Cyber vault di ONTAP

NetApp Solutions

NetApp
September 26, 2024

Sommario

Cyber vault di ONTAP

Panoramica del cyber vault di ONTAP

La principale minaccia che ha reso necessaria l'implementazione di un cyber vault è la crescente prevalenza e l'evoluzione della sofisticazione degli attacchi informatici, in particolare delle violazioni di dati e ransomware. "Con un aumento del phishing" inoltre, metodi sempre più sofisticati per il furto di credenziali, è possibile utilizzare le credenziali per avviare un attacco ransomware per accedere ai sistemi dell'infrastruttura. In questi casi, anche i sistemi infrastrutturali più robusti sono a rischio di attacco. L'unica difesa di un sistema compromesso è la protezione e l'isolamento dei dati in un vault informatico.

Il cyber vault di NetApp basato su ONTAP fornisce alle organizzazioni una soluzione completa e flessibile per proteggere le loro risorse dati più critiche. Sfruttando l'air-gapping logico con solide metodologie di potenziamento, ONTAP ti consente di creare ambienti storage sicuri e isolati in grado di resistere alle minacce informatiche in evoluzione. Con ONTAP, puoi garantire la riservatezza, l'integrità e la disponibilità dei tuoi dati mantenendo al contempo l'agilità e l'efficienza della tua infrastruttura storage.

> A partire da luglio 2024, il contenuto dei report tecnici precedentemente pubblicati come PDF è stato integrato nella documentazione del prodotto ONTAP. Inoltre, i nuovi report tecnici (TR) come questo documento non riceveranno più i numeri TR.

Che cos'è un cyber-vault?

Un cyber vault è una tecnica specifica di data Protection che prevede lo storage di dati critici in un ambiente isolato, separato dall'infrastruttura IT primaria.

Repository di dati "air-gapped", * immutabile* e * indelebile* immune alle minacce che colpiscono la rete principale, come malware, ransomware o persino minacce interne. Un cyber vault può essere realizzato con istantanee **immutabili** e **indelebili**.

I backup ad aria che utilizzano metodi tradizionali implicano la creazione di spazio e la separazione fisica dei supporti primari e secondari. Spostando i supporti fuori sede e/o interrompendo la connettività, i malintenzionati non hanno accesso ai dati. Questo protegge i dati, ma può causare tempi di ripristino più lenti.

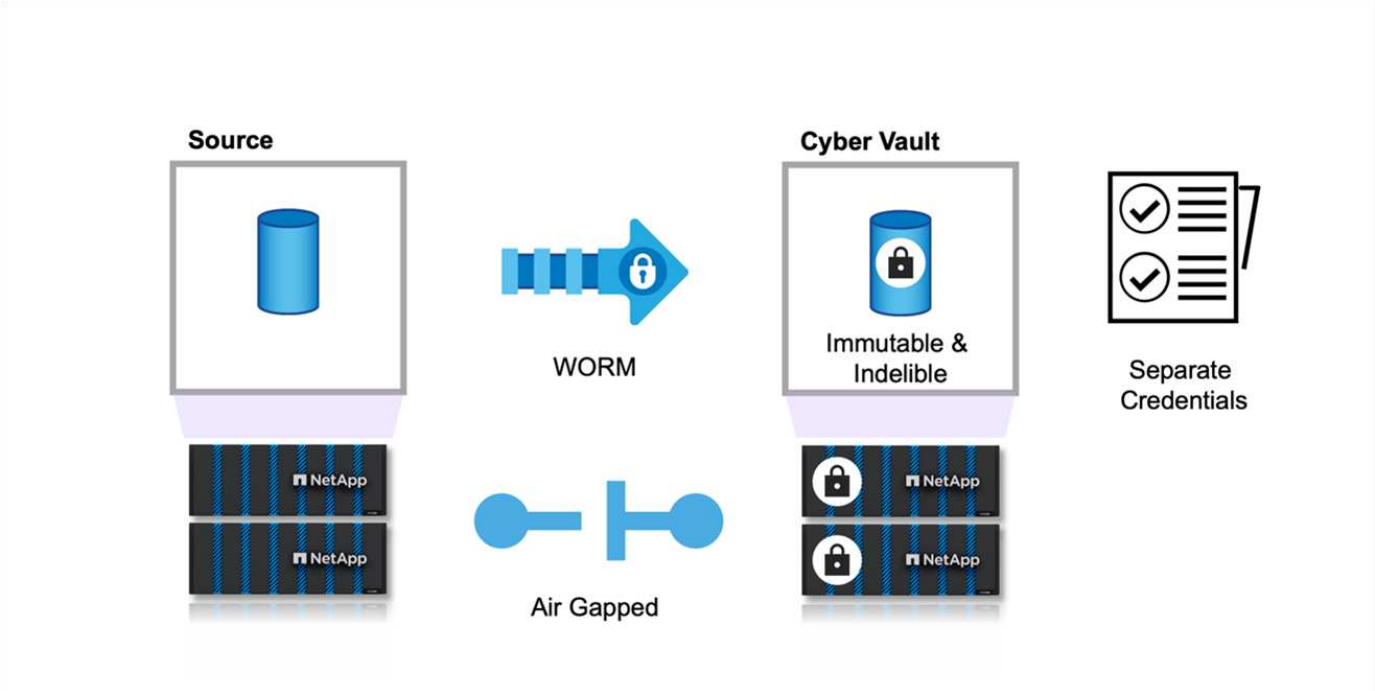
L'approccio di NetApp al cyber vault

Le caratteristiche principali dell'architettura di riferimento NetApp per un cyber vault includono:

- Infrastruttura di storage sicura e isolata (ad esempio, sistemi di stoccaggio a montaggio d'aria)
- Le copie dei dati devono essere sia **immutabili** sia **indelebili** senza eccezioni
- Rigorosi controlli degli accessi e autenticazione a più fattori
- Funzionalità di ripristino rapido dei dati

È possibile utilizzare lo storage NetApp con ONTAP come un cyber vault a mappatura aerea sfruttando "SnapLock Compliance per proteggere le copie Snapshot in modo WORM". È possibile eseguire tutte le attività di base di SnapLock Compliance sul vault Cyber. Una volta configurati, i volumi dei vault Cyber sono protetti automaticamente, eliminando la necessità di assegnare manualmente le copie Snapshot a WORM. Maggiori informazioni sul gapping logico possono essere trovate in questo "blog"

SnapLock Compliance viene utilizzato per conformarsi alle normative bancarie e finanziarie SEC 70-a-4(f), FINRA 4511(c) e CFTC 1,31(c)-(d). È stato certificato da Cohasset Associates per aderire a queste norme (rapporto di controllo disponibile su richiesta). Utilizzando SnapLock Compliance con questa certificazione si ottiene un meccanismo rafforzato per la cattura d'aria dei vostri dati, su cui fanno affidamento i più grandi istituti finanziari del mondo per garantire sia la conservazione che il recupero dei record bancari.



Terminologia di Cyber vault ONTAP

Questi sono i termini comunemente utilizzati nelle architetture dei vault cibernetici.

Autonomous ransomware Protection (ARP) - la funzionalità Autonomous ransomware Protection (ARP) utilizza l'analisi dei workload negli ambienti NAS (NFS e SMB) per rilevare in modo proattivo e in real-time e informare l'utente in caso di attività anomale che potrebbero indicare un attacco ransomware. Quando si sospetta un attacco, ARP crea anche nuove copie Snapshot, oltre alla protezione esistente dalle copie Snapshot pianificate. Per ulteriori informazioni, consultare la "Documentazione di ONTAP sulla protezione autonoma da ransomware"

Air-gap (logico) - è possibile configurare lo storage NetApp con ONTAP come un cyber vault logico a mappatura d'aria sfruttando "SnapLock Compliance per proteggere le copie Snapshot in modo WORM"

Air-gap (Physical) - Un sistema fisico a mappatura d'aria non dispone di connettività di rete. Utilizzando i backup su nastro, è possibile spostare le immagini in un'altra posizione. Il traferro logico SnapLock Compliance è robusto quanto un sistema fisico a nappamento d'aria.

Bastion host - Un computer dedicato su una rete isolata, configurato per resistere agli attacchi.

Copie Snapshot immutabili - copie Snapshot che non possono essere modificate, senza eccezioni (incluse un'organizzazione di supporto o la possibilità di formattare il sistema storage a basso livello).

Copie Snapshot indelebili - copie Snapshot che non possono essere eliminate senza eccezioni (incluse un'organizzazione di supporto o la capacità di formattare il sistema storage a basso livello).

Copie Snapshot antimanomissione - le copie istantanee antimanomissione utilizzano la funzione di clock

SnapLock Compliance per bloccare le copie Snapshot per un periodo specificato. Questi snapshot bloccati non possono essere eliminati da alcun utente o supporto NetApp. Puoi utilizzare copie Snapshot bloccate per ripristinare i dati se un volume viene compromesso da un attacco ransomware, malware, hacker, amministratori non autorizzati o eliminazioni accidentali. Per ulteriori informazioni, consultare la "Documentazione ONTAP sulle copie Snapshot antimanomissione"

SnapLock - SnapLock è una soluzione di conformità ad alte prestazioni per le organizzazioni che utilizzano lo storage WORM per conservare i file in forma non modificata per scopi normativi e di governance. Per ulteriori informazioni, vedere "Documentazione ONTAP su SnapLock".

SnapMirror - SnapMirror è una tecnologia di replica per il disaster recovery, progettata per replicare in modo efficiente i dati. SnapMirror può creare un mirror (o una copia esatta dei dati), un vault (una copia dei dati con una conservazione delle copie Snapshot più lunga) o entrambi in un sistema secondario, on-premise o nel cloud. Queste copie possono essere utilizzate per molti scopi diversi, come un disastro, un bursting nel cloud o un cyber vault (quando si utilizza il criterio del vault e si blocca il vault). Per ulteriori informazioni, consultare la "Documentazione ONTAP su SnapMirror"

SnapVault - in ONTAP 9.3 SnapVault è stato deprecato a favore della configurazione di SnapMirror utilizzando il criterio vault o mirror-vault. Questo è termine, mentre ancora utilizzato, è stato ammortizzato pure. Per ulteriori informazioni, vedere "Documentazione ONTAP su SnapVault".

Dimensioni del vault Cyber con ONTAP

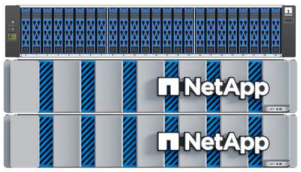
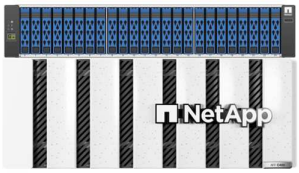
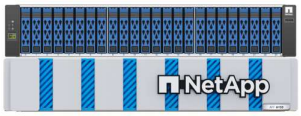
Il dimensionamento di un vault informatico richiede la comprensione di quanti dati devono essere ripristinati in un determinato obiettivo RTO (Recovery Time Objective). Molti fattori giocano nella progettazione corretta di una soluzione cyber vault di dimensioni adeguate. Sia le prestazioni che la capacità devono essere prese in considerazione durante il dimensionamento di un cyber vault.

Considerazioni sul dimensionamento delle performance

1. Quali sono i modelli di piattaforma di origine (FAS v AFF A-Series v AFF C-Series)?
2. Qual è la larghezza di banda e la latenza tra l'origine e il vault dei dati informatici?
3. Quali sono le dimensioni dei file e quanti file?
4. Qual è il vostro obiettivo in termini di tempi di ripristino?
5. Quanti dati è necessario ripristinare all'interno dell'RTO?
6. Quante relazioni di fan-in di SnapMirror verrà ingaggiato il cyber vault?
7. Verranno eseguiti uno o più ripristini contemporaneamente?
8. Questi ripristini multipli accadranno sullo stesso primario?
9. SnapMirror verrà replicato nel vault durante un ripristino da un vault?

Esempi di dimensionamento

Di seguito sono riportati alcuni esempi di diverse configurazioni dei vault cibernetici.

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

Considerazioni sul dimensionamento della capacità

La quantità di spazio su disco necessaria per un volume di destinazione del vault informatico ONTAP dipende da una varietà di fattori, il più importante dei quali è il tasso di variazione per i dati nel volume di origine. È improbabile che la pianificazione di backup e la pianificazione Snapshot sul volume di destinazione influiscano sull'utilizzo del disco sul volume di destinazione e che la velocità di modifica sul volume di origine sia costante. È consigliabile fornire un buffer di capacità di storage aggiuntiva oltre a quello necessario per adattarsi a future modifiche del comportamento di utenti finali o applicazioni.

Il dimensionamento di una relazione per 1 mese di conservazione in ONTAP richiede il calcolo dei requisiti storage in base a diversi fattori, tra cui le dimensioni del set di dati primario, il tasso di cambiamento dei dati (tasso di modifica giornaliero) e i risparmi in termini di deduplica e compressione (se applicabili).

Ecco l'approccio passo passo:

Il primo passo è conoscere le dimensioni del volume o dei volumi di origine che si sta proteggendo con il vault informatico. Questa è la quantità di base di dati che verranno inizialmente replicati nella destinazione del cyber vault. Quindi, stimare la frequenza di modifica giornaliera per il set di dati. Questa è la percentuale di dati che cambia ogni giorno. È fondamentale avere una buona comprensione di come sono dinamici i tuoi dati.

Ad esempio:

- Dimensioni del set di dati primario = 5TB
- Tasso di cambio giornaliero = 5% (0,05)
- Efficienza di deduplica e compressione = 50% (0,50)

Ora, esaminiamo il calcolo:

- Calcolare la velocità di modifica giornaliera dei dati:

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

- Calcolare il totale dei dati modificati per 30 giorni:

  ```
  Total changed data in 30 days = 250 GB * 14 = 3.5TB
  ```

- Calcolare lo storage totale necessario:

  ```
  TOTAL = 5TB + 3.5TB = 8.5TB
  ```

- Applica i risparmi su deduplica e compressione:

```
EFFECTIVE = 8.5TB * 50% = 4.25TB
```

Riepilogo delle esigenze di archiviazione

- Senza efficienza: Richiederebbe **8,5TB** per memorizzare 30 giorni dei dati del vault.
- Con un'efficienza del 50%: Richiederebbe **4,25TB** di storage dopo la deduplica e la compressione.

> Le copie Snapshot possono avere un overhead aggiuntivo a causa dei metadati, ma questo è in genere di entità secondaria.

> Se vengono eseguiti più backup al giorno, regolare il calcolo in base al numero di copie Snapshot acquisite ogni giorno.

> Considerare la crescita dei dati nel tempo per garantire che il dimensionamento sia a prova di futuro.

Creazione di un cyber vault con ONTAP

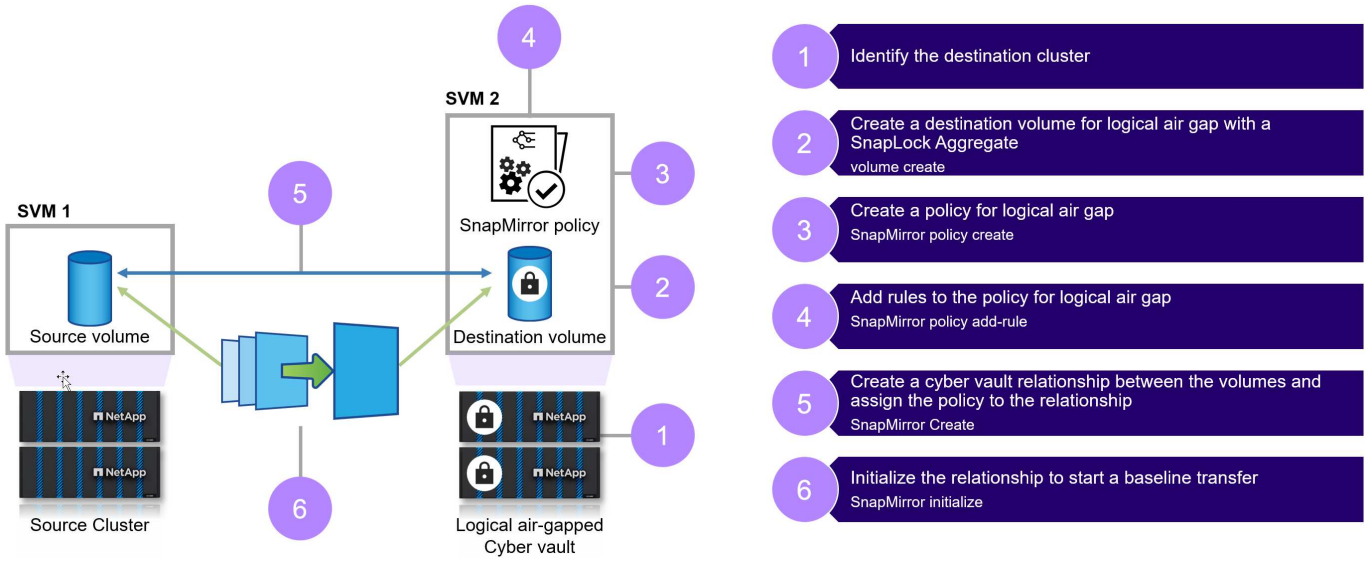
I passaggi riportati di seguito sono utili per la creazione di un cyber vault con ONTAP.

Prima di iniziare

- Il cluster di origine deve eseguire ONTAP 9 o una versione successiva.
- Gli aggregati di origine e destinazione devono essere a 64 bit.
- I volumi di origine e di destinazione devono essere creati in cluster peered con SVM peered. Per ulteriori informazioni, vedere "Peering dei cluster".
- Se la funzione di crescita automatica del volume è disattivata, lo spazio libero sul volume di destinazione deve essere superiore di almeno il cinque percento allo spazio utilizzato sul volume di origine.

A proposito di questa attività

L'illustrazione seguente mostra la procedura per l'inizializzazione di una relazione del vault di SnapLock Compliance:



Fasi

1. Identificare l'array di destinazione per diventare il cyber vault per ricevere i dati con mappatura aerea.
2. Sulla matrice di destinazione, per preparare il cyber vault, "Installare la licenza di ONTAP ONE", "Inizializzare l'orologio di conformità"e, se si sta utilizzando una release ONTAP precedente alla 9.10.1, "Creazione di un aggregato SnapLock Compliance".
3. Sull'array di destinazione, creare un volume di destinazione SnapLock Compliance di tipo DP:

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

4. A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzare l' `-snaplock-type`opzione volume per specificare un tipo di conformità. Nelle versioni ONTAP precedenti a ONTAP 9.10,1, la modalità SnapLock, conformità viene ereditata dall'aggregato. I volumi di destinazione flessibili in base alla versione non sono supportati. L'impostazione della lingua del volume di destinazione deve corrispondere all'impostazione della lingua del volume di origine.

   Il seguente comando crea un volume SnapLock Compliance da 2 GB denominato `dstvolB` in nell' `SVM2`aggregato `node01_aggr`:

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

5. Nel cluster di destinazione, per creare il traferro, impostare il periodo di conservazione predefinito, come descritto in "Impostare il periodo di conservazione predefinito". A un volume SnapLock che è una destinazione del vault è assegnato un periodo di conservazione predefinito. Il valore per questo periodo è inizialmente impostato su un minimo di 0 anni e su un massimo di 30 anni per i volumi SnapLock Compliance. Ogni copia Snapshot di NetApp viene inizialmente impegnata con questo periodo di conservazione predefinito. È necessario modificare il periodo di conservazione predefinito. Il periodo di conservazione può essere prolungato in un secondo momento, se necessario, ma mai abbreviato. Per ulteriori informazioni, vedere "Imposta la panoramica del tempo di conservazione".
6. "Creare una nuova relazione di replica" Tra l'origine non SnapLock e la nuova destinazione SnapLock creata nel passaggio 3.

   Questo esempio crea una nuova relazione SnapMirror con il volume SnapLock di destinazione dstvolB utilizzando un criterio di XDPDefault per il vault delle copie Snapshot etichettate giornalmente e settimanalmente con una pianificazione oraria:

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

   "Creare un criterio di replica personalizzato" o a "programma personalizzato" se le impostazioni predefinite disponibili non sono adatte.

7. Sulla SVM di destinazione, inizializzare la relazione SnapVault creata nella fase 5:

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

8. Il seguente comando inizializza la relazione tra il volume di origine srcvolA su SVM1 e il volume di destinazione dstvolB su SVM2:

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

9. Una volta inizializzata la relazione e inattiva, utilizzare il comando snapshot show sulla destinazione per verificare il tempo di scadenza del SnapLock applicato alle copie Snapshot replicate.

   Questo esempio elenca le copie Snapshot sul volume dstvolB che hanno l'etichetta SnapMirror e la data di scadenza del SnapLock:

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

Protezione da vault Cyber

Questi sono i consigli aggiuntivi per rafforzare un cyber-vault di ONTAP. Per ulteriori consigli e procedure, consultare la guida alla tempra ONTAP riportata di seguito.

Raccomandazioni per la protezione dei dati informatici

- Isolare i piani di gestione del cyber vault
- Non abilitare le LIF dati sul cluster di destinazione perché rappresentano un ulteriore vettore di attacco
- Nel cluster di destinazione, limitare l'accesso intercluster LIF al cluster di origine con una policy di servizio
- Segmentare la LIF di gestione nel cluster di destinazione per l'accesso limitato con una policy di servizio e un host Bastion
- Limitare tutto il traffico di dati dal cluster di origine al cyber vault per consentire solo le porte necessarie per il traffico SnapMirror
- Se possibile, disattivare eventuali metodi di accesso alla gestione non necessari all'interno di ONTAP per ridurre la superficie di attacco
- Abilitare la registrazione degli audit e lo storage remoto dei log
- Abilita la verifica con amministratori multipli e richiede la verifica da parte di un amministratore esterno ai normali amministratori dello storage (ad esempio, staff CISO)
- Implementare il controllo degli accessi in base al ruolo
- Richiede l'autenticazione a più fattori amministrativa per System Manager e ssh
- Utilizzare l'autenticazione basata su token per script e chiamate API REST

Fare riferimento a "Guida alla tempra ONTAP", "Panoramica sulla verifica multi-admin" e "Guida all'autenticazione multifattore di ONTAP" per informazioni su come eseguire queste operazioni di indurimento.

Interoperabilità con il Cyber vault

L'hardware e il software ONTAP possono essere utilizzati per creare una configurazione del cyber vault.

Raccomandazioni sull'hardware ONTAP

Tutti gli array fisici unificati ONTAP possono essere utilizzati per un'implementazione del cyber vault.

- Lo storage ibrido FAS è la soluzione più conveniente.
- AFF C-Series offre il consumo energetico e la densità più efficienti sul mercato.

- AFF A-Series è la piattaforma dalle performance più elevate che offre il miglior RTO. Con il recente annuncio della nostra ultima AFF serie A, questa piattaforma offrirà la migliore efficienza dello storage senza compromessi in termini di performance.

Raccomandazioni software ONTAP

A partire da ONTAP 9.14,1, è possibile specificare i periodi di conservazione per etichette SnapMirror specifiche nei criteri SnapMirror della relazione di SnapMirror, in modo che le copie Snapshot replicate dal volume di origine a quello di destinazione vengano conservate per il periodo di conservazione specificato nella regola. Se non viene specificato alcun periodo di conservazione, viene utilizzato il periodo di conservazione predefinito del volume di destinazione.

A partire da ONTAP 9.13,1, è possibile ripristinare istantaneamente una copia Snapshot bloccata sul volume SnapLock di destinazione di una relazione di vault SnapLock creando una FlexClone con l'opzione di tipo SnapLock impostata su "non SnapLock" e specificando la copia Snapshot come "snapshot padre" quando si esegue l'operazione di creazione del clone del volume. Ulteriori informazioni su "Creazione di un volume FlexClone con un tipo di SnapLock".

Configurazione di MetroCluster

Per le configurazioni MetroCluster, è necessario conoscere quanto segue:

- È possibile creare una relazione SnapVault solo tra le SVM di origine della sincronizzazione, non tra una SVM di origine della sincronizzazione e una SVM di destinazione della sincronizzazione.
- È possibile creare una relazione SnapVault da un volume su una SVM di origine della sincronizzazione a una SVM di servizio dati.
- È possibile creare una relazione SnapVault da un volume su una SVM di servizio dati a un volume DP su una SVM di origine sincronizzazione.

Risorse del Cyber vault

Per ulteriori informazioni sulle informazioni descritte in queste informazioni relative ai vault informatici, fare riferimento alle seguenti informazioni aggiuntive e ai seguenti concetti relativi alla sicurezza.

- "Cyber vault di NetApp: Analisi delle soluzioni per la data Protection multilivello"
- "NetApp ottiene la classificazione AAA per la prima soluzione di rilevamento ransomware on-box basata sull'intelligenza artificiale del settore"
- "Ottimizza la resilienza informatica con lo storage più sicuro al mondo"
- "Guida alla protezione avanzata di ONTAP"
- "NetApp Zero Trust"
- "Resilienza informatica di NetApp"
- "Protezione dei dati NetApp"
- "Panoramica del peering di cluster e SVM con CLI"
- "Archiviazione SnapVault"

Creazione, protezione e verifica di un cyber vault di ONTAP con PowerShell

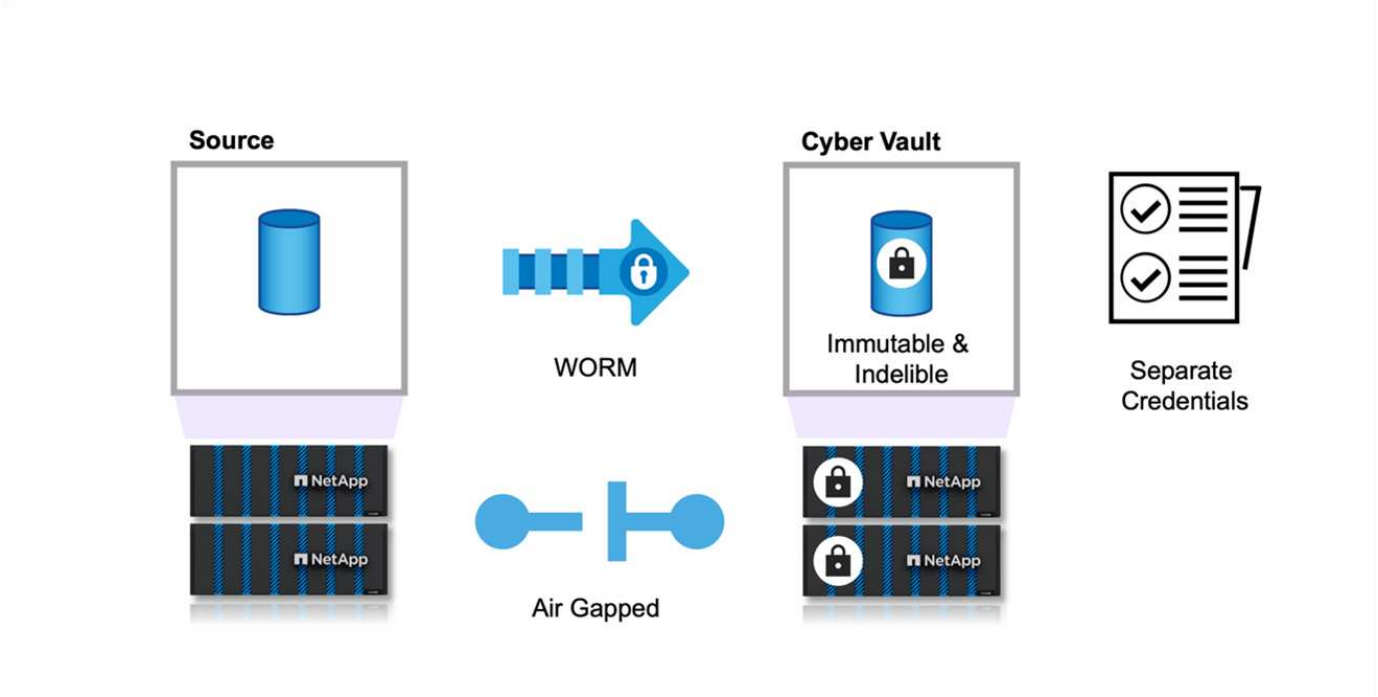
Panoramica del cyber vault di ONTAP con PowerShell

Nel panorama digitale odierno, la salvaguardia delle risorse dati critiche di un'organizzazione non è solo una Best practice, ma un imperativo aziendale. Le minacce informatiche si stanno evolvendo a un ritmo senza precedenti e le misure tradizionali di data Protection non sono più sufficienti per mantenere al sicuro le informazioni sensibili. È qui che entra in gioco un cyber vault. La soluzione all'avanguardia basata su ONTAP di NetApp combina tecniche avanzate di air-gapping con misure di protezione dei dati efficaci per creare una barriera impenetrabile contro le minacce informatiche. Isolando i dati più preziosi con una tecnologia di protezione avanzata, un cyber vault riduce al minimo la superficie di attacco in modo che i dati più critici rimangano confidenziali, intatti e prontamente disponibili quando necessario.

Un cyber vault è una struttura di storage sicura costituita da più livelli di protezione, quali firewall, networking e storage. Questi componenti salvaguardano i dati di recovery fondamentali necessari per operazioni aziendali cruciali. I componenti del cyber vault si sincronizzano regolarmente con i dati di produzione essenziali in base alla policy del vault, ma in caso contrario rimangono inaccessibili. Questa configurazione isolata e disconnessa garantisce che, in caso di attacco informatico che compromette l'ambiente di produzione, sia possibile eseguire facilmente un recupero finale e affidabile dal cyber vault.

NetApp consente di creare facilmente un traferro per il cyber vault configurando la rete, disabilitando le LIF, aggiornando le regole del firewall e isolando il sistema dalle reti esterne e da Internet. Questo approccio robusto scollega efficacemente il sistema dalle reti esterne e da Internet, fornendo una protezione senza precedenti contro gli attacchi informatici remoti e i tentativi di accesso non autorizzati, rendendo il sistema immune alle minacce basate sulla rete e alle intrusioni.

Combinando questo aspetto con la protezione SnapLock Compliance, i dati non possono essere modificati o eliminati, nemmeno dagli amministratori ONTAP o dal supporto NetApp. SnapLock viene sottoposto a una verifica periodica rispetto alle normative SEC e FINRA, accertandosi che la resilienza dei dati soddisfi questi rigorosi requisiti WORM e di conservazione dei dati del settore bancario. NetApp è l'unico storage Enterprise validato da NSA CSFC per la memorizzazione di dati top-secret.



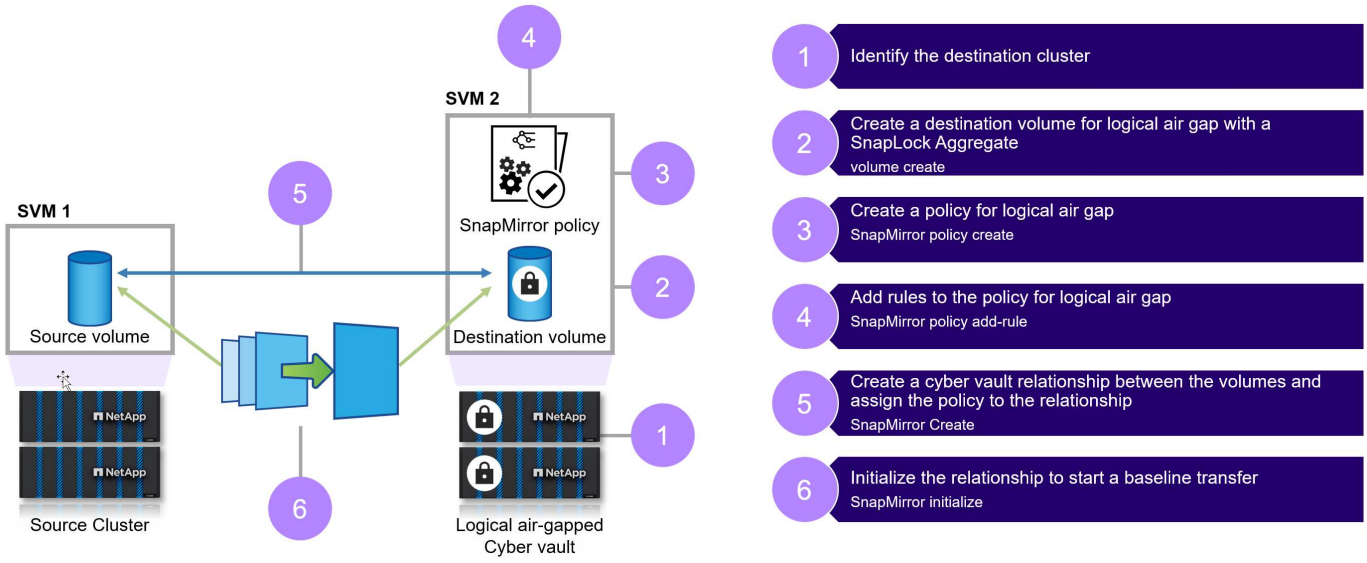
Questo documento descrive la configurazione automatizzata del vault informatico di NetApp per lo storage ONTAP on-premise in un altro storage ONTAP designato con snapshot immutabili che aggiungono un ulteriore livello di protezione dall'aumento degli attacchi informatici per un ripristino rapido. In questa architettura viene applicata l'intera configurazione in base alle Best practice ONTAP. L'ultima sezione contiene istruzioni per eseguire un ripristino in caso di attacco.

> La stessa soluzione è applicabile per creare il cyber vault designato in AWS utilizzando FSX per ONTAP.

Passaggi di alto livello per creare un cyber vault di ONTAP

- Creare una relazione di peering
  - Il sito di produzione che utilizza lo storage ONTAP è sottoposto a peering con lo storage ONTAP dedicato al vault informatico
- Creazione di un volume SnapLock Compliance
- Impostare la relazione e la regola SnapMirror per impostare l'etichetta
  - Vengono configurate la relazione SnapMirror e le pianificazioni appropriate
- Impostare le trattenute prima di avviare il trasferimento SnapMirror (vault)
  - Il blocco di conservazione viene applicato sui dati copiati, per evitare ulteriormente i dati da un interno o guasto dei dati. Utilizzando questa funzione, i dati non possono essere eliminati prima della scadenza del periodo di conservazione
  - Le organizzazioni possono conservare questi dati per poche settimane/mesi, a seconda dei requisiti
- Inizializzare la relazione SnapMirror in base alle etichette
  - Il seeding iniziale e il trasferimento incrementale ininterrotto avvengono in base alla pianificazione del SnapMirror
  - I dati sono protetti (immutabili e indelebili) con SnapLock Compliance, e che sono disponibili per il recovery

- Implementare rigidi controlli di trasferimento dei dati
  - Il vault Cyber viene sbloccato per un periodo limitato con i dati del sito di produzione e sincronizzato con i dati nel vault. Una volta completato il trasferimento, la connessione viene disconnessa, chiusa e nuovamente bloccata
- Recovery rapido
  - Se il server primario è interessato dal sito di produzione, i dati provenienti dal cyber vault vengono ripristinati in modo sicuro nella produzione originale o in un altro ambiente scelto



Componenti della soluzione

NetApp ONTAP con 9.15.1 su cluster di origine e destinazione.

ONTAP One: Licenza All-in-One di NetApp ONTAP.

Funzionalità utilizzate dalla licenza ONTAP ONE:

- Conformità SnapLock
- SnapMirror
- Verifica multi-admin
- Tutte le funzionalità di protezione avanzata esposte da ONTAP
- Separare le credenziali RBAC per il cyber vault

> Tutti gli array fisici unificati ONTAP possono essere utilizzati per un cyber vault, tuttavia i sistemi flash basati sulla capacità AFF C-Series e i sistemi flash ibridi FAS sono le piattaforme ideali più convenienti per questo scopo. Consultare "Dimensionamento dei cyber vault di ONTAP"per le istruzioni sul dimensionamento.

Creazione del cyber vault di ONTAP con PowerShell

I backup ad aria che utilizzano metodi tradizionali implicano la creazione di spazio e la separazione fisica dei supporti primari e secondari. Spostando i supporti off-site e/o interrompendo la connettività, i malintenzionati non hanno accesso ai dati. Questo

protegge i dati, ma può causare tempi di ripristino più lenti. Con SnapLock Compliance, non è necessaria la separazione fisica. SnapLock Compliance protegge le copie point-in-time di sola lettura dello snapshot vault, rendendo i dati rapidamente accessibili, sicuri da eliminazioni o indelebili, al sicuro da modifiche o immutabili.

Prerequisiti

Prima di iniziare con le fasi descritte nella sezione successiva di questo documento, accertarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster di origine deve eseguire ONTAP 9 o una versione successiva.
- Gli aggregati di origine e destinazione devono essere a 64 bit.
- I cluster di origine e di destinazione devono essere peering.
- È necessario eseguire il peering delle SVM di origine e destinazione.
- Assicurarsi che la crittografia di peering dei cluster sia abilitata.

L'impostazione dei trasferimenti di dati a un cyber vault di ONTAP richiede diversi passaggi. Sul volume primario, configurare un criterio di snapshot che specifica le copie da creare e quando crearle utilizzando pianificazioni appropriate e assegnare etichette per specificare quali copie devono essere trasferite da SnapVault. Sul secondario, deve essere creata una policy SnapMirror che specifica le etichette delle copie Snapshot da trasferire e il numero di queste copie da conservare nel cyber vault. Dopo aver configurato questi criteri, creare la relazione SnapVault e stabilire una pianificazione del trasferimento.

> Questo documento presuppone che lo storage primario e il cyber vault ONTAP designato siano già configurati e configurati.

> Il cluster del vault Cyber può trovarsi nello stesso data center o in un data center diverso rispetto ai dati di origine.

Procedura per creare un cyber vault di ONTAP

1. Utilizzare la CLI di ONTAP o Gestione sistema per inizializzare il clock di conformità.
2. Creare un volume di data Protection con SnapLock Compliance abilitato.
3. Utilizza il comando SnapMirror create per creare relazioni di protezione dei dati SnapVault.
4. Consente di impostare il periodo di conservazione SnapLock Compliance predefinito per il volume di destinazione.

> La conservazione predefinita è "impostata al minimo". A un volume SnapLock che è una destinazione del vault è assegnato un periodo di conservazione predefinito. Il valore per questo periodo è inizialmente impostato su un minimo di 0 anni e su un massimo di 30 anni per i volumi SnapLock Compliance. Ogni copia Snapshot di NetApp viene inizialmente impegnata con questo periodo di conservazione predefinito. Il periodo di conservazione può essere prolungato in un secondo momento, se necessario, ma mai abbreviato.

Quanto sopra comprende i passaggi manuali. Gli esperti di sicurezza consigliano di automatizzare il processo per evitare la gestione manuale che introduce un notevole margine di errore. Di seguito è riportato il frammento di codice che automatizza completamente i prerequisiti e la configurazione di SnapLock Compliance e l'inizializzazione dell'orologio.

Ecco un esempio di codice PowerShell per l'inizializzazione del clock di conformità 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
    }
}
```

Ecco un esempio di codice PowerShell per configurare un cyber vault di 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 volta completati i passaggi sopra indicati, è pronto il cyber vault air-gapped che utilizza SnapLock Compliance e SnapVault.

Prima di trasferire i dati snapshot al cyber vault, è necessario inizializzare la relazione SnapVault. Tuttavia, prima di tutto, è necessario eseguire la protezione avanzata per proteggere il vault.

Protezione avanzata dei cyber vault di ONTAP con PowerShell

Il cyber vault di ONTAP offre una migliore resilienza contro gli attacchi informatici rispetto alle soluzioni tradizionali. Quando si progetta un'architettura per migliorare la sicurezza, è fondamentale prendere in considerazione misure per ridurre la superficie di attacco. Ciò può essere ottenuto attraverso vari metodi, come l'implementazione di criteri password rafforzati, l'abilitazione di RBAC, il blocco degli account utente predefiniti, la configurazione dei firewall e l'utilizzo di flussi di approvazione per qualsiasi modifica al sistema del vault. Inoltre, la limitazione dei protocolli di accesso alla rete da uno specifico indirizzo IP può contribuire a limitare potenziali vulnerabilità.

ONTAP fornisce una serie di controlli che consentono di rafforzare lo storage ONTAP. Utilizzare "Guida e impostazioni di configurazione per ONTAP"per aiutare l'organizzazione a soddisfare gli obiettivi di protezione prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

Protezione delle Best practice

Passaggi manuali

1. Creare un utente designato con ruolo amministrativo predefinito e personalizzato.
2. Creare un nuovo IPSpace per isolare il traffico di rete.
3. Creare una nuova SVM che risiede nel nuovo IPSpace.

4. Assicurarsi che i criteri di routing del firewall siano configurati correttamente e che tutte le regole siano regolarmente controllate e aggiornate secondo necessità.

ONTAP CLI o tramite script di automazione

1. Proteggi l'amministrazione con la verifica Multi-Admin (MFA)
2. Abilita la crittografia per dati standard "in-flight" tra cluster.
3. SSH protetto con crittografia sicura e password sicure.
4. Attiva FIPS globale.
5. Telnet e Remote Shell (RSH) devono essere disattivati.
6. Bloccare l'account admin predefinito.
7. Disattiva le interfacce LIF dati e proteggi gli access point remoti.
8. Consente di disattivare e rimuovere i protocolli e i servizi inutilizzati o estranei.
9. Crittografare il traffico di rete.
10. Utilizzare il principio del privilegio minimo quando si impostano i ruoli di superutente e amministratore.
11. Limita HTTPS e SSH da un indirizzo IP specifico utilizzando l'opzione IP consentita.
12. Consente di interrompere e riprendere la replica in base alla pianificazione del trasferimento.

I punti 1-4 richiedono un intervento manuale, ad esempio la designazione di una rete isolata, la separazione dell'IPSpace e così via, e devono essere eseguiti in anticipo. Per informazioni dettagliate sulla configurazione della protezione avanzata, consultare la "Guida alla protezione avanzata di ONTAP". Il resto può essere facilmente automatizzato per facilitare l'implementazione e il monitoraggio. L'obiettivo di questo approccio orchestrato è fornire un meccanismo per automatizzare i passaggi di rafforzamento per testare in futuro il controller del vault. Il periodo di tempo in cui il gioco d'aria del cyber vault è aperto è il più breve possibile. SnapVault sfrutta la tecnologia incrementale per sempre, che sposterà solo le modifiche dall'ultimo aggiornamento nel cyber vault, riducendo così al minimo la quantità di tempo in cui il cyber vault deve rimanere aperto. Per ottimizzare ulteriormente il flusso di lavoro, l'apertura del cyber vault è coordinata con la pianificazione della replica per garantire la finestra di connessione più piccola.

Ecco un esempio di codice PowerShell per rafforzare un controller 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
    }
}
```

Convalida del cyber vault di ONTAP con PowerShell

Un robusto cyber vault dovrebbe essere in grado di resistere a un attacco sofisticato, anche quando l'utente malintenzionato dispone delle credenziali per accedere all'ambiente con Privileges elevato.

Una volta stabilite le regole, un tentativo (supponendo che l'utente malintenzionato sia riuscito a entrare) di eliminare uno snapshot dal lato del vault non riesce. Lo stesso vale per tutte le impostazioni di indurimento, ponendo le restrizioni necessarie e salvaguardando il sistema.

Esempio di codice PowerShell per convalidare la configurazione in base alla pianificazione.

```
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
    }
}
```

Questa schermata mostra che non sono presenti connessioni sul controller del vault.

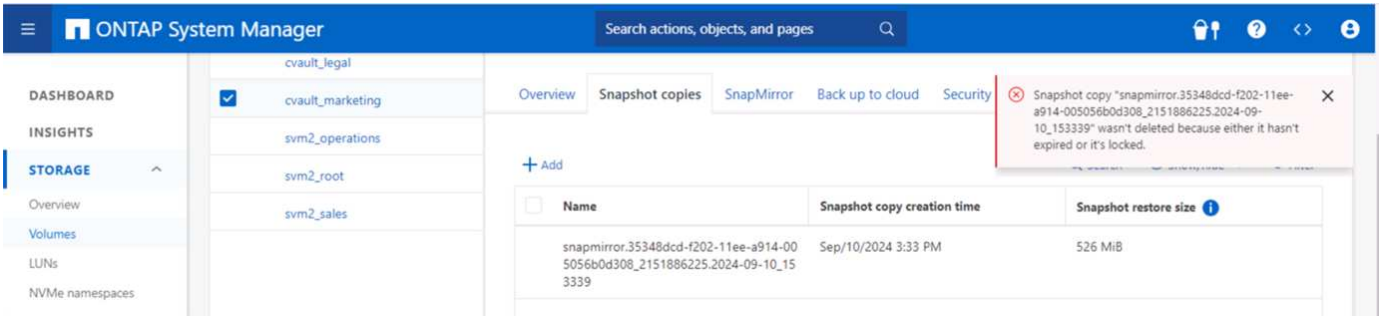
```
cluster2::> network connections  listening show
This table is currently empty.

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

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

cluster2::>
```

Questa screenshot indica che non è possibile manomettere le snapshot.



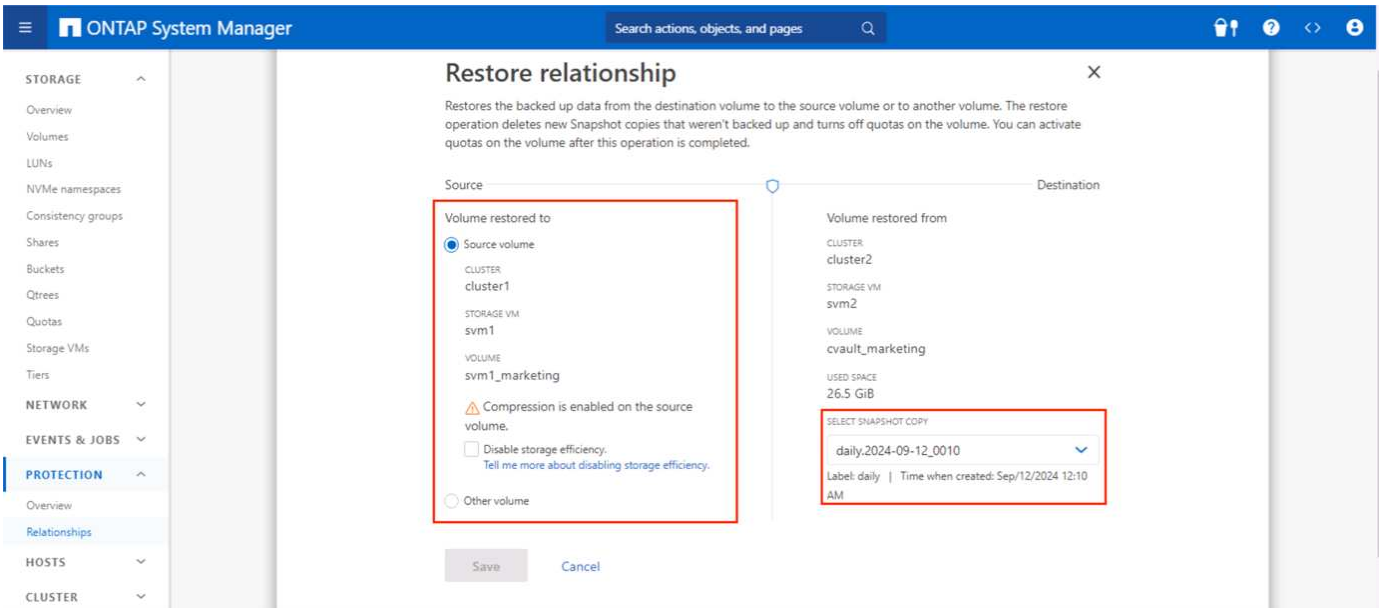
Per convalidare e confermare la funzionalità di air-gapping, attenersi alla seguente procedura:

- Verificare le capacità di isolamento della rete e la possibilità di interrompere una connessione quando i dati non vengono trasferiti.
- Verificare che non sia possibile accedere all'interfaccia di gestione da entità diverse dagli indirizzi IP consentiti.
- Verificare che la verifica Multi-admin sia attiva per fornire un ulteriore livello di approvazione.
- Verificare la capacità di accesso tramite CLI e API REST
- Dall'origine, attivare un'operazione di trasferimento al vault e assicurarsi che la copia del vault non possa essere modificata.
- Provare a eliminare le copie snapshot immutabili trasferite al vault.
- Provare a modificare il periodo di conservazione manomettendo l'orologio di sistema.

Recupero dei dati dei vault informatici di ONTAP

Se i dati vengono distrutti nel data center di produzione, è possibile ripristinare in modo sicuro nell'ambiente scelto i dati provenienti dal vault informatico. A differenza di una soluzione fisicamente a mappatura d'aria, il cyber vault di ONTAP a mappatura d'aria è costruito utilizzando funzionalità native di ONTAP come SnapLock Compliance e SnapMirror. Il risultato è un processo di recovery che è sia rapido che semplice da eseguire.

In caso di attacco ransomware e di necessità di un ripristino dal cyber vault, il processo di recovery è semplice e immediato, poiché le copie snapshot contenute nel cyber vault vengono utilizzate per ripristinare i dati crittografati.



Se il requisito è fornire un metodo più rapido per riportare online i dati quando è necessario per validare rapidamente, isolare e analizzare i dati per il recovery. Ciò può essere ottenuto facilmente utilizzando con FlexClone con l'opzione tipo SnapLock impostata su tipo non SnapLock.

> A partire da ONTAP 9.13,1, ripristinare una copia Snapshot bloccata sul volume SnapLock di destinazione di una relazione vault di SnapLock può essere ripristinato immediatamente creando un FlexClone con l'opzione di tipo SnapLock impostata su "non-SnapLock". Quando si esegue l'operazione di creazione del clone del volume, specificare la copia Snapshot come "snapshot padre". Ulteriori informazioni sulla creazione di un volume FlexClone con un tipo di SnapLock "qui."

> La pratica delle procedure di ripristino dal cyber vault garantirà che vengano stabilite le procedure corrette per la connessione al cyber vault e il recupero dei dati. Pianificare e testare la procedura è essenziale per qualsiasi recupero durante un attacco informatico.

Considerazioni aggiuntive

Ci sono considerazioni aggiuntive nella progettazione e distribuzione di un cyber vault basato su ONTAP.

Considerazioni sul dimensionamento della capacità

La quantità di spazio su disco necessaria per un volume di destinazione del vault informatico ONTAP dipende da una varietà di fattori, il più importante dei quali è il tasso di variazione per i dati nel volume di origine. È improbabile che la pianificazione di backup e la pianificazione Snapshot sul volume di destinazione influiscano sull'utilizzo del disco sul volume di destinazione e che la velocità di modifica sul volume di origine sia costante. È consigliabile fornire un buffer di capacità di storage aggiuntiva oltre a quello necessario per adattarsi a future modifiche del comportamento di utenti finali o applicazioni.

Il dimensionamento di una relazione per 1 mese di conservazione in ONTAP richiede il calcolo dei requisiti storage in base a diversi fattori, tra cui le dimensioni del set di dati primario, il tasso di cambiamento dei dati (tasso di modifica giornaliero) e i risparmi in termini di deduplica e compressione (se applicabili).

Ecco l'approccio passo passo:

Il primo passo è conoscere le dimensioni del volume o dei volumi di origine che si sta proteggendo con il vault informatico. Questa è la quantità di base di dati che verranno inizialmente replicati nella destinazione del cyber vault. Quindi, stimare la frequenza di modifica giornaliera per il set di dati. Questa è la percentuale di dati che cambia ogni giorno. È fondamentale avere una buona comprensione di come sono dinamici i tuoi dati.

Ad esempio:

- Dimensioni del set di dati primario = 5TB
- Tasso di cambio giornaliero = 5% (0,05)
- Efficienza di deduplica e compressione = 50% (0,50)

Ora, esaminiamo il calcolo:

- Calcolare la velocità di modifica giornaliera dei dati:

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

- Calcolare il totale dei dati modificati per 30 giorni:

  ```
  Total changed data in 30 days = 250 GB * 14 = 3.5TB
  ```

- Calcolare lo storage totale necessario:

  ```
  TOTAL = 5TB + 3.5TB = 8.5TB
  ```

- Applica i risparmi su deduplica e compressione:

  ```
  EFFECTIVE = 8.5TB * 50% = 4.25TB
  ```

Riepilogo delle esigenze di archiviazione

- Senza efficienza: Richiederebbe **8,5TB** per memorizzare 30 giorni dei dati del vault.
- Con un'efficienza del 50%: Richiederebbe **4,25TB** di storage dopo la deduplica e la compressione.

> Le copie Snapshot possono avere un overhead aggiuntivo a causa dei metadati, ma questo è in genere di entità secondaria.

> Se vengono eseguiti più backup al giorno, regolare il calcolo in base al numero di copie Snapshot acquisite ogni giorno.

> Considerare la crescita dei dati nel tempo per garantire che il dimensionamento sia a prova di futuro.

Impatto delle performance sui sistemi primari/di origine

Poiché il trasferimento dei dati è un'operazione di pull, l'impatto sulle prestazioni dello storage primario può variare in base al carico di lavoro, al volume di dati e alla frequenza dei backup. Tuttavia, l'impatto complessivo sulle prestazioni sul sistema primario è generalmente moderato e gestibile, poiché il trasferimento dei dati è progettato per trasferire le attività di backup e protezione dei dati al sistema di storage del vault informatico. Durante la configurazione iniziale della relazione e il primo backup completo, una quantità significativa di dati viene trasferita dal sistema primario al sistema del vault cibernetico (il volume SnapLock Compliance). Ciò può

comportare un aumento del traffico di rete e del carico i/o sul sistema primario. Una volta completato il backup completo iniziale, ONTAP deve solo tenere traccia e trasferire i blocchi modificati dall'ultimo backup. Con conseguente riduzione del carico i/o rispetto alla replica iniziale. Gli aggiornamenti incrementali sono efficienti e hanno un impatto minimo sulle performance dello storage primario. Il processo del vault viene eseguito in background, riducendo le possibilità di interferenza con i carichi di lavoro di produzione del sistema primario.

- Garantire che il sistema di storage disponga di risorse sufficienti (CPU, memoria e IOPS) per gestire il carico aggiuntivo riduce l'impatto delle performance.

Configurare, analizzare, cron script

NetApp ha creato un singolo script che può essere scaricato e utilizzato per configurare, verificare e pianificare le relazioni dei vault cibernetici.

Che cosa fa questo script

- Peering dei cluster
- Peering delle SVM
- Creazione di un volume DP
- Relazione e inizializzazione di SnapMirror
- Rafforzare il sistema ONTAP utilizzato per il cyber vault
- Quiete e riprendete la relazione in base al programma di trasferimento
- Convalidare periodicamente le impostazioni di protezione e generare un report che mostri eventuali anomalie

Come utilizzare questo script

Scaricare lo script e per utilizzarlo, seguire semplicemente la procedura riportata di seguito:

- Avviare Windows PowerShell come amministratore.
- Accedere alla directory contenente lo script.
- Eseguire lo script utilizzando `.\` la sintassi insieme ai parametri richiesti

> Assicurarsi di aver inserito tutte le informazioni. Alla prima esecuzione (modalità di configurazione), verranno richieste le credenziali sia per la produzione che per il nuovo sistema di cyber vault. Dopodiché, creerà i volumi e il SnapMirror di peering della SVM (se inesistenti) tra il sistema e li inizializzerà.

> La modalità cron può essere utilizzata per programmare la quiescenza e il ripristino del trasferimento dei dati.

Modalità operative

Lo script di automazione fornisce 3 modalità per l'esecuzione - `configure`, `analyze` e `cron`.

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

- Configura - esegue i controlli di convalida e configura il sistema come dotato di filtro aria.
- Analisi - funzionalità di monitoraggio e reporting automatizzate per inviare informazioni ai gruppi di monitoraggio per rilevare eventuali anomalie e attività sospette, al fine di garantire che le configurazioni non vengano deviate.
- Cron - per abilitare l'infrastruttura disconnessa, la modalità cron automatizza la disattivazione della LIF e chiude la relazione di trasferimento.

Il trasferimento dei dati nei volumi selezionati richiederà del tempo, a seconda delle prestazioni del sistema e della quantità di dati.

```
./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"
```

Conclusioni della soluzione PowerShell relativa al cyber vault di ONTAP

Sfruttando l'air-gapping con solide metodologie di protezione avanzata fornite da ONTAP, NetApp ti consente di creare un ambiente di storage sicuro e isolato in grado di resistere alle minacce informatiche in evoluzione. Tutto questo si ottiene mantenendo l'agilità e l'efficienza dell'infrastruttura storage esistente. Questo accesso sicuro consente alle aziende di raggiungere i loro rigorosi obiettivi in termini di sicurezza e tempi di attività con modifiche minime al personale, ai processi e alla struttura tecnologica esistenti.

Il cyber vault di ONTAP utilizza le funzionalità native di ONTAP è un approccio semplice per una protezione aggiuntiva al fine di creare copie immutabili e indelebili dei dati. L'aggiunta del cyber-vault basato su ONTAP di NetApp alla postura di sicurezza generale consentirà di:

- Creare un ambiente separato e disconnesso dalle reti di produzione e di backup e limitare l'accesso degli utenti.