
cluster2             1-80-123456             Available      ok
```

Resultado

Los clústeres ASA y ASA r2 están interconectados y los datos de las máquinas virtuales de almacenamiento se pueden transferir de forma segura.

¿Cuál es el siguiente?

Ya está listo para preparar su máquina virtual de almacenamiento ASA para la migración.

Paso 3: Preparar la migración de la máquina virtual de almacenamiento desde un clúster ASA a un clúster ASA r2.

Antes de migrar una máquina virtual (VM) de almacenamiento de un clúster ASA a un clúster ASA r2, debe ejecutar una comprobación previa de la migración y solucionar cualquier problema necesario. No se puede realizar la migración hasta que la comprobación previa se supere correctamente.

Paso

1. Desde su clúster ASA r2, ejecute la comprobación previa de la migración:

```
vserver migrate start -vserver <storage_VM> -source-cluster
<asa_cluster> -check-only true
```

Si necesita solucionar algún problema para preparar su clúster ASA para la migración, se mostrarán el problema y la acción correctiva. Solucione el problema y repita la comprobación previa hasta que se complete correctamente.

¿Cuál es el siguiente?

Ya está listo para migrar su máquina virtual de almacenamiento desde su clúster ASA a un clúster ASA r2.

Paso 4: Migrar una máquina virtual de almacenamiento ASA a un clúster ASA r2

Una vez que haya preparado su clúster ASA y creado la relación de pares de clúster necesaria con el clúster ASA r2, puede comenzar la migración de la máquina virtual de almacenamiento.

Al realizar una migración de máquina virtual de almacenamiento, es una buena práctica dejar un 30 % de margen de CPU tanto en el clúster ASA como en el clúster ASA r2 para permitir que se ejecute la carga de trabajo de la CPU.

Acerca de esta tarea

Tras la migración de la máquina virtual de almacenamiento, los clientes se conectan automáticamente al clúster ASA r2 y la máquina virtual de almacenamiento del clúster ASA se elimina automáticamente. La conmutación automática y la eliminación automática de máquinas virtuales de almacenamiento están habilitadas de forma predeterminada. Opcionalmente, puede deshabilitarlos ambos y realizar el cambio y la eliminación de la máquina virtual de almacenamiento manualmente.

Antes de empezar

- El clúster ASA r2 debe tener suficiente espacio libre para alojar la máquina virtual de almacenamiento migrada.
- Si la máquina virtual de almacenamiento ASA contiene volúmenes cifrados, el administrador de claves integrado o el administrador de claves externo en el sistema ASA r2 debe configurarse a nivel de clúster.
- Las siguientes operaciones no pueden ejecutarse en el clúster ASA de origen:
  - Operaciones de conmutación por error
  - WAFLIRON
  - Huella dactilar
  - Transferencia de volumen, rehosting, clonación, creación, conversión o análisis

Pasos

1. Desde el clúster ASA r2, inicie la migración de la máquina virtual de almacenamiento:

```
vserver migrate start -vserver <storage_VM_name> -source-cluster
<ASA_cluster>
```

Para desactivar el cambio automático, utilice el `-auto-cutover false` parámetro. Para deshabilitar la eliminación automática de la máquina virtual de almacenamiento ASA , utilice el `-auto-source`

`-cleanup false` parámetro.

2. Supervisar el estado de la migración

```
vserver migrate show -vserver <storage_VM_name>
```

Cuando la migración esté completa, el **estado** se mostrará como **migración completada**.

> Si necesita pausar o cancelar la migración antes de que comience el cambio automático, utilice la siguiente opción: `vserver migrate pause` y el `vserver migrate abort` comandos. Debes pausar la migración antes de cancelarla. No se puede cancelar la migración una vez que haya comenzado el cambio.

Resultado

La máquina virtual de almacenamiento se migra del clúster ASA al clúster ASA r2. El nombre y el UUID de la máquina virtual de almacenamiento, el nombre de la LIF de datos, la dirección IP y los nombres de los objetos, como el nombre del volumen, permanecen sin cambios. Se actualiza el UUID de los objetos migrados en la máquina virtual de almacenamiento.

¿Cuál es el siguiente?

Si deshabilitaste la conmutación automática y la eliminación automática de máquinas virtuales de almacenamiento,"Migre manualmente sus clientes ASA a su clúster ASA r2 y elimine la máquina virtual de almacenamiento del clúster ASA." .

Migración de clientes y limpieza de la máquina virtual de almacenamiento de origen tras la migración a un sistema ASA r2

Después de migrar una máquina virtual (VM) de almacenamiento de un clúster ASA a un clúster ASA r2, de forma predeterminada, los clientes se transfieren automáticamente al clúster ASA r2 y la VM de almacenamiento en el clúster ASA se elimina automáticamente. Si optó por deshabilitar el cambio automático y la eliminación de la máquina virtual de almacenamiento ASA durante la migración, deberá realizar estos pasos manualmente una vez finalizada la migración.

Tras una migración de máquina virtual de almacenamiento, realice manualmente la migración de los clientes a un sistema ASA r2.

Si deshabilita el cambio automático de cliente durante la migración de una máquina virtual de almacenamiento de un clúster ASA a un clúster ASA r2, una vez completada la migración, realice el cambio manualmente para que la máquina virtual de almacenamiento ASA r2 pueda proporcionar datos a los clientes.

Pasos

1. En el clúster ASA r2, ejecute manualmente el cambio de cliente:

```
vserver migrate cutover -vserver <storage_VM_name>
```

2. Verifique que la operación de migración se haya completado:

```
vserver migrate show
```

Resultado

Los datos se están sirviendo a sus clientes desde la máquina virtual de almacenamiento en su clúster ASA r2.

¿Cuál es el siguiente?

Ahora está listo para eliminar la máquina virtual de almacenamiento del clúster ASA de origen.

Eliminar manualmente una máquina virtual de almacenamiento ASA después de la migración a un clúster ASA r2.

Si deshabilita la limpieza automática de origen durante la migración de una máquina virtual de almacenamiento de un clúster ASA a un clúster ASA r2, una vez completada la migración, elimine la máquina virtual de almacenamiento del clúster ASA para liberar el espacio de almacenamiento.

Antes de empezar

Sus clientes deberían estar recibiendo datos del clúster ASA r2.

Pasos

1. Desde el clúster ASA , verifique que el estado de la máquina virtual de almacenamiento ASA sea **Lista para la limpieza de origen**:

```
vserver migrate show
```

2. Eliminar la máquina virtual de almacenamiento ASA :

```
vserver migrate source-cleanup -vserver <storage_VM_name>
```

Resultado

Se ha eliminado la máquina virtual de almacenamiento de su clúster ASA .

Límites de almacenamiento de ASA R2

Para un rendimiento, configuración y soporte óptimos, debe tener en cuenta los límites de almacenamiento de ASA r2.

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

Los sistemas ASA r2 admiten los siguientes límites de almacenamiento:

	Máximo por par HA	Máximo por grupo
Grupos de consistencia	256	256
Aplicaciones empresariales	100	350
Nodos	2	12

	Máximo por par HA	Máximo por grupo
Grupos de replicación	50	50
Tamaño de la zona de disponibilidad de almacenamiento	2 PB	2 PB
Unidades de almacenamiento	10.000	30.000
Tamaño de la unidad de almacenamiento	128TB	128TB
Unidades de almacenamiento por grupo de consistencia	256	256
Grupos de consistencia de niños por grupo de consistencia de padres	64	64
máquinas virtuales de almacenamiento	• 256 (ONTAP 9.18.1 y posteriores) • 32 (ONTAP 9.17.1 y versiones anteriores)	• 256 (ONTAP 9.18.1 y posteriores) • 32 (ONTAP 9.17.1 y versiones anteriores)
Máquinas virtuales	800	1200

Límites para las relaciones asincrónicas de SnapMirror

Los siguientes límites se aplican a las unidades de almacenamiento y a los grupos de consistencia en una relación de replicación asincrónica de SnapMirror . Para obtener una lista completa de los límites de almacenamiento más recientes de ASA r2,"NetApp Hardware Universe" .

Límite máximo	Por par HA	Por grupo
Grupos de consistencia	250	750
Unidades de almacenamiento	4.000	6.000

Límites para la relación de sincronización activa de SnapMirror

Los siguientes límites se aplican a las unidades de almacenamiento y a los grupos de consistencia en una relación de replicación de sincronización activa de SnapMirror . La sincronización activa de SnapMirror es compatible a partir de ONTAP 9.17.1 solo en clústeres de dos nodos. A partir de ONTAP 9.18.1, la sincronización activa de SnapMirror es compatible con clústeres de cuatro nodos.

Para obtener una lista completa de los límites de almacenamiento más recientes de ASA r2,"NetApp Hardware Universe" .

Límite máximo	Por par HA
Grupos de consistencia	50
Unidades de almacenamiento	400

Proteja sus datos

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

Cree una instantánea para realizar una copia de seguridad de los datos en su sistema ASA r2. Utilice ONTAP System Manager para crear una instantánea manual de una sola unidad de almacenamiento, o para crear un grupo de consistencia y programar instantáneas 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.

A partir de ONTAP 9.18.1, puede configurar el porcentaje de reserva de instantáneas y habilitar la eliminación automática de instantáneas al crear un grupo de consistencia con nuevas unidades de almacenamiento. La reserva de instantáneas es la cantidad de espacio en la unidad de almacenamiento reservada específicamente para instantáneas. Cuando la reserva de instantáneas está configurada con eliminación automática de instantáneas, las instantáneas más antiguas se eliminan automáticamente cuando el espacio utilizado por las instantáneas supera la reserva de instantáneas. Si la reserva de instantáneas y la eliminación automática de instantáneas están habilitadas en un grupo de coherencia principal, se habilitan en todos los grupos de coherencia secundarios existentes. Si se agregan nuevos grupos de coherencia secundarios, estos no heredan la configuración de reserva de instantáneas ni la configuración de eliminación de instantáneas del grupo principal.

"Obtenga más información sobre la reserva de instantáneas en los sistemas de almacenamiento ASA r2.".

A partir de ONTAP 9.16.1, cuando cree grupos de consistencia utilizando nuevas unidades de almacenamiento, puede configurar hasta cinco grupos de consistencia secundarios. "Obtenga más información sobre los grupos de consistencia infantil en los sistemas ASA r2.".

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 crea más de una unidad, cada unidad se crea con la misma capacidad y el mismo sistema operativo host de forma predeterminada. Opcionalmente, puede asignar una capacidad diferente a cada unidad.

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

Opción	Pasos
Asigne una capacidad diferente a cada unidad de almacenamiento	Selecciona **Añadir una capacidad diferente**.
Cambie el nivel de servicio de rendimiento predeterminado	En **Nivel de servicio de rendimiento**, seleccione un nivel de servicio diferente. Los sistemas ASA r2 ofrecen dos niveles de rendimiento. El nivel de rendimiento predeterminado es **Extremo**, que es el nivel más alto disponible. Puedes reducir el nivel de rendimiento a **Rendimiento**.
Modifique la reserva de instantáneas predeterminada y habilite la eliminación automática de instantáneas.	a. En **Porcentaje de reserva de instantáneas**, introduzca el valor numérico del porcentaje del espacio de la unidad de almacenamiento que desea asignar a las instantáneas. b. Seleccione **Eliminar automáticamente las instantáneas antiguas**.
Cree un grupo de consistencia secundario	Seleccione **Agregar grupo de consistencia secundario**.

5. Seleccione el sistema operativo del host y la asignación del host.
6. Seleccione **Agregar**.

El futuro

Has creado un grupo de coherencia que contiene las unidades de almacenamiento que deseas proteger. Ahora puedes 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

Has creado un grupo de coherencia que contiene las unidades de almacenamiento que deseas proteger. Ahora puedes 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

  Puede crear una instantánea bajo demanda de una unidad de almacenamiento en cualquier momento. La unidad de almacenamiento no necesita pertenecer a un grupo de consistencia para estar protegida por una instantánea bajo demanda. Si crea una instantánea a petición de una unidad de almacenamiento que es miembro de un grupo de coherencia, las demás unidades de almacenamiento del grupo de coherencia no se incluirán en la instantánea a petición. Si crea una instantánea bajo demanda de un grupo de consistencia, todas las unidades de almacenamiento del grupo de consistencia se incluirán en la instantánea.

- 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.

Gestionar la reserva de instantáneas

Obtenga información sobre la reserva de instantáneas de ONTAP en el almacenamiento ASA r2.

La reserva de instantáneas es la cantidad de espacio en la unidad de almacenamiento reservada específicamente para instantáneas. Cuando la reserva de instantáneas está configurada con eliminación automática de instantáneas, las instantáneas más antiguas se eliminan automáticamente cuando el espacio utilizado por las instantáneas supera la reserva de instantáneas. Esto evita que las instantáneas consuman espacio en su unidad de almacenamiento destinado a datos de usuario.

La reserva instantánea se establece como un porcentaje del tamaño total de la unidad de almacenamiento. Por ejemplo, si la unidad de almacenamiento es de 50 GB y se configura la reserva de instantáneas en un 10 %, la cantidad de espacio reservado para instantáneas es de 5 GB. Cuando la cantidad de espacio utilizado por las instantáneas alcanza los 5 GB, las instantáneas más antiguas se eliminan automáticamente para dejar espacio para las nuevas. Si el tamaño de la unidad de almacenamiento aumenta a 100 GB, entonces la reserva de instantáneas aumenta a 10 GB. La reserva máxima de instantáneas que puedes configurar es del 200%. Si su unidad de almacenamiento crece hasta el tamaño máximo de 128 TB, una reserva de instantáneas del 200 % le permite tomar 2 instantáneas completas.

Por defecto, la reserva de instantáneas está configurada en 0% y la eliminación automática de instantáneas no está habilitada.

A partir de ONTAP 9.18.1, puede modificar la reserva de instantáneas predeterminada durante o después de la creación de unidades de almacenamiento y durante la creación de grupos de consistencia. También puede modificar la reserva de instantáneas predeterminada en las máquinas virtuales (VM) de almacenamiento existentes. En ONTAP 9.17.1 y versiones anteriores, no se pueden modificar estos ajustes.

La reserva de instantánea se establece en el mismo porcentaje para todas las unidades de almacenamiento en un grupo de consistencia en el momento en que se crea el grupo de consistencia. La reserva de instantánea debe configurarse individualmente en cualquier unidad de almacenamiento que se agregue posteriormente.

Modificar la reserva de instantáneas en un sistema de almacenamiento ASA r2

La reserva de instantáneas es la cantidad de espacio en la unidad de almacenamiento reservada específicamente para instantáneas. Por defecto, la reserva de instantáneas está configurada en 0%. A partir de ONTAP 9.18.1, puede modificar la reserva de instantáneas predeterminada de la unidad de almacenamiento y habilitar la eliminación automática de instantáneas. La eliminación automática de instantáneas está desactivada por defecto. Cuando se establece un valor de reserva de instantáneas y se habilita la eliminación automática de instantáneas, las instantáneas más antiguas se eliminan automáticamente cuando el espacio utilizado por las instantáneas supera la reserva de instantáneas. Esto evita que las instantáneas consuman espacio en su unidad de almacenamiento destinado a datos de usuario.

"Obtenga más información sobre la reserva de instantáneas en los sistemas de almacenamiento ASA r2.".

Modificar la reserva de instantáneas en las unidades de almacenamiento

Para establecer diferentes valores de reserva de instantáneas, configure cada unidad de almacenamiento individualmente. Para utilizar el mismo valor para todas las unidades de almacenamiento, modifique la reserva de instantáneas en la máquina virtual de almacenamiento.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Pase el cursor sobre el nombre de la unidad de almacenamiento para la que desea configurar la reserva de instantáneas.
3. Seleccionar , luego seleccione **Editar**.
4. En **Porcentaje de reserva de instantáneas**, introduzca el valor numérico del porcentaje del espacio de la unidad de almacenamiento que desea asignar a las instantáneas.

5. Verifique que esté seleccionada la opción **Eliminar automáticamente las instantáneas antiguas**.
6. Seleccione **Guardar**.

Resultado

La reserva de instantáneas está configurada en el porcentaje que usted especificó. Si la cantidad de espacio consumido por las instantáneas alcanza la reserva, las instantáneas más antiguas se eliminan automáticamente.

Modificar la reserva de instantáneas en una máquina virtual de almacenamiento

Para establecer la misma reserva de instantáneas para todas las unidades de almacenamiento en una máquina virtual de almacenamiento, aplique el porcentaje deseado a la máquina virtual de almacenamiento. . Cuando se aplica la reserva de instantáneas a la máquina virtual de almacenamiento, se aplica a todas las unidades de almacenamiento recién creadas dentro de la máquina virtual de almacenamiento. No se aplica a las unidades de almacenamiento creadas antes de que usted modificara la configuración.

Pasos

1. En System Manager, seleccione **Clúster > Máquinas virtuales de almacenamiento**; luego seleccione **Configuración**.
2. En **Políticas**, junto a **Instantáneas**, seleccione ⋮ ; luego seleccione **Establecer/editar valor predeterminado de reserva de instantáneas**.
3. En **Porcentaje de reserva de instantáneas**, introduzca el valor numérico del porcentaje del espacio de la unidad de almacenamiento que desea asignar a las instantáneas.
4. Verifique que esté seleccionada la opción **Eliminar automáticamente las instantáneas antiguas**.
5. Seleccione **Guardar**.

Resultado

La reserva de instantáneas para las unidades de almacenamiento recién creadas se establece en el porcentaje que usted especificó. Si la cantidad de espacio consumido por las instantáneas en esas unidades de almacenamiento alcanza la reserva, las instantáneas más antiguas se eliminan automáticamente.

Crear una relación de pares de máquinas virtuales de almacenamiento entre clústeres en sistemas de almacenamiento ASA r2

Una relación de pares define las conexiones de red que permiten que los clústeres y las máquinas virtuales (VM) de almacenamiento intercambien datos de forma segura. Cree relaciones de pares entre las VM de almacenamiento de diferentes clústeres para habilitar la protección de datos y la recuperación ante desastres mediante SnapMirror.

"Aprenda más sobre las relaciones entre pares" .

Antes de empezar

Debe haber establecido una relación de pares de clúster entre los clústeres locales y remotos antes de poder crear una relación de pares de VM de almacenamiento. "Crear una relación de pares de clúster" Si aún no lo has hecho.

Pasos

1. En el Administrador del sistema, seleccione **Protección > Descripción general**.
2. En **Pares de máquinas virtuales de almacenamiento**, seleccione **Agregar un par de máquinas virtuales de almacenamiento**.

3. Seleccione la VM de almacenamiento en el clúster local; luego, seleccione la VM de almacenamiento en el clúster remoto.
4. Seleccione **Agregar un par de VM de almacenamiento**.

Configurar la replicación de snapshots

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 instantáneas para un sistema de almacenamiento ASA r2 solo se admite hacia y desde otro sistema de almacenamiento ASA r2. No se pueden replicar instantáneas de un sistema ASA r2 a un sistema ASA, AFF o FAS , ni de un sistema ASA, AFF o FAS a un sistema ASA r2.

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.

A partir de ONTAP 9.17.1, puede aplicar políticas de replicación asincrónica a grupos de consistencia en una relación jerárquica. La replicación asincrónica no es compatible con grupos de consistencia en relaciones jerárquicas en ONTAP 9.16.1.

"Obtenga más información sobre los grupos de consistencia jerárquicos (padre/hijo)" .

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.

Antes de empezar

Los requisitos previos para el peering de clústeres son los mismos para los sistemas ASA r2 que para otros sistemas ONTAP . "Revise los requisitos previos para el peering de clústeres" .

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 personalizada

La política de replicación define cuándo se replican en el sitio remoto las actualizaciones realizadas en el clúster ASA r2. ONTAP incluye varias políticas de protección de datos predefinidas que puede utilizar para sus relaciones de replicación. Si las políticas predefinidas no satisfacen sus necesidades, puede crear una política de replicación personalizada.

Conozca más sobre"políticas de protección de datos de ONTAP predefinidas" .

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. Para el **Tipo de política**, seleccione **Asíncrona**.

   Con la política asíncrona, los datos se copian al sitio remoto después de escribirse en la fuente. La replicación síncrona no es compatible con los sistemas ASA r2.

6. En **Transferir instantáneas desde el origen**, acepte el programa de transferencia predeterminado o seleccione uno diferente.
7. Seleccione esta opción para transferir todas las instantáneas o para crear reglas para determinar qué instantáneas desea transferir.
8. Opcionalmente, habilitar la compresión de red.
9. 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

- "Obtenga más información sobre las políticas de replicación" .

  Cuando crea una relación de replicación, debe seleccionar la política de replicación adecuada para su relación de replicación. Puede utilizar una política predefinida o crear una política personalizada.

- 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. 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.

Conozca las políticas de protección de datos predefinidas de ONTAP

La política de replicación define cuándo las actualizaciones realizadas en el clúster ASA

r2 se replican en el sitio remoto. ONTAP incluye varias políticas de protección de datos predefinidas que puede utilizar para sus relaciones de replicación.

Si las políticas predefinidas no satisfacen sus necesidades, puede"crear una política de replicación personalizada" .

Los sistemas ASA r2 no admiten replicación síncrona.

Los sistemas ASA r2 admiten las siguientes políticas de protección predefinidas.

Política	Descripción	Tipo de póliza
Asincrónico	Una política asincrónica y de bóveda unificada de SnapMirror para reflejar el último sistema de archivos activo e instantáneas diarias y semanales con un programa de transferencia por hora.	Asincrónico
Conmutación por error automatizada dúplex	Política para SnapMirror sincrónico con garantía de RTO cero y replicación de sincronización bidireccional.	Sincronización activa de SnapMirror
Copia de seguridad predeterminada en la nube	Política de bóveda con regla diaria.	Asincrónico
Copia de seguridad diaria	Política de bóveda con una regla diaria y un cronograma de transferencia diario.	Asincrónico
DPDefault	Política asincrónica de SnapMirror para reflejar todas las instantáneas y el último sistema de archivos activo.	Asincrónico
Espejo de todas las instantáneas	Política asincrónica de SnapMirror para reflejar todas las instantáneas y el último sistema de archivos activo.	Asincrónico
ReflejarTodasLasInstantáneasDescartarRed	Política asincrónica de SnapMirror para reflejar todas las instantáneas y el último sistema de archivos activo, excluidas las configuraciones de red.	Asincrónico
Espejo y bóveda	Una política asincrónica y de bóveda unificada de SnapMirror para reflejar el último sistema de archivos activo e instantáneas diarias y semanales.	Asincrónico
Red de descarte de espejo y bóveda	Una política asincrónica y de bóveda unificada de SnapMirror para reflejar el último sistema de archivos activo e instantáneas diarias y semanales, excluidas las configuraciones de red.	Asincrónico
MirrorLatest	Política asincrónica de SnapMirror para reflejar el último sistema de archivos activo.	Asincrónico
Unified7year	Política unificada de SnapMirror con retención de 7 años.	Asincrónico
XDPDefault	Política de bóveda con reglas diarias y semanales.	Asincrónico

Romper una relación de replicación asincrónica en su sistema ASA r2

En determinadas situaciones, es posible que sea necesario romper una relación de replicación asincrónica. Por ejemplo, si está ejecutando ONTAP 9.16.1 y desea aumentar el tamaño de un grupo de consistencia que está en una relación de replicación asincrónica, debe romper la relación antes de poder modificar el tamaño del grupo de consistencia.

Pasos

1. En System Manager, seleccione **Protección > Replicación**.
2. Seleccione **Destinos locales** o **Fuentes locales**.
3. Junto a la relación que deseas romper, selecciona ; luego seleccione **Interrumpir**.
4. Seleccione **Interrumpir**.

Resultado

La relación asincrónica entre el grupo de consistencia primario y secundario está rota.

Configurar la sincronización activa de SnapMirror

Flujo de trabajo de configuración de sincronización activa de SnapMirror

La protección de datos de sincronización activa de ONTAP SnapMirror permite que los servicios empresariales sigan funcionando incluso ante un fallo total del sitio, permitiendo que las aplicaciones conmuten por error de forma transparente mediante una copia secundaria. Con la sincronización activa de SnapMirror , no se requiere intervención manual ni scripts personalizados para activar una conmutación por error.

Si bien los procedimientos del Administrador del sistema para configurar la sincronización activa de SnapMirror son diferentes en los sistemas ASA r2 que en los sistemas NetApp FAS, AFF y ASA que ejecutan la personalidad unificada de ONTAP , los requisitos, la arquitectura y el funcionamiento de la sincronización activa de SnapMirror son los mismos.

"Conozca más sobre las personalidades de ONTAP" .

> A partir de ONTAP 9.18.1, la sincronización activa de SnapMirror es compatible con configuraciones de cuatro nodos. En ONTAP 9.17.1, la sincronización activa de SnapMirror solo es compatible con configuraciones de dos nodos.

"Obtenga más información sobre la sincronización activa de SnapMirror" .

"Obtenga más información sobre la recuperación ante desastres con SnapMirror Active Sync en su sistema ASA r2"

En sistemas ASA r2, la sincronización activa de SnapMirror admite configuraciones simétricas activo/activo. En una configuración simétrica activo/activo, ambos sitios pueden acceder al almacenamiento local para E/S activas.

Obtenga más información sobre "configuraciones simétricas activas/activas" .

Prepárese para configurar la sincronización activa de SnapMirror .

A "Prepárese para configurar la sincronización activa de SnapMirror" En su sistema ASA r2, debe revisar los requisitos previos de configuración, confirmar la compatibilidad con los sistemas operativos host y tener en cuenta los límites de objetos que podrían afectar la configuración específica.

Confirme la configuración de su clúster.

Antes de configurar la sincronización activa de SnapMirror , debe "Confirme que sus clústeres ASA r2 estén en las relaciones de emparejamiento adecuadas y cumplan con otros requisitos de configuración." .

Instalar ONTAP Mediator.

Puede usar ONTAP Mediator u ONTAP Cloud Mediator para supervisar el estado de su clúster y garantizar la continuidad del negocio. Si usa ONTAP Mediator, debe "instalarlo" En su host. Si usa ONTAP Cloud Mediator, puede omitir este paso.

Configure ONTAP Mediator o ONTAP Cloud Mediator utilizando certificados autofirmados.

Usted debe "configurar el mediador de ONTAP o el mediador de nube de ONTAP" antes de poder comenzar a usarlo con SnapMirror Active Sync para la monitorización del clúster.

Configurar la sincronización activa de SnapMirror .

"Configurar la sincronización activa de SnapMirror" para crear una copia de sus datos en un sitio secundario y permitir que sus aplicaciones host conmuten por error de manera automática y transparente en caso de un desastre.

Prepárese para configurar la sincronización activa de SnapMirror en sistemas ASA r2

Para prepararse para configurar la sincronización activa de SnapMirror en su sistema ASA r2, debe revisar los requisitos previos de configuración, confirmar la compatibilidad con los sistemas operativos de sus hosts y tener en cuenta los límites de objetos que podrían afectar la configuración específica.

Pasos

1. Revisar la sincronización activa de SnapMirror "prerrequisitos" .
2. "Confirme que sus sistemas operativos host sean compatibles" para la sincronización activa de SnapMirror .
3. Revisar el "límites de los objetos" que podrían afectar su configuración.
4. Verifique la compatibilidad del protocolo de host con la sincronización activa de SnapMirror en su sistema ASA r2.

   La compatibilidad con la sincronización activa de SnapMirror en sistemas ASA r2 varía según la versión de ONTAP y el protocolo del host.

Comenzando con ONTAP…	La sincronización activa de SnapMirror admite…
9.17.1	• iSCSI • FC • NVMe/FC • NVMe/TCP
9.16.0	• iSCSI • FC

Limitaciones del protocolo NVMe con la sincronización activa de SnapMirror en sistemas ASA r2

Antes de configurar la sincronización activa de SnapMirror en un sistema ASA r2 con hosts NVMe, debe tener en cuenta ciertas limitaciones del protocolo NVMe.

Todas las unidades de almacenamiento NVMe en el subsistema NVMe deben ser miembros del mismo grupo de consistencia y deben ser parte de la misma relación de sincronización activa de SnapMirror .

Los protocolos NVMe/FC y NVMe/TCP son compatibles con la sincronización activa de SnapMirror de la siguiente manera:

- Sólo en clústeres de 2 nodos
- Sólo en hosts ESXi
- Sólo con configuraciones simétricas activas/activas

  Las configuraciones activas/activas asimétricas no son compatibles con hosts NVMe.

La sincronización activa de SnapMirror con NVMe no admite lo siguiente:

- Subsistemas asignados a más de un grupo de consistencia

  Un grupo de consistencia se puede asignar a múltiples subsistemas, pero cada subsistema solo se puede asignar a un grupo de consistencia.

- Expansión de grupos de consistencia en una relación de sincronización activa de SnapMirror
- Asignación de unidades de almacenamiento NVMe que no están en una relación de sincronización activa de SnapMirror a subsistemas replicados
- Eliminar una unidad de almacenamiento de un grupo de consistencia
- Cambio de geometría del grupo de consistencia
- "Transferencia de datos descargados de Microsoft (ODX)"

¿Cuál es el siguiente?

Después de haber completado la preparación necesaria para habilitar la sincronización activa de SnapMirror , debe "Confirme la configuración de su clúster" .

Confirme la configuración de su clúster ASA r2 antes de configurar la sincronización activa de SnapMirror

La sincronización activa de SnapMirror se basa en clústeres emparejados para proteger sus datos en caso de conmutación por error. Antes de configurar la sincronización activa de SnapMirror , debe confirmar que sus clústeres ASA r2 tengan una relación de emparejamiento compatible y cumplan con los demás requisitos de configuración.

Pasos

1. Confirme que existe una relación de peering de clúster entre los clústeres.

   > La sincronización activa de SnapMirror requiere el espacio IP predeterminado para las relaciones entre pares del clúster. No se admite un espacio IP personalizado.

   "Crear una relación de pares de clúster" .

2. Confirme que exista una relación de pares entre las máquinas virtuales de almacenamiento (VM) en cada clúster.

   "Crear una relación de pares de máquinas virtuales de almacenamiento entre clústeres" .

3. Confirme que se cree al menos un LIF en cada nodo del clúster.

   "Crear un LIF".

4. Confirme que las unidades de almacenamiento necesarias estén creadas y asignadas a grupos de host.

   "Crear una unidad de almacenamiento" y "Asignar la unidad de almacenamiento a un grupo de hosts" .

5. Vuelva a escanear el host de la aplicación para descubrir nuevas unidades de almacenamiento.

El futuro

Después de haber confirmado la configuración de su clúster, estará listo para "instalar ONTAP Mediator" .

Instalar ONTAP Mediator en sistemas ASA r2

Para instalar ONTAP Mediator en su sistema ASA r2, debe seguir el mismo procedimiento utilizado para instalar ONTAP Mediator en todos los demás sistemas ONTAP .

La instalación de ONTAP Mediator incluye la preparación de la instalación, la habilitación del acceso a los repositorios, la descarga del paquete de ONTAP Mediator, la verificación de la firma del código, la instalación del paquete en el host y la realización de tareas posteriores a la instalación.

Para instalar ONTAP Mediator, siga "este flujo de trabajo"

El futuro

Después de instalar ONTAP Mediator, debe: "Configurar ONTAP Mediator mediante certificados autofirmados" .

Configurar ONTAP Mediator o ONTAP Cloud Mediator en sistemas ASA r2

Debe configurar ONTAP Mediator u ONTAP Cloud Mediator antes de poder usar la sincronización activa de SnapMirror para la monitorización de clústeres. Tanto ONTAP Mediator como ONTAP Cloud Mediator proporcionan un almacenamiento persistente y protegido para los metadatos de alta disponibilidad (HA) que utilizan los clústeres de ONTAP en una relación de sincronización activa de SnapMirror . Además, ambos mediadores ofrecen una función de consulta síncrona del estado del nodo para facilitar la determinación del quórum y sirven como proxy de ping para detectar la actividad del controlador.

Antes de empezar

Si está utilizando ONTAP Cloud Mediator, verifique que su sistema ASA r2 cumpla con los requisitos necesarios "prerrequisitos" .

Pasos

1. En el Administrador del sistema, seleccione **Protección > Descripción general**.
2. En el panel derecho, bajo **Mediadores**, seleccione **Agregar un mediador**.
3. Seleccione el **Tipo de mediador**.
4. Para un mediador en la nube, introduzca el ID de la organización, el ID del cliente y el secreto del cliente. Para un mediador local, introduzca la dirección IP, el puerto, el nombre de usuario y la contraseña del mediador.
5. Seleccione el par del clúster de la lista de pares del clúster elegibles o seleccione **Agregar un par del clúster** para agregar uno nuevo.
6. Agregue la información del certificado
   - Si está utilizando un certificado autofirmado, copie el contenido del `intermediate.crt` archivo y péguelo en el campo **Certificado**, o seleccione **Importar** para navegar hasta el `intermediate.crt` archivo e importar la información del certificado.
   - Si está utilizando un certificado de terceros, ingrese la información del certificado en el campo **Certificado**.
7. Seleccione **Agregar**.

El futuro

Después de haber inicializado el mediador, puede "configurar la sincronización activa de SnapMirror" para crear una copia de sus datos en un sitio secundario y permitir que sus aplicaciones host conmuten por error de manera automática y transparente en caso de un desastre.

Configurar la sincronización activa de SnapMirror en sistemas ASA r2

Configure la sincronización activa de SnapMirror para crear una copia de sus datos en un sitio secundario y permitir que sus aplicaciones host conmuten por error de manera automática y transparente en caso de un desastre.

En sistemas ASA r2, la sincronización activa de SnapMirror admite configuraciones simétricas activo/activo. En una configuración simétrica activo/activo, ambos sitios pueden acceder al almacenamiento local para E/S activas.

Si utiliza el protocolo iSCSI o FC y utiliza herramientas ONTAP para VMware Sphere, puede opcionalmente "Utilice ONTAP Tools para VMware para configurar la sincronización activa de SnapMirror" .

Antes de empezar

"Crear un grupo de consistencia" En el sitio principal con nuevas unidades de almacenamiento. Si desea crear una configuración simétrica no uniforme, cree también un grupo de consistencia en el sitio secundario con nuevas unidades de almacenamiento.

Obtenga más información sobre "no uniforme" configuraciones simétricas activas/activas.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Coloque el cursor sobre el nombre del grupo de consistencia que desea proteger con la sincronización activa de SnapMirror .
3. Seleccionar ⋮ y luego seleccione **Proteger**.
4. En **Protección remota**, selecciona **Replicar a un clúster remoto**.
5. Seleccione un par de clúster existente o elija **Agregar uno nuevo**.
6. Seleccione la máquina virtual de almacenamiento.
7. Para la política de replicación, seleccione **AutomatedFailOverDuplex**.
8. Si está creando una configuración activa/activa simétrica no uniforme, seleccione **Configuración de destino**; luego ingrese el nombre del nuevo grupo de consistencia de destino que cree antes de comenzar este procedimiento.
9. Seleccione **Guardar**.

Resultado

La sincronización activa de SnapMirror está configurada para proteger sus datos para que pueda continuar con las operaciones con un objetivo de punto de recuperación (RPO) cercano a cero y un objetivo de tiempo de recuperación (RTO) cercano a cero en caso de un desastre.

Administrar la sincronización activa de SnapMirror

Reconfigurar ONTAP Mediator u ONTAP Cloud Mediator para usar un certificado de terceros en sistemas ASA r2

Si configura ONTAP Mediator o ONTAP Cloud Mediator con un certificado autofirmado, puede reconfigurar el mediador para usar un certificado de terceros. Es posible que su organización prefiera o requiera certificados de terceros por razones de seguridad.

Paso 1: Eliminar la configuración del mediador

Para reconfigurar el mediador, primero debe eliminar su configuración actual del clúster.

Pasos

1. En el Administrador del sistema, seleccione **Protección > Descripción general**.
2. En el panel derecho, en **Mediadores**, seleccione ⋮ junto al par del clúster con la configuración del mediador que desea eliminar, luego seleccione **Eliminar**.

Si tiene varios mediadores instalados y desea eliminar todas las configuraciones, seleccione ⋮ junto a **Mediadores**; luego seleccione **Eliminar**.

3. Seleccione **Eliminar** para confirmar que desea eliminar la configuración del mediador.

Paso 2: Eliminar el certificado autofirmado

Después de eliminar la configuración del mediador, debe eliminar el certificado autofirmado asociado del clúster.

Pasos

1. Seleccione **Cluster > Settings**.
2. En **Seguridad**, seleccione **Certificados**.
3. Seleccione el certificado que desea eliminar.
4. ⋮ Seleccione ; y, a continuación, seleccione **Eliminar**.

Paso 3: Reinstale el mediador con un certificado de terceros

Después de eliminar el certificado autofirmado asociado, puede volver a configurar el mediador con el certificado de terceros.

Pasos

1. Seleccione **Protección > Descripción general**.
2. En el panel derecho, en **Mediadores**, seleccione **Agregar un mediador**.
3. Seleccione el **Tipo de mediador**.
4. Para un mediador en la nube, introduzca el ID de la organización, el ID del cliente y el secreto del cliente. Para un mediador **local**, ingrese la dirección IP, el puerto, el nombre de usuario del mediador y la contraseña del mediador.
5. Seleccione un par del clúster de la lista de pares del clúster elegibles o seleccione **Agregar un par del clúster** para agregar uno nuevo.
6. En **Certificado**, ingrese la información del certificado de terceros.
7. Seleccione **Agregar**.

Resultado

El ONTAP Mediator o el ONTAP Cloud Mediator se reconfigura para utilizar el certificado de terceros. Ahora puede utilizar el mediador para administrar las relaciones de sincronización activa de SnapMirror .

Realizar una conmutación por error planificada de clústeres ASA r2 en una relación de sincronización activa de SnapMirror

La sincronización activa de SnapMirror ofrece disponibilidad continua para aplicaciones críticas para el negocio mediante la creación de una copia de sus datos en un sitio secundario y la conmutación por error automática y transparente de sus aplicaciones host en caso de desastre. Es posible que necesite realizar una conmutación por error planificada de su relación de sincronización activa de SnapMirror para probar el proceso de conmutación por error o para realizar tareas de mantenimiento en el sitio principal.

Antes de empezar

- La relación de sincronización activa de SnapMirror debe estar sincronizada.
- No se puede iniciar una conmutación por error planificada cuando hay en proceso una operación no disruptiva, como el traslado de una unidad de almacenamiento.
- ONTAP Mediator o ONTAP Cloud Mediator debe estar configurado, conectado y en quórum.

Pasos

1. Seleccione **Protección > Replicación**.
2. Seleccione la relación de sincronización activa de SnapMirror que desea conmutar por error.
3. Seleccionar ⋮ ; luego seleccione **Conmutación por error**.

Lo siguiente

Utilice el `snapmirror failover show` comando en la interfaz de línea de comandos (CLI) de ONTAP para monitorear el estado de la conmutación por error.

Restablezca la relación de sincronización activa de SnapMirror después de una conmutación por error no planificada de sus clústeres ASA r2

En los sistemas ASA r2, SnapMirror active sync admite configuraciones activas/activas simétricas. En una configuración activa/activa simétrica ambos sitios pueden acceder al almacenamiento local para E/S activas. Si el clúster de origen falla o se aísla, el mediador activa una conmutación por error automática no planificada (AUFO) y sirve todas las E/S del clúster de destino hasta que el clúster de origen se recupere.

Si experimentas un AUFO de tu relación de sincronización activa SnapMirror, deberías restablecer la relación y reanudar las operaciones en el clúster de origen después de que vuelva a estar en línea.

Antes de empezar

- La relación de sincronización activa de SnapMirror debe estar sincronizada.
- No se puede iniciar una conmutación por error planificada cuando hay en proceso una operación no disruptiva, como el traslado de una unidad de almacenamiento.
- El mediador de ONTAP debe estar configurado, conectado y en quórum.
- Para recuperar rutas de E/S perdidas o actualizar estados de rutas de E/S en sus hosts, debe realizar un nuevo escaneo del adaptador/almacenamiento en los hosts después de que el clúster de almacenamiento principal reanude su operación.

Pasos

1. Seleccione **Protección > Replicación**.
2. Seleccione la relación de sincronización activa de SnapMirror que necesita restablecer.
3. Espere hasta que el estado de la relación muestre **InSync**.
4. Seleccionar ⋮ ; luego seleccione **Conmutación por error** para reanudar las operaciones en el clúster primario original.

Eliminar una relación de sincronización activa de SnapMirror en su sistema ASA r2

Si ya no necesita RPO y RTO cercanos a cero para una aplicación comercial, debe eliminar la protección de sincronización activa de SnapMirror eliminando la relación de sincronización activa de SnapMirror asociada. Si está ejecutando ONTAP 9.16.1 en un

sistema ASA r2, es posible que también deba eliminar la relación de sincronización activa de SnapMirror antes de poder realizar ciertos cambios de geometría en los grupos de consistencia en una relación de sincronización activa de SnapMirror .

Paso 1: Finalizar la replicación del host

Si el grupo de hosts del clúster de origen se replica en el clúster de destino y los grupos de consistencia de destino se asignan al grupo de hosts replicado, debe finalizar la replicación de host en el clúster de origen antes de poder eliminar la relación de sincronización activa de SnapMirror .

Pasos

1. En System Manager, seleccione **Host**.
2. Junto a un host que contiene el grupo de hosts que desea dejar de replicar, seleccione ⋮ y luego seleccione **Editar**.
3. Anule la selección de **Replicar configuración de host** y, a continuación, seleccione **Actualizar**.

Paso 2: Eliminar la relación de sincronización activa de SnapMirror

Para eliminar la protección de sincronización activa de SnapMirror de un grupo de consistencia, debe eliminar la relación de sincronización activa de SnapMirror .

Pasos

1. En System Manager, seleccione **Protección > Replicación**.
2. Seleccione **Destinos locales** o **Fuentes locales**.
3. Junto a la relación de sincronización activa de SnapMirror que desea eliminar, seleccione ⋮ ; luego seleccione **Eliminar**.
4. Seleccione **Liberar las instantáneas base del grupo de consistencia de origen**.
5. Seleccione **Eliminar**.

Resultado

Se elimina la relación de sincronización activa de SnapMirror y se liberan las instantáneas base del grupo de consistencia de origen. Las unidades de almacenamiento del grupo de consistencia ya no están protegidas por la sincronización activa de SnapMirror .

El futuro

"Configurar la replicación de snapshots"para copiar el grupo de consistencia a una ubicación geográficamente remota para realizar copias de seguridad y recuperación ante desastres.

Elimine ONTAP Mediator u ONTAP Cloud Mediator de su sistema ASA r2

Solo puede usar un tipo de mediador a la vez para la sincronización activa de SnapMirror en su sistema ASA r2. Si decide cambiar su tipo de mediador, deberá eliminar su instancia actual antes de instalar otra instancia.

Pasos

Debe utilizar la interfaz de línea de comandos (CLI) de ONTAP para eliminar ONTAP Mediator o ONTAP Cloud Mediator.

Mediador de ONTAP

1. Eliminar el mediador de ONTAP :

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   Ejemplo:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

Mediador de la nube de ONTAP

1. Eliminar ONTAP Cloud Mediator:

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   Ejemplo:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Información relacionada

- "eliminar mediador de snapmirror"

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 coherencia

Obtenga información sobre los grupos de consistencia de ONTAP en los sistemas de almacenamiento ASA r2

Un grupo de consistencia es una colección de unidades de almacenamiento que se administran como una sola unidad. Utilice grupos de consistencia para una gestión simplificada del almacenamiento.

Por ejemplo, supongamos que tiene una base de datos que consta de 10 unidades de almacenamiento en un grupo de consistencia y necesita realizar una copia de seguridad de toda la base de datos. En lugar de realizar una copia de seguridad de cada unidad de almacenamiento, puede realizar una copia de seguridad de toda la base de datos simplemente agregando protección de datos de instantáneas al grupo de consistencia. Realizar una copia de seguridad de las unidades de almacenamiento como un grupo de consistencia en lugar de hacerlo individualmente también proporciona una copia de seguridad consistente de todas las unidades, mientras que realizar una copia de seguridad de las unidades individualmente podría crear potencialmente inconsistencias.

A partir de ONTAP 9.16.1, puede usar el Administrador del sistema para crear grupos de consistencia jerárquicos en su sistema ASA r2. En una estructura jerárquica, uno o más grupos de consistencia se configuran como hijos de un grupo de consistencia padre.

Los grupos de coherencia jerárquicos le permiten aplicar políticas Snapshot individuales a cada grupo de coherencia secundario y replicar las snapshots de todos los grupos de coherencia secundarios en un clúster remoto como una sola unidad mediante la replicación del elemento primario. De esta forma se simplifica la protección y la gestión de datos para estructuras de datos complejas. Por ejemplo, suponga que crea un grupo de consistencia primario llamado `SVM1_app` que contiene dos grupos de consistencia secundarios: `SVM1app_data` Para los datos de la aplicación y `SVM1app_logs` para los registros de la aplicación. Se realizan Snapshots de `SVM1app_data` cada 15 minutos y se realizan Snapshots de `SVM1app_logs` cada hora. El grupo de coherencia primario `SVM1_app`, tiene una política SnapMirror que replica las copias Snapshot de `SVM1app_data` tanto como `SVM1app_logs` en un clúster remoto cada 24 horas. El grupo de coherencia primario `SVM1_app` se administra como una unidad única y los grupos de coherencia secundarios se gestionan como unidades independientes.

Grupos de consistencia en relaciones de replicación

A partir de ONTAP 9.17.1, puede realizar los siguientes cambios de geometría en los grupos de consistencia en una relación de replicación asincrónica o en una relación de sincronización activa de SnapMirror sin interrumpir ni eliminar la relación. Cuando se produce un cambio de geometría en el grupo de consistencia principal, el cambio se replica en el grupo de consistencia secundario.

- "Modificar el tamaño de una unidad de almacenamiento"añadiendo o quitando unidades de almacenamiento.
- "Promover un único grupo de consistencia"a un grupo de consistencia padre.
- "Degradar un grupo de consistencia principal"a un solo grupo de consistencia.
- "Separar un grupo de consistencia secundario"de un grupo de consistencia padre.
- "Cree un grupo de consistencia secundario"utilizando un grupo de consistencia existente.

En ONTAP 9.16.1, debe"romper la relación de replicación asincrónica" y"eliminar la relación de sincronización

activa de SnapMirror" antes de realizar cambios de geometría en el grupo de consistencia.

Proteja los grupos de consistencia en su sistema ASA r2 con instantáneas

Cree instantáneas de los grupos de consistencia en su sistema de almacenamiento ASA r2 para proteger los datos en las unidades de almacenamiento que forman parte del grupo de consistencia. Si ya no necesita proteger los datos en ninguna de las unidades de almacenamiento del grupo de consistencia, puede eliminar la protección de instantáneas del grupo de consistencia.

Si ya no necesita proteger los datos de unidades de almacenamiento específicas en el grupo de consistencia, puede eliminar esas unidades de almacenamiento del grupo de consistencia.

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 **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.

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.

Modificar el tamaño de los grupos de consistencia en su sistema ASA r2

Aumente o disminuya el tamaño de un grupo de consistencia modificando la cantidad de unidades de almacenamiento en el grupo de consistencia.

Añada unidades de almacenamiento a un grupo de consistencia

Amplíe la cantidad de almacenamiento administrado por un grupo de consistencia agregando unidades de almacenamiento nuevas o existentes al grupo de consistencia.

A partir de ONTAP 9.18.1, puede configurar la reserva de instantáneas y la eliminación automática de instantáneas para limitar la cantidad de espacio utilizado por las instantáneas en sus unidades de almacenamiento. Cuando se agrega una unidad de almacenamiento a un grupo de consistencia existente, la reserva de instantáneas y la eliminación automática de instantáneas se configuran de la siguiente manera de forma predeterminada.

Si añades…	El porcentaje de reserva de instantánea está configurado en…	La eliminación automática de instantáneas es…
Nuevas unidades de almacenamiento	0	Desactivado
Unidades de almacenamiento existentes	Sin alterar	Sin alterar

Puede modificar la configuración predeterminada de las nuevas unidades de almacenamiento al crearlas. También puedes"modificar las unidades de almacenamiento existentes" para actualizar su configuración actual.

"Obtenga más información sobre la reserva de instantáneas en los sistemas de almacenamiento ASA r2.".

Antes de empezar

Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia que desea expandir está en una relación de sincronización activa de SnapMirror , debe"eliminar la relación de sincronización activa de SnapMirror" antes de poder agregar unidades de almacenamiento. Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia está en una relación de replicación asincrónica, debe"romper la relación" antes de poder expandir el grupo de consistencia. No es necesario eliminar la relación de sincronización activa de SnapMirror ni romper la relación asincrónica antes de expandir un grupo de consistencia en ONTAP 9.17.1 y versiones posteriores.

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 creará con la misma capacidad y el mismo sistema operativo host. Para asignar una capacidad diferente a cada unidad, seleccione **Agregar 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

Elimine una unidad de almacenamiento de un grupo de consistencia para borrarla, administrarla como parte de un grupo de consistencia diferente o dejar de proteger sus datos. Eliminar una unidad de almacenamiento de un grupo de consistencia rompe la relación entre la unidad de almacenamiento y el grupo de consistencia, pero no 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 grupos de consistencia en su sistema ASA r2

Si ya no necesita 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 que estaban anteriormente en el grupo permanecen activas en el clúster. Si el grupo de consistencia estaba en una relación de replicación, las copias replicadas permanecen en el clúster remoto.

Antes de empezar

Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia que desea eliminar está en una relación de sincronización activa de SnapMirror , debe"eliminar la relación de sincronización activa de SnapMirror" antes de eliminar el grupo de consistencia. No es necesario eliminar esta relación antes de modificar un grupo de consistencia en ONTAP 9.17.1 y versiones posteriores.

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.

Administrar grupos de consistencia jerárquica en su sistema ASA r2

A partir de ONTAP 9.16.1, puede usar el Administrador del sistema para crear grupos de consistencia jerárquicos en su sistema ASA r2. En una estructura jerárquica, uno o más

grupos de consistencia se configuran como hijos de un grupo de consistencia padre. Puede aplicar políticas de instantáneas individuales a cada grupo de consistencia secundario y replicar las instantáneas de todos los grupos de consistencia secundarios a un clúster remoto como una sola unidad replicando el grupo primario. Esto simplifica la protección y gestión de datos para estructuras de datos complejas.

Promocionar un grupo de consistencia existente a un grupo de consistencia principal

Si promueve un grupo de consistencia existente a padre, se crea un nuevo grupo de consistencia hijo y las unidades de almacenamiento que pertenecen al grupo de consistencia promocionado se mueven al nuevo grupo de consistencia hijo. Las unidades de almacenamiento no se pueden asociar directamente con un grupo de consistencia principal.

Antes de empezar

Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia que desea promover está en una relación de sincronización activa de SnapMirror , debe"eliminar la relación de sincronización activa de SnapMirror" antes de que se pueda promover el grupo de consistencia. Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia está en una relación de replicación asincrónica, debe"romper la relación" antes de poder promover el grupo de consistencia. No es necesario eliminar la relación de sincronización activa de SnapMirror ni romper la relación asincrónica antes de promover un grupo de consistencia en ONTAP 9.17.1 y versiones posteriores.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón por el grupo de consistencia que desea convertir en un grupo de consistencia primario.
3. Seleccione ; y, a continuación, seleccione **Promocionar al grupo de consistencia primario**.
4. Ingrese un nombre para el nuevo grupo de consistencia secundario o acepte el nombre predeterminado; luego seleccione el tipo de componente del grupo de consistencia.
5. Selecciona **Promocionar**.

El futuro

Puede crear grupos de consistencia secundarios adicionales dentro del grupo de consistencia principal. También puedes"configurar la replicación de snapshots" para copiar los grupos de consistencia padre e hijo a una ubicación geográficamente remota para realizar copias de seguridad y recuperación ante desastres.

Degrade un grupo de consistencia primario a un grupo de consistencia único

Cuando se degrada un grupo de consistencia principal a un solo grupo de consistencia, las unidades de almacenamiento de los grupos de consistencia secundarios asociados se agregan al grupo de consistencia principal. Los grupos de consistencia secundarios se eliminan y el grupo de consistencia principal se administra como un solo grupo de consistencia.

Antes de empezar

Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia que desea degradar está en una relación de sincronización activa de SnapMirror , debe"eliminar la relación de sincronización activa de SnapMirror" antes de que el grupo de consistencia pueda ser degradado. Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia está en una relación de replicación asincrónica, debe"romper la relación" antes de poder degradar el grupo de consistencia. No es necesario eliminar la relación de sincronización activa de SnapMirror ni romper la relación asincrónica antes de expandir un grupo de consistencia en ONTAP 9.17.1 y versiones posteriores.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón por el grupo de consistencia primario que desea degradar.
3. Seleccione ⋮; y, a continuación, seleccione **Descender a un único grupo de consistencia**.
4. Selecciona **Descender**

El futuro

"Añada una política de Snapshot" al grupo de coherencia degradado para proteger las unidades de almacenamiento que se gestionaron anteriormente por los grupos de coherencia secundarios.

Cree un grupo de consistencia secundario

La creación de grupos de consistencia secundarios le permite aplicar políticas de instantáneas individuales a cada secundario. A partir de ONTAP 9.17.1, también puede aplicar políticas de replicación individuales directamente a cada hijo. En ONTAP 9.16.1, las políticas de replicación solo se pueden aplicar en el nivel principal.

Puede crear un grupo de consistencia secundario a partir de un grupo de consistencia nuevo o existente.

Desde un nuevo grupo de consistencia

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Pase el ratón por el grupo de consistencia primario al que desea añadir un grupo de consistencia secundario.
3. Seleccione ⋮; y, a continuación, seleccione **Agregar un nuevo grupo de consistencia hijo**.
4. Introduzca un nombre para el grupo de consistencia secundario o acepte el nombre predeterminado y, a continuación, seleccione el tipo de componente del grupo de consistencia.
5. Seleccione esta opción para agregar unidades de almacenamiento existentes al grupo de consistencia hijo o para crear nuevas unidades de almacenamiento.

   Si crea nuevas unidades de almacenamiento, introduzca la cantidad de unidades que desea crear y la capacidad por unidad; a continuación, introduzca la información del host.

   Si se crea más de una unidad de almacenamiento, 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**.

6. Seleccione **Agregar**.

Desde un grupo de consistencia existente

Antes de empezar

Si el grupo de consistencia que desea utilizar ya es hijo de otro grupo de consistencia, debe"separarlo del grupo de consistencia principal existente" antes de poder moverlo a un nuevo grupo de consistencia principal.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Seleccione el grupo de consistencia existente que desea convertir en un grupo de consistencia secundario.
3. Seleccione ⋮; y, a continuación, seleccione **Mover bajo grupo de consistencia diferente**.
4. Introduzca un nombre nuevo para el grupo de consistencia secundario o acepte el nombre predeterminado y, a continuación, seleccione el tipo de componente del grupo de consistencia.
5. Seleccione el grupo de consistencia existente que desea que sea el grupo de consistencia primario o seleccione para crear un nuevo grupo de consistencia primario.

   Si selecciona crear un nuevo grupo de consistencia primario, introduzca un nombre para el grupo de consistencia primario o acepte el nombre predeterminado y, a continuación, seleccione el tipo de componente de aplicación de consistencia.

6. Selecciona **Mover**.

El futuro

Después de crear un grupo de consistencia secundario, puede"aplique políticas de protección de snapshots individuales" a cada grupo de consistencia infantil. También puedes"configurar políticas de replicación" en los grupos de consistencia padre e hijo para replicar los grupos de consistencia en una ubicación remota.

Desvincular un grupo de consistencia secundario de un grupo de consistencia primario

Cuando se separa un grupo de consistencia secundario de un grupo de consistencia principal, el grupo de consistencia secundario se elimina del grupo de consistencia principal y se administra como un solo grupo de consistencia. La política de replicación aplicada al padre ya no se aplica al grupo de consistencia secundario separado.

Antes de empezar

Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia que desea separar está en una relación de sincronización activa de SnapMirror , debe"eliminar la relación de sincronización activa de SnapMirror" antes de que se pueda separar el grupo de consistencia. Si está ejecutando ONTAP 9.16.1 y el grupo de consistencia está en una relación de replicación asincrónica, debe"romper la relación" antes de poder separar el grupo de consistencia. No es necesario eliminar la relación de sincronización activa de SnapMirror ni romper la relación asincrónica antes de expandir un grupo de consistencia en ONTAP 9.17.1 y versiones posteriores.

Pasos

1. En System Manager, seleccione **Protección > Grupos de consistencia**.
2. Seleccione el grupo de consistencia primario.
3. Seleccione el grupo de consistencia secundario que desea desvincular.
4. Seleccione ⋮; y, a continuación, seleccione **Desasociar de padre**.
5. Introduzca un nuevo nombre para el grupo de consistencia que desea desvincular o acepte el nombre predeterminado; a continuación, seleccione el tipo de aplicación del grupo de consistencia.
6. Seleccione **Detach**.

El futuro

"Configure una política de replicación"para replicar las instantáneas del grupo de consistencia secundario separado en un clúster remoto.

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.

En los sistemas ASA r2, los SED solo son compatibles con SSD basados en NVMe.

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.

Migre las claves de cifrado de datos de ONTAP entre gestores de claves de su sistema ASA R2

Puede gestionar las claves de cifrado de datos mediante el administrador de claves incorporado de ONTAP en el sistema ASA R2 o un gestor de claves externo (o ambos). Solo es posible habilitar los administradores de claves externos en el nivel de máquina virtual de almacenamiento. En el nivel de clúster de ONTAP, es posible habilitar el gestor de claves incorporado o un gestor de claves externo.

Si habilita su gestor de claves en…	Puede usar…
Solo a nivel de cluster	Puede usar el gestor de claves incorporado o un gestor de claves externo
Solo a nivel de máquina virtual de almacenamiento	Solo un gestor de claves externo

Si habilita su gestor de claves en…	Puede usar…
Tanto el clúster como el nivel de la máquina virtual de almacenamiento	Una de las siguientes combinaciones de gestor de claves: • Opción 1 Nivel de clúster: Gestor de claves incorporado Nivel de máquina virtual de almacenamiento: Administrador de claves externo • Opción 2 Nivel de clúster: Gestor de claves externo Nivel de máquina virtual de almacenamiento: Administrador de claves externo

Migre claves entre gestores de claves en el nivel del clúster de ONTAP

A partir de ONTAP 9.16.1, puede utilizar la interfaz de línea de comandos (CLI) de ONTAP para migrar claves entre gestores de claves en el nivel del clúster.

De a bordo a externo

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Cree una configuración del gestor de claves externo inactivo:

```
security key-manager external create-config
```

3. Cambie al gestor de claves externo:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type KMIP
```

4. Elimine la configuración del gestor de claves incorporado:

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type OKM
```

5. Configure el nivel de privilegio en admin:

```
set -privilege admin
```

De externo a incorporado

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Cree una configuración de gestor de claves incorporada inactiva:

```
security key-manager onboard create-config
```

3. Habilite la configuración del gestor de claves incorporado:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type OKM
```

4. Elimine la configuración del gestor de claves externo

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type KMIP
```

5. Configure el nivel de privilegio en admin:

```
set -privilege admin
```

Migrar claves entre los administradores de claves en todo el clúster de ONTAP y los niveles de máquina virtual de almacenamiento

Puede usar la interfaz de línea de comandos (CLI) de ONTAP para migrar claves entre el administrador de claves en el nivel del clúster y un administrador de claves en el nivel de máquina virtual de almacenamiento.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Migrar las claves:

```
security key-manager key migrate -from-vserver <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. Configure el nivel de privilegio en admin:

```
set -privilege admin
```

Protéjase contra ataques de ransomware

Cree instantáneas a prueba de manipulaciones para protegerse contra ataques de ransomware en los 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".

Habilite la protección autónoma contra ransomware con IA en sus sistemas de almacenamiento ASA r2

A partir de ONTAP 9.17.1, puede usar la Protección Autónoma contra Ransomware con Inteligencia Artificial (ARP/IA) para proteger los datos de su sistema ASA r2. ARP/IA detecta rápidamente posibles amenazas de ransomware, crea automáticamente una instantánea de ARP para proteger sus datos y muestra un mensaje de advertencia en el Administrador del Sistema para alertarle sobre actividad sospechosa.

ARP mejora la ciberresiliencia al adoptar un modelo de aprendizaje automático para el análisis antiransomware que detecta formas de ransomware en constante evolución con un 98% de precisión para entornos SAN. El modelo de aprendizaje automático de ARP está preentrenado con un gran conjunto de datos de archivos tanto antes como después de un ataque de ransomware simulado. Este entrenamiento intensivo en recursos se realiza fuera de ONTAP, y el modelo preentrenado que resulta de este entrenamiento se incluye en la caja con ONTAP. Este modelo no es accesible ni modificable. ARP/AI está activo inmediatamente después de la habilitación; no hay "período de aprendizaje".

> Ningún sistema de detección o prevención de ransomware puede garantizar completamente la seguridad frente a un ataque de ransomware. Aunque un ataque podría pasar desapercibido, ARP/AI actúa como una capa adicional importante de defensa si el software anti-virus no detecta una intrusión.

Acerca de esta tarea

- El soporte ARP/AI está incluido en el "Licencia ONTAP One" .
- ARP/AI no es compatible con unidades de almacenamiento protegidas por SnapMirror active sync, SnapMirror synchronous o SnapLock.
- A partir de ONTAP 9.18.1, ARP/AI se activa por defecto en todas las unidades de almacenamiento recién creadas 12 horas después de actualizar a ONTAP 9.18.1 o de inicializar un nuevo clúster ASA r2 de

ONTAP 9.18.1.

- Después de haber habilitado ARP/AI, debe "Habilite las actualizaciones automáticas para sus archivos de seguridad" para recibir automáticamente nuevas actualizaciones de seguridad.

Habilita ARP/AI en todas las unidades de almacenamiento del clúster

Si estás ejecutando ONTAP 9.17.1, puedes activar ARP/AI en todas las unidades de almacenamiento creadas en el clúster por defecto.

En ONTAP 9.18.1 y versiones posteriores, ARP/AI está habilitado por defecto en todas las unidades de almacenamiento nuevas. Si tienes unidades de almacenamiento creadas en ONTAP 9.17.1 para las que ARP/AI no está habilitado, puedes habilitarlo manualmente.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Junto a **Anti-ransomware**, selecciona ⋮ y luego selecciona **Habilitar en todas las unidades de almacenamiento existentes**.
3. Seleccione **Habilitar**.

Habilitar ARP/AI en todas las unidades de almacenamiento en una máquina virtual de almacenamiento

Si estás ejecutando ONTAP 9.17.1, puedes habilitar ARP/AI en todas las unidades de almacenamiento creadas en una máquina virtual de almacenamiento (VM) por defecto. Esto significa que cualquier unidad de almacenamiento nueva creada en la VM de almacenamiento tendrá ARP/AI habilitado automáticamente. También puedes aplicar ARP/AI a las unidades de almacenamiento existentes en la VM de almacenamiento.

En ONTAP 9.18.1 y versiones posteriores, ARP/AI está habilitado por defecto en todas las unidades de almacenamiento nuevas. Si tienes unidades de almacenamiento creadas en ONTAP 9.17.1 para las que ARP/AI no está habilitado, puedes habilitarlo manualmente.

Pasos

1. En el Administrador del sistema, seleccione **Clúster > Máquinas virtuales de almacenamiento**.
2. Seleccione la máquina virtual de almacenamiento en la que desea habilitar ARP/AI.
3. En la sección **Seguridad**, junto a **Anti-ransomware**, seleccione ⋮ ; luego seleccione **Editar configuración anti-ransomware**.
4. Seleccione **Habilitar anti-ransomware**.

   Esto habilita ARP/AI en todas las unidades de almacenamiento futuras creadas en la máquina virtual de almacenamiento seleccionada de forma predeterminada.

5. Para aplicar ARP a las unidades de almacenamiento existentes en la máquina virtual de almacenamiento seleccionada, seleccione **Aplicar este cambio a todas las unidades de almacenamiento existentes aplicables en esta máquina virtual de almacenamiento**.
6. Seleccione **Guardar**.

Resultado

Todas las nuevas unidades de almacenamiento que cree en la máquina virtual de almacenamiento están protegidas de forma predeterminada contra ataques de ransomware, y se le informa de cualquier actividad sospechosa en el Administrador del sistema.

Habilitar ARP/AI en unidades de almacenamiento específicas en una máquina virtual de almacenamiento

Si estás ejecutando ONTAP 9.17.1 y no quieres activar ARP/AI en todas las unidades de almacenamiento de una storage VM, puedes seleccionar las unidades específicas que quieras activar.

En ONTAP 9.18.1 y versiones posteriores, ARP/AI está habilitado por defecto en todas las unidades de almacenamiento nuevas. Si tienes unidades de almacenamiento creadas en ONTAP 9.17.1 para las que ARP/AI no está habilitado, puedes habilitarlo manualmente.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Seleccione las unidades de almacenamiento para las que desea habilitar ARP/AI.
3. Seleccionar ⋮ ; luego seleccione **Habilitar anti-ransomware**.
4. Seleccione **Habilitar**.

Resultado

Las unidades de almacenamiento que usted seleccionó están protegidas contra ataques de ransomware y cualquier actividad sospechosa se le informa en el Administrador del sistema.

Desactiva la protección autónoma contra ransomware predeterminada en tus sistemas de almacenamiento ASA r2

Cuando inicializas un nuevo clúster ASA r2 de ONTAP 9.18.1 o actualizas tu clúster a ONTAP 9.18.1, ARP/AI se habilita automáticamente por defecto en todas las unidades de almacenamiento nuevas después de un periodo de gracia de 12 horas. Si no desactivas ARP/AI durante el periodo de gracia, se habilita en todo el clúster para las unidades de almacenamiento nuevas cuando termina el periodo de gracia.

Las unidades de almacenamiento creadas en ONTAP 9.17.1 deben ser "activado manualmente" para ARP/AI.

Pasos

Puedes desactivar la activación por defecto durante o después del periodo de gracia inicial de 12 horas.

System Manager

1. Seleccione **Cluster > Settings**.
2. Desactiva ARP:
   - Para desactivar durante el periodo de gracia de 12 horas:
     i. En **Anti-ransomware**, selecciona **No activar** y luego selecciona **Desactivar**.
   - Para desactivar después del periodo de gracia de 12 horas:
     i. En **Anti-ransomware**, selecciona y luego desmarca **Activar para nuevas unidades de almacenamiento**.
     ii. Selecciona **Guardar**

CLI

1. Verifica el estado de habilitación predeterminado:

```
security anti-ransomware auto-enable show
```

2. Desactiva la activación por defecto para volúmenes existentes y nuevos:

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Modificar los períodos de retención de instantáneas de ARP/AI en los sistemas de almacenamiento ASA r2

Si la Protección Autónoma contra Ransomware con Inteligencia Artificial (ARP/IA) detecta actividad anormal en una o más unidades de almacenamiento de su sistema ASA r2, crea automáticamente una instantánea de ARP para proteger los datos de la unidad. Según su capacidad de almacenamiento y las necesidades de su negocio, podría querer aumentar o reducir el periodo de retención predeterminado de las instantáneas de ARP. Por ejemplo, podría querer aumentar el periodo de retención de las aplicaciones críticas para la empresa para, si es necesario, disponer de periodos de retención más largos para la recuperación de datos, o bien, podría querer reducir el periodo de retención de las aplicaciones no críticas para ahorrar espacio de almacenamiento.

El período de retención predeterminado para la instantánea de ARP varía según la acción que realice en respuesta a la actividad anormal.

Si realiza esta acción…	Las instantáneas ARP se conservan de forma predeterminada durante…
Marcar como falso positivo	12 horas
Marcar como posible ataque de ransomware	7 días

Si realiza esta acción…	Las instantáneas ARP se conservan de forma predeterminada durante…
No tome medidas inmediatas	10 días

Los períodos de retención predeterminados se pueden modificar mediante la interfaz de línea de comandos (CLI) de ONTAP . Consulte "Modificar las opciones para las instantáneas automáticas de ONTAP" para conocer los pasos para cambiar el período de retención predeterminado.

Responda a la protección autónoma contra ransomware con alertas de IA en los sistemas de almacenamiento ASA r2

Si la Protección Autónoma contra Ransomware con Inteligencia Artificial (ARP/IA) detecta actividad anormal en una o más unidades de almacenamiento de su sistema ASA r2, se generará una advertencia en el panel del Administrador del Sistema. Debe revisar la advertencia, verificar la actividad y, si es necesario, tomar medidas para detener cualquier posible amenaza a sus datos.

Si se muestra un mensaje de advertencia de ARP/AI, antes de actuar, debe usar el verificador de integridad de la aplicación adecuado para verificar la integridad de los datos en la unidad de almacenamiento. Verificar la integridad de los datos de la unidad de almacenamiento le ayuda a determinar si la actividad es aceptable o si se trata de un posible ataque de ransomware.

Si la actividad anormal es…	Entonces haz esto…
Aceptable	Marcar la actividad como falso positivo.
Un posible ataque de ransomware	Marcar la actividad como un posible ataque de ransomware.
Indeterminado	No actúe de inmediato. Supervise la unidad de almacenamiento hasta por 7 días. Si la unidad de almacenamiento continúa funcionando con normalidad, marque la actividad como falso positivo. Si la unidad de almacenamiento continúa mostrando actividad anormal, marque la actividad como un posible ataque de ransomware.

Pasos

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

   Si ARP ha detectado actividad anormal en una o más unidades de almacenamiento, aparece un mensaje en **Advertencias**.

2. Seleccione el mensaje de advertencia.
3. En **Descripción general de eventos**, seleccione el mensaje **Advertencias** que indica la cantidad de unidades de almacenamiento con actividad anormal.
4. En **Unidades de almacenamiento con actividad anormal**, seleccione la unidad de almacenamiento.
5. Seleccione **Seguridad**.

   Si hay actividad anormal en la unidad de almacenamiento, se muestra un mensaje debajo de **Anti-ransomware**.

6. Seleccione **Elegir una acción**.
7. Seleccione **Marcar como falso positivo** o seleccione **Marcar como posible ataque de ransomware**.

El futuro

Si sabes de aumentos repentinos en la actividad de tu unidad de almacenamiento, ya sea un aumento puntual o uno que sea característico de una nueva normalidad, deberías reportarlos como seguros. Reportar manualmente estos aumentos como seguros ayuda a mejorar la precisión de las evaluaciones de amenazas de ARP. Aprende cómo "informar los aumentos de ARP/AI conocidos".

Pause o reanude la protección autónoma contra ransomware con IA en sus sistemas de almacenamiento ASA r2

A partir de ONTAP 9.17.1, puede usar la Protección Autónoma contra Ransomware con Inteligencia Artificial (ARP/IA) para proteger los datos de su sistema ASA r2. Si planea un evento inusual en su carga de trabajo, puede suspender temporalmente el análisis de ARP/IA para evitar detecciones de falsos positivos de ataques de ransomware. Una vez finalizado el evento, puede reanudar el análisis de ARP/IA.

Pausa ARP/AI

Antes de comenzar un evento de carga de trabajo inusual, es posible que deba suspender temporalmente el análisis ARP/AI para evitar detecciones de falsos positivos de ataques de ransomware.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Seleccione las unidades de almacenamiento para las que desea pausar ARP/AI.
3. Seleccione **Pausar anti-ransomware**.

Resultado

El análisis de ARP/AI se pausa para las unidades de almacenamiento seleccionadas y no se le informa ninguna actividad sospechosa en el Administrador del sistema hasta que reanude ARP/AI.

Reanudar ARP/AI

Si pausa ARP/AI durante una carga de trabajo inusual, una vez completada la carga de trabajo, debe reanudarla para proteger sus datos contra ataques de ransomware.

Pasos

1. En System Manager, seleccione **Almacenamiento**.
2. Seleccione las unidades de almacenamiento para las que desea reanudar ARP/AI.
3. Seleccione **Reanudar anti-ransomware**.

Resultado

Se reanuda el análisis de posibles ataques de ransomware y se le informa sobre cualquier actividad sospechosa en el Administrador del sistema.

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.

Proteja las conexiones IP en sus sistemas de almacenamiento ASA R2

Si utiliza el protocolo IP en su sistema ASA R2, puede configurar la seguridad IP (IPsec) para mejorar la seguridad de sus datos. IPSec es un estándar de Internet que proporciona cifrado de datos en tránsito, autenticación para el tráfico que fluye entre los puntos finales de red a nivel de IP y protección contra ataques de reinyección y de intermediario malintencionados contra sus datos.

Para los sistemas ASA R2, IPsec está disponible para hosts iSCSI y NVMe/TCP.

En ciertos sistemas ASA R2, varias de las operaciones criptográficas, como el cifrado y las comprobaciones de integridad, pueden descargarse a una tarjeta de controladora de interfaz de red (NIC) compatible. El rendimiento de las operaciones descargadas en la tarjeta NIC es aproximadamente del 5% o menos. Esto puede mejorar significativamente el rendimiento y el rendimiento del tráfico de red protegido por IPsec.

A partir de ONTAP 9.18.1, la descarga de hardware de IPsec compatible se extiende al tráfico IPv6.

Las siguientes tarjetas NIC son compatibles con la descarga de hardware en los siguientes sistemas ASA r2 y versiones de ONTAP :

Tarjeta NIC compatible	Sistemas ASA r2	Versión ONTAP
X50135A (controlador Ethernet 2p, 40G/100G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.17.1 y posteriores

Tarjeta NIC compatible	Sistemas ASA r2	Versión ONTAP
X60135A (controlador Ethernet 2p, 40G/100G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.17.1 y posteriores
X50131A - (controlador Ethernet 2P, 40G/100g/200g/400G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.16.1 y posteriores
X60132A - (controlador Ethernet 4p, 10G/25G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 y posteriores

Ver el"NetApp Hardware Universe" Para obtener más información sobre los sistemas y tarjetas compatibles.

El futuro

IPsec se configura en su sistema ASA r2 de la misma manera que en otros sistemas ONTAP . Para obtener más información, consulte "Prepárese para configurar la seguridad IP para la red ONTAP.".