Use ONTAP para gestionar sus datos

ASA r2

NetApp
September 26, 2024

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

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

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

Pasos

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

3. Introduzca el número de unidades que desea crear.

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

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

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

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

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

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

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

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

7. Seleccione **Agregar**.

El futuro

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

Si quiere más información

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

Añada iniciadores de host

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

Antes de empezar

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

Añada iniciadores de host para los hosts SCSI o NVMe.

Hosts SCSI

Pasos

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

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

5. Añada hosts nuevos o existentes.

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

6. Seleccione **Agregar**.

El futuro

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

Hosts NVMe

Pasos

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

El futuro

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

almacenamiento.

Cree grupos de hosts

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

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

Pasos

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

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

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

El futuro

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

Asignar la unidad de almacenamiento a un host

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

Pasos

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

El futuro

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

Completar el aprovisionamiento en el lado del host

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

Pasos

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

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

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

El futuro

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

Si quiere más información

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

Clone datos en sistemas de almacenamiento R2 de ASA

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

Clonar unidades de almacenamiento

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

Pasos

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

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

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

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

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

7. Seleccione **Clonar**.

El futuro

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

Clonar grupos de consistencia

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

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

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

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

Clone mediante instantánea local

Pasos

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

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

8. Seleccione **Clonar**.

Clone mediante instantánea remota

Pasos

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

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

El futuro

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

El futuro

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

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

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

Aumente la capacidad

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

Modificar las asignaciones de hosts

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

Modifique la política de calidad de servicio

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

- Límite de rendimiento de calidad de servicio

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

- Garantía de rendimiento de calidad de servicio

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

Pasos

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

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

El futuro

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

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

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

Antes de empezar

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

Pasos

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

El futuro

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

Límites de almacenamiento de ASA R2

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

Los sistemas ASA R2 ofrecen lo siguiente:

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

Si quiere más información

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

Proteja sus datos

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

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

Paso 1: Opcionalmente, cree un grupo de consistencia

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

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

Utilice nuevas unidades de almacenamiento

Pasos

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

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

El futuro

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

Utilice las unidades de almacenamiento existentes

Pasos

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

El futuro

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

Paso 2: Crear una instantánea

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

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

Tipos de Snapshot

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

almacenamiento.

- Snapshots bajo demanda

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

- Snapshots automatizadas

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

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

Snapshot de un grupo de coherencia

Pasos

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

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

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

      El destino remoto usa la etiqueta de SnapMirror.

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

   a. Seleccione una política de Snapshot.

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

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

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

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

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

7. Seleccione **Guardar**.

Instantánea de la unidad de almacenamiento

Pasos

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

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

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

   El destino remoto usa la etiqueta de SnapMirror.

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

   a. Seleccione una política de Snapshot.

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

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

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

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

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

7. Seleccione **Guardar**.

El futuro

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

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

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

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

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

Paso 1: Crear una relación de paridad entre clústeres

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

Pasos

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

El futuro

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

Paso 2: Opcionalmente, cree una política de replicación

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

Pasos

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

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

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

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

6. Seleccione **Guardar**.

El futuro

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

Si quiere más información

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

Paso 3: Crear una relación de replicación

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

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

Antes de empezar

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

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

Con instantáneas bloqueadas

Pasos

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

   Debe seleccionar una política de replicación *vault*.

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

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

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

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

11. Seleccione **Guardar**.

Sin instantáneas bloqueadas

Pasos

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

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

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

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

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

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

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

6. Seleccione **Guardar**.

El futuro

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

Paso 4: Pruebe la conmutación por error de replicación

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

Pasos

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

El futuro

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

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

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

Si quiere más información

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

Restauración de los datos en sistemas de almacenamiento R2 de ASA

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

Restaure un grupo de consistencia

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

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

Restaurar desde una instantánea local

Pasos

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

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

Restaurar desde una snapshot remota

Pasos

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

Resultado

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

Restaurar una unidad de almacenamiento

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

Pasos

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

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

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

Resultado

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

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

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

Añade protección de datos de snapshot a un grupo de coherencia

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

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

Pasos

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

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

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

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

6. Seleccione **Editar**.

El futuro

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

Quite la protección de datos Snapshot de un grupo de coherencia

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

Pasos

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

Resultado

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

Añada unidades de almacenamiento a un grupo de consistencia

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

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

Agregue unidades de almacenamiento existentes

Pasos

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

Añada nuevas unidades de almacenamiento

Pasos

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

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

6. Seleccione **Expandir**.

Lo siguiente

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

El futuro

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

Quitar una unidad de almacenamiento de un grupo de consistencia

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

Pasos

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

Resultado

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

El futuro

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

Eliminar un grupo de consistencia

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

Antes de empezar

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

Pasos

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

El futuro

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

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

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

Crear una nueva programación de políticas de protección

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

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

Pasos

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

El futuro

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

Crear una política de Snapshot

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

Pasos

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

El futuro

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

Aplicar una política Snapshot a un grupo de coherencia

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

Pasos

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

instantánea.

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

El futuro

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

Editar, eliminar o deshabilitar una política de Snapshot

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

Pasos

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

Resultado

Ha modificado, eliminado o deshabilitado la política de snapshots.

Editar una política de replicación

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

Pasos

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

Resultado

Modificó la política de replicación.

Proteja sus datos

Cifrado de datos estáticos en sistemas de almacenamiento R2 de ASA

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

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

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

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

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

Pasos

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

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

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

El futuro

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

Protéjase contra ataques de ransomware en sistemas de almacenamiento ASA R2

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

ransomware.

Inicialice el reloj de SnapLock Compliance

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

Pasos

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

¿Cuál es el siguiente?

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

Proteja las conexiones NVMe en sus sistemas de almacenamiento ASA R2

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

Pasos

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

Resultado

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