Protección de datos con la bóveda cibernética de ONTAP

NetApp data management solutions

NetApp
August 18, 2025

Tabla de contenidos

Protección de datos con la bóveda cibernética de ONTAP

Descripción general de la bóveda cibernética de ONTAP

La principal amenaza que impulsa la implementación de una bóveda cibernética es la creciente prevalencia y la creciente sofisticación de los ciberataques, en particular el ransomware y las violaciones de datos. "Con el aumento del phishing" y métodos cada vez más sofisticados de robo de credenciales; las credenciales utilizadas para iniciar un ataque de ransomware podrían luego usarse para acceder a sistemas de infraestructura. En estos casos, incluso los sistemas de infraestructura más reforzados corren el riesgo de sufrir ataques. La única defensa contra un sistema comprometido es tener sus datos protegidos y aislados en una bóveda cibernética.

La bóveda cibernética basada en ONTAP de NetApp ofrece a las organizaciones una solución integral y flexible para proteger sus activos de datos más críticos. Al aprovechar la separación de aire lógica con metodologías de refuerzo robustas, ONTAP le permite crear entornos de almacenamiento seguros y aislados que son resistentes a las amenazas cibernéticas en evolución. Con ONTAP, puede garantizar la confidencialidad, integridad y disponibilidad de sus datos manteniendo la agilidad y eficiencia de su infraestructura de almacenamiento.

> A partir de julio de 2024, el contenido de los informes técnicos publicados anteriormente en formato PDF se integrará con la documentación del producto ONTAP . Además, los nuevos informes técnicos (TR) como este documento ya no recibirán números de TR.

¿Qué es una bóveda cibernética?

Una bóveda cibernética es una técnica específica de protección de datos que implica almacenar datos críticos en un entorno aislado, separado de la infraestructura de TI principal.

Repositorio de datos "air-gapped", **inmutable** e **indeleble** que es inmune a las amenazas que afectan a la red principal, como malware, ransomware o incluso amenazas internas. Es posible crear una bóveda cibernética con instantáneas **inmutables** e **indelebles**.

Las copias de seguridad con espacio de aire que utilizan métodos tradicionales implican la creación de espacio y la separación física de los medios primarios y secundarios. Al trasladar los medios fuera del sitio y/o cortar la conectividad, los actores maliciosos no tienen acceso a los datos. Esto protege los datos pero puede generar tiempos de recuperación más lentos.

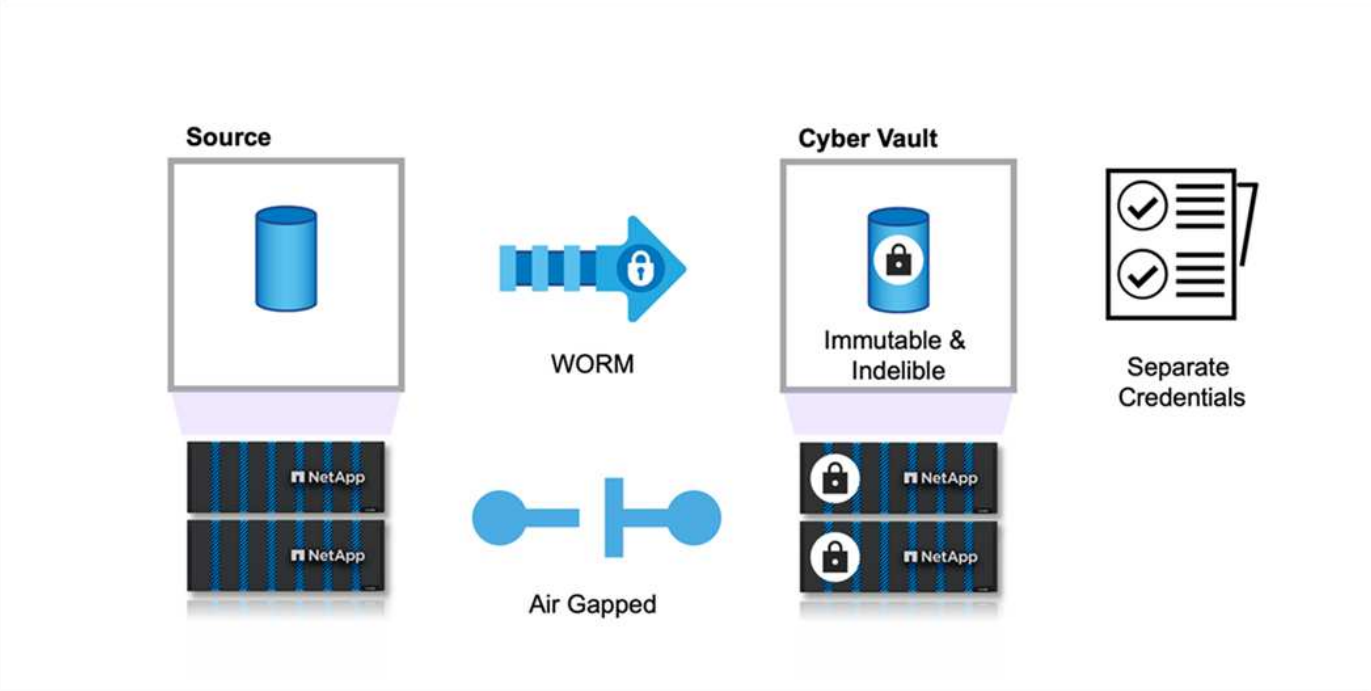
El enfoque de NetApp para la bóveda cibernética

Las características clave de la arquitectura de referencia de NetApp para una bóveda cibernética incluyen:

- Infraestructura de almacenamiento segura y aislada (por ejemplo, sistemas de almacenamiento con espacio de aire)
- Las copias de los datos deben ser **inmutables** e **indelebles** sin excepción
- Controles de acceso estrictos y autenticación multifactor
- Capacidades de restauración rápida de datos

Puede utilizar el almacenamiento de NetApp con ONTAP como una bóveda cibernética aislada aprovechando"SnapLock Compliance para proteger copias de instantáneas con WORM" . Puede realizar todas las tareas básicas de SnapLock Compliance en Cyber Vault. Una vez configurados, los volúmenes de Cyber Vault se protegen automáticamente, lo que elimina la necesidad de confirmar manualmente las copias Snapshot en WORM. Puede encontrar más información sobre el entrehierro lógico en este"blog"

SnapLock Compliance se utiliza para cumplir con las regulaciones bancarias y financieras SEC 70-a-4(f), FINRA 4511(c) y CFTC 1.31(c)-(d). Cohasset Associates ha certificado que cumple con estas regulaciones (informe de auditoría disponible a pedido). Al utilizar SnapLock Compliance con esta certificación, usted obtiene un mecanismo reforzado para aislar sus datos, en el que confían las instituciones financieras más grandes del mundo para asegurar tanto la retención como la recuperación de registros bancarios.



Terminología de Cyber Vault ONTAP

Éstos son los términos comúnmente utilizados en las arquitecturas de bóvedas cibernéticas.

Protección autónoma contra ransomware (ARP): la función de protección autónoma contra ransomware (ARP) utiliza el análisis de la carga de trabajo en entornos NAS (NFS y SMB) para detectar y advertir de forma proactiva y en tiempo real sobre actividad anormal que podría indicar un ataque de ransomware. Cuando se sospecha de un ataque, ARP también crea nuevas copias de Snapshot, además de la protección existente contra copias de Snapshot programadas. Para obtener más información, consulte la"Documentación de ONTAP sobre la protección autónoma contra ransomware"

Espacio de aire (lógico): puede configurar el almacenamiento de NetApp con ONTAP como una bóveda cibernética lógica con espacio de aire aprovechando"SnapLock Compliance para proteger copias de instantáneas con WORM"

Espacio de aire (físico): un sistema con espacio de aire físico no tiene conectividad de red. Al utilizar copias de seguridad en cinta, puede mover las imágenes a otra ubicación. El espacio de aire lógico de SnapLock Compliance es tan robusto como un sistema con espacio de aire físico.

Host bastión: una computadora dedicada en una red aislada, configurada para resistir ataques.

Copias instantáneas inmutables: copias instantáneas que no se pueden modificar, sin excepción (incluida una organización de soporte o la capacidad de formatear a bajo nivel el sistema de almacenamiento).

Copias instantáneas indelebles: copias instantáneas que no se pueden eliminar, sin excepción (incluida una organización de soporte o la capacidad de formatear a bajo nivel el sistema de almacenamiento).

Copias instantáneas a prueba de manipulaciones: las copias instantáneas a prueba de manipulaciones utilizan la función de reloj de SnapLock Compliance para bloquear las copias instantáneas durante un período específico. Ningún usuario ni el soporte de NetApp pueden eliminar estas instantáneas bloqueadas. Puede utilizar copias de instantáneas bloqueadas para recuperar datos si un volumen se ve comprometido por un ataque de ransomware, malware, pirata informático, administrador deshonesto o eliminación accidental. Para obtener más información, consulte la"Documentación de ONTAP sobre copias instantáneas a prueba de manipulaciones"

- SnapLock* - SnapLock es una solución de cumplimiento de alto rendimiento para organizaciones que utilizan almacenamiento WORM para conservar archivos sin modificaciones con fines regulatorios y de gobernanza. Para obtener más información, consulte "Documentación de ONTAP sobre SnapLock" .
- SnapMirror* - SnapMirror es una tecnología de replicación de recuperación ante desastres, diseñada para replicar datos de manera eficiente. SnapMirror puede crear un espejo (o copia exacta de los datos), una bóveda (una copia de los datos con una retención de copia Snapshot más prolongada) o ambos en un sistema secundario, en las instalaciones o en la nube. Estas copias se pueden usar para muchos propósitos diferentes, como en caso de desastre, enviarlas a la nube o como bóveda cibernética (cuando se utiliza la política de bóveda y se bloquea la bóveda). Para obtener más información, consulte la"Documentación de ONTAP sobre SnapMirror"
- SnapVault* - En ONTAP 9.3, SnapVault quedó obsoleto y se optó por configurar SnapMirror mediante la política de bóveda o bóveda espejo. Este término, aunque todavía se utiliza, también ha caído en desuso. Para obtener más información, consulte "Documentación de ONTAP sobre SnapVault" .

Dimensionamiento de bóvedas cibernéticas con ONTAP

Para dimensionar una bóveda cibernética es necesario comprender cuántos datos será necesario restaurar en un Objetivo de tiempo de recuperación (RTO) determinado. Hay muchos factores que intervienen a la hora de diseñar correctamente una solución de bóveda cibernética del tamaño adecuado. Al dimensionar una bóveda cibernética se debe tener en cuenta tanto el rendimiento como la capacidad.

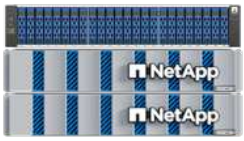
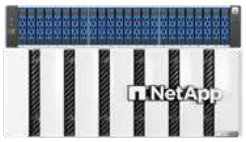
Consideraciones sobre el dimensionamiento del rendimiento

1. ¿Cuáles son los modelos de plataforma de origen (FAS v AFF A-Series v AFF C-Series)?
2. ¿Cuál es el ancho de banda y la latencia entre la fuente y la bóveda cibernética?
3. ¿Qué tamaño tienen los archivos y cuántos archivos?
4. ¿Cuál es su objetivo de tiempo de recuperación?
5. ¿Cuántos datos es necesario recuperar dentro del RTO?
6. ¿Cuántas relaciones de fanáticos de SnapMirror absorberá la bóveda cibernética?
7. ¿Habrá una o varias recuperaciones al mismo tiempo?
8. ¿Esas recuperaciones múltiples se producirán en la misma etapa primaria?

9. ¿ SnapMirror se replicará en la bóveda durante una recuperación desde una bóveda?

Ejemplos de tallas

A continuación se muestran ejemplos de diferentes configuraciones de bóvedas cibernéticas.

Platform	AFF A1K	AFF C400	AFF C250	FAS70
Estimated RTO (100TB)	5 HR	18 HR	24 HR	24> HR
Relative cost	High	Moderate	Low	Ultra Low

Consideraciones sobre el tamaño de la capacidad

La cantidad de espacio en disco necesaria para un volumen de destino de bóveda cibernética de ONTAP depende de diversos factores, el más importante de los cuales es la tasa de cambio de los datos en el volumen de origen. Tanto la programación de copias de seguridad como la programación de instantáneas en el volumen de destino afectan el uso del disco en el volumen de destino, y no es probable que la tasa de cambio en el volumen de origen sea constante. Es una buena idea proporcionar un buffer de capacidad de almacenamiento adicional al que se requiere para acomodar cambios futuros en el comportamiento del usuario final o de la aplicación.

Para dimensionar una relación para 1 mes de retención en ONTAP es necesario calcular los requisitos de almacenamiento en función de varios factores, incluidos el tamaño del conjunto de datos principal, la tasa de cambio de los datos (tasa de cambio diaria) y los ahorros de deduplicación y compresión (si corresponde).

A continuación se muestra el enfoque paso a paso:

El primer paso es conocer el tamaño de los volúmenes de origen que está protegiendo con la bóveda cibernética. Esta es la cantidad base de datos que se replicarán inicialmente en el destino de la bóveda cibernética. A continuación, estime la tasa de cambio diaria para el conjunto de datos. Este es el porcentaje de datos que cambia cada día. Es fundamental tener una buena comprensión de cuán dinámicos son sus datos.

Por ejemplo:

- Tamaño del conjunto de datos principal = 5 TB
- Tasa de cambio diaria = 5% (0,05)
- Eficiencia de deduplicación y compresión = 50% (0,50)

Ahora, veamos el cálculo:

- Calcular la tasa de cambio de datos diaria:

```
Changed data per day = 5000 * 5% = 250GB
```

- Calcular el total de datos modificados durante 30 días:

```
Total changed data in 30 days = 250 GB * 30 = 7.5TB
```

- Calcular el almacenamiento total requerido:

```
TOTAL = 5TB + 7.5TB = 12.5TB
```

- Aplicar ahorros de deduplicación y compresión:

```
EFFECTIVE = 12.5TB * 50% = 6.25TB
```

Resumen de las necesidades de almacenamiento

- Sin eficiencia: se necesitarían **12,5 TB** para almacenar 30 días de datos de la bóveda cibernética.
- Con un 50% de eficiencia: se requerirían **6,25 TB** de almacenamiento después de la deduplicación y la compresión.

> Las copias instantáneas pueden tener un costo adicional debido a los metadatos, pero esto suele ser menor.

> Si se realizan varias copias de seguridad por día, ajuste el cálculo según la cantidad de copias instantáneas tomadas cada día.

> Tenga en cuenta el crecimiento de los datos a lo largo del tiempo para garantizar que el tamaño esté preparado para el futuro.

Creación de una bóveda cibernética con ONTAP

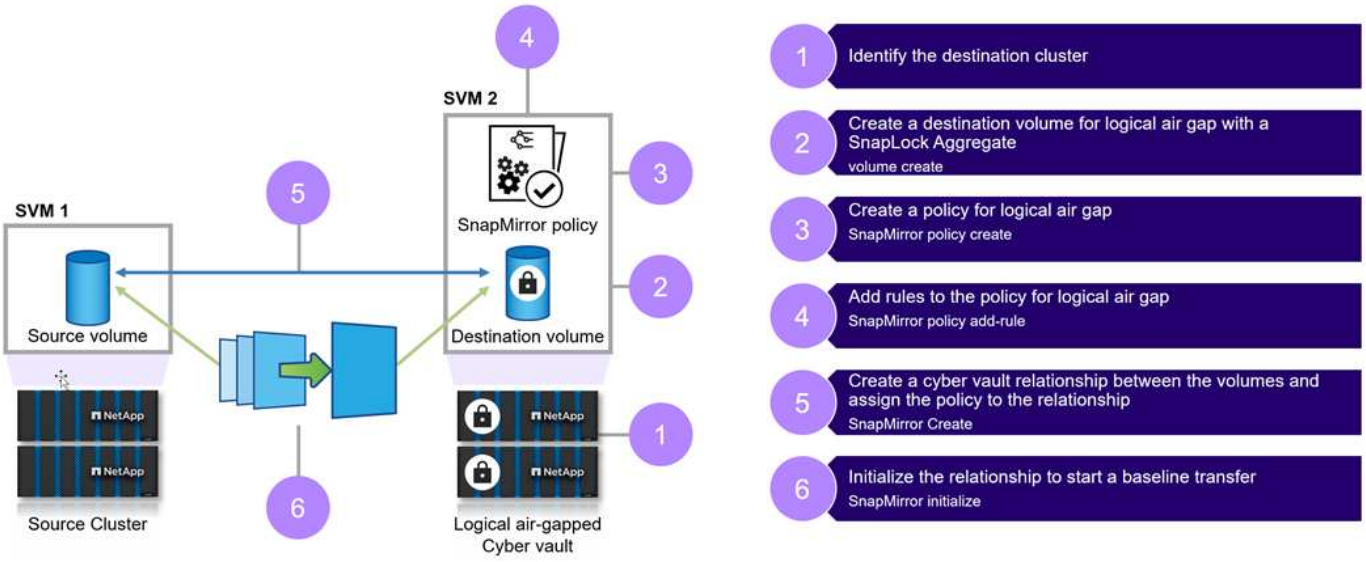
Los pasos a continuación le ayudarán a crear una bóveda cibernética con ONTAP.

Antes de empezar

- El clúster de origen debe ejecutar ONTAP 9 o posterior.
- Los agregados de origen y destino deben ser de 64 bits.
- Los volúmenes de origen y destino se deben crear en clústeres emparejados con SVM emparejados. Para obtener más información, consulte "Peering de clúster" .
- Si el crecimiento automático del volumen está deshabilitado, el espacio libre en el volumen de destino debe ser al menos un cinco por ciento mayor que el espacio utilizado en el volumen de origen.

Acerca de esta tarea

La siguiente ilustración muestra el procedimiento para inicializar una relación de bóveda de SnapLock Compliance :



Pasos

1. Identifique la matriz de destino que se convertirá en la bóveda cibernética para recibir los datos aislados.
2. En la matriz de destino, para preparar la bóveda cibernética,"instalar la licencia de ONTAP One" ,"inicializar el reloj de cumplimiento" , y, si está utilizando una versión de ONTAP anterior a 9.10.1,"crear un agregado de SnapLock Compliance" .
3. En la matriz de destino, cree un volumen de destino de SnapLock Compliance del tipo DP:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
   -snaplock-type compliance|enterprise -type DP -size size
   ```

4. A partir de ONTAP 9.10.1, los volúmenes SnapLock y no SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado SnapLock separado si está usando ONTAP 9.10.1. Usas el volumen `-snaplock-type` Opción para especificar un tipo de cumplimiento. En versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock , Compliance, se hereda del agregado. No se admiten volúmenes de destino con versiones flexibles. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

   El siguiente comando crea un volumen de SnapLock Compliance de 2 GB llamado `dstvolB` en `SVM2` en el agregado `node01_aggr` :

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr
   -snaplock-type compliance -type DP -size 2GB
   ```

5. En el clúster de destino, para crear el espacio de aire, configure el período de retención predeterminado, como se describe en"Establecer el período de retención predeterminado" . A un volumen SnapLock que es un destino de bóveda se le asigna un período de retención predeterminado. El valor para este período se establece inicialmente en un mínimo de 0 años y un máximo de 100 años (a partir de ONTAP 9.10.1. Para versiones anteriores de ONTAP , el valor es 0 - 70) para volúmenes de SnapLock Compliance . Cada copia de NetApp Snapshot se confirma con este período de retención predeterminado al principio. Se debe cambiar el período de retención predeterminado. El período de retención puede extenderse posteriormente, si es necesario, pero nunca acortarse. Para obtener más información, consulte "Descripción general del tiempo de retención establecido" .

Los proveedores de servicios deben considerar las fechas de finalización del contrato del cliente al determinar el período de retención. Por ejemplo, si el período de retención de la bóveda cibernética es de 30 días y el contrato del cliente finaliza antes de que expire el período de retención, los datos de la bóveda cibernética no se podrán eliminar hasta que expire el período de retención.

6. "Crear una nueva relación de replicación"entre la fuente que no es SnapLock y el nuevo destino SnapLock que creó en el Paso 3.

   Este ejemplo crea una nueva relación SnapMirror con el volumen de destino SnapLock dstvolB utilizando una política de XDPDefault para almacenar copias de instantáneas etiquetadas diariamente y semanalmente según un cronograma por hora:

   ```
   cluster2::> snapmirror create -source-path SVM1:srcvolA -destination-path
   SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
   ```

   "Crear una política de replicación personalizada"o una"horario personalizado" Si los valores predeterminados disponibles no son adecuados.

7. En la SVM de destino, inicialice la relación SnapVault creada en el paso 5:

   ```
   snapmirror initialize -destination-path destination_path
   ```

8. El siguiente comando inicializa la relación entre el volumen de origen srcvolA en SVM1 y el volumen de destino dstvolB en SVM2:

   ```
   cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

9. Una vez inicializada e inactiva la relación, utilice el comando snapshot show en el destino para verificar el tiempo de expiración de SnapLock aplicado a las copias de Snapshot replicadas.

   Este ejemplo enumera las copias de instantáneas en el volumen dstvolB que tienen la etiqueta SnapMirror y la fecha de vencimiento de SnapLock :

   ```
   cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields snapmirror-
   label, snaplock-expiry-time
   ```

Refuerzo de la bóveda cibernética

Estas son las recomendaciones adicionales para fortalecer una bóveda cibernética de ONTAP . Consulte la guía de endurecimiento de ONTAP a continuación para obtener más recomendaciones y procedimientos.

Recomendaciones para reforzar las bóvedas cibernéticas

- Aislar los planos de gestión de la bóveda cibernética
- No habilite los LIF de datos en el clúster de destino, ya que son un vector de ataque adicional
- En el clúster de destino, limite el acceso LIF entre clústeres al clúster de origen con una política de servicio
- Segmente el LIF de administración en el clúster de destino para un acceso limitado con una política de servicio y un host bastión

- Restrinja todo el tráfico de datos desde el clúster de origen a la bóveda cibernética para permitir solo los puertos necesarios para el tráfico de SnapMirror
- Siempre que sea posible, deshabilite cualquier método de acceso de administración innecesario dentro de ONTAP para disminuir la superficie de ataque.
- Habilitar el registro de auditoría y el almacenamiento de registros remotos
- Habilite la verificación de múltiples administradores y requiera la verificación de un administrador externo a sus administradores de almacenamiento habituales (por ejemplo, personal de CISO)
- Implementar controles de acceso basados en roles
- Requerir autenticación administrativa multifactor para System Manager y ssh
- Utilice autenticación basada en token para scripts y llamadas API REST

Por favor consulte la"Guía de endurecimiento de ONTAP" ,"Descripción general de la verificación de múltiples administradores" y"Guía de autenticación multifactor de ONTAP" para saber cómo llevar a cabo estos pasos de endurecimiento.

Interoperabilidad de bóvedas cibernéticas

El hardware y el software de ONTAP se pueden utilizar para crear una configuración de bóveda cibernética.

Recomendaciones de hardware de ONTAP

Todas las matrices físicas unificadas de ONTAP se pueden utilizar para la implementación de una bóveda cibernética.

- El almacenamiento híbrido FAS ofrece la solución más rentable.
- La serie C de AFF ofrece el consumo de energía y la densidad más eficientes.
- AFF A-Series es la plataforma de mayor rendimiento que ofrece el mejor RTO. Con el reciente anuncio de nuestra última Serie AFF A, esta plataforma ofrecerá la mejor eficiencia de almacenamiento sin comprometer el rendimiento.

Recomendaciones de software de ONTAP

A partir de ONTAP 9.14.1, puede especificar períodos de retención para etiquetas SnapMirror específicas en la política SnapMirror de la relación SnapMirror de modo que las copias de Snapshot replicadas desde el volumen de origen al volumen de destino se conserven durante el período de retención especificado en la regla. Si no se especifica ningún período de retención, se utiliza el período de retención predeterminado del volumen de destino.

A partir de ONTAP 9.13.1, puede restaurar instantáneamente una copia de Snapshot bloqueada en el volumen SnapLock de destino de una relación de bóveda SnapLock creando un FlexClone con la opción snaplock-type establecida en "non-snaplock" y especificando la copia de Snapshot como la "instantánea principal" al ejecutar la operación de creación de clon de volumen. Obtenga más información sobre "creando un volumen FlexClone con un tipo SnapLock" .

Configuración de MetroCluster

Para las configuraciones de MetroCluster , debe tener en cuenta lo siguiente:

- Puede crear una relación SnapVault solo entre SVM de origen de sincronización, no entre un SVM de origen de sincronización y un SVM de destino de sincronización.
- Puede crear una relación SnapVault desde un volumen en un SVM de origen de sincronización a un SVM de servicio de datos.
- Puede crear una relación SnapVault desde un volumen en un SVM de servicio de datos a un volumen DP en un SVM de origen de sincronización.

Preguntas frecuentes sobre Cyber Vault

Estas preguntas frecuentes están dirigidas a los clientes y socios de NetApp . Responde preguntas frecuentes sobre la arquitectura de referencia de bóveda cibernética basada en ONTAP de NetApp.

¿Qué es una bóveda cibernética de NetApp ?

La bóveda cibernética es una técnica específica de protección de datos que implica almacenar datos en un entorno aislado, separado de la infraestructura de TI principal.

Cyber Vault es un repositorio de datos "aislado", inmutable e indeleble que es inmune a las amenazas que afectan a los datos primarios, como malware, ransomware o amenazas internas. Se puede lograr una bóveda cibernética con copias Snapshot inmutables de NetApp ONTAP y hacerla indeleble con NetApp SnapLock Compliance. Mientras está bajo la protección de SnapLock Compliance , los datos no se pueden modificar ni eliminar, ni siquiera por los administradores de ONTAP o el soporte de NetApp .

Las copias de seguridad con espacio de aire que utilizan métodos tradicionales implican la creación de espacio y la separación física de los medios primarios y secundarios. La separación de aire con una bóveda cibernética incluye el uso de una red de replicación de datos separada fuera de las redes de acceso a datos estándar para replicar copias instantáneas en un destino indeleble.

Otros pasos más allá de las redes con espacio de aire implican deshabilitar todos los protocolos de acceso y replicación de datos en la bóveda cibernética cuando no sean necesarios. Esto evita el acceso a los datos o la exfiltración de datos en el sitio de destino. Con SnapLock Compliance, no se requiere separación física. SnapLock Compliance protege sus copias Snapshot almacenadas, en un punto en el tiempo y de solo lectura, lo que da como resultado una recuperación rápida de datos que es segura contra la eliminación y es inmutable.

El enfoque de NetApp para la bóveda cibernética

La bóveda cibernética de NetApp , impulsada por SnapLock, proporciona a las organizaciones una solución integral y flexible para proteger sus activos de datos más críticos. Al aprovechar las tecnologías de refuerzo en ONTAP, NetApp le permite crear una bóveda cibernética aislada, segura y con espacio de aire que es inmune a las amenazas cibernéticas en evolución. Con NetApp, puede garantizar la confidencialidad, integridad y disponibilidad de sus datos manteniendo la agilidad y la eficiencia de su infraestructura de almacenamiento.

Las características clave de la arquitectura de referencia de NetApp para una bóveda cibernética incluyen:

- Infraestructura de almacenamiento segura y aislada (por ejemplo, sistemas de almacenamiento con espacio de aire)
- Las copias de seguridad de sus datos son inmutables e indelebles
- Controles de acceso estrictos y separados, verificación de múltiples administradores y autenticación multifactor

- Capacidades de restauración rápida de datos

Preguntas frecuentes sobre Cyber Vault

¿Cyber Vault es un producto de NetApp?

No, "bóveda cibernética" es un término que se utiliza ampliamente en la industria. NetApp ha creado una arquitectura de referencia para que a los clientes les resulte fácil construir sus propias bóvedas cibernéticas y aprovechar las docenas de funciones de seguridad de ONTAP para proteger sus datos de las amenazas cibernéticas. Hay más información disponible en"Sitio de documentación de ONTAP" .

¿Cyber Vault con NetApp es simplemente otro nombre para LockVault o SnapVault?

LockVault era una característica de Data ONTAP 7-mode que no está disponible en las versiones actuales de ONTAP.

SnapVault era un término heredado para lo que ahora se logra con la política de bóveda de SnapMirror. Esta política permite que el destino conserve una cantidad diferente de copias de instantáneas que el volumen de origen.

Cyber Vault utiliza SnapMirror con la política de bóveda y SnapLock Compliance juntos para crear una copia inmutable e indeleble de los datos.

¿Qué hardware de NetApp puedo usar para una bóveda cibernética, FAS, flash de capacidad o flash de rendimiento?

Esta arquitectura de referencia para bóveda cibernética se aplica a todo el portafolio de hardware de ONTAP . Los clientes pueden utilizar las plataformas AFF A-Series, AFF C-Series o FAS como bóveda. Las plataformas basadas en Flash proporcionarán los tiempos de recuperación más rápidos, mientras que las plataformas basadas en disco proporcionarán la solución más rentable. Dependiendo de la cantidad de datos que se estén recuperando y si se están realizando múltiples recuperaciones en paralelo, el uso de sistemas basados en discos (FAS) puede demorar días o semanas en completarse. Consulte con un representante de NetApp o un socio para dimensionar adecuadamente una solución de bóveda cibernética para satisfacer los requisitos comerciales.

¿Puedo utilizar Cloud Volumes ONTAP como fuente de bóveda cibernética?

Sí, sin embargo, el uso de CVO como fuente requiere que los datos se repliquen en un destino de bóveda cibernética local, ya que la SnapLock Compliance es un requisito para una bóveda cibernética ONTAP . La replicación de datos desde una instancia CVO basada en hiperescalador puede generar cargos de salida.

¿Puedo utilizar Cloud Volumes ONTAP como destino de bóveda cibernética?

La arquitectura de Cyber Vault se basa en la indelebilidad de SnapLock Compliance de ONTAP y está diseñada para implementaciones locales. Se están investigando arquitecturas de Cyber Vault basadas en la nube para su futura publicación.

¿Puedo utilizar ONTAP Select como fuente de bóveda cibernética?

Sí, ONTAP Select se puede utilizar como fuente para un destino de bóveda cibernética basada en hardware local.

¿Puedo utilizar ONTAP Select como destino de bóveda cibernética?

No, ONTAP Select no debe usarse como destino de bóveda cibernética ya que no tiene la capacidad de usar SnapLock Compliance.

¿Una bóveda cibernética con NetApp solo utiliza SnapMirror?

No, una arquitectura de bóveda cibernética de NetApp aprovecha muchas características de ONTAP para crear una copia de datos segura, aislada, protegida y reforzada. Para obtener más información sobre qué técnica adicional se puede utilizar consulte la siguiente pregunta.

¿Existe alguna otra tecnología o configuración utilizada para la bóveda cibernética?

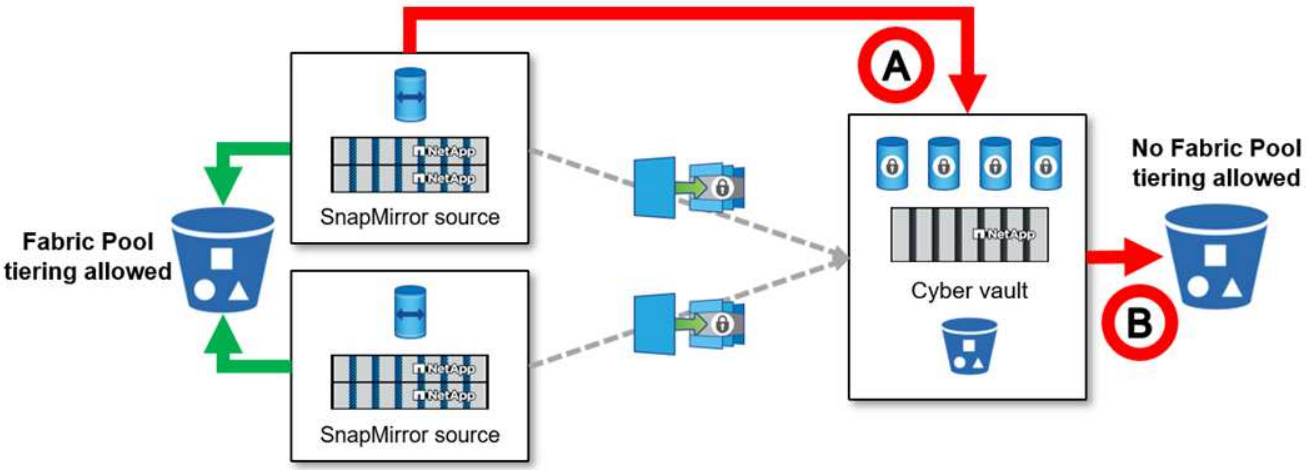
La base de una bóveda cibernética de NetApp es SnapMirror y SnapLock Compliance, pero el uso de funciones ONTAP adicionales como copias Snapshot a prueba de manipulaciones, autenticación multifactor (MFA), verificación de múltiples administradores, control de acceso basado en roles y registro de auditoría local y remoto mejora la seguridad de los datos.

¿Qué hace que las copias instantáneas de ONTAP sean mejores que otras para una bóveda cibernética?

Las copias instantáneas de ONTAP son inmutables de manera predeterminada y pueden hacerse indelebles con SnapLock Compliance. Ni siquiera el soporte de NetApp puede eliminar las copias de SnapLock Snapshot. La mejor pregunta que podemos hacer es qué hace que la bóveda cibernética de NetApp sea mejor que otras bóvedas cibernéticas de la industria. En primer lugar, ONTAP es el almacenamiento más seguro del planeta y ha obtenido la validación CSfC, que permite el almacenamiento de datos secretos y de alto secreto en reposo tanto en la capa de hardware como en la de software. Más información sobre"El CSfC se puede encontrar aquí" . Además, ONTAP puede tener un espacio de aire en la capa de almacenamiento, y el sistema de bóveda cibernética puede controlar la replicación, lo que permite crear un espacio de aire dentro de la red de bóveda cibernética.

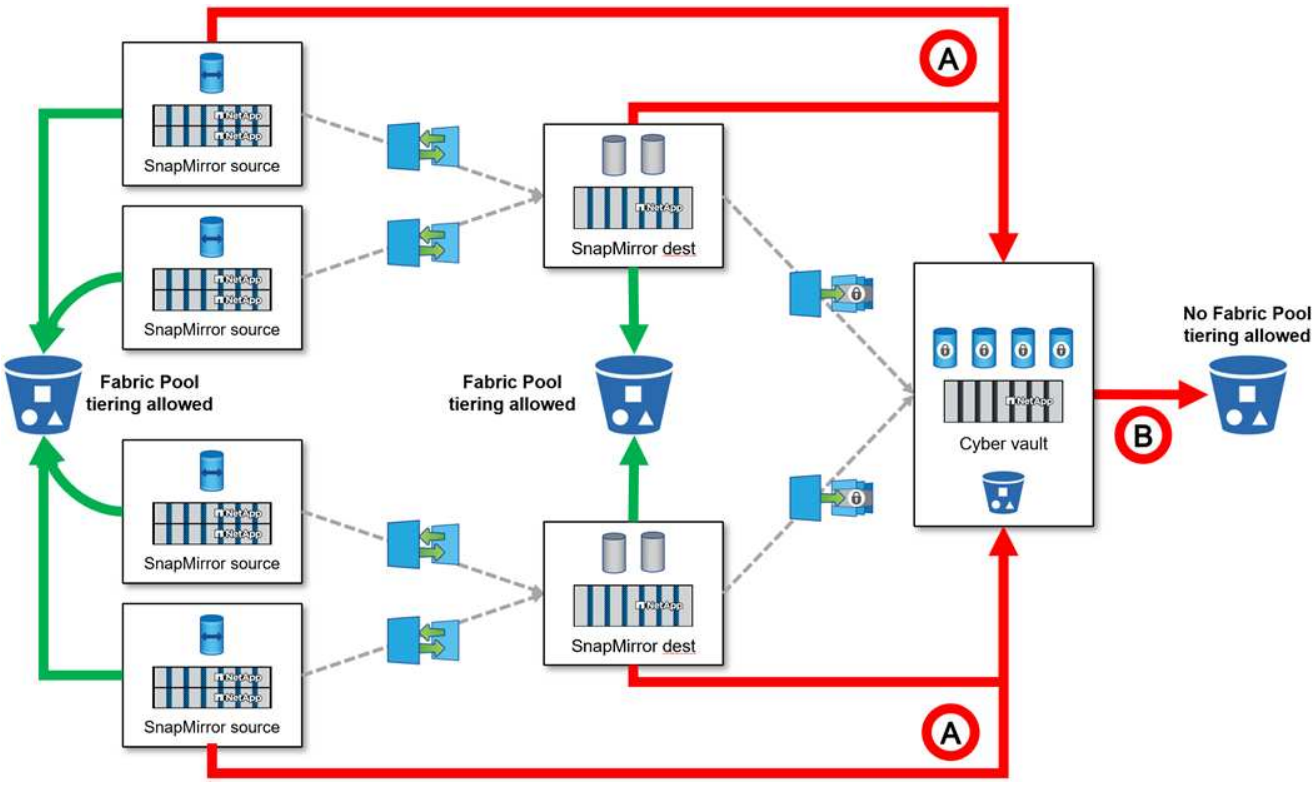
¿Puede un volumen de una bóveda cibernética utilizar ONTAP Fabric Pool?

No, un volumen de bóveda cibernética (destino SnapMirror de SnapLock Compliance) no se puede organizar en niveles mediante Fabric Pool, independientemente de la política.



Existen múltiples escenarios en los que el pool de fabric **no** puede usarse con una bóveda cibernética.

1. Los niveles fríos de Fabric Pool **no pueden** usar un clúster de bóveda cibernética. Esto se debe a que habilitar el protocolo S3 invalida la naturaleza segura de la arquitectura de referencia de la bóveda cibernética. Además, el bucket S3 utilizado para el pool de Fabric no se puede proteger.
2. Los volúmenes de SnapLock Compliance en la bóveda cibernética **no pueden** organizarse en niveles en un bucket S3 ya que los datos están bloqueados en el volumen.



¿ ONTAP S3 Worm está disponible en una bóveda cibernética?

No, S3 es un protocolo de acceso a datos que invalida la naturaleza segura de la arquitectura de referencia.

¿ NetApp Cyber Vault se ejecuta en una personalidad o perfil de ONTAP diferente?

No, es una arquitectura de referencia. Los clientes pueden utilizar el"arquitectura de referencia" y construir una bóveda cibernética, o puede utilizar el"Scripts de PowerShell para crear, reforzar y validar" una bóveda cibernética.

¿Puedo activar protocolos de datos como NFS, SMB y S3 en una bóveda cibernética?

De forma predeterminada, los protocolos de datos deben estar deshabilitados en la bóveda cibernética para que sea segura. Sin embargo, se pueden habilitar protocolos de datos en la bóveda cibernética para acceder a los datos para su recuperación o cuando sea necesario. Esto debe hacerse de forma temporal y desactivarse una vez que se haya completado la recuperación.

¿Es posible convertir un entorno SnapVault existente en una bóveda cibernética o es necesario volver a sembrar todo?

Sí. Se podría tomar un sistema que sea un destino de SnapMirror (con política de bóveda), deshabilitar los protocolos de datos, fortalecer el sistema según la política."Guía de endurecimiento de ONTAP" , aislarlo en una ubicación segura y seguir los demás procedimientos de la arquitectura de referencia para convertirlo en una bóveda cibernética sin tener que volver a sembrar el destino.

¿Tiene preguntas adicionales? Envíe un correo electrónico a ng-cyber-vault@netapp.com ¡con sus preguntas! Responderemos y agregaremos sus preguntas a las preguntas frecuentes.

Recursos de bóveda cibernética

Para obtener más información sobre la información descrita en esta bóveda cibernética, consulte la siguiente información adicional y conceptos de seguridad.

- "Bóveda cibernética de NetApp : Resumen de soluciones de protección de datos multicapa"
- "NetApp obtiene la calificación AAA por su primera solución integrada de detección de ransomware basada en IA."
- "Aumente la resiliencia cibernética con el almacenamiento más seguro del planeta"
- "Guía de refuerzo de seguridad de ONTAP"
- "Confianza cero de NetApp"
- "Ciberresiliencia de NetApp"
- "Protección de datos de NetApp"
- "Descripción general del emparejamiento de clústeres y SVM con la CLI"
- "Archivado de SnapVault"
- "Configurar, analizar, script cron"

Creación, fortalecimiento y validación de una bóveda cibernética de ONTAP con PowerShell

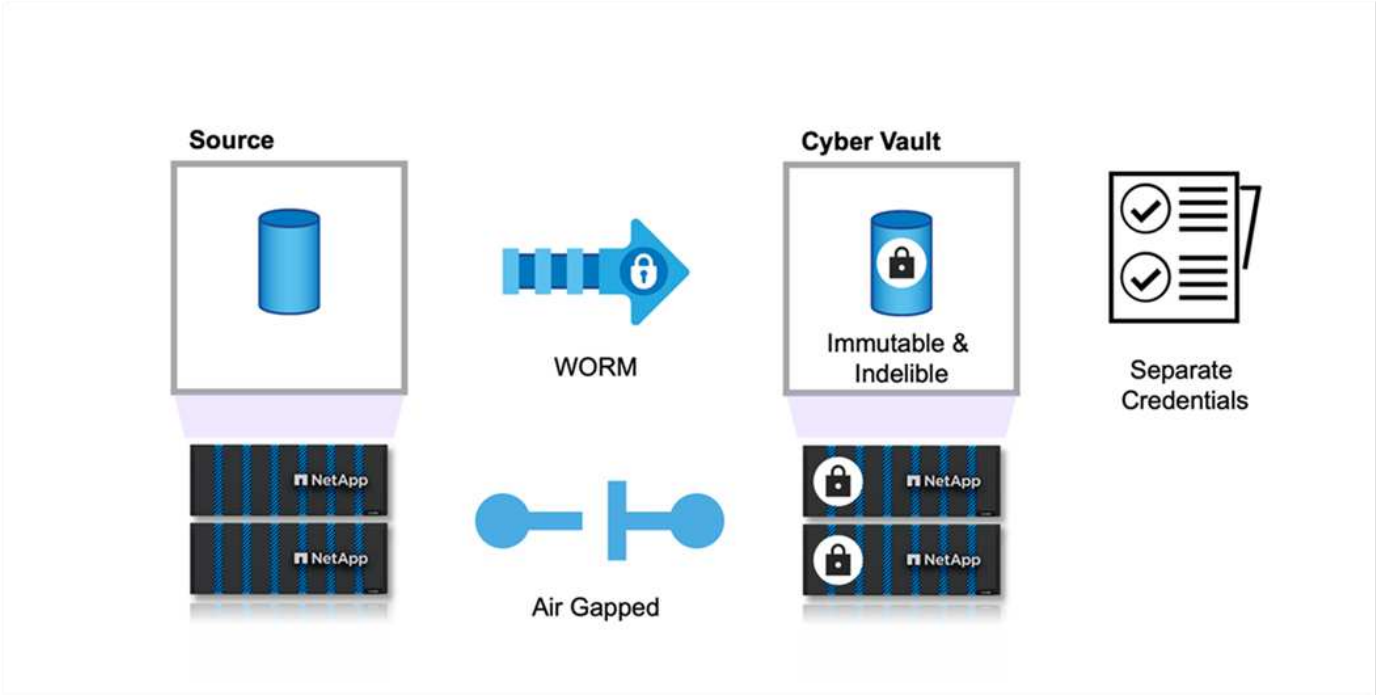
Descripción general de la bóveda cibernética de ONTAP con PowerShell

En el panorama digital actual, proteger los activos de datos críticos de una organización no es solo una buena práctica: es un imperativo comercial. Las amenazas cibernéticas están evolucionando a un ritmo sin precedentes y las medidas tradicionales de protección de datos ya no son suficientes para mantener segura la información confidencial. Ahí es donde entra en juego una bóveda cibernética. La solución de vanguardia basada en ONTAP de NetApp combina técnicas avanzadas de separación de aire con sólidas medidas de protección de datos para crear una barrera impenetrable contra las amenazas cibernéticas. Al aislar los datos más valiosos con tecnología de refuerzo seguro, una bóveda cibernética minimiza la superficie de ataque para que los datos más críticos permanezcan confidenciales, intactos y fácilmente disponibles cuando sea necesario.

Una bóveda cibernética es una instalación de almacenamiento segura que consta de múltiples capas de protección, como firewalls, redes y almacenamiento. Estos componentes protegen datos de recuperación vitales necesarios para operaciones comerciales cruciales. Los componentes de la bóveda cibernética se sincronizan periódicamente con los datos de producción esenciales según la política de la bóveda, pero de lo contrario permanecen inaccesibles. Esta configuración aislada y desconectada garantiza que, en caso de un ciberataque que comprometa el entorno de producción, se pueda realizar fácilmente una recuperación final y confiable desde la bóveda cibernética.

NetApp permite la creación sencilla de un espacio de aire para la bóveda cibernética configurando la red, deshabilitando LIF, actualizando las reglas del firewall y aislando el sistema de redes externas e Internet. Este enfoque robusto desconecta eficazmente el sistema de las redes externas e Internet, brindando una protección incomparable contra ataques cibernéticos remotos e intentos de acceso no autorizado, haciendo que el sistema sea inmune a las amenazas e intrusiones basadas en la red.

Al combinar esto con la protección de SnapLock Compliance , los datos no se pueden modificar ni eliminar, ni siquiera por los administradores de ONTAP o el soporte de NetApp . SnapLock se audita periódicamente de acuerdo con las regulaciones de la SEC y FINRA, lo que garantiza que la resiliencia de los datos cumpla con estas estrictas regulaciones WORM y de retención de datos de la industria bancaria. NetApp es el único almacenamiento empresarial validado por NSA CSfC para almacenar datos de alto secreto.



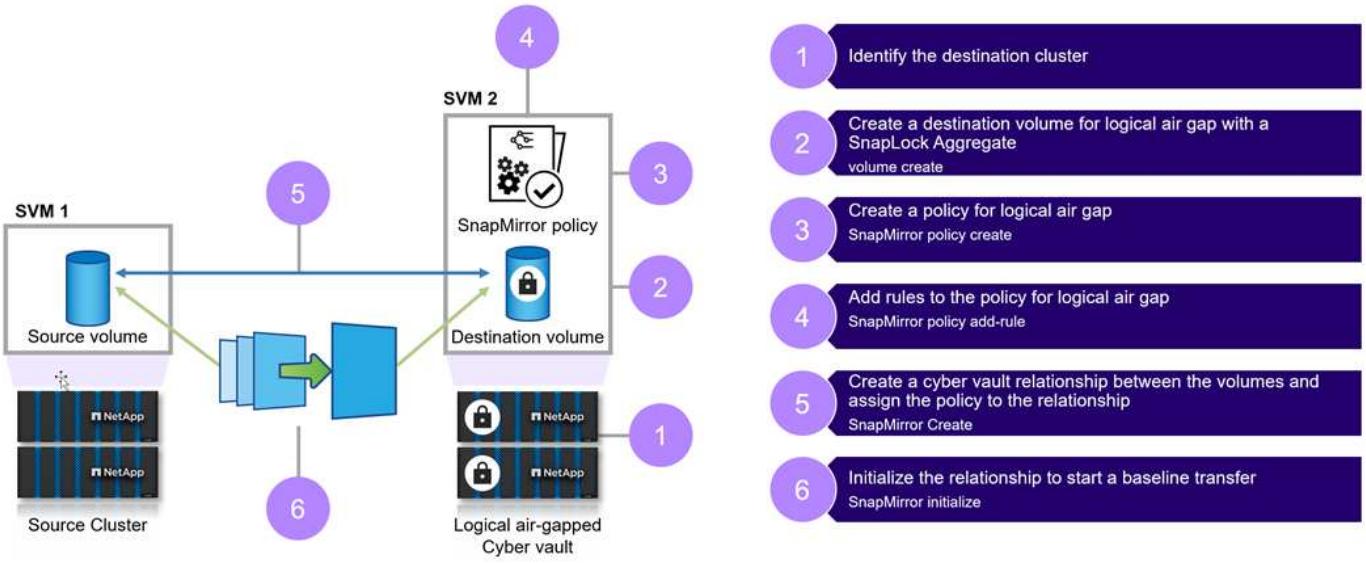
Este documento describe la configuración automatizada de la bóveda cibernética de NetApp para el almacenamiento ONTAP local a otro almacenamiento ONTAP designado con instantáneas inmutables, lo que agrega una capa adicional de protección contra los crecientes ataques cibernéticos para una recuperación rápida. Como parte de esta arquitectura, toda la configuración se aplica según las mejores prácticas de ONTAP . La última sección tiene instrucciones para realizar una recuperación en caso de un ataque.

La misma solución se puede aplicar para crear la bóveda cibernética designada en AWS usando FSx ONTAP.

Pasos de alto nivel para crear una bóveda cibernética ONTAP

- Crear una relación de peering
  - El sitio de producción que utiliza el almacenamiento ONTAP está conectado a una bóveda cibernética designada con el almacenamiento ONTAP
- Crear volumen de SnapLock Compliance
- Configurar la relación y la regla de SnapMirror para establecer la etiqueta
  - Se configuran la relación SnapMirror y los horarios adecuados
- Establecer retenciones antes de iniciar la transferencia de SnapMirror (bóveda)
  - Se aplica un bloqueo de retención a los datos copiados, lo que evita además que cualquier persona interna pueda acceder a ellos o que se produzcan fallos en los datos. Con esto, los datos no se pueden eliminar antes de que expire el período de retención.
  - Las organizaciones pueden conservar estos datos durante algunas semanas o meses según sus requisitos.
- Inicializar la relación SnapMirror en función de las etiquetas
  - La siembra inicial y la transferencia incremental permanente se realizan según el cronograma de SnapMirror
  - Los datos están protegidos (son inmutables e indelebles) con la conformidad con SnapLock y están disponibles para su recuperación.

- Implementar controles estrictos de transferencia de datos
  - La bóveda cibernética se desbloquea por un período limitado con datos del sitio de producción y se sincroniza con los datos de la bóveda. Una vez completada la transferencia, la conexión se desconecta, se cierra y se bloquea nuevamente.
- Recuperación rápida
  - Si el sistema primario se ve afectado en el sitio de producción, los datos de la bóveda cibernética se recuperan de forma segura en la producción original o en otro entorno elegido.



Componentes de la solución

NetApp ONTAP ejecutando 9.15.1 en clústeres de origen y destino.

ONTAP One: la licencia todo en uno de NetApp ONTAP.

Capacidades utilizadas de la licencia ONTAP One:

- SnapLock Compliance
- SnapMirror
- Verificación multiadministrador
- Todas las capacidades de endurecimiento expuestas por ONTAP
- Credenciales RBAC independientes para la bóveda cibernética

> Todas las matrices físicas unificadas de ONTAP se pueden usar para una bóveda cibernética, sin embargo, los sistemas flash basados en capacidad de la serie C de AFF y los sistemas flash híbridos FAS son las plataformas ideales más rentables para este propósito. Por favor consulte el"Dimensionamiento de la bóveda cibernética de ONTAP" para orientación sobre el tamaño.

Creación de una bóveda cibernética de ONTAP con PowerShell

Las copias de seguridad con espacio de aire que utilizan métodos tradicionales implican la creación de espacio y la separación física de los medios primarios y secundarios. Al trasladar los medios fuera del sitio y/o cortar la conectividad, los actores maliciosos no

tienen acceso a los datos. Esto protege los datos pero puede generar tiempos de recuperación más lentos. Con SnapLock Compliance, no se requiere separación física. SnapLock Compliance protege las copias de instantáneas almacenadas en un punto específico del tiempo y de solo lectura, lo que da como resultado datos a los que se puede acceder rápidamente, que son seguros contra eliminación o indelebles, y seguros contra modificación o inmutables.

Prerrequisitos

Antes de comenzar con los pasos de la siguiente sección de este documento, asegúrese de que se cumplan los siguientes requisitos previos:

- El clúster de origen debe ejecutar ONTAP 9 o posterior.
- Los agregados de origen y destino deben ser de 64 bits.
- Los clústeres de origen y destino deben estar emparejados.
- Las SVM de origen y destino deben estar emparejadas.
- Asegúrese de que el cifrado de intercambio de clústeres esté habilitado.

La configuración de transferencias de datos a una bóveda cibernética de ONTAP requiere varios pasos. En el volumen principal, configure una política de instantáneas que especifique qué copias crear y cuándo crearlas mediante programaciones apropiadas y asigne etiquetas para especificar qué copias debe transferir SnapVault. En el secundario, se debe crear una política SnapMirror que especifique las etiquetas de las copias Snapshot que se transferirán y cuántas de estas copias se deben conservar en la bóveda cibernética. Después de configurar estas políticas, cree la relación SnapVault y establezca un programa de transferencia.

> Este documento asume que el almacenamiento principal y la bóveda cibernética ONTAP designada ya están instalados y configurados.

> El clúster de bóveda cibernética puede estar en el mismo centro de datos que los datos de origen o en uno diferente.

Pasos para crear una bóveda cibernética ONTAP

1. Utilice la CLI de ONTAP o el Administrador del sistema para inicializar el reloj de cumplimiento.
2. Cree un volumen de protección de datos con la compatibilidad con SnapLock habilitada.
3. Utilice el comando de creación de SnapMirror para crear relaciones de protección de datos de SnapVault .
4. Establezca el período de retención de SnapLock Compliance predeterminado para el volumen de destino.

> La retención predeterminada es "Establecer al mínimo". A un volumen SnapLock que es un destino de bóveda se le asigna un período de retención predeterminado. El valor para este período se establece inicialmente en un mínimo de 0 años y un máximo de 100 años (a partir de ONTAP 9.10.1. Para versiones anteriores de ONTAP , el valor es 0 - 70) para volúmenes de SnapLock Compliance . Cada copia de NetApp Snapshot se confirma con este período de retención predeterminado al principio. El período de retención puede extenderse posteriormente, si es necesario, pero nunca acortarse. Para obtener más información, consulte "Descripción general del tiempo de retención establecido" .

Lo anterior abarca los pasos manuales. Los expertos en seguridad aconsejan automatizar el proceso para

evitar la gestión manual que introduce un gran margen de error. A continuación se muestra el fragmento de código que automatiza completamente los requisitos previos y la configuración del cumplimiento de SnapLock y la inicialización del reloj.

Aquí hay un ejemplo de código de PowerShell para inicializar el reloj de cumplimiento de ONTAP .

```
function initializeSnapLockComplianceClock {
    try {
        $nodes = Get-NcNode

        $isInitialized = $false
        logMessage -message "Cheking if snaplock compliance clock is
initialized"
        foreach($node in $nodes) {
            $check = Get-NcSnaplockComplianceClock -Node $node.Node
            if ($check.SnaplockComplianceClockSpecified -eq "True") {
                $isInitialized = $true
            }
        }

        if ($isInitialized) {
            logMessage -message "SnapLock Compliance clock already
initialized" -type "SUCCESS"
        } else {
            logMessage -message "Initializing SnapLock compliance clock"
            foreach($node in $nodes) {
                Set-NcSnaplockComplianceClock -Node $node.Node
            }
            logMessage -message "Successfully initialized SnapLock
Compliance clock" -type "SUCCESS"
        }
    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

A continuación se muestra un ejemplo de código de PowerShell para configurar una bóveda cibernética ONTAP .

```
function configureCyberVault {
    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if the volume already exists and is of type
snaplock compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
```

```
$DESTINATION_VSERVER"
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
$DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                # Create SnapLock Compliance volume
                logMessage -message "Creating SnapLock Compliance volume:
$($DESTINATION_VOLUME_NAMES[$i])"
                New-NcVol -Name $DESTINATION_VOLUME_NAMES[$i] -Aggregate
$DESTINATION_AGGREGATE_NAMES[$i] -SnaplockType Compliance -Type DP -Size
$DESTINATION_VOLUME_SIZES[$i] -ErrorAction Stop | Select-Object -Property
Name, State, TotalSize, Aggregate, Vserver
                logMessage -message "Volume $($DESTINATION_VOLUME_NAMES[
$i]) created successfully" -type "SUCCESS"
            }

            # Set SnapLock volume attributes
            logMessage -message "Setting SnapLock volume attributes for
volume: $($DESTINATION_VOLUME_NAMES[$i])"
            Set-NcSnaplockVolAttr -Volume $DESTINATION_VOLUME_NAMES[$i]
-MinimumRetentionPeriod $SNAPLOCK_MIN_RETENTION -MaximumRetentionPeriod
$SNAPLOCK_MAX_RETENTION -ErrorAction Stop | Select-Object -Property Type,
MinimumRetentionPeriod, MaximumRetentionPeriod
            logMessage -message "SnapLock volume attributes set
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"

            # checking snapmirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
SourceLocation, DestinationCluster, DestinationLocation, Status,
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and ($_.Status
-eq "snapmirrored" -or $_.Status -eq "uninitialized") }
            if($snapmirror) {
                $snapmirror
```

```
                logMessage -message "SnapMirror relationship already
exists for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            } else {
                # Create SnapMirror relationship
                logMessage -message "Creating SnapMirror relationship for
volume: $($DESTINATION_VOLUME_NAMES[$i])"
                New-NcSnapmirror -SourceCluster $SOURCE_ONTAP_CLUSTER_NAME
-SourceVserver $SOURCE_VSERVER -SourceVolume $SOURCE_VOLUME_NAMES[$i]
-DestinationCluster $DESTINATION_ONTAP_CLUSTER_NAME -DestinationVserver
$DESTINATION_VSERVER -DestinationVolume $DESTINATION_VOLUME_NAMES[$i]
-Policy $SNAPMIRROR_PROTECTION_POLICY -Schedule $SNAPMIRROR_SCHEDULE
-ErrorAction Stop | Select-Object -Property SourceCluster, SourceLocation,
DestinationCluster, DestinationLocation, Status, Policy, Schedule
                logMessage -message "SnapMirror relationship created
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            }

        } catch {
            handleError -errorMessage $_.Exception.Message
        }
    }
}
```

1. Una vez completados los pasos anteriores, la bóveda cibernética con espacio de aire que utiliza SnapLock Compliance y SnapVault estará lista.

Antes de transferir datos de instantáneas a la bóveda cibernética, se debe inicializar la relación SnapVault . Sin embargo, antes de eso, es necesario realizar un refuerzo de seguridad para proteger la bóveda.

Refuerzo de la bóveda cibernética de ONTAP con PowerShell

La bóveda cibernética de ONTAP proporciona una mayor resiliencia contra los ciberataques en comparación con las soluciones tradicionales. Al diseñar una arquitectura para mejorar la seguridad, es fundamental considerar medidas para reducir la superficie de ataque. Esto se puede lograr mediante varios métodos, como implementar políticas de contraseñas reforzadas, habilitar RBAC, bloquear cuentas de usuario predeterminadas, configurar firewalls y utilizar flujos de aprobación para cualquier cambio en el sistema de bóveda. Además, restringir los protocolos de acceso a la red desde direcciones IP específicas puede ayudar a limitar posibles vulnerabilidades.

ONTAP proporciona un conjunto de controles que permiten fortalecer el almacenamiento de ONTAP . Utilice el"Orientación y configuración de ONTAP" para ayudar a la organización a cumplir los objetivos de seguridad prescritos para la confidencialidad, integridad y disponibilidad del sistema de información.

Fortalecimiento de las mejores prácticas

Pasos manuales

1. Cree un usuario designado con un rol administrativo predefinido y personalizado.
2. Cree un nuevo espacio IP para aislar el tráfico de red.
3. Cree una nueva SVM que resida en el nuevo espacio IP.
4. Asegúrese de que las políticas de enrutamiento del firewall estén configuradas correctamente y que todas las reglas se auditen y actualicen periódicamente según sea necesario.

CLI de ONTAP o mediante script de automatización

1. Proteja la administración con la verificación multiadministrador (MFA)
2. Habilitar el cifrado para datos estándar "en tránsito" entre clústeres.
3. Asegure SSH con un cifrado fuerte y aplique contraseñas seguras.
4. Habilitar FIPS global.
5. Telnet y Remote Shell (RSH) deben estar deshabilitados.
6. Bloquear la cuenta de administrador predeterminada.
7. Deshabilite los LIF de datos y proteja los puntos de acceso remoto.
8. Deshabilite y elimine protocolos y servicios no utilizados o extraños.
9. Cifrar el tráfico de red.
10. Utilice el principio del mínimo privilegio al configurar roles administrativos y de superusuario.
11. Restrinja HTTPS y SSH desde una dirección IP específica usando la opción de IP permitida.
12. Poner en pausa y reanudar la replicación según el programa de transferencia.

Los puntos 1 a 4 requieren intervención manual, como designar una red aislada, segregar el espacio IP, etc., y deben realizarse de antemano. La información detallada para configurar el endurecimiento se puede encontrar en el"Guía de refuerzo de seguridad de ONTAP" . El resto se puede automatizar fácilmente para facilitar la implementación y el monitoreo. El objetivo de este enfoque orquestado es proporcionar un mecanismo para automatizar los pasos de fortalecimiento para proteger el controlador de la bóveda en el futuro. El período durante el cual el espacio de aire de la bóveda cibernética permanece abierto es el más breve posible. SnapVault aprovecha la tecnología incremental permanente, que solo moverá los cambios desde la última actualización a la bóveda cibernética, minimizando así la cantidad de tiempo que la bóveda cibernética debe permanecer abierta. Para optimizar aún más el flujo de trabajo, la apertura de la bóveda cibernética se coordina con el cronograma de replicación para garantizar la ventana de conexión más pequeña.

Aquí hay un ejemplo de código de PowerShell para fortalecer un controlador ONTAP .

```
function removeSvmDataProtocols {
    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            # Remove NFS
            logMessage -message "Removing NFS protocol on vServer :
```

```
$DESTINATION_VSERVER"
            Remove-NcNfsService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "NFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
            # Remove SMB/CIFS
            logMessage -message "Removing SMB/CIFS protocol on vServer :
$DESTINATION_VSERVER"
            $domainAdministratorUsername = Read-Host -Prompt "Enter Domain
administrator username"
            $domainAdministratorPassword = Read-Host -Prompt "Enter Domain
administrator password" -AsSecureString
            $plainPassword = [Runtime.InteropServices.Marshal
]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($
domainAdministratorPassword))
            Remove-NcCifsServer -VserverContext $DESTINATION_VSERVER
-AdminUsername $domainAdministratorUsername -AdminPassword $plainPassword
-Confirm:$false -ErrorAction Stop
            logMessage -message "SMB/CIFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            # Remove iSCSI
            logMessage -message "Removing iSCSI protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcIscsiService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "iSCSI protocol removed on vServer :
```

```
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
            # Remove FCP
            logMessage -message "Removing FC protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcFcpService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "FC protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function disableSvmDataLifs {
    try {
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address

        logMessage -message "Disabling all data lifs on vServer :
$DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
            $disableLif = Set-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName -AdministrativeStatus down -ErrorAction Stop
            $disableLif | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address
        }
```

```
        logMessage -message "Disabled all data lifs on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function configureMultiAdminApproval {
    try {

        # check if multi admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
            logMessage -message "Setting Multi-admin verification rules"
            # Define the commands to be restricted
            $rules = @(
                "cluster peer delete",
                "vserver peer delete",
                "volume snapshot policy modify",
                "volume snapshot rename",
                "vserver audit modify",
                "vserver audit delete",
                "vserver audit disable"
            )
            foreach($rule in $rules) {
                Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
rule create -operation `"$rule`""
            }

            logMessage -message "Creating multi admin verification group
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
```

```
approval-group create -name $MULTI_ADMIN_APPROVAL_GROUP_NAME -approvers
$MULTI_ADMIN_APPROVAL_USERS -email `"$MULTI_ADMIN_APPROVAL_EMAIL`""
            logMessage -message "Created multi admin verification group
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification group
$MULTI_ADMIN_APPROVAL_GROUP_NAME"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -approval-groups $MULTI_ADMIN_APPROVAL_GROUP_NAME -required
-approvers 1 -enabled true"
            logMessage -message "Enabled multi admin verification group
$MULTI_ADMIN_APPROVAL_GROUP_NAME" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"
        }

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function additionalSecurityHardening {
    try {
        $command = "set -privilege advanced -confirmations off;security
protocol modify -application telnet -enabled false;"
        logMessage -message "Disabling Telnet"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
```

```
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Disabled Telnet" -type "SUCCESS"

        #$command = "set -privilege advanced -confirmations off;security
config modify -interface SSL -is-fips-enabled true;"
        #logMessage -message "Enabling Global FIPS"
        ##Invoke-SSHCommand -SessionId $sshSession.SessionId -Command
$command -ErrorAction Stop
        #logMessage -message "Enabled Global FIPS" -type "SUCCESS"

        $command = "set -privilege advanced -confirmations off;network
interface service-policy modify-service -vserver cluster2 -policy default-
management -service management-https -allowed-addresses $ALLOWED_IPS;"
        logMessage -message "Restricting IP addresses $ALLOWED_IPS for
Cluster management HTTPS"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Successfully restricted IP addresses
$ALLOWED_IPS for Cluster management HTTPS" -type "SUCCESS"

        #logMessage -message "Checking if audit logs volume audit_logs
exists"
        #$volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Name
audit_logs -ErrorAction Stop

        #if($volume) {
        #    logMessage -message "Volume audit_logs already exists!
Skipping creation"
        #} else {
        #    # Create audit logs volume
        #    logMessage -message "Creating audit logs volume : audit_logs"
        #    New-NcVol -Name audit_logs -Aggregate
$DESTINATION_AGGREGATE_NAME -Size 5g -ErrorAction Stop | Select-Object
-Property Name, State, TotalSize, Aggregate, Vserver
        #    logMessage -message "Volume audit_logs created successfully"
-type "SUCCESS"
        #}

        ## Mount audit logs volume to path /vol/audit_logs
        #logMessage -message "Creating junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER"
        #Mount-NcVol -VserverContext $DESTINATION_VSERVER -Name audit_logs
-JunctionPath /audit_logs | Select-Object -Property Name, -JunctionPath
        #logMessage -message "Created junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER" -type "SUCCESS"
```

```
        #logMessage -message "Enabling audit logging for vServer
$DESTINATION_VSERVER at path /vol/audit_logs"
        #$command = "set -privilege advanced -confirmations off;vserver
audit create -vserver $DESTINATION_VSERVER -destination /audit_logs
-format xml;"
        #Invoke-SSHCommand -SessionI  $sshSession.SessionId -Command
$command -ErrorAction Stop
        #logMessage -message "Successfully enabled audit logging for
vServer $DESTINATION_VSERVER at path /vol/audit_logs"

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

Validación de bóveda cibernética de ONTAP con PowerShell

Una bóveda cibernética robusta debe ser capaz de resistir un ataque sofisticado, incluso cuando el atacante tiene credenciales para acceder al entorno con privilegios elevados.

Una vez que las reglas están en su lugar, un intento (asumiendo que de alguna manera el atacante pudo ingresar) de eliminar una instantánea del lado de la bóveda fallará. Lo mismo se aplica a todas las configuraciones de endurecimiento, aplicando las restricciones necesarias y protegiendo el sistema.

Ejemplo de código de PowerShell para validar la configuración de forma programada.

```
function analyze {

    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if volume is of type SnapLock Compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
-type "SUCCESS"
            } else {
                handleError -errorMessage "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) does not exist in vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
```

```
`"configure`" to create and configure the cyber vault SnapLock Compliance
volume"
            }

            # checking SnapMirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
SourceLocation, DestinationCluster, DestinationLocation, Status,
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and $_.Status
-eq "snapmirrored" }
            if($snapmirror) {
                $snapmirror
                logMessage -message "SnapMirror relationship successfully
configured and in healthy state" -type "SUCCESS"
            } else {
                handleError -errorMessage "SnapMirror relationship does
not exist between the source volume $($SOURCE_VOLUME_NAMES[$i]) and
destination SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])
(or) SnapMirror status uninitialized/unhealthy. Recommendation: Run the
script with SCRIPT_MODE `"configure`" to create and configure the cyber
vault SnapLock Compliance volume and configure the SnapMirror
relationship"
            }
        }
        catch {
            handleError -errorMessage $_.Exception.Message
        }
    }

    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            handleError -errorMessage "NFS service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable NFS on vServer $DESTINATION_VSERVER"
        } else {
```

```
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
            handleError -errorMessage "CIFS/SMB server running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable CIFS/SMB on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            handleError -errorMessage "iSCSI service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable iSCSI on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
            handleError -errorMessage "FCP service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable FCP on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking if all data lifs are disabled on vServer
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
```

```
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address

        logMessage -message "Checking if all data lifs are disabled for
vServer : $DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
            $checkLif = Get-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName | Where-Object { $_.OpStatus -eq "down" }
            if($checkLif) {
                logMessage -message "Data lif $($lif.InterfaceName)
disabled for vServer $DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                handleError -errorMessage "Data lif $($lif.InterfaceName)
is enabled. Recommendation: Run the script with SCRIPT_MODE `"configure`"
to disable Data lifs for vServer $DESTINATION_VSERVER"
            }
        }
        logMessage -message "All data lifs are disabled for vServer :
$DESTINATION_VSERVER" -type "SUCCESS"

        # check if multi-admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
            handleError -errorMessage "Multi-admin verification is not
configured or not enabled. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to enable and configure Multi-admin verification"
        }

        # check if telnet is disabled
        logMessage -message "Checking if telnet is disabled"
        $telnetConfig = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; security protocol show -application
telnet"
```

```
        if ($telnetConfig.Value -match "enabled" -and $telnetConfig.Value
-match "false") {
            logMessage -message "Telnet is disabled" -type "SUCCESS"
        } else {
            handleError -errorMessage "Telnet is enabled. Recommendation:
Run the script with SCRIPT_MODE `"configure`" to disable telnet"
        }

        # check if network https is restricted to allowed IP addresses
        logMessage -message "Checking if HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS"
        $networkServicePolicy = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; network interface service-policy show"
        if ($networkServicePolicy.Value -match "management-https:
$($ALLOWED_IPS)") {
            logMessage -message "HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS" -type "SUCCESS"
        } else {
            handleError -errorMessage "HTTPS is not restricted to allowed
IP addresses $ALLOWED_IPS. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to restrict allowed IP addresses for HTTPS management"
        }
    }
    catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

Esta captura de pantalla muestra que no hay conexiones en el controlador de bóveda.

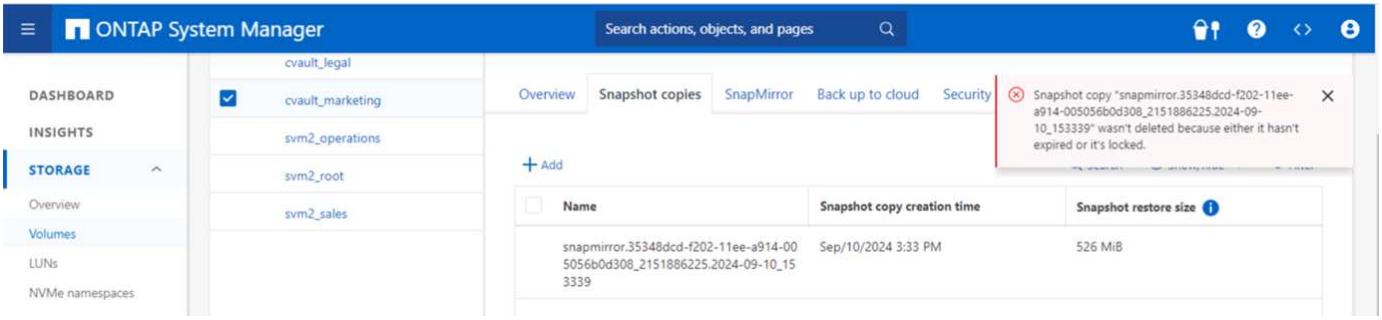
```
cluster2::> network connections  listening show
This table is currently empty.

cluster2::> network connections active show-services
This table is currently empty.

cluster2::> network connections active show-protocols
This table is currently empty.

cluster2::>
```

Esta captura de pantalla muestra que no es posible manipular las instantáneas.



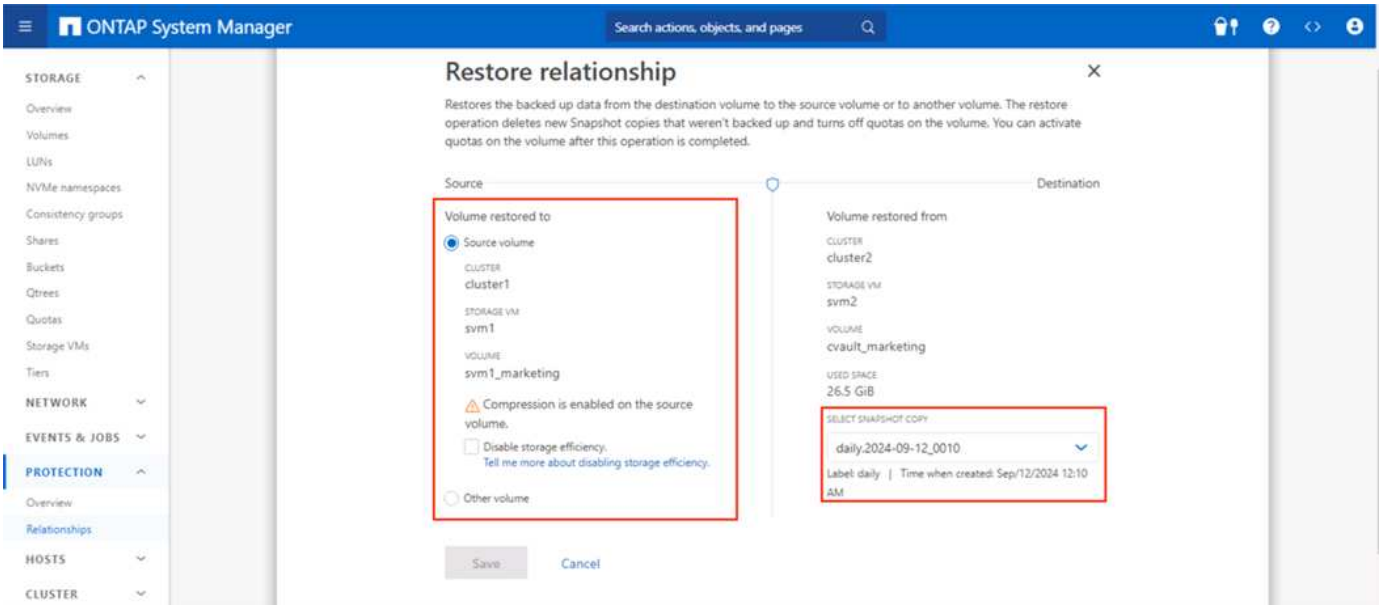
Para validar y confirmar la funcionalidad del espacio de aire, siga los pasos a continuación:

- Pruebe las capacidades de aislamiento de la red y la capacidad de suspender una conexión cuando no se transfieren datos.
- Verifique que no se pueda acceder a la interfaz de administración desde ninguna entidad aparte de las direcciones IP permitidas.
- Verificar La verificación de múltiples administradores está implementada para proporcionar una capa adicional de aprobación.
- Validar la capacidad de acceder a través de CLI y API REST
- Desde la fuente, active una operación de transferencia a la bóveda y asegúrese de que la copia almacenada no se pueda modificar.
- Intente eliminar las copias de instantáneas inmutables que se transfieren al almacén.
- Intente modificar el período de retención manipulando el reloj del sistema.

Recuperación de datos de bóvedas cibernéticas de ONTAP

Si se destruyen datos en el centro de datos de producción, los datos de la bóveda cibernética se pueden recuperar de forma segura en el entorno elegido. A diferencia de una solución con espacio de aire físico, la bóveda cibernética ONTAP con espacio de aire está construida utilizando funciones nativas de ONTAP como SnapLock Compliance y SnapMirror. El resultado es un proceso de recuperación rápido y fácil de ejecutar.

En caso de un ataque de ransomware y necesidad de recuperarse de la bóveda cibernética, el proceso de recuperación es simple y fácil, ya que las copias instantáneas alojadas en la bóveda cibernética se utilizan para restaurar los datos cifrados.



Si el requisito es proporcionar un método más rápido para volver a poner los datos en línea cuando sea necesario validarlos, aislarlos y analizarlos rápidamente para su recuperación. Esto se puede lograr fácilmente al usar FlexClone con la opción de tipo snaplock establecida en tipo sin snaplock.

> A partir de ONTAP 9.13.1, restaurar una copia de Snapshot bloqueada en el volumen SnapLock de destino de una relación de bóveda SnapLock se puede restaurar instantáneamente creando un FlexClone con la opción de tipo snaplock establecida en "no snaplock". Al ejecutar la operación de creación de clonación de volumen, especifique la copia de instantánea como la "instantánea principal". Más información sobre la creación de un volumen FlexClone con un tipo SnapLock"aquí."

> Practicar procedimientos de recuperación desde la bóveda cibernética garantizará que se establezcan los pasos adecuados para conectarse a la bóveda cibernética y recuperar datos. Planificar y probar el procedimiento es esencial para cualquier recuperación durante un evento de ciberataque.

Consideraciones adicionales

Existen consideraciones adicionales al diseñar e implementar una bóveda cibernética basada en ONTAP .

Consideraciones sobre el tamaño de la capacidad

La cantidad de espacio en disco necesaria para un volumen de destino de bóveda cibernética de ONTAP depende de diversos factores, el más importante de los cuales es la tasa de cambio de los datos en el volumen de origen. Tanto la programación de copias de seguridad como la programación de instantáneas en el volumen de destino afectan el uso del disco en el volumen de destino, y no es probable que la tasa de cambio en el volumen de origen sea constante. Es una buena idea proporcionar un buffer de capacidad de almacenamiento adicional al que se requiere para acomodar cambios futuros en el comportamiento del usuario final o de la aplicación.

Para dimensionar una relación para 1 mes de retención en ONTAP es necesario calcular los requisitos de almacenamiento en función de varios factores, incluidos el tamaño del conjunto de datos principal, la tasa de cambio de los datos (tasa de cambio diaria) y los ahorros de deduplicación y compresión (si corresponde).

A continuación se muestra el enfoque paso a paso:

El primer paso es conocer el tamaño de los volúmenes de origen que está protegiendo con la bóveda cibernética. Esta es la cantidad base de datos que se replicarán inicialmente en el destino de la bóveda cibernética. A continuación, estime la tasa de cambio diaria para el conjunto de datos. Este es el porcentaje de datos que cambia cada día. Es fundamental tener una buena comprensión de cuán dinámicos son sus datos.

Por ejemplo:

- Tamaño del conjunto de datos principal = 5 TB
- Tasa de cambio diaria = 5% (0,05)
- Eficiencia de deduplicación y compresión = 50% (0,50)

Ahora, veamos el cálculo:

- Calcular la tasa de cambio de datos diaria:

```
Changed data per day = 5000 * 5% = 250GB
```

- Calcular el total de datos modificados durante 30 días:

```
Total changed data in 30 days = 250 GB * 30 = 7.5TB
```

- Calcular el almacenamiento total requerido:

```
TOTAL = 5TB + 7.5TB = 12.5TB
```

- Aplicar ahorros de deduplicación y compresión:

```
EFFECTIVE = 12.5TB * 50% = 6.25TB
```

Resumen de las necesidades de almacenamiento

- Sin eficiencia: se necesitarían **12,5 TB** para almacenar 30 días de datos de la bóveda cibernética.
- Con un 50% de eficiencia: se requerirían **6,25 TB** de almacenamiento después de la deduplicación y la compresión.

Las copias instantáneas pueden tener un costo adicional debido a los metadatos, pero esto suele ser menor.

Si se realizan varias copias de seguridad por día, ajuste el cálculo según la cantidad de copias instantáneas tomadas cada día.

Tenga en cuenta el crecimiento de los datos a lo largo del tiempo para garantizar que el tamaño esté preparado para el futuro.

Impacto en el rendimiento de la fuente primaria

Dado que la transferencia de datos es una operación de extracción, el impacto en el rendimiento del almacenamiento primario puede variar según la carga de trabajo, el volumen de datos y la frecuencia de las copias de seguridad. Sin embargo, el impacto general en el rendimiento del sistema principal es generalmente

moderado y manejable, ya que la transferencia de datos está diseñada para descargar las tareas de protección de datos y de respaldo al sistema de almacenamiento de la bóveda cibernética. Durante la configuración inicial de la relación y la primera copia de seguridad completa, se transfiere una cantidad significativa de datos del sistema principal al sistema de bóveda cibernética (el volumen SnapLock Compliance). Esto puede generar un mayor tráfico de red y carga de E/S en el sistema principal. Una vez que se completa la copia de seguridad completa inicial, ONTAP solo necesita rastrear y transferir los bloques que han cambiado desde la última copia de seguridad. Esto da como resultado una carga de E/S mucho menor en comparación con la replicación inicial. Las actualizaciones incrementales son eficientes y tienen un impacto mínimo en el rendimiento del almacenamiento principal. El proceso de bóveda se ejecuta en segundo plano, lo que reduce las posibilidades de interferencia con las cargas de trabajo de producción del sistema principal.

- Asegurarse de que el sistema de almacenamiento tenga suficientes recursos (CPU, memoria y IOP) para manejar la carga adicional mitiga el impacto en el rendimiento.

Configurar, analizar, script cron

NetApp ha creado una"Un solo script que se puede descargar" y se utiliza para configurar, verificar y programar relaciones de bóvedas cibernéticas.

Qué hace este script

- Emparejamiento de clústeres
- Emparejamiento de SVM
- Creación de volumen DP
- Relación e inicialización de SnapMirror
- Fortalecer el sistema ONTAP utilizado para la bóveda cibernética
- Poner fin y reanudar la relación según el cronograma de transferencia
- Validar periódicamente la configuración de seguridad y generar un informe que muestre cualquier anomalía

Cómo utilizar este script

"Descargar el script"y para utilizar el script, simplemente siga los pasos a continuación:

- Inicie Windows PowerShell como administrador.
- Navegue hasta el directorio que contiene el script.
- Ejecute el script usando `.\` sintaxis junto con los parámetros requeridos

> Asegúrese de ingresar toda la información. En la primera ejecución (modo de configuración), solicitará credenciales tanto para el sistema de producción como para el nuevo sistema de bóveda cibernética. Después de eso, creará los peerings SVM (si no existen), los volúmenes y el SnapMirror entre el sistema y los inicializará.

> El modo Cron se puede utilizar para programar la suspensión y reanudación de la transferencia de datos.

Modos de funcionamiento

El script de automatización proporciona 3 modos de ejecución: `configure` , `analyze` y `cron` .

```
if($SCRIPT_MODE -eq "configure") {
        configure
    } elseif ($SCRIPT_MODE -eq "analyze") {
        analyze
    } elseif ($SCRIPT_MODE -eq "cron") {
        runCron
    }
```

- Configurar: realiza las comprobaciones de validación y configura el sistema como con espacio de aire.
- Analizar: función de monitoreo y generación de informes automatizados para enviar información a grupos de monitoreo en busca de anomalías y actividades sospechosas para garantizar que las configuraciones no se desvíen.
- Cron: para habilitar la infraestructura desconectada, el modo cron automatiza la desactivación del LIF e inactiva la relación de transferencia.

Tomará tiempo transferir los datos en esos volúmenes seleccionados dependiendo del rendimiento del sistema y de la cantidad de datos.

```
./script.ps1 -SOURCE_ONTAP_CLUSTER_MGMT_IP "172.21.166.157"
-SOURCE_ONTAP_CLUSTER_NAME "NTAP915_Src" -SOURCE_VSERVER "svm_NFS"
-SOURCE_VOLUME_NAME "Src_RP_Vol01" -DESTINATION_ONTAP_CLUSTER_MGMT_IP
"172.21.166.159" -DESTINATION_ONTAP_CLUSTER_NAME "NTAP915_Destn"
-DESTINATION_VSERVER "svm_nim_nfs" -DESTINATION_AGGREGATE_NAME
"NTAP915_Destn_01_VM_DISK_1" -DESTINATION_VOLUME_NAME "Dst_RP_Vol01_Vault"
-DESTINATION_VOLUME_SIZE "5g" -SNAPLOCK_MIN_RETENTION "15minutes"
-SNAPLOCK_MAX_RETENTION "30minutes" -SNAPMIRROR_PROTECTION_POLICY
"XDPDefault" -SNAPMIRROR_SCHEDULE "5min" -DESTINATION_CLUSTER_USERNAME
"admin" -DESTINATION_CLUSTER_PASSWORD "PASSWORD123"
```

Conclusión de la solución PowerShell de bóveda cibernética de ONTAP

Al aprovechar la separación de aire con metodologías de refuerzo robustas proporcionadas por ONTAP, NetApp le permite crear un entorno de almacenamiento aislado y seguro que es resistente a las amenazas cibernéticas en evolución. Todo esto se logra manteniendo la agilidad y la eficiencia de la infraestructura de almacenamiento existente. Este acceso seguro permite a las empresas alcanzar sus estrictos objetivos de seguridad y tiempo de funcionamiento con cambios mínimos en su marco de personal, procesos y tecnología existentes.

La bóveda cibernética de ONTAP utiliza funciones nativas de ONTAP y constituye un enfoque sencillo para brindar protección adicional y crear copias inmutables e indelebles de sus datos. La incorporación de la bóveda cibernética basada en ONTAP de NetApp a la postura de seguridad general permitirá lo siguiente:

- Cree un entorno que esté separado y desconectado de las redes de producción y de respaldo y restrinja el acceso de los usuarios a él.

Información de copyright

Información de la marca comercial