Protezione dei dati con il cyber vault ONTAP

NetApp data management solutions

NetApp
January 27, 2026

Sommario

Protezione dei dati con il cyber vault ONTAP

Panoramica del cyber vault ONTAP

La principale minaccia che rende necessaria l'implementazione di un cyber vault è la crescente diffusione e la crescente sofisticatezza degli attacchi informatici, in particolare ransomware e violazioni dei dati. "Con l'aumento del phishing" e metodi sempre più sofisticati di furto di credenziali, le credenziali utilizzate per avviare un attacco ransomware potrebbero poi essere utilizzate per accedere ai sistemi infrastrutturali. In questi casi, anche i sistemi infrastrutturali più resistenti sono a rischio di attacco. L'unica difesa contro un sistema compromesso è quella di proteggere e isolare i propri dati in un cyber vault.

Il cyber vault basato su ONTAP di NetApp fornisce alle organizzazioni una soluzione completa e flessibile per proteggere le risorse di dati più critiche. Sfruttando l'air-gapping logico con solide metodologie di rafforzamento, ONTAP consente di creare ambienti di archiviazione sicuri e isolati, resilienti alle minacce informatiche in continua 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 di storage.

> A partire da luglio 2024, i contenuti dei report tecnici precedentemente pubblicati in formato PDF sono stati integrati nella documentazione del prodotto ONTAP . Inoltre, i nuovi report tecnici (TR) come questo documento non riceveranno più numeri TR.

Cos'è un cyber vault?

Un cyber vault è una tecnica specifica di protezione dei dati che prevede l'archiviazione di dati critici in un ambiente isolato, separato dall'infrastruttura IT primaria.

Repository dati "air-gapped", **immutabile** e **indelebile**, immune alle minacce che colpiscono la rete principale, come malware, ransomware o persino minacce interne. È possibile realizzare un caveau informatico con snapshot **immutabili** e **indelebili**.

I backup air-gapping che utilizzano metodi tradizionali comportano la creazione di spazio e la separazione fisica del supporto primario e secondario. Spostando i media fuori sede e/o interrompendo la connettività, i malintenzionati non hanno accesso ai dati. Ciò protegge i dati ma può comportare tempi di ripristino più lenti.

L'approccio di NetApp al cyber vault

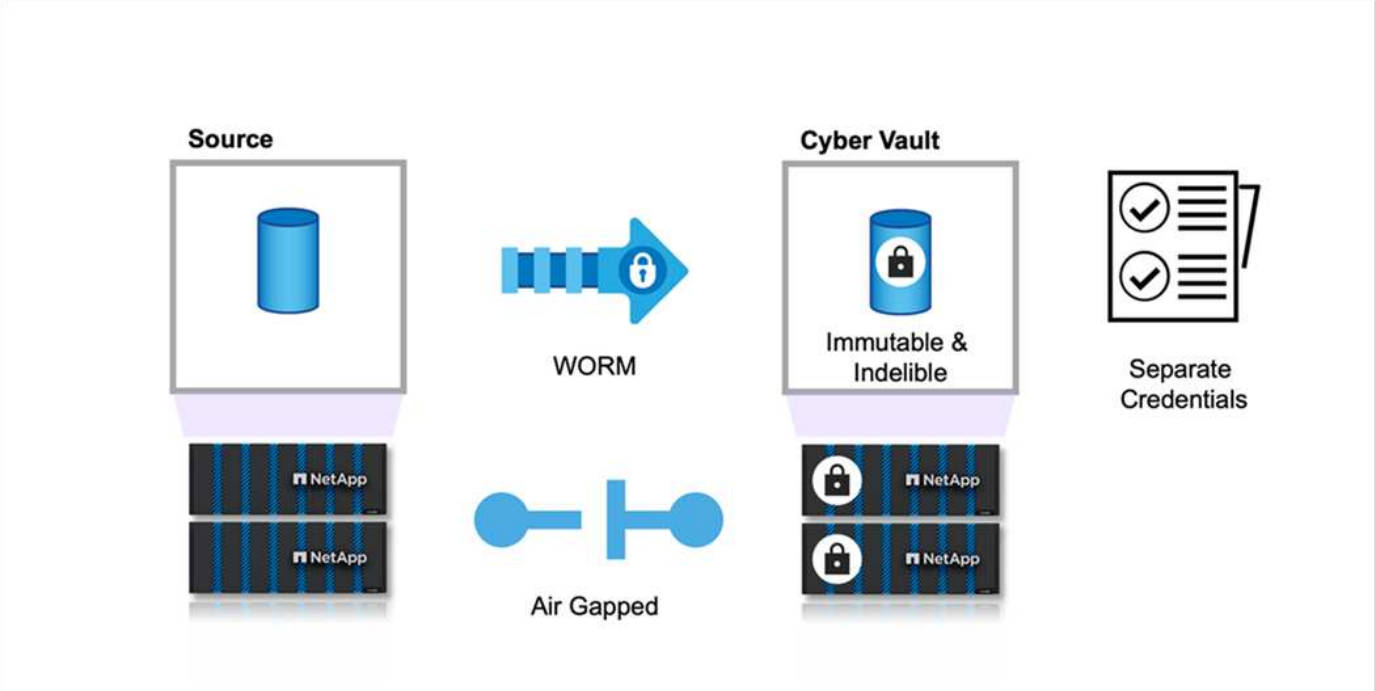
Le caratteristiche principali dell'architettura di riferimento NetApp per un cyber vault includono:

- Infrastruttura di archiviazione sicura e isolata (ad esempio, sistemi di archiviazione air-gapped)
- Le copie dei dati devono essere sia **immutabili** che **indelebili** senza eccezioni
- Controlli di accesso rigorosi e autenticazione a più fattori
- Capacità di ripristino rapido dei dati

È possibile utilizzare lo storage NetApp con ONTAP come un cyber vault air-gapped sfruttando"SnapLock Compliance per proteggere le copie Snapshot da WORM" . È possibile eseguire tutte le attività di base SnapLock Compliance sul Cyber Vault. Una volta configurati, i volumi del Cyber Vault vengono protetti automaticamente, eliminando la necessità di inviare manualmente le copie Snapshot a WORM. Ulteriori

informazioni sull'air-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 normative (rapporto di audit disponibile su richiesta). Utilizzando SnapLock Compliance con questa certificazione, otterrai un meccanismo rafforzato per l'air-gapping dei tuoi dati, su cui fanno affidamento i più grandi istituti finanziari del mondo per garantire sia la conservazione che il recupero dei registri bancari.



Terminologia ONTAP del Cyber Vault

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

Protezione autonoma da ransomware (ARP) - La funzionalità di protezione autonoma da ransomware (ARP) utilizza l'analisi del carico di lavoro negli ambienti NAS (NFS e SMB) per rilevare e avvisare in modo proattivo e in tempo reale 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 maggiori informazioni, vedere il"Documentazione ONTAP sulla protezione autonoma dal ransomware"

Air-gap (logico) - È possibile configurare lo storage NetApp con ONTAP come un cyber vault logico air-gap sfruttando"SnapLock Compliance per proteggere le copie Snapshot da WORM"

Air-gap (fisico) - Un sistema fisico air-gap non ha connettività di rete. Utilizzando i backup su nastro, è possibile spostare le immagini in un'altra posizione. L'air-gap logico SnapLock Compliance è robusto quanto un sistema con air-gap fisico.

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 (inclusa un'organizzazione di supporto o la possibilità di formattare a basso livello il sistema di archiviazione).

Copie Snapshot indelebili: copie Snapshot che non possono essere eliminate, senza eccezioni (inclusa un'organizzazione di supporto o la possibilità di formattare a basso livello il sistema di archiviazione).

Copie Snapshot antimanomissione - Le copie Snapshot antimanomissione utilizzano la funzione di orologio SnapLock Compliance per bloccare le copie Snapshot per un periodo di tempo specificato. Questi snapshot bloccati non possono essere eliminati da nessun utente o dal supporto NetApp . È possibile utilizzare copie Snapshot bloccate per recuperare i dati se un volume viene compromesso da un attacco ransomware, malware, hacker, amministratore non autorizzato o eliminazione accidentale. Per maggiori informazioni, vedere il"Documentazione ONTAP sulle copie Tamperproof Snapshot"

- SnapLock* - SnapLock è una soluzione di conformità ad alte prestazioni per le organizzazioni che utilizzano l'archiviazione WORM per conservare i file in formato non modificato per scopi normativi e di governance. Per ulteriori informazioni, consultare il sito "Documentazione ONTAP su SnapLock" .
- SnapMirror* - SnapMirror è una tecnologia di replicazione per il disaster recovery, progettata per replicare in modo efficiente i dati. SnapMirror può creare uno specchio (o una copia esatta dei dati), un vault (una copia dei dati con una conservazione più lunga della copia Snapshot) o entrambi su un sistema secondario, in sede o nel cloud. Queste copie possono essere utilizzate per molti scopi diversi, ad esempio in caso di calamità, trasferimento nel cloud o creazione di un caveau informatico (quando si utilizza la policy del caveau e si blocca il caveau). Per maggiori informazioni, vedere il"Documentazione ONTAP su SnapMirror"
- SnapVault* - In ONTAP 9.3 SnapVault è stato deprecato in favore della configurazione SnapMirror tramite la policy vault o mirror-vault. Anche questo termine, pur essendo ancora utilizzato, è stato deprezzato. Per ulteriori informazioni, consultare il sito "Documentazione ONTAP su SnapVault" .

Dimensionamento del caveau informatico con ONTAP

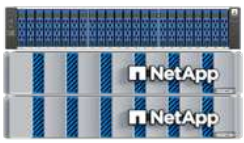
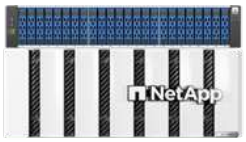
Per dimensionare un cyber vault è necessario capire quanti dati dovranno essere ripristinati entro un determinato Recovery Time Objective (RTO). Sono molti i fattori che entrano in gioco nella progettazione corretta di una soluzione di cyber vault delle dimensioni giuste. Quando si dimensiona un cyber vault, è necessario considerare sia le prestazioni che la capacità.

Considerazioni sulle dimensioni delle prestazioni

1. Quali sono i modelli di piattaforma sorgente (FAS , AFF A-Series, AFF C-Series)?
2. Qual è la larghezza di banda e la latenza tra la sorgente e il cyber vault?
3. Quanto sono grandi i file e quanti sono?
4. Qual è il tuo obiettivo in termini di tempo di recupero?
5. Quanti dati devono essere recuperati entro l'RTO?
6. Quante relazioni fan-in SnapMirror saranno assorbite dal caveau informatico?
7. Ci saranno recuperi singoli o multipli contemporaneamente?
8. Questi molteplici recuperi avverranno sullo stesso primario?
9. SnapMirror eseguirà la replica nel vault durante un ripristino da un vault?

Esempi di dimensionamento

Ecco alcuni esempi di diverse configurazioni di cyber vault.

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

Considerazioni sul dimensionamento della capacità

La quantità di spazio su disco richiesta per un volume di destinazione del cyber vault ONTAP dipende da diversi fattori, il più importante dei quali è la velocità di modifica dei dati nel volume di origine. Sia la pianificazione del backup che la pianificazione degli snapshot sul volume di destinazione influiscono sull'utilizzo del disco sul volume di destinazione e la velocità di modifica sul volume di origine non è probabile che sia costante. È una buona idea fornire un buffer di capacità di archiviazione aggiuntiva oltre a quella necessaria per far fronte a futuri cambiamenti nel comportamento dell'utente finale o dell'applicazione.

Per dimensionare una relazione per 1 mese di conservazione in ONTAP è necessario calcolare i requisiti di archiviazione in base a diversi fattori, tra cui la dimensione del set di dati primario, la frequenza di modifica dei dati (frequenza di modifica giornaliera) e i risparmi di deduplicazione e compressione (se applicabili).

Ecco l'approccio passo dopo passo:

Il primo passo è conoscere le dimensioni del/i volume/i sorgente/i che si desidera proteggere con il cyber vault. Questa è la quantità base di dati che inizialmente verrà replicata nella destinazione del cyber vault. Successivamente, stimare il tasso di variazione giornaliero del set di dati. Questa è la percentuale di dati che cambia ogni giorno. È fondamentale comprendere bene quanto siano dinamici i tuoi dati.

Per esempio:

- Dimensione del set di dati primario = 5 TB
- Tasso di variazione giornaliero = 5% (0,05)
- Efficienza di deduplicazione e compressione = 50% (0,50)

Ora, analizziamo il calcolo:

- Calcola il tasso di variazione giornaliero dei dati:

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

- Calcola il totale dei dati modificati in 30 giorni:

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

- Calcola lo spazio di archiviazione totale richiesto:

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

- Applica i risparmi derivanti dalla deduplicazione e dalla compressione:

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

Riepilogo delle esigenze di archiviazione

- Senza efficienza: sarebbero necessari **12,5 TB** per archiviare 30 giorni di dati del cyber vault.
- Con un'efficienza del 50%: richiederebbe **6,25 TB** di spazio di archiviazione dopo la deduplicazione e la compressione.

Le copie snapshot potrebbero comportare un sovraccarico aggiuntivo dovuto ai metadati, ma solitamente si tratta di un problema di lieve entità.

Se vengono eseguiti più backup al giorno, adattare il calcolo in base al numero di copie Snapshot eseguite ogni giorno.

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

Creazione di un caveau informatico con ONTAP

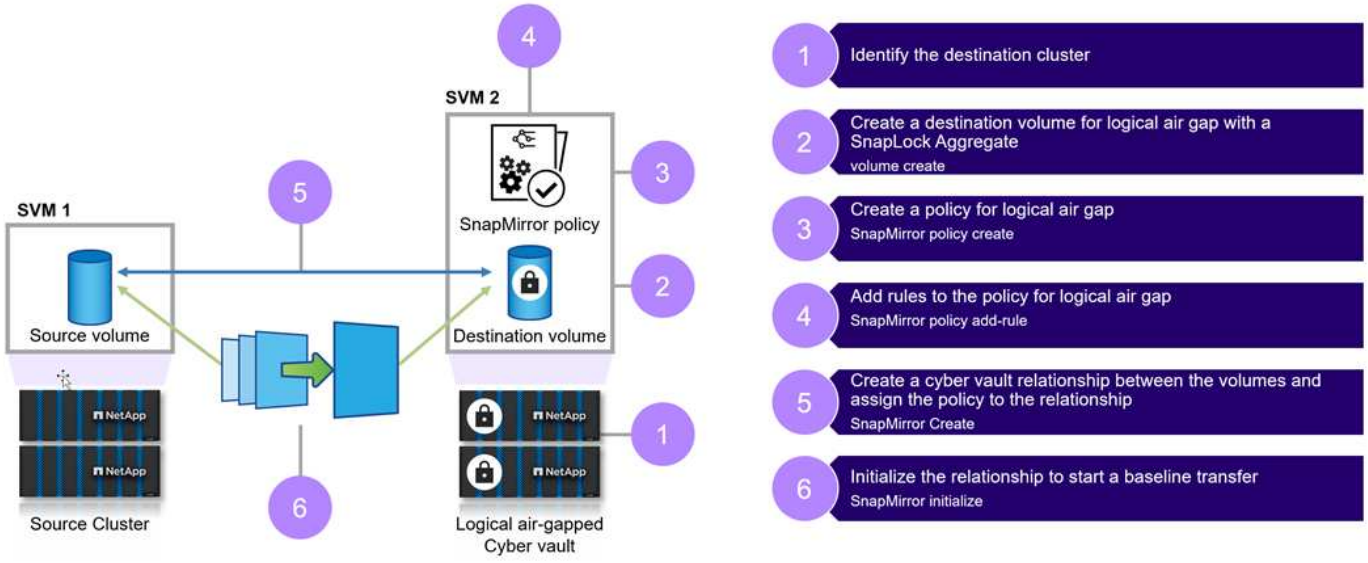
I passaggi seguenti aiuteranno a creare un cyber vault con ONTAP.

Prima di iniziare

- Il cluster di origine deve eseguire ONTAP 9 o 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, consultare "Cluster Peering" .
- Se l'aumento automatico del volume è disabilitato, lo spazio libero sul volume di destinazione deve essere almeno il cinque percento superiore allo spazio utilizzato sul volume di origine.

Informazioni su questo compito

L'illustrazione seguente mostra la procedura per inizializzare una relazione di vault SnapLock Compliance :



Passi

1. Identificare l'array di destinazione che diventerà il caveau informatico in cui ricevere i dati isolati.

2. Sulla matrice di destinazione, per preparare il cyber vault,"installare la licenza ONTAP One" ,"inizializzare il Compliance Clock" e, se si utilizza una versione ONTAP precedente alla 9.10.1,"creare un aggregato SnapLock Compliance" .
3. Nell'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 coesistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzi il volume `-snaplock-type` opzione per specificare un tipo di conformità. Nelle versioni ONTAP precedenti a ONTAP 9.10.1, la modalità SnapLock , Compliance, viene ereditata dall'aggregato. I volumi di destinazione con versione flessibile 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 `SVM2` nel complesso `node01_aggr` :

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

5. Sul cluster di destinazione, per creare l'air-gap, impostare il periodo di conservazione predefinito, come descritto in"Imposta il periodo di conservazione predefinito" . A un volume SnapLock che è una destinazione di vault è assegnato un periodo di conservazione predefinito. Il valore per questo periodo è inizialmente impostato su un minimo di 0 anni e un massimo di 100 anni (a partire da ONTAP 9.10.1. Per le versioni precedenti ONTAP , il valore è 0 - 70.) per i volumi SnapLock Compliance . Inizialmente, ogni copia NetApp Snapshot viene impegnata con questo periodo di conservazione predefinito. Il periodo di conservazione predefinito deve essere modificato. Se necessario, il periodo di conservazione può essere esteso in seguito, ma non può mai essere abbreviato. Per ulteriori informazioni, consultare "Panoramica del tempo di conservazione impostato" .

   > I fornitori di servizi devono tenere conto delle date di scadenza del contratto del cliente quando determinano il periodo di conservazione. Ad esempio, se il periodo di conservazione del cyber vault è di 30 giorni e il contratto del cliente termina prima della scadenza del periodo di conservazione, i dati nel cyber vault non potranno essere eliminati fino alla scadenza del periodo di conservazione.

6. "Crea una nuova relazione di replicazione"tra la sorgente 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 XDPDefault per archiviare le copie Snapshot etichettate giornalmente e settimanalmente in base a una pianificazione oraria:

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

   "Creare una politica di replica personalizzata"o un"programma personalizzato" se le impostazioni predefinite disponibili non sono adatte.

7. Sulla SVM di destinazione, inizializzare la relazione SnapVault creata nel passaggio 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. Dopo che la relazione è stata inizializzata e resa inattiva, utilizzare il comando snapshot show sulla destinazione per verificare il tempo di scadenza SnapLock applicato alle copie Snapshot replicate.

   In questo esempio sono elencate le copie Snapshot sul volume dstvolB che hanno l'etichetta SnapMirror e la data di scadenza SnapLock :

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

Rafforzamento del caveau informatico

Ecco i consigli aggiuntivi per rafforzare un cyber vault ONTAP . Per ulteriori consigli e procedure, consultare la guida all'indurimento ONTAP riportata di seguito.

Raccomandazioni per il rafforzamento del cyber vault

- Isolare i piani di gestione del cyber vault
- Non abilitare i LIF dei dati sul cluster di destinazione poiché rappresentano un ulteriore vettore di attacco
- Sul cluster di destinazione, limitare l'accesso LIF intercluster al cluster di origine con una policy di servizio
- Segmentare la gestione LIF sul cluster di destinazione per un accesso limitato con una policy di servizio e un host bastion
- Limita tutto il traffico dati dal cluster di origine al cyber vault per consentire solo le porte necessarie per il traffico SnapMirror
- Se possibile, disabilitare tutti i metodi di accesso alla gestione non necessari all'interno di ONTAP per ridurre la superficie di attacco
- Abilita la registrazione degli audit e l'archiviazione dei log remoti
- Abilita la verifica multi-amministratore e richiedi la verifica da un amministratore esterno ai tuoi normali amministratori di storage (ad esempio, personale CISO)
- Implementare controlli di accesso basati sui ruoli
- Richiedi l'autenticazione multifattoriale amministrativa per System Manager e ssh
- Utilizzare l'autenticazione basata su token per gli script e le chiamate API REST

Si prega di fare riferimento al"Guida all'indurimento ONTAP" ,"Panoramica della verifica multi-amministratore" E"Guida all'autenticazione multifattoriale ONTAP" per scoprire come realizzare questi passaggi di indurimento.

Interoperabilità del caveau informatico

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

Raccomandazioni hardware ONTAP

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

- Lo storage ibrido FAS offre la soluzione più conveniente.
- La serie AFF C offre la massima efficienza in termini di consumo energetico e densità.
- AFF A-Series è la piattaforma più performante che offre il miglior RTO. Con il recente annuncio della nostra ultima serie AFF A, questa piattaforma offrirà la migliore efficienza di archiviazione senza compromessi in termini di prestazioni.

Raccomandazioni software ONTAP

A partire da ONTAP 9.14.1, è possibile specificare periodi di conservazione per etichette SnapMirror specifiche nella policy SnapMirror della relazione 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 un FlexClone con l'opzione snaplock-type impostata su "non-snaplock" e specificando la copia Snapshot come "parent-snapshot" durante l'esecuzione dell'operazione di creazione del clone del volume. Scopri di più su "creazione di un volume FlexClone con un tipo SnapLock" .

Configurazione MetroCluster

Per le configurazioni MetroCluster , è necessario tenere presente quanto segue:

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

Domande frequenti sul Cyber Vault

Queste FAQ sono destinate ai clienti e ai partner NetApp . Risponde alle domande più frequenti sull'architettura di riferimento del cyber vault basata su ONTAP di NetApp.

Cos'è un cyber vault NetApp ?

Il Cyber Vault è una tecnica specifica di protezione dei dati che prevede l'archiviazione dei dati in un ambiente isolato, separato dall'infrastruttura IT primaria.

Il cyber vault è un archivio dati "air-gapped", immutabile e indelebile, immune alle minacce che colpiscono i dati primari, come malware, ransomware o minacce interne. È possibile realizzare un cyber vault con copie immutabili di NetApp ONTAP Snapshot e renderlo indelebile con NetApp SnapLock Compliance. Durante la protezione SnapLock Compliance , i dati non possono essere modificati o eliminati, nemmeno dagli amministratori ONTAP o dal supporto NetApp .

I backup air-gapping effettuati con metodi tradizionali comportano la creazione di spazio e la separazione fisica del supporto primario e secondario. L'air-gapping con il cyber vault prevede l'utilizzo di una rete di replicazione dei dati separata, esterna alle reti di accesso ai dati standard, per replicare le copie Snapshot in una destinazione indelebile.

Ulteriori misure oltre alle reti air-gapped prevedono la disattivazione di tutti i protocolli di accesso e replicazione dei dati sul cyber vault quando non sono necessari. Ciò impedisce l'accesso ai dati o l'esfiltrazione dei dati nel sito di destinazione. Con SnapLock Compliance non è richiesta alcuna separazione fisica. SnapLock Compliance protegge le tue copie Snapshot archiviate, point-in-time e di sola lettura, garantendo un rapido ripristino dei dati, al sicuro dall'eliminazione e immutabili.

L'approccio di NetApp al cyber vault

NetApp Cyber Vault, basato su SnapLock, offre alle organizzazioni una soluzione completa e flessibile per proteggere le risorse di dati più critiche. Sfruttando le tecnologie di rafforzamento di ONTAP, NetApp consente di creare un cyber vault sicuro, isolato e protetto, immune alle minacce informatiche in continua evoluzione. Con NetApp puoi garantire la riservatezza, l'integrità e la disponibilità dei tuoi dati, mantenendo al contempo l'agilità e l'efficienza della tua infrastruttura di storage.

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

- Infrastruttura di archiviazione sicura e isolata (ad esempio, sistemi di archiviazione air-gapped)
- Le copie di backup dei tuoi dati sono immutabili e indelebili
- Controlli di accesso rigorosi e separati, verifica multi-amministratore e autenticazione multi-fattore
- Capacità di ripristino rapido dei dati

Domande frequenti sul Cyber Vault

Cyber Vault è un prodotto NetApp?

No, "cyber vault" è un termine che si applica a tutto il settore. NetApp ha creato un'architettura di riferimento per consentire ai clienti di creare facilmente i propri archivi informatici e sfruttare le decine di funzionalità di sicurezza ONTAP per proteggere i propri dati dalle minacce informatiche. Ulteriori informazioni sono disponibili sul"Sito di documentazione ONTAP" .

Cyber Vault di NetApp è solo un altro nome per LockVault o SnapVault?

LockVault era una funzionalità di Data ONTAP 7-mode che non è disponibile nelle versioni attuali di ONTAP.

SnapVault era un termine obsoleto per indicare ciò che oggi viene realizzato con la politica di vaulting di SnapMirror. Questa policy consente alla destinazione di conservare una quantità di copie Snapshot diversa rispetto al volume di origine.

Cyber Vault utilizza SnapMirror con la policy Vault e SnapLock Compliance insieme per creare una copia immutabile e indelebile dei dati.

Quale hardware NetApp posso utilizzare per un cyber vault, FAS, capacity flash o performance flash?

Questa architettura di riferimento per il cyber vaulting si applica all'intero portafoglio hardware ONTAP . I clienti possono utilizzare le piattaforme AFF A-Series, AFF C-Series o FAS come caveau. Le piattaforme basate su flash garantiranno i tempi di ripristino più rapidi, mentre le piattaforme basate su disco offriranno la soluzione più conveniente. A seconda della quantità di dati da recuperare e se più recuperi vengono eseguiti in parallelo, l'utilizzo di sistemi basati su disco (FAS) potrebbe richiedere da giorni a settimane. Si prega di consultare un rappresentante NetApp o un partner per dimensionare correttamente una soluzione di cyber vault in base alle esigenze aziendali.

Posso utilizzare Cloud Volumes ONTAP come sorgente di cyber vault?

Sì, tuttavia l'utilizzo di CVO come origine richiede che i dati vengano replicati in una destinazione di cyber vault locale, poiché la SnapLock Compliance è un requisito per un cyber vault ONTAP . La replica dei dati da un'istanza CVO basata su hyperscaler potrebbe comportare costi di uscita.

Posso utilizzare Cloud Volumes ONTAP come destinazione di un cyber vault?

L'architettura Cyber Vault si basa sull'indelebilità di SnapLock Compliance di ONTAP ed è progettata per implementazioni on-premise. Le architetture Cyber Vault basate su cloud sono in fase di studio per future pubblicazioni.

Posso utilizzare ONTAP Select come sorgente di cyber vault?

Sì, ONTAP Select può essere utilizzato come origine per una destinazione di cyber vault basata su hardware on-premise.

Posso utilizzare ONTAP Select come destinazione di un cyber vault?

No, ONTAP Select non deve essere utilizzato come destinazione di un cyber vault poiché non è in grado di utilizzare SnapLock Compliance.

Un caveau informatico con NetApp utilizza solo SnapMirror?

No, l'architettura di un cyber vault NetApp sfrutta numerose funzionalità ONTAP per creare una copia dei dati sicura, isolata, protetta e rafforzata. Per maggiori informazioni su quali ulteriori tecniche possono essere utilizzate, vedere la domanda successiva.

Esistono altre tecnologie o configurazioni utilizzate per il cyber vault?

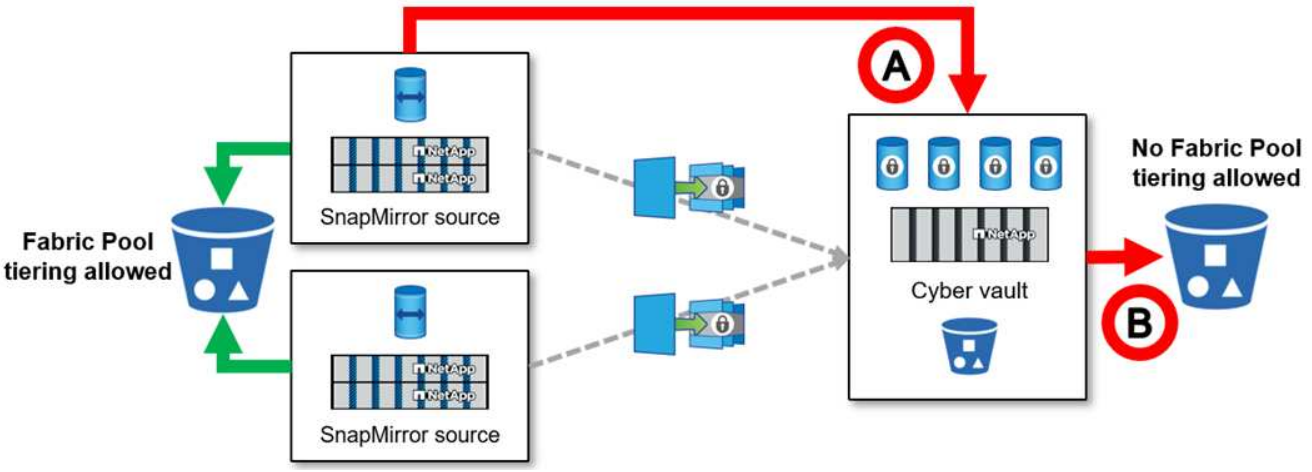
Le basi di un cyber vault NetApp sono SnapMirror e SnapLock Compliance, ma l'utilizzo di funzionalità ONTAP aggiuntive, come copie Snapshot antimanomissione, autenticazione a più fattori (MFA), verifica multi-amministratore, controllo degli accessi basato sui ruoli e registrazione degli audit locali e remoti, migliora la sicurezza e la protezione dei dati.

Cosa rende le copie ONTAP Snapshot migliori di altre per un cyber vault?

Le copie Snapshot ONTAP sono immutabili per impostazione predefinita e possono essere rese indelebili con SnapLock Compliance. Nemmeno il supporto NetApp riesce a eliminare le copie SnapLock Snapshot. La domanda più opportuna è: cosa rende NetApp Cyber Vault migliore rispetto ad altri Cyber Vault del settore? Innanzitutto, ONTAP è lo storage più sicuro al mondo e ha ottenuto la convalida CSfC, che consente l'archiviazione di dati segreti e top secret a riposo sia a livello hardware che software. Maggiori informazioni su"Il CSfC può essere trovato qui" . Inoltre, ONTAP può essere isolato a livello di storage, con il sistema di cyber vault che controlla la replica, consentendo la creazione di un isolamento all'interno della rete di cyber vault.

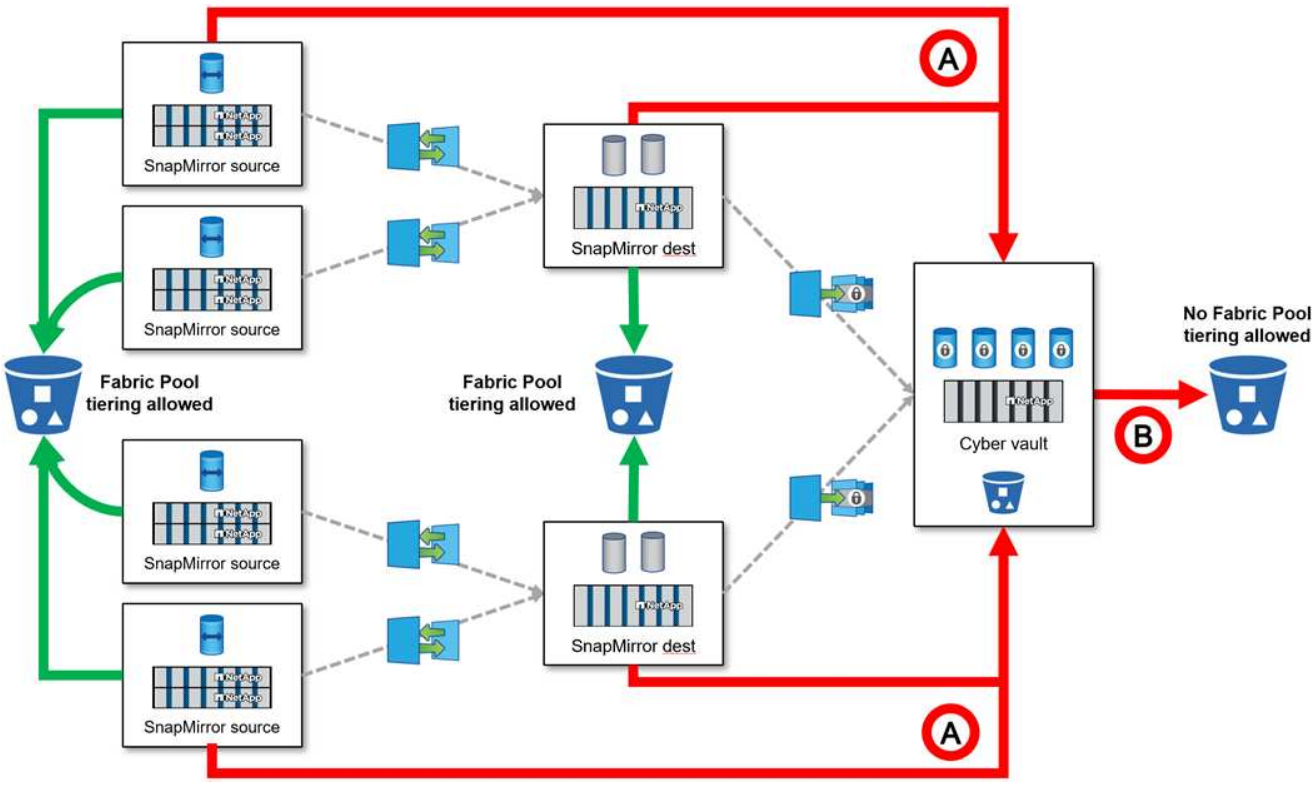
Un volume su un cyber vault può utilizzare ONTAP Fabric Pool?

No, un volume di Cyber Vault (destinazione SnapLock Compliance SnapMirror) non può essere suddiviso in livelli tramite Fabric Pool, indipendentemente dalla policy.



Esistono molteplici scenari in cui il pool Fabric **non** può essere utilizzato con un cyber vault.

1. I livelli freddi del Fabric Pool **non possono** utilizzare un cluster di cyber vault. Questo perché l'abilitazione del protocollo S3 invalida la natura sicura dell'architettura di riferimento del cyber vault. Inoltre, il bucket S3 utilizzato per il pool Fabric non può essere protetto.
2. I volumi SnapLock Compliance sul cyber vault **non possono** essere suddivisi in livelli in un bucket S3 poiché i dati sono bloccati nel volume.



ONTAP S3 Worm è disponibile in un cyber vault?

No, S3 è un protocollo di accesso ai dati che invalida la natura sicura dell'architettura di riferimento.

NetApp Cyber Vault funziona su una personalità o un profilo ONTAP diverso?

No, è un'architettura di riferimento. I clienti possono utilizzare il"architettura di riferimento" e costruire un caveau informatico, oppure può utilizzare il"Script PowerShell per creare, rafforzare e convalidare" un caveau informatico.

Posso attivare protocolli dati come NFS, SMB e S3 in un cyber vault?

Per impostazione predefinita, i protocolli dati dovrebbero essere disabilitati sul cyber vault per renderlo sicuro. Tuttavia, è possibile abilitare i protocolli dati sul cyber vault per accedere ai dati a scopo di recupero o quando necessario. Questa operazione dovrebbe essere eseguita temporaneamente e disattivata una volta completato il ripristino.

È possibile convertire un ambiente SnapVault esistente in un cyber vault oppure è necessario riseminare tutto?

Sì. Si potrebbe prendere un sistema che è una destinazione SnapMirror (con policy di vault), disabilitare i protocolli dati, rafforzare il sistema secondo"Guida all'indurimento ONTAP" , isolarlo in una posizione sicura e seguire le altre procedure nell'architettura di riferimento per trasformarlo in un cyber vault senza dover effettuare il seeding della destinazione.

Hai altre domande? Invia un'e-mail a ng-cyber-vault@netapp.com con le tue domande! Risponderemo alle tue domande e le aggiungeremo alle FAQ.

Risorse del caveau informatico

Per saperne di più sulle informazioni descritte in questa informativa sul cyber vault, fare riferimento alle seguenti informazioni aggiuntive e ai concetti di sicurezza.

- "NetApp Cyber Vault: breve sintesi delle soluzioni di protezione dei dati multistrato"
- "NetApp ottiene la valutazione AAA per la prima soluzione on-box per il rilevamento dei ransomware basata sull'intelligenza artificiale"
- "Aumenta la resilienza informatica con lo storage più sicuro del pianeta"
- "Guida al rafforzamento della sicurezza ONTAP"
- "NetApp Zero Trust"
- "Resilienza informatica NetApp"
- "Protezione dei dati NetApp"
- "Panoramica del peering di cluster e SVM con la CLI"
- "Archiviazione SnapVault"
- "Configurare, analizzare, cron script"

Creazione, rafforzamento e convalida di un cyber vault ONTAP con PowerShell

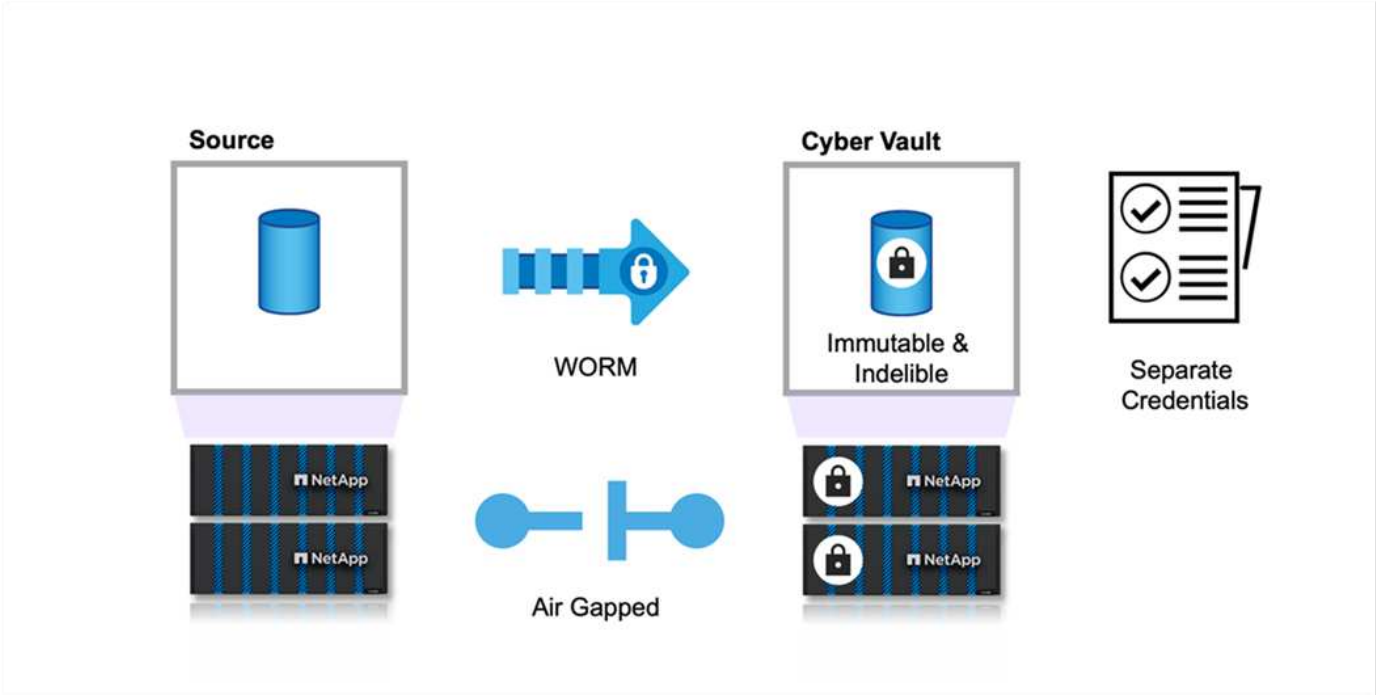
Panoramica di ONTAP Cyber Vault con PowerShell

Nel panorama digitale odierno, la salvaguardia delle risorse di dati critiche di un'organizzazione non è solo una buona pratica, ma un imperativo aziendale. Le minacce informatiche si evolvono a un ritmo senza precedenti e le tradizionali misure di protezione dei dati non sono più sufficienti a proteggere 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 solide misure di protezione dei dati per creare una barriera impenetrabile contro le minacce informatiche. Isolando i dati più preziosi con una tecnologia di rafforzamento della sicurezza, un cyber vault riduce al minimo la superficie di attacco, in modo che i dati più critici rimangano riservati, intatti e facilmente accessibili quando necessario.

Un cyber vault è un deposito sicuro costituito da più livelli di protezione, come firewall, reti e storage. Questi componenti salvaguardano i dati di recupero vitali necessari per le operazioni aziendali cruciali. I componenti del cyber vault si sincronizzano regolarmente con i dati di produzione essenziali in base alla policy del vault, ma per il resto restano inaccessibili. Questa configurazione isolata e disconnessa garantisce che, nel caso in cui un attacco informatico comprometta l'ambiente di produzione, sia possibile eseguire facilmente un ripristino affidabile e definitivo dal cyber vault.

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

Combinando questo 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 controlli periodici in base alle normative SEC e FINRA, garantendo che la resilienza dei dati soddisfi le severe normative WORM e di conservazione dei dati del settore bancario. NetApp è l'unico storage aziendale convalidato da NSA CSfC per l'archiviazione di dati top secret.



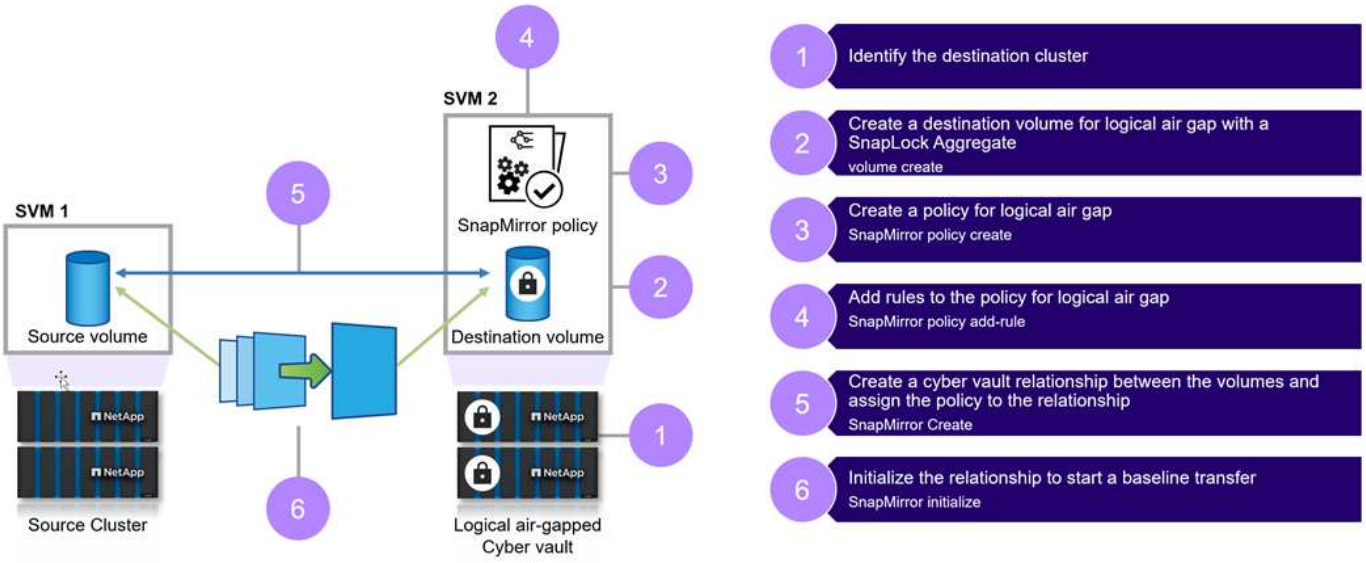
Questo documento descrive la configurazione automatizzata del cyber vault di NetApp per l'archiviazione ONTAP on-premise su un altro storage ONTAP designato con snapshot immutabili che aggiungono un ulteriore livello di protezione dai crescenti attacchi informatici per un rapido ripristino. Come parte di questa architettura, l'intera configurazione viene applicata secondo le 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 ONTAP.

Passaggi di alto livello per creare un cyber vault ONTAP

- Creare una relazione di peering
  - Il sito di produzione che utilizza l'archiviazione ONTAP è collegato all'archiviazione ONTAP del cyber vault designato
- Crea volume SnapLock Compliance
- Imposta la relazione SnapMirror e la regola per impostare l'etichetta
  - La relazione SnapMirror e le pianificazioni appropriate sono configurate
- Impostare le ritenzioni prima di avviare il trasferimento SnapMirror (vault)
  - Il blocco di conservazione viene applicato ai dati copiati, impedendo ulteriormente l'accesso ai dati da parte di utenti interni o da errori. In questo modo i dati non possono essere eliminati prima della scadenza del periodo di conservazione
  - Le organizzazioni possono conservare questi dati per alcune settimane/mesi a seconda delle loro esigenze
- Inizializza la relazione SnapMirror in base alle etichette
  - Il seeding iniziale e il trasferimento incrementale per sempre avvengono in base alla pianificazione SnapMirror
  - I dati sono protetti (immutabili e indelebili) con la conformità SnapLock e sono disponibili per il ripristino

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



Componenti della soluzione

NetApp ONTAP in esecuzione nella versione 9.15.1 sui cluster di origine e di destinazione.

ONTAP One: la licenza all-in-one di NetApp ONTAP.

Funzionalità utilizzate dalla licenza ONTAP One:

- SnapLock Compliance
- SnapMirror
- Verifica multi-amministratore
- Tutte le capacità di rafforzamento esposte da ONTAP
- Credenziali RBAC separate per il cyber vault

Tutti gli array fisici unificati ONTAP possono essere utilizzati per un cyber vault, tuttavia i sistemi flash basati sulla capacità della serie C AFF e i sistemi flash ibridi FAS rappresentano le piattaforme ideali più convenienti per questo scopo. Si prega di consultare il"Dimensionamento del caveau informatico ONTAP" per indicazioni sulle taglie.

Creazione di un cyber vault ONTAP con PowerShell

I backup air-gapping che utilizzano metodi tradizionali comportano la creazione di spazio e la separazione fisica del supporto primario e secondario. Spostando i media fuori sede e/o interrompendo la connettività, i malintenzionati non hanno accesso ai dati. Ciò

protegge i dati ma può comportare tempi di ripristino più lenti. Con SnapLock Compliance non è richiesta alcuna separazione fisica. SnapLock Compliance protegge le copie di sola lettura e punto nel tempo degli snapshot archiviati, garantendo dati rapidamente accessibili, al sicuro da cancellazioni o indelebili e al sicuro da modifiche o immutabili.

Prerequisiti

Prima di iniziare con i passaggi descritti nella sezione successiva di questo documento, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster di origine deve eseguire ONTAP 9 o versione successiva.
- Gli aggregati di origine e destinazione devono essere a 64 bit.
- I cluster di origine e di destinazione devono essere peering.
- Le SVM di origine e di destinazione devono essere peering.
- Assicurarsi che la crittografia del peering del cluster sia abilitata.

L'impostazione del trasferimento dei dati in un cyber vault ONTAP richiede diversi passaggi. Sul volume primario, configurare un criterio di snapshot che specifichi quali copie creare e quando crearle utilizzando pianificazioni appropriate e assegnare etichette per specificare quali copie devono essere trasferite da SnapVault. Sul secondario, è necessario creare una policy SnapMirror che specifichi le etichette delle copie Snapshot da trasferire e quante di queste copie devono essere conservate nel cyber vault. Dopo aver configurato queste policy, creare la relazione SnapVault e stabilire una pianificazione del trasferimento.

Questo documento presuppone che l'archiviazione primaria e il cyber vault ONTAP designato siano già impostati e configurati.

Il cluster di Cyber Vault può trovarsi nello stesso data center dei dati di origine o in un data center diverso.

Passaggi per creare un cyber vault ONTAP

1. Utilizzare ONTAP CLI o System Manager per inizializzare il clock di conformità.
2. Creare un volume di protezione dati con la conformità SnapLock abilitata.
3. Utilizzare il comando di creazione SnapMirror per creare relazioni di protezione dei dati SnapVault .
4. Imposta il periodo di conservazione predefinito SnapLock Compliance per il volume di destinazione.

La conservazione predefinita è "Impostata al minimo". A un volume SnapLock che è una destinazione di vault è assegnato un periodo di conservazione predefinito. Il valore per questo periodo è inizialmente impostato su un minimo di 0 anni e un massimo di 100 anni (a partire da ONTAP 9.10.1. Per le versioni precedenti ONTAP , il valore è 0 - 70.) per i volumi SnapLock Compliance . Inizialmente, ogni copia NetApp Snapshot viene impegnata con questo periodo di conservazione predefinito. Se necessario, il periodo di conservazione può essere esteso in seguito, ma non può mai essere abbreviato. Per ulteriori informazioni, consultare "Panoramica del tempo di conservazione impostato" .

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

Ecco un esempio di codice PowerShell per inizializzare il 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 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 descritti, il caveau informatico air-gapped che utilizza SnapLock Compliance e SnapVault è pronto.

Prima di trasferire i dati degli snapshot al cyber vault, è necessario inizializzare la relazione SnapVault . Tuttavia, prima di ciò, è necessario eseguire un rafforzamento della sicurezza per proteggere il caveau.

Protezione del cyber vault ONTAP con PowerShell

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

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

Rafforzamento delle migliori pratiche

Passaggi manuali

1. Crea un utente designato con ruolo amministrativo predefinito e personalizzato.
2. Crea un nuovo spazio IP per isolare il traffico di rete.
3. Creare un nuovo SVM residente nel nuovo IPspace.

4. Assicurarsi che le policy di routing del firewall siano configurate correttamente e che tutte le regole vengano regolarmente verificate e aggiornate secondo necessità.

ONTAP CLI o tramite script di automazione

1. Proteggi l'amministrazione con la verifica multi-amministratore (MAV) in aggiunta all'autenticazione a più fattori (MFA), migliorando la sicurezza per l'accesso amministrativo alla VM di archiviazione dati.
2. Abilita la crittografia per i dati standard "in transito" tra cluster.
3. Proteggere l'SSH con un potente sistema di crittografia e applicare password sicure.
4. Abilita FIPS globale.
5. Telnet e Remote Shell (RSH) dovrebbero essere disabilitati.
6. Blocca l'account amministratore predefinito.
7. Disattivare i LIF dei dati e proteggere i punti di accesso remoti.
8. Disattivare e rimuovere protocolli e servizi non utilizzati 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 indirizzi IP specifici utilizzando l'opzione IP consentita.
12. Interrompere e riprendere la replicazione in base alla pianificazione del trasferimento.

I punti da 1 a 4 richiedono un intervento manuale, come la designazione di una rete isolata, la segregazione dello spazio IP e così via, e devono essere eseguiti in anticipo. Informazioni dettagliate per configurare l'indurimento possono essere trovate nel"Guida al rafforzamento della sicurezza ONTAP" . Il resto può essere facilmente automatizzato per agevolare l'implementazione e il monitoraggio. L'obiettivo di questo approccio orchestrato è quello di fornire un meccanismo per automatizzare le fasi di rafforzamento per proteggere il controller del vault in futuro. Il lasso di tempo in cui l'air-gap del cyber vault rimane aperto è il più breve possibile. SnapVault sfrutta la tecnologia incrementale per sempre, che sposta nel cyber vault solo le modifiche apportate dopo l'ultimo aggiornamento, riducendo così al minimo il 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 replicazione per garantire la finestra di connessione più piccola possibile.

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 ONTAP con PowerShell

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

Una volta che le regole sono in vigore, un tentativo (supponendo che in qualche modo l'aggressore sia riuscito a entrare) di eliminare uno snapshot dal lato vault fallirà. Lo stesso vale per tutte le impostazioni di rafforzamento, applicando le restrizioni necessarie e salvaguardando il sistema.

Esempio di codice PowerShell per convalidare la configurazione in base a una 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 ci sono connessioni sul controller del vault.

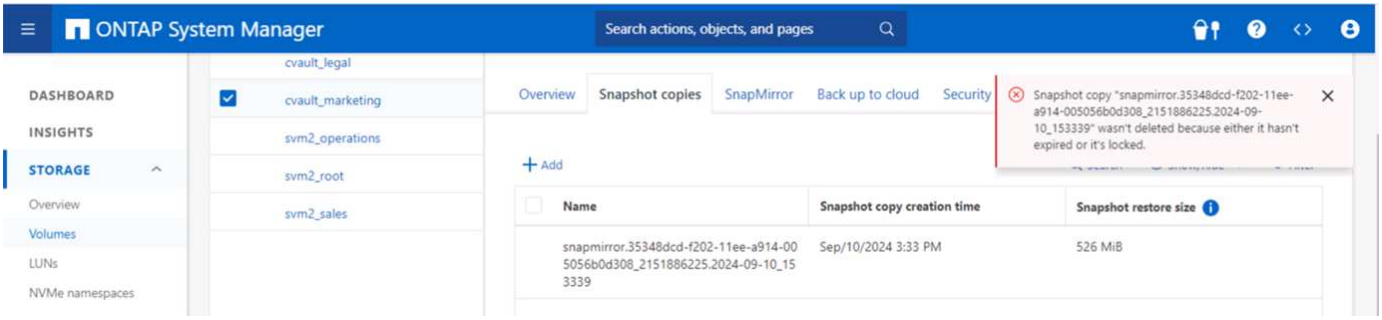
```
cluster2::> network connections  listening show
This table is currently empty.

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

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

cluster2::>
```

Questa schermata mostra che non è possibile manomettere gli snapshot.



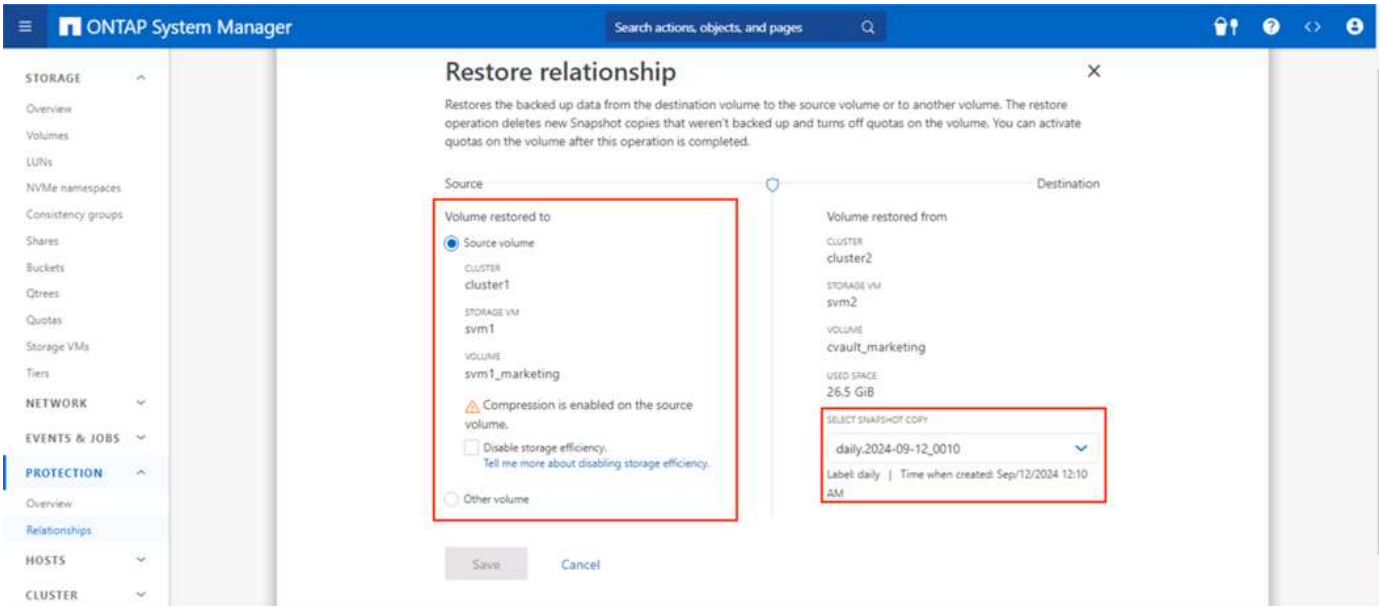
Per convalidare e confermare la funzionalità di air gapping, seguire i passaggi seguenti:

- Testare le capacità di isolamento della rete e la possibilità di disattivare una connessione quando non vengono trasferiti dati.
- Verificare che l'interfaccia di gestione non sia accessibile da entità diverse dagli indirizzi IP consentiti.
- Verifica La verifica multi-amministratore è in atto per fornire un ulteriore livello di approvazione.
- Convalidare la capacità di accesso tramite CLI e REST API
- Dall'origine, avviare un'operazione di trasferimento al vault e assicurarsi che la copia archiviata non possa essere modificata.
- Provare a eliminare le copie snapshot immutabili trasferite nel vault.
- Provare a modificare il periodo di conservazione manomettendo l'orologio di sistema.

Recupero dati da cyber vault ONTAP

Se i dati vengono distrutti nel data center di produzione, i dati del cyber vault possono essere recuperati in modo sicuro nell'ambiente scelto. A differenza di una soluzione fisicamente isolata, il cyber vault ONTAP isolato è realizzato utilizzando funzionalità ONTAP native come SnapLock Compliance e SnapMirror. Il risultato è un processo di recupero rapido e facile da eseguire.

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



Se il requisito è quello di fornire un metodo più rapido per riportare i dati online quando necessario, per convalidare, isolare e analizzare rapidamente i dati per il ripristino. Ciò può essere facilmente ottenuto utilizzando FlexClone con l'opzione snaplock-type impostata su non-snaplock type.

A partire da ONTAP 9.13.1, è possibile ripristinare all'istante una copia Snapshot bloccata sul volume SnapLock di destinazione di una relazione di vault SnapLock creando un FlexClone con l'opzione snaplock-type impostata su "non-snaplock". Quando si esegue l'operazione di creazione del clone del volume, specificare la copia Snapshot come "parent-snapshot". Ulteriori informazioni sulla creazione di un volume FlexClone con un tipo SnapLock"Qui."

L'esecuzione di procedure di recupero dal cyber vault garantirà che vengano stabiliti i passaggi corretti per la connessione al cyber vault e il recupero dei dati. Pianificare e testare la procedura è essenziale per qualsiasi ripristino durante un attacco informatico.

Considerazioni aggiuntive

Quando si progetta e si implementa un cyber vault basato su ONTAP , è necessario tenere in considerazione ulteriori considerazioni.

Considerazioni sul dimensionamento della capacità

La quantità di spazio su disco richiesta per un volume di destinazione del cyber vault ONTAP dipende da diversi fattori, il più importante dei quali è la velocità di modifica dei dati nel volume di origine. Sia la pianificazione del backup che la pianificazione degli snapshot sul volume di destinazione influiscono sull'utilizzo del disco sul volume di destinazione e la velocità di modifica sul volume di origine non è probabile che sia costante. È una buona idea fornire un buffer di capacità di archiviazione aggiuntiva oltre a quella necessaria per far fronte a futuri cambiamenti nel comportamento dell'utente finale o dell'applicazione.

Per dimensionare una relazione per 1 mese di conservazione in ONTAP è necessario calcolare i requisiti di archiviazione in base a diversi fattori, tra cui la dimensione del set di dati primario, la frequenza di modifica dei dati (frequenza di modifica giornaliera) e i risparmi di deduplicazione e compressione (se applicabili).

Ecco l'approccio passo dopo passo:

Il primo passo è conoscere le dimensioni del/i volume/i sorgente/i che si desidera proteggere con il cyber vault. Questa è la quantità base di dati che inizialmente verrà replicata nella destinazione del cyber vault. Successivamente, stimare il tasso di variazione giornaliero del set di dati. Questa è la percentuale di dati che cambia ogni giorno. È fondamentale comprendere bene quanto siano dinamici i tuoi dati.

Per esempio:

- Dimensione del set di dati primario = 5 TB
- Tasso di variazione giornaliero = 5% (0,05)
- Efficienza di deduplicazione e compressione = 50% (0,50)

Ora, analizziamo il calcolo:

- Calcola il tasso di variazione giornaliero dei dati:

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

- Calcola il totale dei dati modificati in 30 giorni:

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

- Calcola lo spazio di archiviazione totale richiesto:

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

- Applica i risparmi derivanti dalla deduplicazione e dalla compressione:

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

Riepilogo delle esigenze di archiviazione

- Senza efficienza: sarebbero necessari **12,5 TB** per archiviare 30 giorni di dati del cyber vault.
- Con un'efficienza del 50%: richiederebbe **6,25 TB** di spazio di archiviazione dopo la deduplicazione e la compressione.

Le copie snapshot potrebbero comportare un sovraccarico aggiuntivo dovuto ai metadati, ma solitamente si tratta di un problema di lieve entità.

Se vengono eseguiti più backup al giorno, adattare il calcolo in base al numero di copie Snapshot eseguite ogni giorno.

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

Impatto sulle prestazioni su primario/sorgente

Poiché il trasferimento dei dati è un'operazione pull, l'impatto sulle prestazioni dell'archiviazione primaria può variare a seconda del carico di lavoro, del volume dei dati e della frequenza dei backup. Tuttavia, l'impatto complessivo sulle prestazioni del sistema primario è generalmente moderato e gestibile, poiché il trasferimento dei dati è progettato per scaricare le attività di protezione e backup dei dati sul sistema di archiviazione del cyber vault. Durante la configurazione iniziale della relazione e il primo backup completo, una quantità significativa di dati viene trasferita dal sistema primario al sistema di sicurezza informatica (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 tracciare e trasferire i blocchi che sono stati modificati dall'ultimo backup. Ciò si traduce in un carico di I/O molto più piccolo rispetto alla replica iniziale. Gli aggiornamenti incrementali sono efficienti e hanno un impatto minimo sulle prestazioni dello storage primario. Il processo Vault viene eseguito in background, riducendo così le possibilità di interferenze con i carichi di lavoro di produzione del sistema primario.

- Assicurare che il sistema di archiviazione disponga di risorse sufficienti (CPU, memoria e IOP) per gestire il carico aggiuntivo attenua l'impatto sulle prestazioni.

Configurare, analizzare, cron script

NetApp ha creato un"singolo script scaricabile" e utilizzato per configurare, verificare e pianificare le relazioni del cyber vault.

Cosa fa questo script

- Peering dei cluster

- Peering SVM
- Creazione del volume DP
- Relazione e inizializzazione SnapMirror
- Rafforzare il sistema ONTAP utilizzato per il cyber vault
- Interrompere e riprendere la relazione in base al programma di trasferimento
- Convalidare periodicamente le impostazioni di sicurezza e generare un report che mostri eventuali anomalie

Come usare questo script

"Scarica lo script"e per utilizzare lo script, basta seguire i passaggi seguenti:

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

> Si prega di verificare che tutte le informazioni siano state inserite. Alla prima esecuzione (modalità di configurazione), verranno richieste le credenziali sia per il sistema di produzione sia per il nuovo sistema di cyber vault. Dopodiché, creerà i peering SVM (se non esistenti), i volumi e lo SnapMirror tra il sistema e li inizializzerà.

> La modalità Cron può essere utilizzata per pianificare la sospensione e la ripresa del trasferimento dei dati.

Modalità di funzionamento

Lo script di automazione fornisce 3 modalità di 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 air-gapped.
- Analizza: funzionalità di monitoraggio e reporting automatizzata per inviare informazioni ai gruppi di monitoraggio in caso di anomalie e attività sospette, per garantire che le configurazioni non vengano deviate.
- Cron - Per abilitare l'infrastruttura disconnessa, la modalità cron automatizza la disabilitazione del LIF e mette in pausa 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"
```

Conclusione della soluzione PowerShell per il cyber vault ONTAP

Sfruttando l'air-gapping con le solide metodologie di rafforzamento fornite da ONTAP, NetApp consente di creare un ambiente di storage sicuro e isolato, resiliente alle minacce informatiche in continua evoluzione. Tutto ciò viene realizzato mantenendo l'agilità e l'efficienza dell'infrastruttura di storage esistente. Questo accesso sicuro consente alle aziende di raggiungere i loro rigorosi obiettivi di sicurezza e di operatività con modifiche minime al personale, ai processi e alla struttura tecnologica esistente.

ONTAP Cyber Vault utilizza le funzionalità native di ONTAP , un approccio semplice per una protezione aggiuntiva che consente di creare copie immutabili e indelebili dei dati. L'aggiunta del cyber vault basato su ONTAP di NetApp alla sicurezza complessiva consentirà di:

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

Informazioni sul copyright

Informazioni sul marchio commerciale