Ciberalmacén de ONTAP

NetApp Solutions

NetApp
December 19, 2024

Tabla de contenidos

Ciberalmacén de ONTAP

Descripción general de ciberalmacén de ONTAP

La principal amenaza motriz que requiere la implementación de un cibervault es la creciente prevalencia y sofisticación de los ciberataques, en particular ransomware y filtraciones de datos. "Con un aumento en el phishing" y métodos cada vez más sofisticados de robo de credenciales, las credenciales utilizadas para iniciar un ataque de ransomware podrían usarse para acceder a los sistemas de infraestructura. En estos casos, incluso los sistemas de infraestructura reforzados están en riesgo de ataque. La única defensa de un sistema comprometido es tener los datos protegidos y aislados en un ciberalmacén.

El ciberalmacén basado en ONTAP de NetApp ofrece a las organizaciones una solución completa y flexible para proteger sus activos de datos más importantes. Gracias a la separación lógica con metodologías de refuerzo sólidas, ONTAP permite crear entornos de almacenamiento aislados y seguros que son resilientes frente a ciberamenazas en constante evolución. Con ONTAP, puede garantizar la confidencialidad, la integridad y la disponibilidad de sus datos y mantener la agilidad y la eficiencia de su infraestructura de almacenamiento.

> A partir de julio de 2024, el contenido de informes técnicos previamente publicados como archivos PDF se integró con la documentación de los productos de ONTAP. Además, los nuevos informes técnicos (TRS) como este documento ya no obtendrán números TR.

¿Qué es un ciberalmacén?

Una bóveda cibernética es una técnica específica de protección de datos que incluye almacenar datos críticos en un entorno aislado, independiente de la infraestructura de TI primaria.

Repositorio de datos “airgapped”, **inmutable** e **indeleble** que es inmune a las amenazas que afectan a la red principal, como malware, ransomware o incluso amenazas internas. Una bóveda cibernética se puede lograr con instantáneas **inmutable** e **indeleble**.

Las copias de seguridad que utilizan métodos tradicionales implican la creación de espacio y la separación física de los medios primarios y secundarios. Al mover los medios fuera de las instalaciones o cortar la conectividad, los atacantes no tienen acceso a los datos. Esto protege los datos, pero puede producir tiempos de recuperación más lentos.

El enfoque de NetApp del cibervault

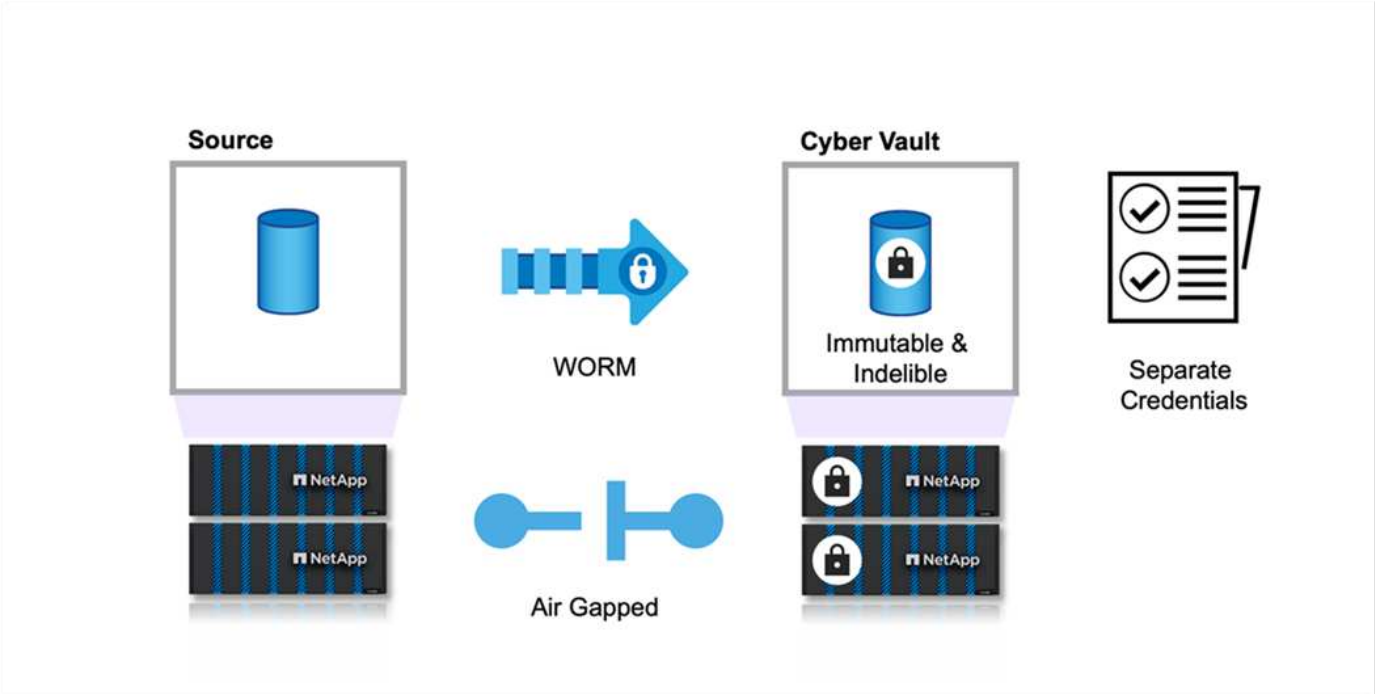
Algunas de las funciones clave de la arquitectura de referencia de NetApp para un ciberalmacén son:

- Infraestructura de almacenamiento aislada y segura (p. ej., sistemas de almacenamiento de red desconectada)
- Las copias de los datos deben ser tanto **inmutable** como **indeleble** sin excepción
- Estrictos controles de acceso y autenticación multifactor
- Funciones de restauración de datos rápida

Puede utilizar almacenamiento de NetApp con ONTAP como ciberalmacén aislado aprovechando el

"SnapLock Compliance para proteger WORM las copias Snapshot". Puede realizar todas las tareas básicas de SnapLock Compliance en el Cibervault. Una vez configurados, los volúmenes de Cyber vault se protegen de forma automática, lo que elimina la necesidad de comprometer manualmente las copias Snapshot en WORM. En esto se puede encontrar más información sobre el chorro lógico de aire "blog"

SnapLock Compliance se utiliza para cumplir las regulaciones bancarias y financieras SEC 70-a-4(f), FINRA 4511(c) y CFTC 1,31(c)-(d). Ha sido certificado por Cohasset Associates para adherirse a estas regulaciones (informe de auditoría disponible a petición). Gracias al uso de SnapLock Compliance con esta certificación, obtendrá un mecanismo reforzado para el intercambio aéreo de datos en el que confían las mayores instituciones financieras del mundo para garantizar tanto la retención como la recuperación de registros bancarios.



Terminología de Cyber vault ONTAP

Estos son los términos comúnmente utilizados en las arquitecturas de ciberalmacén.

- Protección autónoma contra ransomware (ARP) *: La función de protección autónoma contra ransomware (ARP) utiliza análisis de carga de trabajo en entornos de NAS (NFS y SMB) para detectar y advertir de forma proactiva y en tiempo real sobre actividades anormales que podrían indicar un ataque de ransomware. Cuando se sospecha una presencia de un ataque, ARP también crea nuevas copias Snapshot, además de la protección existente frente a copias Snapshot programadas. Para obtener más información, consulte "Documentación de ONTAP sobre protección autónoma frente a ransomware (en inglés)"
- Espacio aéreo (Lógico) * - Puede configurar el almacenamiento NetApp con ONTAP como una cámara cibernética lógica con aire acondicionado mediante el aprovechamiento "SnapLock Compliance para proteger WORM las copias Snapshot"

Air-gap (físico) - Un sistema físico de aire acondicionado no tiene conectividad de red a él. Con las copias de seguridad en cinta, puede mover las imágenes a otra ubicación. La red de aire lógica SnapLock Compliance es tan robusta como un sistema físico de aire acondicionado.

Bastion host - Un ordenador dedicado en una red aislada, configurado para resistir ataques.

Copias instantáneas inmutables - Copias instantáneas que no se pueden modificar, sin excepción (incluida una organización de soporte o la capacidad de dar un formato de bajo nivel al 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 el sistema de almacenamiento de bajo nivel).

- Copias instantáneas a prueba de manipulaciones * - Las copias instantáneas a prueba de manipulaciones utilizan la función de reloj SnapLock Compliance para bloquear las copias instantáneas durante un período específico. Estos snapshots bloqueados no pueden ser eliminados por ningún usuario o soporte de NetApp. Puede utilizar copias de Snapshot bloqueadas para recuperar datos si un volumen se ve afectado por un ataque de ransomware, malware, hackers, administrador malintencionado o una eliminación accidental. Para obtener más información, consulte "Documentación de ONTAP en copias Snapshot a prueba de manipulaciones"

SnapLock - SnapLock es una solución de cumplimiento de alto rendimiento para organizaciones que utilizan almacenamiento WORM para retener archivos en forma no modificada con fines regulatorios y de gobierno. Para obtener más información, consulte la "Documentación de ONTAP en SnapLock".

SnapMirror - SnapMirror es una tecnología de replicación de recuperación de desastres, diseñada para replicar datos de manera eficiente. SnapMirror puede crear un mirroring (o una copia exacta de los datos), un almacén (una copia de los datos con una mayor retención de copia de Snapshot) o ambos en un sistema secundario, en las instalaciones o en el cloud. Estas copias pueden utilizarse para distintos fines, como un desastre, una irrupción en el cloud o un ciberalmacén (cuando se usa la normativa de almacén y se bloquea el vault). Para obtener más información, consulte "Documentación de ONTAP en SnapMirror"

SnapVault - En ONTAP 9.3 SnapVault fue descartado a favor de la configuración de SnapMirror usando la política de vault o mirror-vault. Este es el término, aunque todavía se utiliza, también se ha depreciado. Para obtener más información, consulte la "Documentación de ONTAP en SnapVault".

Dimensionamiento de cibervault con ONTAP

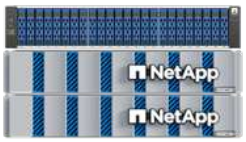
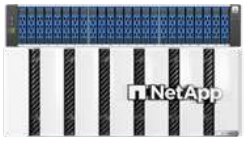
Para ajustar el tamaño de un ciberalmacén es necesario comprender cuántos datos se necesitarán restaurar en un determinado objetivo de tiempo de recuperación. Hay muchos factores que influyen en el diseño adecuado de una solución de ciberalmacén del tamaño adecuado. Se debe tener en cuenta tanto el rendimiento como la capacidad al ajustar el tamaño de un cibervault.

Consideraciones sobre el tamaño 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 el origen y el ciberalmacén?
3. ¿Qué tamaño tienen los archivos y cuántos archivos?
4. ¿Cuál es su objetivo de tiempo de recuperación?
5. ¿Qué cantidad de datos necesita recuperar dentro del RTO?
6. ¿Cuántas relaciones de fan-in de SnapMirror procesará el cibervault?
7. ¿Se producirán recuperaciones únicas o múltiples al mismo tiempo?
8. ¿Ocurrirán esas múltiples recuperaciones en el mismo primario?
9. ¿SnapMirror se replicará en el almacén durante una recuperación desde un almacén?

Ejemplos de tamaños

A continuación se muestran ejemplos de diferentes configuraciones de ciberalmacén.

				
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 ciberalmacén ONTAP depende de diversos factores, siendo el más importante la tasa de cambio de los datos del volumen de origen. La programación de backups y la programación de Snapshot en el volumen de destino afectan tanto al uso de disco del volumen de destino como a la tasa de cambio del volumen de origen no es probable que sea constante. Es una buena idea proporcionar un búfer de capacidad de almacenamiento adicional superior a la necesaria para adaptarse a los cambios futuros en el comportamiento de los usuarios finales o las aplicaciones.

Para dimensionar una relación durante 1 mes de retención en ONTAP, debe calcular los requisitos de almacenamiento en función de varios factores, como el tamaño del conjunto de datos principal, la tasa de cambio de los datos (tasa de cambio diaria) y el ahorro en deduplicación y compresión (si procede).

Este es el enfoque paso a paso:

El primer paso es conocer el tamaño de los volúmenes de origen que está protegiendo con el almacén cibernético. Esta es la cantidad base de datos que se replicará inicialmente en el destino del ciberalmacén. A continuación, calcule la tasa de cambio diaria del conjunto de datos. Este es el porcentaje de datos que cambia cada día. Es crucial tener una buena comprensión de lo dinámicos que son los datos.

Por ejemplo:

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

Ahora, veamos el cálculo:

- Calcule la tasa de cambio diaria de datos:

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

- Calcule los datos totales modificados en 30 días:

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

- Calcule el almacenamiento total necesario:

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

- Aplique el ahorro en deduplicación y compresión:

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

Resumen de las necesidades de almacenamiento

- Sin eficiencia: Requeriría **12,5TB** para almacenar 30 días de los datos de la bóveda cibernética.
- Con una eficiencia del 50%: Requeriría **6,25TB** de almacenamiento después de la deduplicación y la compresión.

Las copias Snapshot pueden tener una sobrecarga adicional debido a los metadatos, pero esto suele ser menor.

Si se realizan varios backups por día, ajuste el cálculo según el número de copias snapshot realizadas cada día.

Factor de crecimiento de datos a lo largo del tiempo para garantizar que el tamaño esté preparado para el futuro.

Crear un ciberalmacén con ONTAP

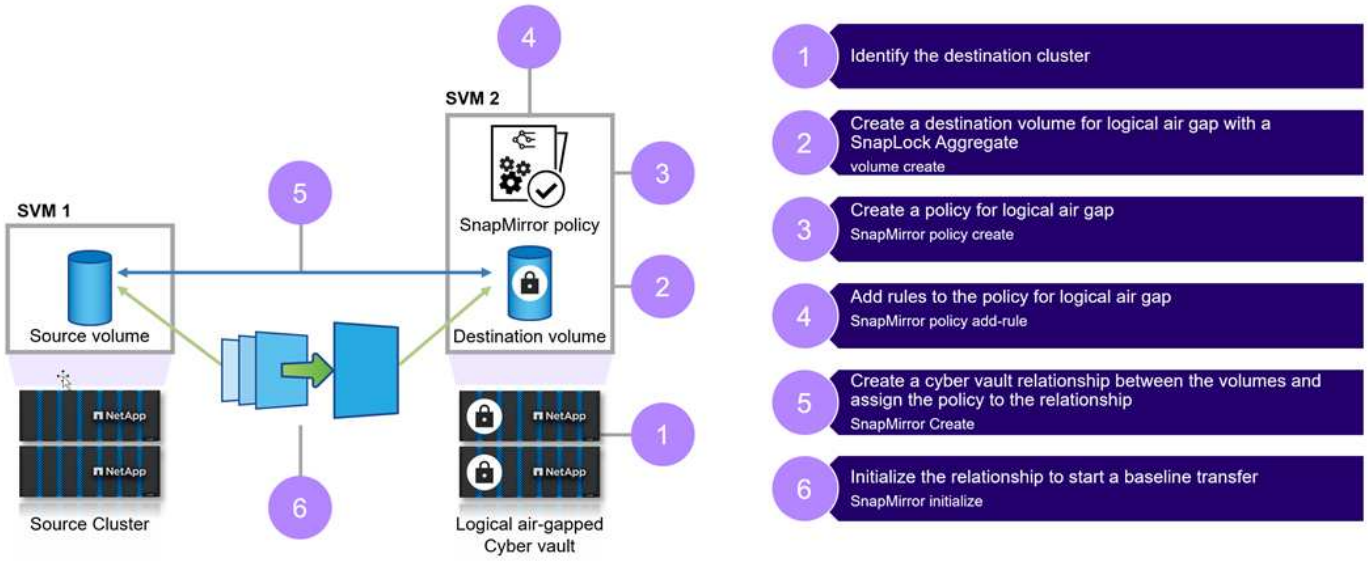
Los pasos a continuación ayudarán con la creación de una bóveda cibernética con ONTAP.

Antes de empezar

- El clúster de origen debe ejecutar ONTAP 9 o una versión posterior.
- Los agregados de origen y destino deben tener 64 bits.
- Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM. Para obtener más información, consulte "Conexión de clústeres entre iguales".
- Si se deshabilita el crecimiento automático de un volumen, el espacio libre en el volumen de destino debe ser al menos un cinco por ciento mayor que el espacio usado en el volumen de origen.

Acerca de esta tarea

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de almacén de SnapLock Compliance:



Pasos

1. Identifique la cabina de destino que se convertirá en el ciberalmacén para recibir los datos aislados.
2. En la matriz de destino, para preparar el almacén cibernético, "Instale la licencia de ONTAP One" "Inicialice el reloj de cumplimiento", y, si está utilizando una versión de ONTAP anterior a 9.10.1, "Cree un agregado de SnapLock Compliance".
3. En la cabina de destino, cree un volumen de destino 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 de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. Puede usar `-snaplock-type` la opción volume para especificar un tipo Compliance. En las versiones de ONTAP anteriores a ONTAP 9.10,1, en el modo SnapLock, Compliance se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. 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 SnapLock Compliance de 2GB GB llamado `dstvolB SVM2` en el agregado `node01_aggr`:

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

5. En el clúster de destino, para crear el espacio de aire, establezca el período de retención predeterminado, como se describe en "Establecer el período de retención predeterminado". Un volumen SnapLock que es un destino de almacén tiene asignado un período de retención predeterminado. El valor de este período se establece inicialmente en un mínimo de 0 años y un máximo de 100 años (a partir de ONTAP 9.10,1. En versiones anteriores de ONTAP, el valor es 0 - 70) para volúmenes SnapLock Compliance. Cada copia de Snapshot de NetApp se compromete con el primer período de retención predeterminado. Debe cambiarse el período de retención predeterminado. El período de retención se puede ampliar más tarde, si es necesario, pero nunca acortar. Para obtener más información, consulte "Establecer información general sobre el tiempo de retención".

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 del ciberalmacén es de 30 días y el contrato del cliente finaliza antes de que expire el período de retención, los datos del ciberalmacén no se podrán eliminar hasta que expire el período de retención.

6. "Cree una nueva relación de replicación" Entre el origen que no es de SnapLock y el nuevo destino de SnapLock que creó en el Paso 3.

   Este ejemplo crea una nueva relación de SnapMirror con el volumen SnapLock de destino dstvolB mediante una política de XDPDefault para almacenar copias Snapshot etiquetadas diariamente y semanalmente en una programación horaria:

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

   "Cree una política de replicación personalizada" o un "programación personalizada" si los valores predeterminados disponibles no son adecuados.

7. En la SVM de destino, inicialice la relación de 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 y inactiva la relación, utilice el comando snapshot show en el destino para comprobar el tiempo de caducidad de la SnapLock aplicado a las copias Snapshot replicadas.

   En este ejemplo, se enumeran las copias Snapshot en el volumen dstvolB que tienen la etiqueta de SnapMirror y la fecha de vencimiento de SnapLock:

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

Endurecimiento de Cyber vault

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

Recomendaciones de endurecimiento de Cyber vault

- Aísle los planos de gestión del ciberalmacén
- No habilite las LIF de datos en el clúster de destino porque son una vía de ataque adicional
- En el clúster de destino, limite el acceso de LIF entre clústeres al clúster de origen mediante una política de servicio
- Segmente el LIF de gestión en el clúster de destino para disfrutar de un acceso limitado con una política

de servicio y un host de bastion

- Restrinja todo el tráfico de datos del clúster de origen al ciberalmacén para permitir solo los puertos necesarios para el tráfico de SnapMirror
- Siempre que sea posible, deshabilita los métodos de acceso a la gestión innecesarios de ONTAP para reducir la superficie de ataque
- Active el registro de auditoría y el almacenamiento remoto de registros
- Permite la verificación multiadministradora y requiere la verificación de un administrador externo a los habituales de su almacenamiento (por ejemplo, personal de CISO).
- Implemente controles de acceso basados en roles
- Requiere una autenticación multifactor administrativa para System Manager y ssh
- Use la autenticación basada en tokens para los scripts y las llamadas de la API DE REST

Consulte la "Guía de endurecimiento de ONTAP", "Información general de verificación de varios administradores" y "Guía de autenticación multifactor de ONTAP" para obtener información sobre cómo llevar a cabo estos pasos de endurecimiento.

Interoperabilidad de Cyber vault

El hardware y software de ONTAP se pueden usar para crear una configuración de ciberalmacén.

Recomendaciones de hardware de ONTAP

Todas las cabinas físicas unificadas de ONTAP se pueden utilizar para la implementación de ciberalmacén.

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

Recomendaciones de software de ONTAP

A partir de ONTAP 9.14,1, puede especificar períodos de retención para etiquetas de SnapMirror específicas en la política de SnapMirror de la relación de SnapMirror, de modo que las copias Snapshot replicadas del volumen de origen al 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 al instante una copia Snapshot bloqueada en el volumen SnapLock de destino de una relación de almacén de SnapLock. Para ello, cree una FlexClone con la opción de tipo SnapLock configurada en «non-SnapLock» y especifique la copia Snapshot como la «snapshot principal» al ejecutar la operación de creación de clones de volúmenes. Más información sobre "Creación de un volumen FlexClone con un tipo de SnapLock".

Configuración de MetroCluster

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

- Solo puede crear relaciones de SnapVault entre varias SVM sincronizada en origen, no entre una SVM sincronizada en origen y una SVM sincronizada en destino.
- Puede crear una relación de SnapVault entre un volumen en una SVM sincronizada en origen y una SVM que sirva datos.
- Puede crear una relación de SnapVault entre un volumen en una SVM que sirva datos y un volumen de DP en una SVM sincronizada en origen.

Preguntas frecuentes sobre Cyber Vault

Estas preguntas frecuentes están dirigidas a clientes y partners de NetApp. Responde a preguntas frecuentes acerca de la arquitectura de referencia de ciberalmacenes basada en ONTAP de NetApp.

¿Qué es un ciberalmacén de NetApp?

Cyber vault es una técnica específica de protección de datos que implica almacenar datos en un entorno aislado, independiente de la infraestructura TECNOLÓGICA primaria.

Cyber vault es un repositorio de datos «aislado», inmutable e indeleble que es inmune a las amenazas que afectan a los datos principales, como malware, ransomware o amenazas internas. Un ciberalmacén se puede conseguir con copias Snapshot inmutables de NetApp ONTAP y hacerlo indeleble con NetApp SnapLock Compliance. Mientras se encuentra en la protección SnapLock Compliance, los datos no se pueden modificar ni eliminar, ni siquiera por los administradores de ONTAP ni el soporte de NetApp.

El intercambio de aire que utiliza métodos tradicionales implica la creación de espacio y la separación física de los medios primarios y secundarios. La falta de aire con cibervault incluye el uso de una red de replicación de datos independiente fuera de las redes de acceso a datos estándar para replicar las copias Snapshot en un destino indeleble.

Otros pasos más allá de las redes aisladas implican deshabilitar todos los protocolos de acceso a los datos y replicación en el ciberalmacén cuando no son necesarios. De este modo se evita el acceso a los datos o la exfiltración de datos en el sitio de destino. Con SnapLock Compliance no es necesaria la separación física. SnapLock Compliance protege las copias snapshot vault de un momento específico y de solo lectura, lo que permite recuperar datos rápidamente, evitar la eliminación e inalterable.

El enfoque de NetApp del cibervault

El ciberalmacén de NetApp, con tecnología de SnapLock, ofrece a las organizaciones una solución completa y flexible para proteger sus activos de datos más importantes. Al aprovechar las tecnologías de refuerzo de ONTAP, NetApp te permite crear un cibervault seguro, aislado y sin explotar que sea inmune a las ciberamenazas en constante evolución. Con NetApp, puede garantizar la confidencialidad, la integridad y la disponibilidad de sus datos y mantener la agilidad y la eficiencia de su infraestructura de almacenamiento.

Algunas de las funciones clave de la arquitectura de referencia de NetApp para un ciberalmacén son:

- Infraestructura de almacenamiento aislada y segura (p. ej., sistemas de almacenamiento de red desconectada)
- Las copias de backup de sus datos son inalterables e indelebles
- Controles de acceso estrictos y separados, verificación multiadministrador y autenticación multifactor
- Funciones de restauración de datos rápida

Preguntas frecuentes sobre Cyber Vault

¿El ciberalmacén es un producto de NetApp?

No, «ciberalmacén» es un término que se aplica a todo el sector. NetApp ha creado una arquitectura de referencia para que los clientes puedan crear sus propias bóvedas cibernéticas y aprovechar las numerosas funciones de seguridad de ONTAP para ayudar a proteger sus datos de las ciberamenazas. Más información está disponible en el "Sitio de documentación de ONTAP".

¿El ciberalmacén con NetApp es solo otro nombre para LockVault o SnapVault?

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

SnapVault era un término heredado para lo que se logra ahora con la política de almacén de SnapMirror. Esta política permite al destino conservar una cantidad distinta de copias Snapshot al volumen de origen.

Cyber vault está usando SnapMirror con la política de almacén y SnapLock Compliance juntos para crear una copia de datos inalterable e indeleble.

¿Qué hardware de NetApp puedo usar para un ciberalmacén, FAS, flash de capacidad o flash de rendimiento?

Esta arquitectura de referencia para copias vault se aplica a toda la cartera de hardware de ONTAP. Los clientes pueden usar las plataformas AFF A-Series, AFF C-Series o FAS como almacén. Las plataformas basadas en Flash proporcionarán los tiempos de recuperación más rápidos, mientras que las plataformas basadas en disco proporcionarán la solución más rentable. Según la cantidad de datos que se recuperen y si se realizan varias recuperaciones en paralelo, el uso de sistemas basados en disco (FAS) puede tardar entre días y semanas en completarse. Póngase en contacto con un representante de NetApp o de un partner para determinar correctamente la solución de ciberalmacén y cumplir los requisitos del negocio.

¿Puedo usar Cloud Volumes ONTAP como fuente de ciberalmacén?

Sí, sin embargo, el uso de CVO como origen requiere la replicación de los datos en un destino de ciberalmacén on-premises, ya que SnapLock Compliance es un requisito para un ciberalmacén de ONTAP. La replicación de datos de una instancia de CVO basada en un proveedor a hiperescala puede incurrir en cargos por salida.

¿Puedo usar Cloud Volumes ONTAP como destino de ciberalmacén?

La arquitectura de Cyber Vault se basa en la imposibilidad de borrado de SnapLock Compliance de ONTAP y está diseñada para implementaciones en las instalaciones. Las arquitecturas Cyber Vault basadas en la nube están siendo investigadas para su futura publicación.

¿Puedo usar ONTAP Select como fuente de ciberalmacén?

Sí, ONTAP Select se puede usar como origen en un destino de ciberalmacén basado en hardware en las instalaciones.

¿Puedo usar ONTAP Select como destino de ciberalmacén?

No, no se debe utilizar ONTAP Select como destino de ciberalmacenes, ya que no tiene la capacidad de utilizar SnapLock Compliance.

¿Un ciberalmacén con NetApp solo usa SnapMirror?

No, una arquitectura de almacén cibernético de NetApp aprovecha muchas funciones de ONTAP para crear una copia de datos segura, aislada, con conexión inalámbrica y reforzada. Para obtener más información sobre qué técnicas adicionales se pueden utilizar, consulte la siguiente pregunta.

¿Se utiliza alguna otra tecnología o configuración para el cibervault?

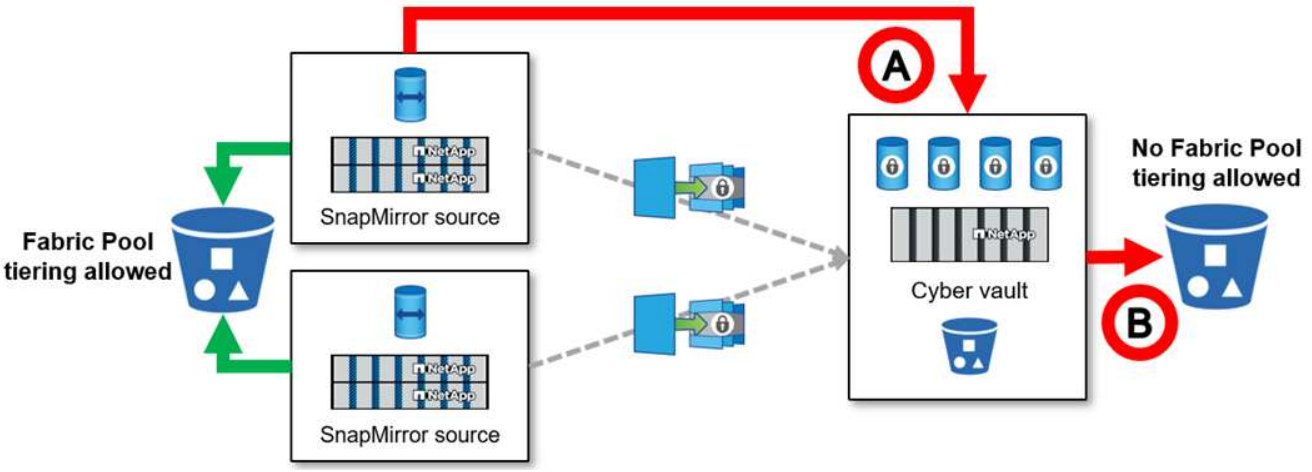
La base de un ciberalmacén de NetApp es SnapMirror y SnapLock Compliance, pero el uso de funciones de ONTAP adicionales, como copias Snapshot a prueba de manipulaciones, autenticación multifactor (MFA), verificación de administrador múltiple, control de acceso basado en roles y registro de auditorías local y remoto, mejora la seguridad de los datos.

¿Qué hace que las copias Snapshot de ONTAP sean mejores que otras para un ciberalmacén?

Las copias Snapshot de ONTAP son inmutables de forma predeterminada y se pueden hacer indelebles con SnapLock Compliance. Ni siquiera la compatibilidad con NetApp puede eliminar las copias Snapshot de SnapLock. La mejor pregunta que se debe hacer es qué hace que la ciberbóveda de NetApp sea mejor que otras bóvedas cibernéticas en 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 en "CSfC se puede encontrar aquí". Además, la tecnología ONTAP puede conectarse mediante aire en la capa de almacenamiento, mientras que el sistema de ciberalmacén controla la replicación, lo que permite crear una red desconectada en la red de ciberalmacenes.

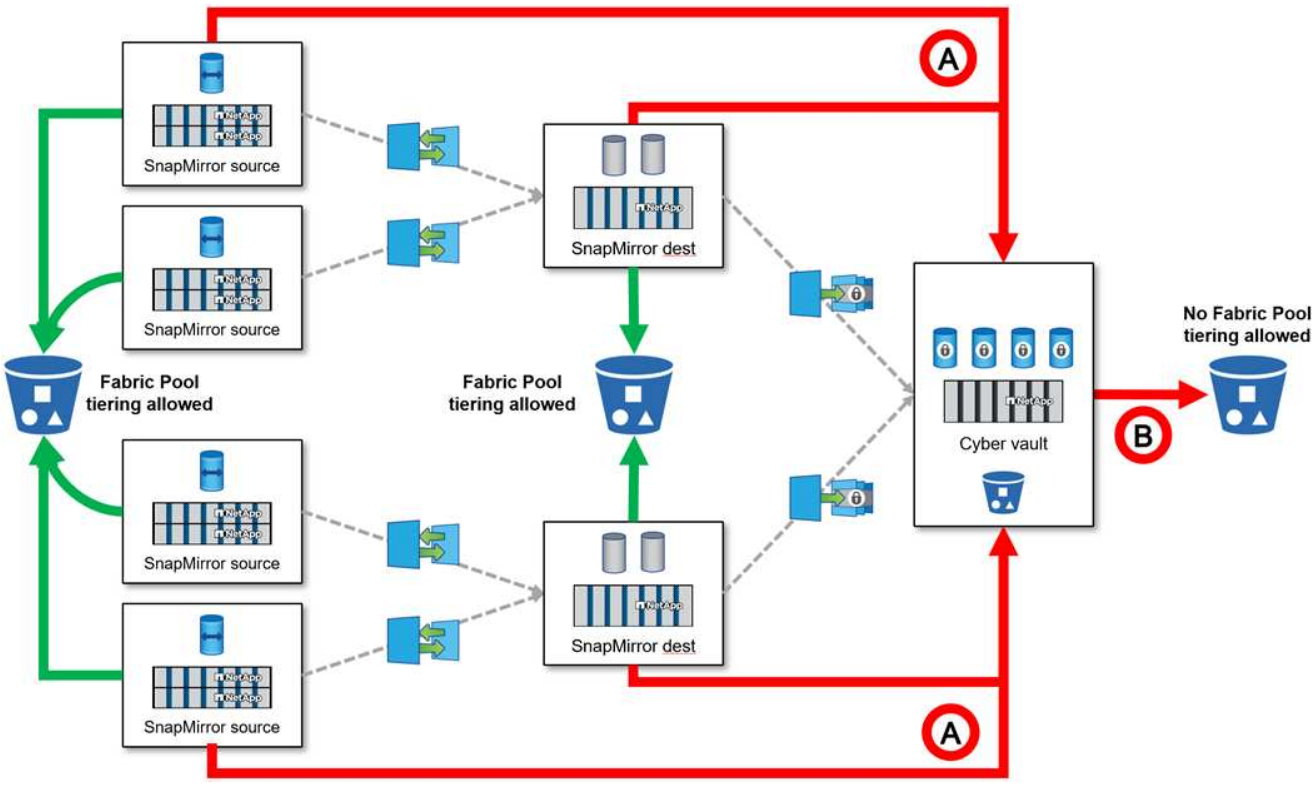
¿Un volumen de un ciberalmacén puede usar Fabric Pool de ONTAP?

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



Hay múltiples escenarios en los que Fabric pool **no** se puede utilizar con una bóveda cibernética.

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



¿Está disponible ONTAP S3 Worm en un ciberalmacén?

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

¿El ciberalmacén de NetApp se ejecuta en una personalidad o un perfil de ONTAP diferente?

No, es una arquitectura de referencia. Los clientes pueden usar "flexible y escalable"y construir una bóveda cibernética, o pueden usar "Scripts de PowerShell para crear, reforzar y validar"una bóveda cibernética.

¿Puedo activar protocolos de datos como NFS, SMB y S3 en un ciberalmacén?

De forma predeterminada, los protocolos de datos deben desactivarse en el ciberalmacén para que sea seguro. Sin embargo, se pueden habilitar los protocolos de datos en el ciberalmacén para acceder a los datos para su recuperación o cuando sea necesario. Debe realizarse de forma temporal y desactivarse una vez finalizada la recuperación.

¿Puede convertir un entorno existente de SnapVault en un ciberalmacén, o tiene que revender todo?

Sí. Uno podría tomar un sistema que es un destino SnapMirror (con directiva de almacén), deshabilitar los protocolos de datos, endurecer el sistema según "Guía de endurecimiento de ONTAP", aislarlo de una ubicación segura y seguir los demás procedimientos de la arquitectura de referencia para convertirlo en un almacén cibernético sin tener que revender el destino.

Tiene preguntas adicionales? Por favor envíe un correo electrónico a: Ng-cyber-vault@NetApp.com[ng-cyber-vault@NetApp.com^,Preguntas sobre Cyber vault,Me gustaría saber más sobre:] Con sus preguntas! Responderemos y añadiremos sus preguntas a la FAQ.

Recursos de cibervault

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

- "Cibervault de NetApp: Resumen de soluciones de protección de datos en varias capas"
- "NetApp obtiene la calificación AAA para la primera solución de detección de ransomware integrada basada en IA del sector"
- "Mejora la resiliencia digital con el almacenamiento más seguro del planeta"
- "Guía de fortalecimiento de seguridad de ONTAP"
- "Confianza cero de NetApp"
- "Resiliencia digital de NetApp"
- "Protección de datos de NetApp"
- "Información general sobre relaciones entre iguales de clústeres y SVM con la CLI"
- "Archivado SnapVault"
- "Configurar, analizar, cron script"

Creación, refuerzo y validación de un ciberalmacén de ONTAP con PowerShell

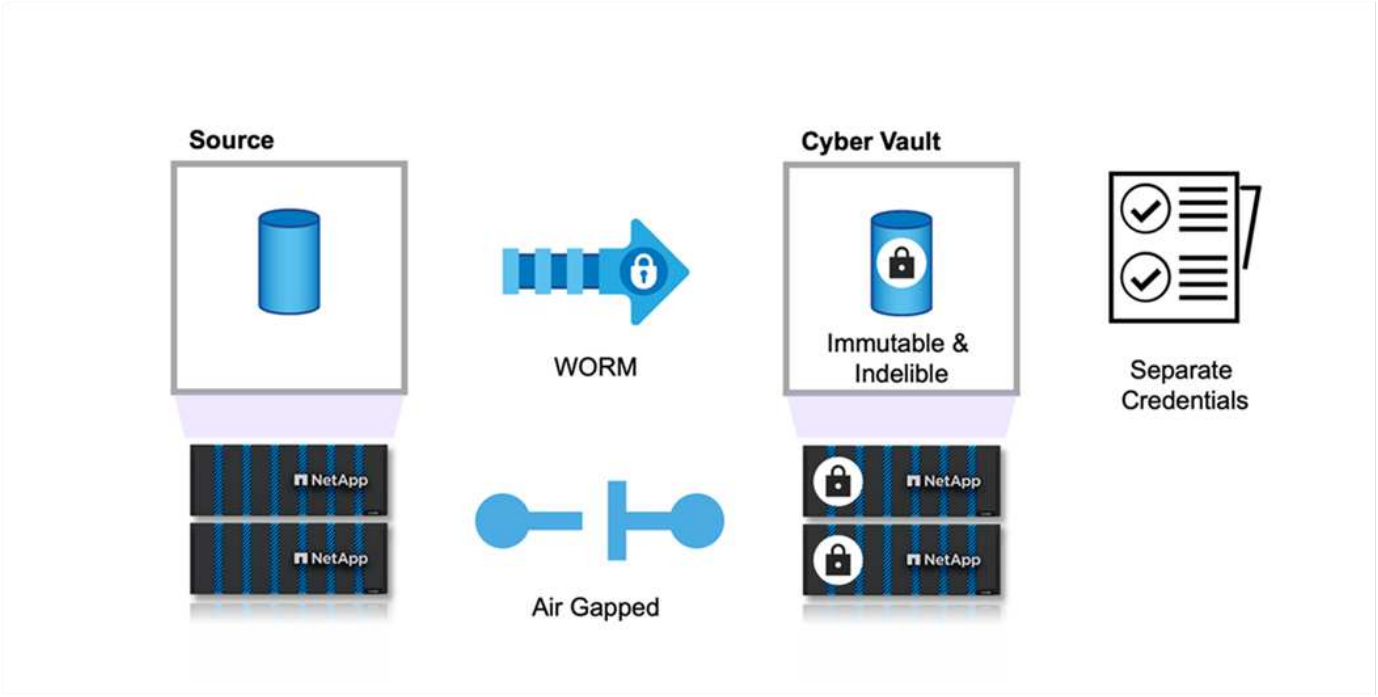
Descripción general de ONTAP cyber vault con PowerShell

En el panorama digital actual, proteger los activos de datos importantes de una empresa no es solo una práctica recomendada: Es un imperativo empresarial. Las amenazas cibernéticas evolucionan a un ritmo sin precedentes y las medidas tradicionales de protección de datos ya no son suficientes para proteger la información confidencial. Aquí es donde entra en juego una ciberbóveda, la solución de vanguardia basada en ONTAP de NetApp combina técnicas avanzadas de chorro de aire con sólidas medidas de protección de datos para crear una barrera impenetrable contra las ciberamenazas. Al aislar los datos más valiosos con tecnología de endurecimiento seguro, un ciberalmacén minimiza la superficie de ataque para que los datos más cruciales permanezcan confidenciales, intactos y disponibles cuando sea necesario.

Un ciberalmacén es una instalación de almacenamiento seguro que consta de varias capas de protección, como firewalls, redes y almacenamiento. Estos componentes protegen los datos esenciales de recuperación necesarios para operaciones empresariales cruciales. Los componentes del almacén cibernético se sincronizan regularmente con los datos de producción esenciales basados en la política de almacén, 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 fiable desde el ciberalmacén.

NetApp permite crear fácilmente una red desconectada para ciberalmacén mediante la configuración de la red, la deshabilitación de las LIF, la actualización de las reglas de firewall y el aislamiento del sistema de redes externas e Internet. Este enfoque robusto desconecta efectivamente el sistema de las redes externas e Internet, proporcionando una protección sin igual 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.

Si se combina esto con la protección de SnapLock Compliance, los datos no se pueden modificar ni eliminar, ni siquiera por los administradores de ONTAP ni por los servicios de soporte de NetApp. SnapLock realiza una auditoría periódica contra las normativas SEC y FINRA, garantizando que la resiliencia de los datos cumpla las estrictas normativas en materia de retención de DATOS y WORM del sector bancario. NetApp es el único sistema de almacenamiento empresarial validado por NSA CSfC que almacena datos confidenciales.



Este documento describe la configuración automatizada del ciberalmacén de NetApp para el almacenamiento ONTAP en las instalaciones a otro almacenamiento ONTAP designado con copias Snapshot inmutables. Además, se añade una capa adicional de protección frente al aumento de ciberataques para una rápida recuperación. Como parte de esta arquitectura, se aplica toda la configuración según las prácticas recomendadas de ONTAP. La última sección tiene instrucciones para realizar una recuperación en caso de un ataque.

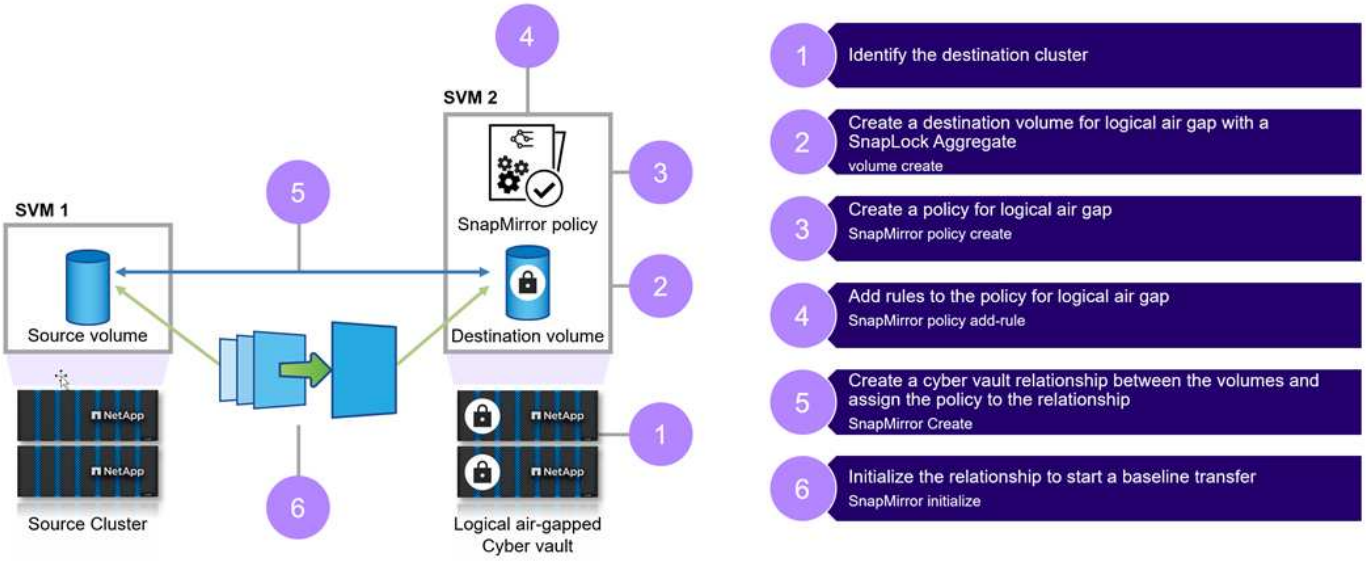
La misma solución se puede aplicar para crear el ciberalmacén designado en AWS mediante FSx ONTAP.

Pasos de alto nivel para crear una bóveda cibernética ONTAP

- Creación de una relación entre iguales
  - El sitio de producción que utiliza el almacenamiento de ONTAP está relacionado con el almacenamiento ONTAP de ciberalmacén designado
- Crear volumen de SnapLock Compliance
- Configure la relación y la regla de SnapMirror para definir la etiqueta
  - Se configura la relación con SnapMirror y los programas apropiados
- Establecer retenciones antes de iniciar la transferencia SnapMirror (almacén)
  - El bloqueo de retención se aplica a los datos copiados, lo que evita aún más que los datos puedan provocar fallos internos o de datos. Con esto, los datos no se pueden eliminar antes de que expire el período de retención
  - Las organizaciones pueden conservar estos datos durante varias semanas o meses en función de sus requisitos
- Inicialice la relación de SnapMirror según las etiquetas
  - La propagación inicial y la transferencia permanente incremental se producen según la programación de SnapMirror
  - Los datos se protegen (inmutables e indelebles) con SnapLock Compliance, y que los datos están

disponibles para recuperar

- Implemente estrictos controles de transferencia de datos
  - Cyber vault se desbloquea durante un período limitado con datos del sitio de producción y se sincroniza con los datos del almacén. Una vez completada la transferencia, la conexión se desconecta, se cierra y se vuelve a bloquear
- Recuperación rápida
  - Si los datos primarios se ven afectados en el sitio de producción, los datos del ciberalmacén se recuperan de forma segura a la producción original o a otro entorno elegido



Componentes de la solución

NetApp ONTAP que ejecuta 9.15.1 en los clústeres de origen y destino.

ONTAP One: Licencia todo en uno de NetApp ONTAP.

Funcionalidades que se usan con la licencia de ONTAP One:

- Cumplimiento de normativas SnapLock
- SnapMirror
- Verificación de varios administradores
- Todas las capacidades de fortalecimiento a las que ONTAP expone
- Credenciales de RBAC independientes para el almacén cibernético

Todas las cabinas físicas unificadas ONTAP se pueden usar para un ciberalmacén, sin embargo, los sistemas flash basados en capacidad de la serie C de AFF y los sistemas de flash híbrido FAS son las plataformas ideales más rentables para este fin. Consulte "Ajuste de tamaño de cibervault de ONTAP"para obtener orientación sobre el tamaño.

Creación de ciberalmacenes de ONTAP con PowerShell

Las copias de seguridad que utilizan métodos tradicionales implican la creación de espacio y la separación física de los medios primarios y secundarios. Al mover los

medios fuera del sitio o cortar la conectividad, los atacantes no tienen acceso a los datos. Esto protege los datos, pero puede producir tiempos de recuperación más lentos. Con SnapLock Compliance no es necesaria la separación física. SnapLock Compliance protege las copias vault de un momento específico y de solo lectura, lo que permite acceder a los datos con rapidez, a los que se pueden eliminar o indelebles, y a salvo de las modificaciones o inmutables.

Requisitos previos

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

- El clúster de origen debe ejecutar ONTAP 9 o una versión posterior.
- Los agregados de origen y destino deben tener 64 bits.
- Los clústeres de origen y destino deben tener una relación entre iguales.
- Las SVM de origen y destino deben tener una relación entre iguales.
- Asegúrese de que el cifrado de interconexión de clústeres esté habilitado.

La configuración de las transferencias de datos a un ciberalmacén de ONTAP requiere varios pasos. En el volumen primario, configure una política de Snapshot que especifique qué copias crear y cuándo crearlas mediante programaciones adecuadas y etiquetas para especificar qué copias debe transferir SnapVault. En el almacenamiento secundario, debe crearse una política de SnapMirror que especifique las etiquetas de las copias snapshot que se van a transferir y cuántas de estas copias deben guardarse en el ciberalmacén. Después de configurar estas políticas, cree la relación SnapVault y establezca una programación de transferencia.

Este documento asume que el almacenamiento principal y el ciberalmacén designado de ONTAP ya están instalados y configurados.

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

Pasos para crear un ciberalmacén ONTAP

1. Use la interfaz de línea de comandos de ONTAP o System Manager para inicializar el reloj de cumplimiento de normativas.
2. Crear un volumen de protección de datos con SnapLock Compliance habilitado.
3. Use el comando SnapMirror create 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 se establece en Mínimo. Un volumen SnapLock que es un destino de almacén tiene asignado un período de retención predeterminado. El valor de este período se establece inicialmente en un mínimo de 0 años y un máximo de 100 años (a partir de ONTAP 9.10,1. En versiones anteriores de ONTAP, el valor es 0 - 70) para volúmenes SnapLock Compliance. Cada copia de Snapshot de NetApp se compromete con el primer período de retención predeterminado. El período de retención se puede ampliar más tarde, si es necesario, pero nunca acortar. Para obtener más información, consulte "Establecer información general sobre el tiempo de retención".

Lo anterior abarca pasos manuales. Los expertos en seguridad aconsejan automatizar el proceso para evitar la gestión manual, lo que introduce un gran margen de error. A continuación se muestra el fragmento de código que automatiza completamente los requisitos previos y la configuración de SnapLock Compliance y la inicialización del reloj.

Este es un ejemplo de código de PowerShell para inicializar el reloj de cumplimiento de normativas 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
    }
}
```

Este es un ejemplo de código de PowerShell para configurar un ciberalmacén 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 que se hayan completado los pasos anteriores, el ciber vault de red aérea con SnapLock Compliance y SnapVault está listo.

Antes de transferir datos de snapshots al ciberalmacén, debe inicializarse la relación de SnapVault. Sin embargo, antes de eso, es necesario realizar un refuerzo de la seguridad para proteger el almacén.

Refuerzo del ciberalmacén de ONTAP con PowerShell

El ciberalmacén de ONTAP proporciona una mayor resiliencia contra ciberataques en comparación con las soluciones tradicionales. Al diseñar una arquitectura para mejorar la seguridad, es crucial considerar medidas para reducir la superficie de ataque. Esto se puede lograr a través de 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 del almacén. Además, restringir los protocolos de acceso a la red desde una dirección IP específica puede ayudar a limitar las vulnerabilidades potenciales.

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

Refuerzo de las prácticas recomendadas

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 de que todas las reglas se auditen y actualicen regularmente según sea necesario.

ONTAP CLI o a través de secuencias de comandos de automatización

1. Protege la administración con la verificación multiadministrador (MFA)
2. Habilite el cifrado de datos estándar en tránsito entre clústeres.
3. Asegure SSH con cifrado fuerte y aplique contraseñas seguras.
4. Habilite FIPS global.
5. Telnet y Remote Shell (RSH) deben estar desactivados.
6. Bloquear cuenta de administrador predeterminada.
7. Desactive las LIF de datos y los puntos de acceso remoto seguros.
8. Desactive y elimine los protocolos y servicios no utilizados o ajenos.
9. Cifrar el tráfico de red.
10. Utilice el principio de privilegio mínimo al configurar roles de superusuario y administrativos.
11. Restrinja HTTPS y SSH desde una dirección IP específica mediante la opción IP permitida.
12. Desactivar y reanudar la replicación según la programación de transferencias.

Bullets 1-4 necesita intervención manual como designar una red aislada, segregar el espacio IP, etc., y debe realizarse de antemano. La información detallada para configurar el endurecimiento se puede encontrar en el "Guía de fortalecimiento de seguridad de ONTAP". El resto se puede automatizar fácilmente para facilitar la implementación y la supervisión. El objetivo de este enfoque coordinado es proporcionar un mecanismo para automatizar los pasos de endurecimiento para probar el controlador de vault en el futuro. El intervalo de tiempo que la brecha de aire de la bóveda cibernética está abierta es lo más corto posible. SnapVault aprovecha la tecnología incremental Forever, 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 del almacén cibernético se coordina con el programa de replicación para garantizar la ventana de conexión más pequeña.

A continuación se muestra un ejemplo de código de PowerShell para endurecer 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 ciberalmacén de ONTAP con PowerShell

Un ciberalmacén robusto debería ser capaz de soportar un ataque sofisticado, incluso cuando el atacante tiene credenciales para acceder al entorno con Privileges elevado.

Una vez que las reglas están en su lugar, un intento (asumiendo de alguna manera que el atacante pudo entrar) de eliminar una instantánea en el lado del almacén fallará. Lo mismo se aplica con todos los ajustes de endurecimiento mediante la colocación de las restricciones necesarias y la protección del sistema.

Ejemplo de código de PowerShell para validar la configuración según la programación.

```
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 del almacén.

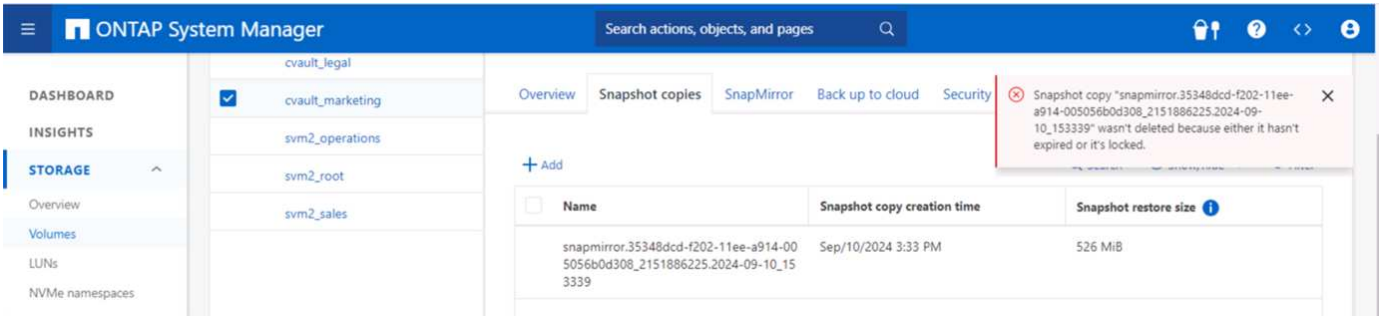
```
cluster2::> network connections  listening show
This table is currently empty.

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 hay posibilidad de alterar las instantáneas.



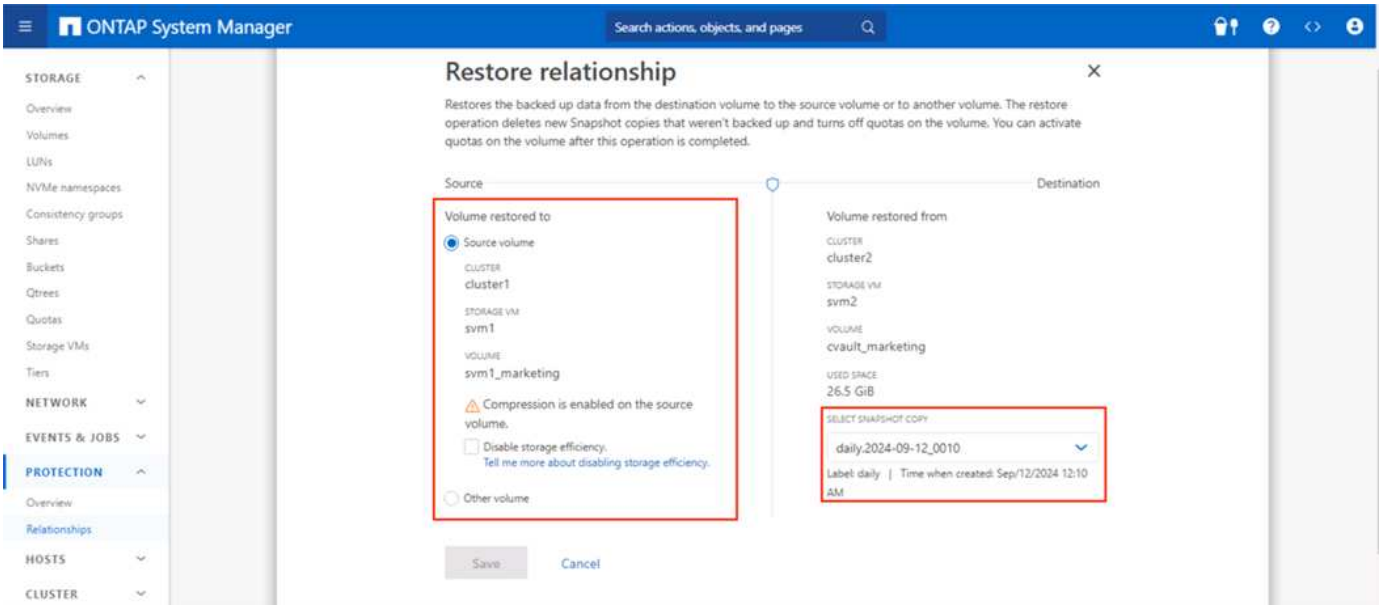
Para validar y confirmar la funcionalidad de aire-gapping, siga los pasos siguientes:

- Probar las capacidades de aislamiento de red y la capacidad de desactivar una conexión cuando no se transfieren datos.
- Compruebe que no se pueda acceder a la interfaz de gestión desde ninguna entidad, aparte de las direcciones IP permitidas.
- Compruebe que existe una verificación multiadministrador para proporcionar una capa adicional de aprobación.
- Valide la capacidad de acceso a través de la interfaz de línea de comandos y la API DE REST
- Desde el origen, active una operación de transferencia al almacén y asegúrese de que la copia en almacén no se pueda modificar.
- Intente eliminar las copias snapshot inmutables que se transfieren al almacén.
- Intente modificar el período de retención alterando el reloj del sistema.

Recuperación de datos de ciberalmacenes de ONTAP

Si los datos se destruyen en el centro de datos de producción, los datos del ciberalmacén se pueden recuperar de forma segura en el entorno elegido. A diferencia de una solución físicamente desconectada, el ciberalmacén de ONTAP de red desconectada se ha creado 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 ataque de ransomware y necesidad de recuperarse del almacén cibernético, el proceso de recuperación es sencillo y sencillo, ya que se utilizan las copias snapshot alojadas en el almacén cibernético para restaurar los datos cifrados.



Si el requisito es proporcionar un método más rápido para volver a conectar los datos cuando sea necesario para validar, aislar y analizar rápidamente los datos para recuperarlos. Esto se puede lograr fácilmente usando FlexClone con la opción de tipo SnapLock definida en el tipo no SnapLock.

> A partir de ONTAP 9.13,1, puede restaurarse instantáneamente una copia Snapshot bloqueada en el volumen SnapLock de destino de una relación de almacén SnapLock creando un FlexClone con la opción de tipo SnapLock establecida en «non-SnapLock». Al ejecutar la operación de creación de clones de volúmenes, especifique la copia Snapshot como el «parent-snapshot». Más información sobre la creación de un volumen de FlexClone con un tipo de SnapLock "aquí."

> La práctica de los procedimientos de recuperación desde la bóveda cibernética garantizará que se establezcan los pasos adecuados para conectarse al bóveda cibernética y recuperar datos. La planificación y prueba del procedimiento es esencial para cualquier recuperación durante un evento de ciberataque.

Consideraciones adicionales

Hay consideraciones adicionales a la hora de diseñar e implementar un ciberalmacén basado en ONTAP.

Consideraciones sobre el tamaño de la capacidad

La cantidad de espacio en disco necesaria para un volumen de destino de ciberalmacén ONTAP depende de diversos factores, siendo el más importante la tasa de cambio de los datos del volumen de origen. La programación de backups y la programación de Snapshot en el volumen de destino afectan tanto al uso de disco del volumen de destino como a la tasa de cambio del volumen de origen no es probable que sea constante. Es una buena idea proporcionar un búfer de capacidad de almacenamiento adicional superior a la necesaria para adaptarse a los cambios futuros en el comportamiento de los usuarios finales o las aplicaciones.

Para dimensionar una relación durante 1 mes de retención en ONTAP, debe calcular los requisitos de almacenamiento en función de varios factores, como el tamaño del conjunto de datos principal, la tasa de cambio de los datos (tasa de cambio diaria) y el ahorro en deduplicación y compresión (si procede).

Este es el enfoque paso a paso:

El primer paso es conocer el tamaño de los volúmenes de origen que está protegiendo con el almacén cibernético. Esta es la cantidad base de datos que se replicará inicialmente en el destino del ciberalmacén. A continuación, calcule la tasa de cambio diaria del conjunto de datos. Este es el porcentaje de datos que cambia cada día. Es crucial tener una buena comprensión de lo dinámicos que son los datos.

Por ejemplo:

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

Ahora, veamos el cálculo:

- Calcule la tasa de cambio diaria de datos:

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

- Calcule los datos totales modificados en 30 días:

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

- Calcule el almacenamiento total necesario:

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

- Aplique el ahorro en deduplicación y compresión:

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

Resumen de las necesidades de almacenamiento

- Sin eficiencia: Requeriría **12,5TB** para almacenar 30 días de los datos de la bóveda cibernética.
- Con una eficiencia del 50%: Requeriría **6,25TB** de almacenamiento después de la deduplicación y la compresión.

Las copias Snapshot pueden tener una sobrecarga adicional debido a los metadatos, pero esto suele ser menor.

Si se realizan varios backups por día, ajuste el cálculo según el número de copias snapshot realizadas cada día.

Factor de crecimiento de datos a lo largo del tiempo para garantizar que el tamaño esté preparado para el futuro.

Impacto en el rendimiento primario/fuente

Dado que la transferencia de datos es una operación de extracción, el impacto en el rendimiento del almacenamiento principal puede variar en función de la carga de trabajo, el volumen de datos y la frecuencia de los backups. Sin embargo, el impacto en el rendimiento general en el sistema principal suele ser moderado

y gestionable, ya que la transferencia de datos está diseñada para descargar las tareas de backup y protección de datos en el sistema de almacenamiento cibernético. Durante la configuración inicial de las relaciones y el primer backup completo, se transfiere una cantidad significativa de datos del sistema primario al sistema cibervault (el volumen SnapLock Compliance). Esto puede provocar un aumento del tráfico de red y de la carga de E/S en el sistema principal. Una vez que se ha completado el primer backup completo, ONTAP solo necesita hacer un seguimiento y transferir los bloques que han cambiado desde el último backup. Esto da como resultado una carga de I/O mucho menor en comparación con la replicación inicial. Las actualizaciones incrementales son eficientes y tienen un impacto mínimo en el rendimiento del almacenamiento primario. El proceso de almacén 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 e IOPS) para gestionar la carga adicional reduce el impacto en el rendimiento.

Configurar, analizar, cron script

NetApp ha creado un "script único que se puede descargar" y se utiliza para configurar, verificar y programar relaciones de ciberalmacén.

Qué hace este script

- Conexión de clústeres entre iguales
- Relaciones entre iguales de SVM
- Creación de volúmenes DP
- Relación de SnapMirror e inicialización
- Reforzar el sistema ONTAP utilizado para el ciberalmacén
- Desactivar y reanudar la relación según la programación de transferencias
- Valide la configuración de seguridad periódicamente y genere un informe en el que se muestren las anomalías

Cómo utilizar este script

"Descargue el script" y para usar el script, simplemente siga los siguientes pasos:

- Iniciar Windows PowerShell como administrador.
- Navegue hasta el directorio que contiene el script.
- Ejecute el script mediante `.\` la sintaxis junto con los parámetros necesarios

> Asegúrese de introducir toda la información. En la primera ejecución (modo de configuración), pedirá credenciales tanto para la producción como para el nuevo sistema de ciber bóveda. Después, creará los pares de SVM (si no existen), los volúmenes y la SnapMirror entre el sistema e inicializarlos.

> El modo cron se puede utilizar para programar la pausa y la 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 de aire acondicionado.
- Analizar: Función de supervisión e informes automatizada para enviar información a los grupos de supervisión en busca de anomalías y actividades sospechosas a fin de garantizar que las configuraciones no se desvíen.
- Cron: Para habilitar la infraestructura desconectada, el modo CRON automatiza la deshabilitación del LIF y desactiva la relación de transferencia.

Necesitará tiempo para transferir los datos en los volúmenes seleccionados en función del rendimiento y 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 ciberalmacén de ONTAP

Gracias a la separación de aire con sólidas metodologías de refuerzo proporcionadas por ONTAP, NetApp te permite crear un entorno de almacenamiento aislado y seguro resiliente frente a las ciberamenazas en constante evolución. Todo esto se logra al tiempo que se mantiene 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 actividad con un cambio mínimo en el marco de trabajo de sus personas, procesos y tecnología existentes.

El ciberalmacén de ONTAP utiliza funciones nativas de ONTAP es un enfoque sencillo para obtener protección adicional y crear copias inalterables e indelebles de sus datos. Añadir cibervault basado en ONTAP de NetApp a la política de seguridad general:

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

Información de copyright

Información de la marca comercial