Datenschutz mit ONTAP Cyber Vault

NetApp data management solutions

NetApp
January 28, 2026

Inhalt

Datenschutz mit ONTAP Cyber Vault

ONTAP Cyber Vault-Übersicht

Die größte Bedrohung, die die Implementierung eines Cyber-Tresors erforderlich macht, ist die zunehmende Verbreitung und zunehmende Raffinesse von Cyber-Angriffen, insbesondere Ransomware und Datenschutzverletzungen. "Mit einem Anstieg des Phishing" und immer ausgefeiltere Methoden zum Diebstahl von Anmeldeinformationen. Die Anmeldeinformationen, die zum Starten eines Ransomware-Angriffs verwendet werden, könnten dann für den Zugriff auf Infrastruktursysteme verwendet werden. In diesen Fällen besteht selbst bei gehärteten Infrastruktursystemen die Gefahr eines Angriffs. Die einzige Verteidigung gegen ein kompromittiertes System besteht darin, Ihre Daten in einem Cyber-Tresor zu schützen und zu isolieren.

Der ONTAP -basierte Cyber Vault von NetApp bietet Unternehmen eine umfassende und flexible Lösung zum Schutz ihrer wichtigsten Datenbestände. Durch die Nutzung logischer Air-Gapping-Funktionen mit robusten Härtungsmethoden ermöglicht Ihnen ONTAP die Erstellung sicherer, isolierter Speicherumgebungen, die widerstandsfähig gegen sich entwickelnde Cyberbedrohungen sind. Mit ONTAP können Sie die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten sicherstellen und gleichzeitig die Agilität und Effizienz Ihrer Speicherinfrastruktur aufrechterhalten.

Ab Juli 2024 werden Inhalte aus technischen Berichten, die zuvor als PDFs veröffentlicht wurden, in die ONTAP Produktdokumentation integriert. Darüber hinaus erhalten neue technische Berichte (TRs) wie dieses Dokument keine TR-Nummern mehr.

Was ist ein Cyber-Tresor?

Ein Cyber-Tresor ist eine spezielle Datenschutztechnik, bei der kritische Daten in einer isolierten Umgebung, getrennt von der primären IT-Infrastruktur, gespeichert werden.

„Air-gapped“, **unveränderliches** und **unauslöschliches** Daten-Repository, das immun gegen Bedrohungen ist, die das Hauptnetzwerk betreffen, wie etwa Malware, Ransomware oder sogar Insider-Bedrohungen. Ein Cyber-Tresor kann mit **unveränderlichen** und **unauslöschlichen** Snapshots erreicht werden.

Bei Air-Gapping-Backups mit herkömmlichen Methoden müssen Platz geschaffen und das primäre und sekundäre Medium physisch getrennt werden. Durch die Verlagerung der Medien an einen anderen Standort und/oder die Trennung der Verbindung haben böswillige Akteure keinen Zugriff auf die Daten. Dies schützt die Daten, kann jedoch zu längeren Wiederherstellungszeiten führen.

NetApps Ansatz für Cyber Vault

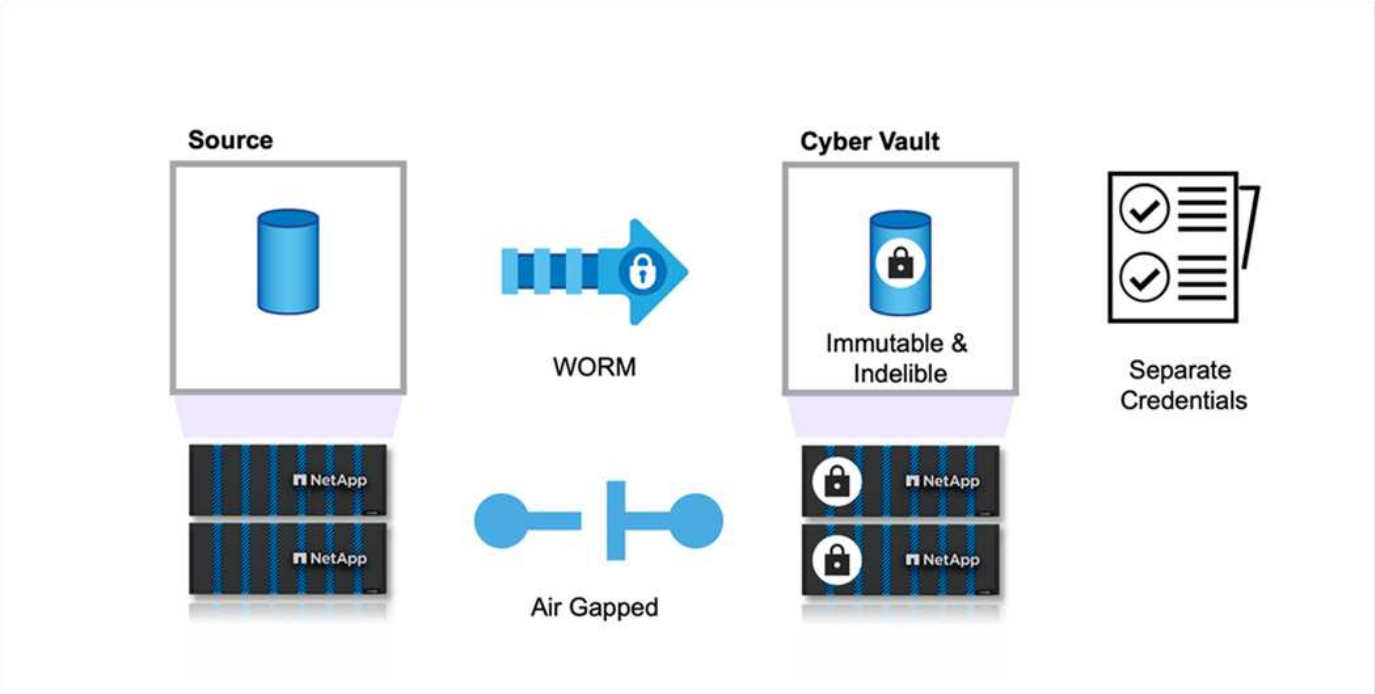
Zu den wichtigsten Funktionen der NetApp Referenzarchitektur für einen Cyber Vault gehören:

- Sichere, isolierte Speicherinfrastruktur (z. B. Air-Gapped-Speichersysteme)
- Kopien der Daten müssen ausnahmslos sowohl **unveränderlich** als auch **unlöschbar** sein
- Strenge Zugriffskontrollen und Multi-Faktor-Authentifizierung
- Schnelle Datenwiederherstellungsfunktionen

Sie können NetApp Storage mit ONTAP als Air-Gap-Cyber-Tresor verwenden, indem Sie"SnapLock

Compliance zum WORM-Schutz von Snapshot-Kopien" . Sie können alle grundlegenden SnapLock Compliance -Aufgaben im Cyber-Tresor ausführen. Nach der Konfiguration werden Cyber Vault-Volumes automatisch geschützt, sodass die Snapshot-Kopien nicht manuell in WORM übertragen werden müssen. Weitere Informationen zum logischen Air-Gapping finden Sie in diesem"Blog"

SnapLock Compliance wird verwendet, um die Bank- und Finanzvorschriften SEC 70-a-4(f), FINRA 4511(c) und CFTC 1.31(c)-(d) einzuhalten. Die Einhaltung dieser Vorschriften wurde von Cohasset Associates zertifiziert (Prüfbericht auf Anfrage erhältlich). Durch die Verwendung von SnapLock Compliance mit dieser Zertifizierung erhalten Sie einen gehärteten Mechanismus zum Air-Gapping Ihrer Daten, auf den sich die größten Finanzinstitute der Welt verlassen, um sowohl die Aufbewahrung als auch den Abruf von Bankunterlagen sicherzustellen.



Cyber Vault ONTAP Terminologie

Dies sind die in Cyber-Vault-Architekturen üblicherweise verwendeten Begriffe.

Autonomous Ransomware Protection (ARP) – Die Funktion Autonomous Ransomware Protection (ARP) nutzt eine Workload-Analyse in NAS-Umgebungen (NFS und SMB), um proaktiv und in Echtzeit abnormale Aktivitäten zu erkennen und davor zu warnen, die auf einen Ransomware-Angriff hindeuten könnten. Bei Verdacht auf einen Angriff erstellt ARP zusätzlich zum bestehenden Schutz durch geplante Snapshot-Kopien auch neue Snapshot-Kopien. Weitere Informationen finden Sie im"ONTAP -Dokumentation zum autonomen Ransomware-Schutz"

Air-Gap (Logisch) - Sie können NetApp Storage mit ONTAP als logischen Air-Gap-Cyber-Vault konfigurieren, indem Sie"SnapLock Compliance zum WORM-Schutz von Snapshot-Kopien"

Air-Gap (physisch) – Ein physisches Air-Gap-System hat keine Netzwerkverbindung. Mithilfe von Bandsicherungen können Sie die Bilder an einen anderen Ort verschieben. Der logische Air-Gap von SnapLock Compliance ist genauso robust wie ein physisches Air-Gap-System.

Bastion-Host – Ein dedizierter Computer in einem isolierten Netzwerk, der so konfiguriert ist, dass er Angriffen standhält.

Unveränderliche Snapshot-Kopien – Snapshot-Kopien, die ausnahmslos nicht geändert werden können (einschließlich einer Supportorganisation oder der Möglichkeit, das Speichersystem auf niedriger Ebene zu formatieren).

Unlöschbare Snapshot-Kopien – Snapshot-Kopien, die ausnahmslos nicht gelöscht werden können (einschließlich einer Supportorganisation oder der Möglichkeit, das Speichersystem auf niedriger Ebene zu formatieren).

Manipulationssichere Snapshot-Kopien – Manipulationssichere Snapshot-Kopien verwenden die SnapLock Compliance Clock-Funktion, um Snapshot-Kopien für einen bestimmten Zeitraum zu sperren. Diese gesperrten Snapshots können von keinem Benutzer oder NetApp Support gelöscht werden. Sie können gesperrte Snapshot-Kopien verwenden, um Daten wiederherzustellen, wenn ein Volume durch einen Ransomware-Angriff, Malware, Hacker, einen betrügerischen Administrator oder eine versehentliche Löschung kompromittiert wurde. Weitere Informationen finden Sie im"ONTAP -Dokumentation zu manipulationssicheren Snapshot-Kopien"

- SnapLock* – SnapLock ist eine leistungsstarke Compliance-Lösung für Organisationen, die WORM-Speicher verwenden, um Dateien aus regulatorischen und Governance-Gründen in unveränderter Form aufzubewahren. Weitere Informationen finden Sie im "ONTAP -Dokumentation zu SnapLock" .
- SnapMirror* – SnapMirror ist eine Replikationstechnologie zur Notfallwiederherstellung, die für die effiziente Replikation von Daten entwickelt wurde. SnapMirror kann einen Spiegel (oder eine exakte Kopie der Daten), einen Tresor (eine Kopie der Daten mit längerer Aufbewahrung der Snapshot-Kopie) oder beides auf einem sekundären System vor Ort oder in der Cloud erstellen. Diese Kopien können für viele verschiedene Zwecke verwendet werden, beispielsweise im Katastrophenfall, zum Burst in die Cloud oder in einen Cyber-Tresor (bei Verwendung der Tresorrichtlinie und Sperren des Tresors). Weitere Informationen finden Sie im"ONTAP -Dokumentation zu SnapMirror"
- SnapVault* – In ONTAP 9.3 wurde SnapVault zugunsten der Konfiguration von SnapMirror mithilfe der Vault- oder Mirror-Vault-Richtlinie verworfen. Dieser Begriff wird zwar noch verwendet, hat aber ebenfalls an Bedeutung verloren. Weitere Informationen finden Sie im "ONTAP -Dokumentation zu SnapVault" .

Cyber Vault-Dimensionierung mit ONTAP

Um die Größe eines Cyber-Tresors zu bestimmen, müssen Sie wissen, wie viele Daten innerhalb einer bestimmten Recovery Time Objective (RTO) wiederhergestellt werden müssen. Bei der Entwicklung einer Cyber-Vault-Lösung in der richtigen Größe spielen viele Faktoren eine Rolle. Bei der Dimensionierung eines Cyber-Tresors müssen sowohl Leistung als auch Kapazität berücksichtigt werden.

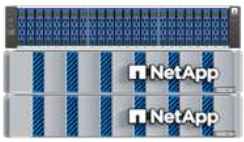
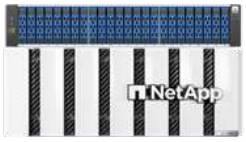
Überlegungen zur Leistungsdimensionierung

1. Was sind die Quellplattformmodelle (FAS v AFF A-Serie v AFF C-Serie)?
2. Wie hoch sind Bandbreite und Latenz zwischen Quelle und Cyber-Tresor?
3. Wie groß sind die Dateigrößen und wie viele Dateien?
4. Was ist Ihr Ziel für die Wiederherstellungszeit?
5. Wie viele Daten müssen innerhalb der RTO wiederhergestellt werden?
6. Wie viele SnapMirror Fan-In-Beziehungen wird der Cyber-Tresor aufnehmen?
7. Wird es eine oder mehrere Wiederherstellungen gleichzeitig geben?
8. Werden diese mehrfachen Wiederherstellungen bei derselben Primärquelle erfolgen?

9. Wird SnapMirror während einer Wiederherstellung aus einem Tresor eine Replikation in den Tresor durchführen?

Größenbeispiele

Hier sind Beispiele für verschiedene Cyber-Vault-Konfigurationen.

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

Überlegungen zur Kapazitätsdimensionierung

Die Menge an Speicherplatz, die für ein ONTAP Cyber Vault-Zielvolume erforderlich ist, hängt von einer Reihe von Faktoren ab. Der wichtigste davon ist die Änderungsrate der Daten im Quellvolume. Sowohl der Sicherungszeitplan als auch der Snapshot-Zeitplan auf dem Zielvolume wirken sich auf die Datenträgernutzung auf dem Zielvolume aus, und die Änderungsrate auf dem Quellvolume ist wahrscheinlich nicht konstant. Es empfiehlt sich, einen Puffer an zusätzlicher Speicherkapazität bereitzustellen, der über den erforderlichen Wert hinausgeht, um zukünftigen Änderungen im Endbenutzer- oder Anwendungsverhalten Rechnung zu tragen.

Um die Größe einer Beziehung für eine einmonatige Aufbewahrung in ONTAP festzulegen, müssen die Speicheranforderungen anhand mehrerer Faktoren berechnet werden, darunter die Größe des primären Datensatzes, die Datenänderungsrate (tägliche Änderungsrate) und die Einsparungen durch Deduplizierung und Komprimierung (falls zutreffend).

Hier ist die schrittweise Vorgehensweise:

Der erste Schritt besteht darin, die Größe des/der Quellvolumes/-volumes zu kennen, das/die Sie mit dem Cyber Vault schützen. Dies ist die Basisdatenmenge, die zunächst zum Cyber-Vault-Ziel repliziert wird. Schätzen Sie als Nächstes die tägliche Änderungsrate für den Datensatz. Dies ist der Prozentsatz der Daten, der sich täglich ändert. Es ist entscheidend, ein gutes Verständnis dafür zu haben, wie dynamisch Ihre Daten sind.

Beispiel:

- Größe des primären Datensatzes = 5 TB
- Tägliche Änderungsrate = 5 % (0,05)
- Deduplizierungs- und Komprimierungseffizienz = 50 % (0,50)

Lassen Sie uns nun die Berechnung durchgehen:

- Berechnen Sie die tägliche Datenänderungsrate:

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

- Berechnen Sie die gesamten geänderten Daten für 30 Tage:

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

- Berechnen Sie den insgesamt erforderlichen Speicher:

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

- Einsparungen durch Deduplizierung und Komprimierung anwenden:

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

Zusammenfassung des Speicherbedarfs

- Ohne Effizienz: Es wären **12,5 TB** erforderlich, um 30 Tage der Cyber-Vault-Daten zu speichern.
- Bei 50 % Effizienz: Nach Deduplizierung und Komprimierung wären **6,25 TB** Speicherplatz erforderlich.

Snapshot-Kopien können aufgrund von Metadaten zusätzlichen Aufwand verursachen, dieser ist jedoch normalerweise geringfügig.

Wenn mehrere Sicherungen pro Tag durchgeführt werden, passen Sie die Berechnung an die Anzahl der täglich erstellten Snapshot-Kopien an.

Berücksichtigen Sie das Datenwachstum im Laufe der Zeit, um sicherzustellen, dass die Dimensionierung zukunftssicher ist.

Erstellen eines Cyber-Tresors mit ONTAP

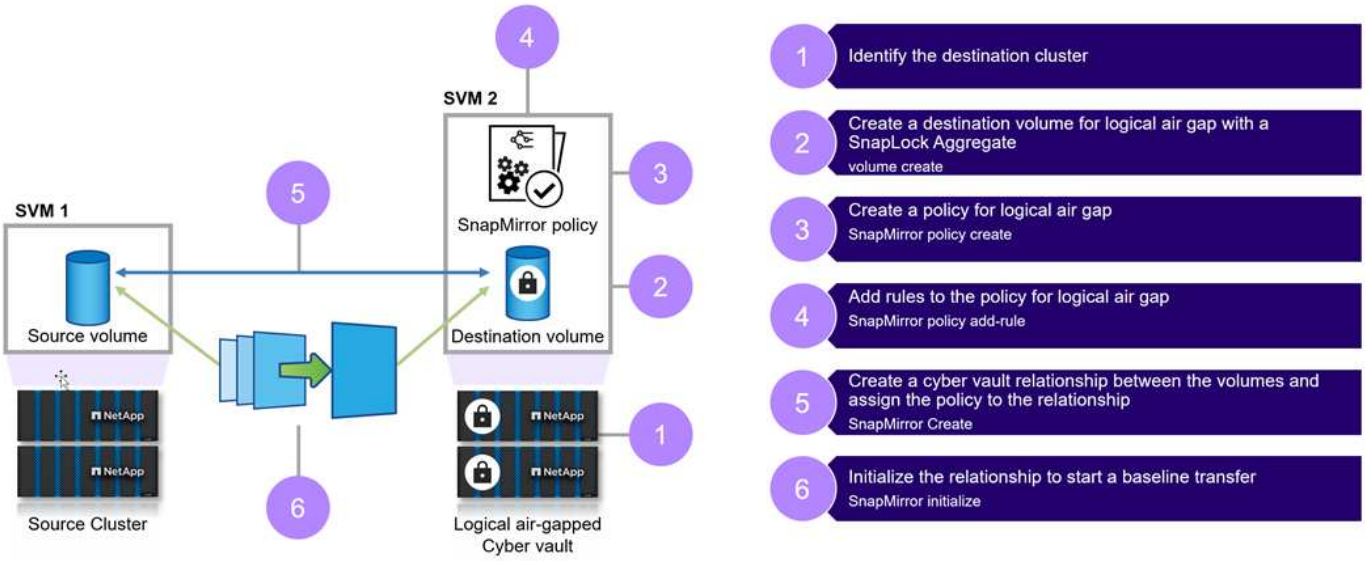
Die folgenden Schritte helfen bei der Erstellung eines Cyber-Tresors mit ONTAP.

Bevor Sie beginnen

- Auf dem Quellcluster muss ONTAP 9 oder höher ausgeführt werden.
- Die Quell- und Zielaggregate müssen 64-Bit sein.
- Die Quell- und Zielvolumes müssen in Peering-Clustern mit Peering-SVMs erstellt werden. Weitere Informationen finden Sie unter "Cluster-Peering" .
- Wenn die automatische Volumevergrößerung deaktiviert ist, muss der freie Speicherplatz auf dem Zielvolume mindestens fünf Prozent größer sein als der verwendete Speicherplatz auf dem Quellvolume.

Informationen zu diesem Vorgang

Die folgende Abbildung zeigt das Verfahren zum Initialisieren einer SnapLock Compliance Vault-Beziehung:



Schritte

1. Identifizieren Sie das Ziel-Array, das zum Cyber-Tresor für den Empfang der Air-Gap-Daten werden soll.
2. Um den Cyber-Tresor auf dem Ziel-Array vorzubereiten,"Installieren Sie die ONTAP One-Lizenz" ,"Initialisieren Sie die Compliance Clock" , und wenn Sie eine ONTAP Version vor 9.10.1 verwenden,"Erstellen Sie ein SnapLock Compliance -Aggregat" .
3. Erstellen Sie auf dem Ziel-Array ein SnapLock Compliance -Zielvolume vom Typ DP:

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

4. Ab ONTAP 9.10.1 können SnapLock und Nicht- SnapLock -Volumes auf demselben Aggregat vorhanden sein. Daher müssen Sie bei Verwendung von ONTAP 9.10.1 kein separates SnapLock -Aggregat mehr erstellen. Sie verwenden die Lautstärke `-snaplock-type` Option zum Angeben eines Compliance-Typs. In ONTAP Versionen vor ONTAP 9.10.1 wird der SnapLock -Modus „Compliance“ vom Aggregat übernommen. Versionsflexible Zielvolumes werden nicht unterstützt. Die Spracheinstellung des Zielvolumes muss mit der Spracheinstellung des Quellvolumes übereinstimmen.

   Der folgende Befehl erstellt ein 2 GB SnapLock Compliance Volume mit dem Namen `dstvolB` In `SVM2` auf das Aggregat `node01_aggr` :

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

5. Um den Air-Gap zu erstellen, legen Sie im Zielcluster die Standardaufbewahrungsdauer fest, wie in"Festlegen der Standardaufbewahrungsdauer" . Einem SnapLock -Volume, das ein Tresorziel ist, ist eine Standardaufbewahrungsdauer zugewiesen. Der Wert für diesen Zeitraum ist zunächst auf mindestens 0 Jahre und höchstens 100 Jahre eingestellt (ab ONTAP 9.10.1). Bei früheren ONTAP Versionen liegt der Wert zwischen 0 und 70.) für SnapLock Compliance Volumes. Jede NetApp Snapshot-Kopie wird zunächst mit dieser Standardaufbewahrungsdauer festgeschrieben. Die Standardaufbewahrungsdauer muss geändert werden. Die Aufbewahrungsfrist kann bei Bedarf später verlängert, jedoch nie verkürzt werden. Weitere Informationen finden Sie unter "Übersicht über die eingestellte Aufbewahrungsdauer" .

Dienstanbieter sollten bei der Festlegung der Aufbewahrungsfrist das Vertragsende des Kunden berücksichtigen. Wenn beispielsweise die Aufbewahrungsfrist für den Cyber-Tresor 30 Tage beträgt und der Vertrag des Kunden vor Ablauf der Aufbewahrungsfrist endet, können die Daten im Cyber-Tresor erst nach Ablauf der Aufbewahrungsfrist gelöscht werden.

6. "Erstellen einer neuen Replikationsbeziehung"zwischen der Nicht- SnapLock -Quelle und dem neuen SnapLock Ziel, das Sie in Schritt 3 erstellt haben.

   In diesem Beispiel wird eine neue SnapMirror -Beziehung mit dem SnapLock Zielvolume „dstvolB“ erstellt. Dabei wird die Richtlinie „XDPDefault“ verwendet, um Snapshot-Kopien mit täglichen und wöchentlichen Bezeichnungen stündlich zu speichern:

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

   "Erstellen einer benutzerdefinierten Replikationsrichtlinie"oder ein"benutzerdefinierter Zeitplan" wenn die verfügbaren Voreinstellungen nicht geeignet sind.

7. Initialisieren Sie auf der Ziel-SVM die in Schritt 5 erstellte SnapVault -Beziehung:

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

8. Der folgende Befehl initialisiert die Beziehung zwischen dem Quellvolume srcvolA auf SVM1 und dem Zielvolume dstvolB auf SVM2:

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

9. Nachdem die Beziehung initialisiert und im Leerlauf ist, verwenden Sie den Befehl „Snapshot Show“ am Ziel, um die auf die replizierten Snapshot-Kopien angewendete SnapLock -Ablaufzeit zu überprüfen.

   In diesem Beispiel werden die Snapshot-Kopien auf dem Volume „dstvolB“ aufgelistet, die über die Bezeichnung „SnapMirror“ und das Ablaufdatum „SnapLock“ verfügen:

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

Cyber-Tresor-Härtung

Dies sind die zusätzlichen Empfehlungen zum Härten eines ONTAP Cyber Vault. Weitere Empfehlungen und Vorgehensweisen finden Sie im ONTAP Härtungshandbuch weiter unten.

Empfehlungen zur Cyber-Tresorhärtung

- Isolieren Sie die Verwaltungsebenen des Cyber-Tresors
- Aktivieren Sie keine Daten-LIFs auf dem Zielcluster, da diese einen zusätzlichen Angriffsvektor darstellen.
- Beschränken Sie auf dem Zielcluster den Intercluster-LIF-Zugriff auf den Quellcluster mit einer Servicerichtlinie.
- Segmentieren Sie das Management-LIF auf dem Zielcluster für eingeschränkten Zugriff mit einer

Servicerichtlinie und einem Bastion-Host

- Beschränken Sie den gesamten Datenverkehr vom Quellcluster zum Cyber Vault, um nur die für den SnapMirror Verkehr erforderlichen Ports zuzulassen
- Deaktivieren Sie nach Möglichkeit alle nicht benötigten Verwaltungszugriffsmethoden innerhalb von ONTAP , um die Angriffsfläche zu verringern.
- Aktivieren Sie die Überwachungsprotokollierung und die Remote-Protokollspeicherung
- Aktivieren Sie die Multi-Admin-Verifizierung und verlangen Sie die Verifizierung durch einen Administrator außerhalb Ihrer regulären Speicheradministratoren (z. B. CISO-Mitarbeiter).
- Implementieren Sie rollenbasierte Zugriffskontrollen
- Administrative Multifaktor-Authentifizierung für System Manager und SSH erforderlich
- Verwenden Sie die tokenbasierte Authentifizierung für Skripte und REST-API-Aufrufe

Bitte beachten Sie die"ONTAP -Härtungshandbuch" ,"Übersicht über die Multi-Admin-Verifizierung" Und"ONTAP Multifaktor-Authentifizierungshandbuch" Informationen zum Durchführen dieser Härtungsschritte.

Cyber-Tresor-Interoperabilität

Mit ONTAP -Hardware und -Software kann eine Cyber-Vault-Konfiguration erstellt werden.

ONTAP Hardware-Empfehlungen

Alle einheitlichen physischen Arrays von ONTAP können für eine Cyber-Vault-Implementierung verwendet werden.

- FAS Hybridspeicher bietet die kosteneffizienteste Lösung.
- Die AFF C-Serie bietet den effizientesten Stromverbrauch und die höchste Dichte.
- Die AFF A-Serie ist die leistungsstärkste Plattform mit der besten RTO. Mit der kürzlichen Ankündigung unserer neuesten AFF A-Serie bietet diese Plattform die beste Speichereffizienz ohne Leistungseinbußen.

ONTAP Softwareempfehlungen

Ab ONTAP 9.14.1 können Sie Aufbewahrungszeiträume für bestimmte SnapMirror Labels in der SnapMirror Richtlinie der SnapMirror Beziehung angeben, sodass die replizierten Snapshot-Kopien vom Quell- zum Zielvolume für den in der Regel angegebenen Aufbewahrungszeitraum aufbewahrt werden. Wenn keine Aufbewahrungsdauer angegeben ist, wird die Standardaufbewahrungsdauer des Zielvolumes verwendet.

Ab ONTAP 9.13.1 können Sie eine gesperrte Snapshot-Kopie auf dem Ziel SnapLock Volume einer SnapLock Vault-Beziehung sofort wiederherstellen, indem Sie einen FlexClone mit der Snaplock-Typ-Option „Nicht-Snaplock“ erstellen und die Snapshot-Kopie beim Ausführen des Vorgangs zum Erstellen des Volume-Klons als „übergeordneten Snapshot“ angeben. Erfahren Sie mehr über "Erstellen eines FlexClone -Volumes mit einem SnapLock -Typ" .

MetroCluster -Konfiguration

Bei MetroCluster -Konfigurationen sollten Sie Folgendes beachten:

- Sie können eine SnapVault Beziehung nur zwischen Synchronisierungsquellen-SVMs erstellen, nicht zwischen einer Synchronisierungsquellen-SVM und einer Synchronisierungsziel-SVM.

- Sie können eine SnapVault Beziehung von einem Volume auf einem SVM mit Synchronisierungsquelle zu einem SVM zur Datenbereitstellung erstellen.
- Sie können eine SnapVault Beziehung von einem Volume auf einem Daten bereitstellenden SVM zu einem DP-Volume auf einem Synchronisierungsquellen-SVM erstellen.

Häufig gestellte Fragen zum Cyber-Tresor

Diese FAQ richten sich an Kunden und Partner von NetApp . Es beantwortet häufig gestellte Fragen zur ONTAP -basierten Cyber Vault-Referenzarchitektur von NetApp.

Was ist ein NetApp Cyber Vault?

Cyber Vault ist eine spezielle Datenschutztechnik, bei der Daten in einer isolierten Umgebung gespeichert werden, getrennt von der primären IT-Infrastruktur.

Cyber Vault ist ein „luftgekapselter“, unveränderlicher und unauslöschlicher Datenspeicher, der immun gegen Bedrohungen ist, die die Primärdaten beeinträchtigen, wie etwa Malware, Ransomware oder Insider-Bedrohungen. Ein Cyber-Tresor kann mit unveränderlichen NetApp ONTAP Snapshot-Kopien erstellt und mit NetApp SnapLock Compliance unlöschbar gemacht werden. Während des SnapLock Compliance Schutzes können Daten weder geändert noch gelöscht werden, nicht einmal von ONTAP Administratoren oder dem NetApp Support.

Bei Air-Gapping-Backups mit herkömmlichen Methoden müssen Platz geschaffen und das primäre und sekundäre Medium physisch getrennt werden. Beim Air-Gapping mit Cyber Vault wird ein separates Datenreplikationsnetzwerk außerhalb der Standard-Datenzugriffsnetzwerke verwendet, um Snapshot-Kopien an einem unlöschbaren Ziel zu replizieren.

Weitere Schritte über Air-Gapped-Netzwerke hinaus umfassen das Deaktivieren aller Datenzugriffs- und Replikationsprotokolle im Cyber-Tresor, wenn sie nicht benötigt werden. Dies verhindert den Datenzugriff oder die Datenexfiltration am Zielstandort. Mit SnapLock Compliance ist keine physische Trennung erforderlich. SnapLock Compliance schützt Ihre im Tresor gespeicherten, zeitpunktbezogenen, schreibgeschützten Snapshot-Kopien und ermöglicht so eine schnelle Datenwiederherstellung, die vor Löschung geschützt und unveränderlich ist.

NetApps Ansatz für Cyber Vault

NetApp Cyber Vault, unterstützt durch SnapLock, bietet Unternehmen eine umfassende und flexible Lösung zum Schutz ihrer wichtigsten Datenbestände. Durch die Nutzung der Härtungstechnologien in ONTAP ermöglicht NetApp Ihnen die Erstellung eines sicheren, luftgekapselten und isolierten Cyber-Tresors, der immun gegen sich entwickelnde Cyber-Bedrohungen ist. Mit NetApp können Sie die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten sicherstellen und gleichzeitig die Agilität und Effizienz Ihrer Speicherinfrastruktur aufrechterhalten.

Zu den wichtigsten Funktionen der NetApp Referenzarchitektur für einen Cyber Vault gehören:

- Sichere, isolierte Speicherinfrastruktur (z. B. Air-Gapped-Speichersysteme)
- Sicherungskopien Ihrer Daten sind unveränderlich und unlöschbar
- Strenge und separate Zugriffskontrollen, Multi-Administrator-Verifizierung und Multi-Faktor-Authentifizierung
- Schnelle Datenwiederherstellungsfunktionen

Häufig gestellte Fragen zum Cyber-Tresor

Ist Cyber Vault ein Produkt von NetApp?

Nein, „Cyber Vault“ ist ein branchenweiter Begriff. NetApp hat eine Referenzarchitektur erstellt, die es Kunden erleichtert, ihre eigenen Cyber-Tresore aufzubauen und die Dutzenden von ONTAP Sicherheitsfunktionen zu nutzen, um ihre Daten vor Cyber-Bedrohungen zu schützen. Weitere Informationen finden Sie auf der"ONTAP -Dokumentationssite" .

Ist Cyber Vault mit NetApp nur ein anderer Name für LockVault oder SnapVault?

LockVault war eine Funktion des Data ONTAP 7-Modus, die in den aktuellen Versionen von ONTAP nicht verfügbar ist.

SnapVault war ein veralteter Begriff für das, was jetzt mit der Tresorrichtlinie von SnapMirror erreicht wird. Diese Richtlinie ermöglicht es dem Ziel, eine andere Anzahl von Snapshot-Kopien aufzubewahren als das Quellvolume.

Cyber Vault verwendet SnapMirror zusammen mit der Vault-Richtlinie und SnapLock Compliance, um eine unveränderliche und unauslöschliche Kopie der Daten zu erstellen.

Welche NetApp -Hardware kann ich für einen Cyber Vault, FAS, Capacity Flash oder Performance Flash verwenden?

Diese Referenzarchitektur für Cyber Vaulting gilt für das gesamte ONTAP Hardwareportfolio. Kunden können Plattformen der AFF A-Serie, AFF C-Serie oder FAS als Tresor verwenden. Flash-basierte Plattformen bieten die schnellsten Wiederherstellungszeiten, während festplattenbasierte Plattformen die kostengünstigste Lösung darstellen. Je nachdem, wie viele Daten wiederhergestellt werden und ob mehrere Wiederherstellungen parallel erfolgen, kann die Verwendung von festplattenbasierten Systemen (FAS) Tage bis Wochen dauern. Bitte wenden Sie sich an einen Vertreter von NetApp oder einem Partner, um die richtige Größe für eine Cyber-Vault-Lösung zu finden, die Ihren Geschäftsanforderungen entspricht.

Kann ich Cloud Volumes ONTAP als Cyber-Vault-Quelle verwenden?

Ja, allerdings erfordert die Verwendung von CVO als Quelle, dass die Daten an ein lokales Cyber-Vault-Ziel repliziert werden, da SnapLock Compliance eine Voraussetzung für ein ONTAP Cyber-Vault ist. Für die Datenreplikation von einer auf Hyperscaler basierenden CVO-Instanz können Ausgangsgebühren anfallen.

Kann ich Cloud Volumes ONTAP als Cyber-Vault-Ziel verwenden?

Die Cyber Vault-Architektur basiert auf der Unauslöschlichkeit der SnapLock Compliance von ONTAP und ist für On-Premise-Implementierungen konzipiert. Cloudbasierte Cyber-Vault-Architekturen werden für eine zukünftige Veröffentlichung untersucht.

Kann ich ONTAP Select als Cyber-Vault-Quelle verwenden?

Ja, ONTAP Select kann als Quelle für ein hardwarebasiertes Cyber-Vault-Ziel vor Ort verwendet werden.

Kann ich ONTAP Select als Cyber-Vault-Ziel verwenden?

Nein, ONTAP Select sollte nicht als Cyber-Vault-Ziel verwendet werden, da es nicht über die Möglichkeit verfügt, SnapLock Compliance zu verwenden.

Verwendet ein Cyber-Tresor mit NetApp nur SnapMirror?

Nein, eine NetApp Cyber Vault-Architektur nutzt viele ONTAP Funktionen, um eine sichere, isolierte, luftgekapselte und gehärtete Kopie der Daten zu erstellen. Weitere Informationen dazu, welche zusätzlichen technischen Möglichkeiten genutzt werden können, finden Sie in der nächsten Frage.

Gibt es andere Technologien oder Konfigurationen, die für Cyber Vault verwendet werden?

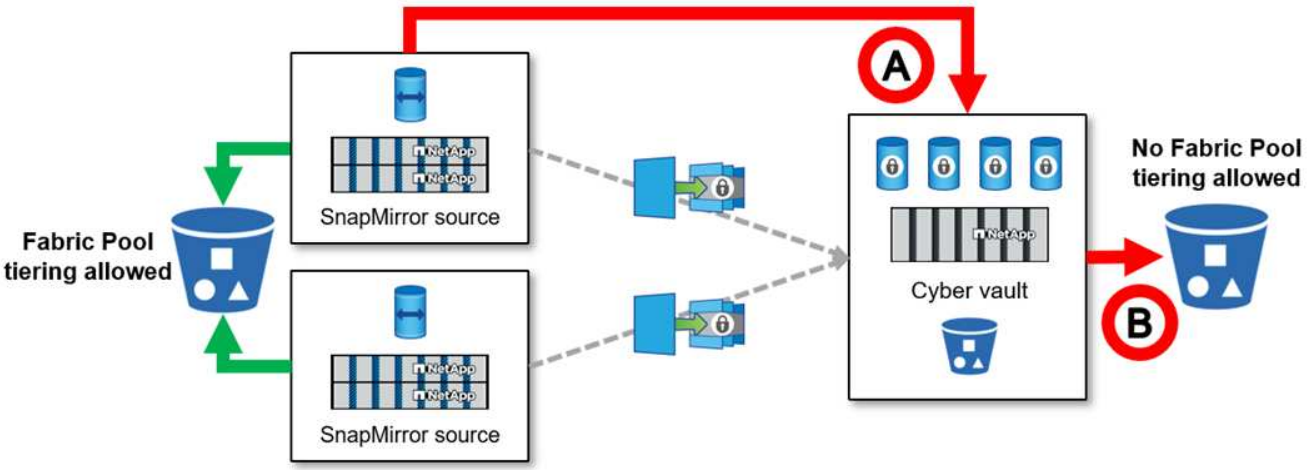
Die Grundlage eines NetApp Cyber Vaults ist SnapMirror und SnapLock Compliance , aber die Verwendung zusätzlicher ONTAP -Funktionen wie manipulationssichere Snapshot-Kopien, Multi-Faktor-Authentifizierung (MFA), Multi Admin Verify, rollenbasierte Zugriffskontrolle sowie Remote- und lokale Audit-Protokollierung verbessert die Sicherheit Ihrer Daten.

Warum sind ONTAP Snapshot-Kopien für einen Cyber-Tresor besser geeignet als andere?

ONTAP Snapshot-Kopien sind standardmäßig unveränderlich und können mit SnapLock Compliance unlöschbar gemacht werden. Nicht einmal der NetApp Support kann die SnapLock -Snapshot-Kopien löschen. Die bessere Frage ist, was NetApp Cyber Vault besser macht als andere Cyber Vaults in der Branche. Erstens ist ONTAP der sicherste Speicher der Welt und verfügt über die CSfC-Validierung, die die Speicherung geheimer und streng geheimer Daten im Ruhezustand sowohl auf Hardware- als auch auf Softwareebene ermöglicht. Weitere Informationen zu"CSfC finden Sie hier" . Darüber hinaus kann ONTAP auf der Speicherebene mit einem Air Gap versehen werden, wobei das Cyber Vault-System die Replikation steuert und so innerhalb des Cyber Vault-Netzwerks ein Air Gap erstellt werden kann.

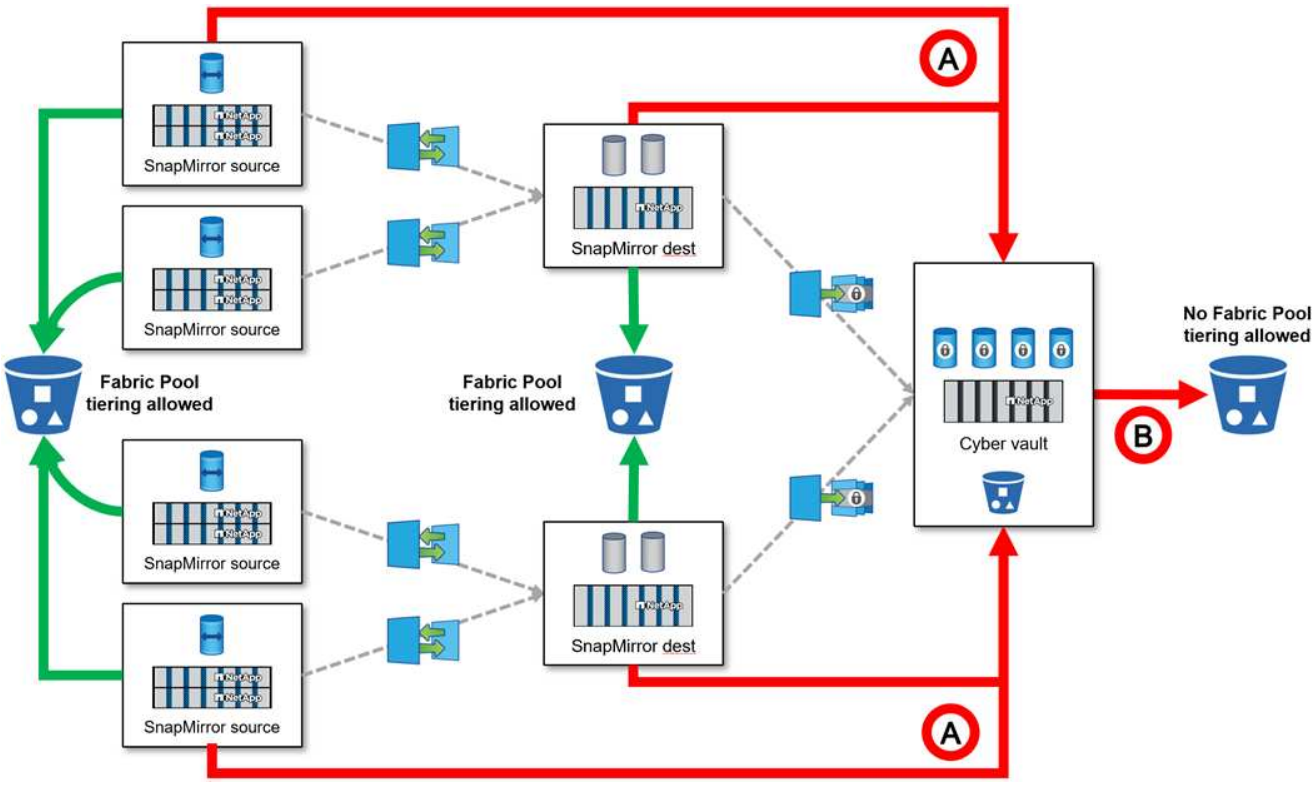
Kann ein Volume in einem Cyber Vault den ONTAP Fabric Pool verwenden?

Nein, ein Cyber-Vault-Volume (SnapLock Compliance SnapMirror Ziel) kann unabhängig von der Richtlinie nicht mithilfe von Fabric Pool abgestuft werden.



Es gibt mehrere Szenarien, in denen Fabric Pool **nicht** mit einem Cyber Vault verwendet werden kann.

1. Fabric Pool Cold Tiers **können** keinen Cyber Vault-Cluster verwenden. Dies liegt daran, dass durch die Aktivierung des S3-Protokolls die Sicherheit der Cyber-Vault-Referenzarchitektur aufgehoben wird. Darüber hinaus kann der für den Fabric-Pool verwendete S3-Bucket nicht geschützt werden.
2. SnapLock Compliance Volumes im Cyber-Vault **können** nicht auf einen S3-Bucket gestaffelt werden, da die Daten im Volume gesperrt sind.



Ist ONTAP S3 Worm in einem Cyber Vault verfügbar?

Nein, S3 ist ein Datenzugriffsprotokoll, das die Sicherheit der Referenzarchitektur außer Kraft setzt.

Läuft NetApp Cyber Vault auf einer anderen ONTAP Persönlichkeit oder einem anderen ONTAP-Profil?

Nein, es ist eine Referenzarchitektur. Kunden können die"Referenzarchitektur" und bauen Sie einen Cyber-Tresor, oder können die"PowerShell-Skripte zum Erstellen, Härten und Validieren" ein Cyber-Tresor.

Kann ich Datenprotokolle wie NFS, SMB und S3 in einem Cyber Vault aktivieren?

Standardmäßig sollten Datenprotokolle im Cyber-Tresor deaktiviert sein, um ihn zu sichern. Allerdings können Datenprotokolle im Cyber-Tresor aktiviert werden, um zur Wiederherstellung oder bei Bedarf auf die Daten zuzugreifen. Dies sollte vorübergehend erfolgen und nach Abschluss der Wiederherstellung deaktiviert werden.

Können Sie eine vorhandene SnapVault Umgebung in einen Cyber-Tresor umwandeln oder müssen Sie alles neu einrichten?

Ja. Man könnte ein System nehmen, das ein SnapMirror -Ziel ist (mit Tresorrichtlinie), die Datenprotokolle deaktivieren, das System gemäß den"ONTAP -Härtungshandbuch" , isolieren Sie es an einem sicheren Ort und befolgen Sie die anderen Verfahren in der Referenzarchitektur, um es zu einem Cyber-Tresor zu machen, ohne das Ziel erneut festlegen zu müssen.

Haben Sie weitere Fragen? Senden Sie Ihre Fragen bitte per E-Mail an ng-cyber-vault@netapp.com! Wir werden antworten und Ihre Fragen zu den FAQ hinzufügen.

Cyber-Tresor-Ressourcen

Weitere Informationen zu den in diesen Cyber-Tresor-Informationen beschriebenen Informationen finden Sie in den folgenden zusätzlichen Informationen und Sicherheitskonzepten.

- "NetApp Cyber Vault: Kurzbeschreibung mehrschichtiger Datenschutzlösungen"
- "NetApp erhält AAA-Bewertung für die branchenweit erste KI-gesteuerte On-Box-Lösung zur Ransomware-Erkennung"
- "Erhöhen Sie Ihre Cyber-Resilienz mit dem sichersten Speicher der Welt"
- "Leitfaden zur ONTAP -Sicherheitshärtung"
- "NetApp Zero Trust"
- "NetApp Cyber-Resilienz"
- "NetApp Datenschutz"
- "Übersicht über Cluster- und SVM-Peering mit der CLI"
- "SnapVault -Archivierung"

- "Konfigurieren, Analysieren, Cron-Skript"

Erstellen, Härten und Validieren eines ONTAP Cyber Vault mit PowerShell

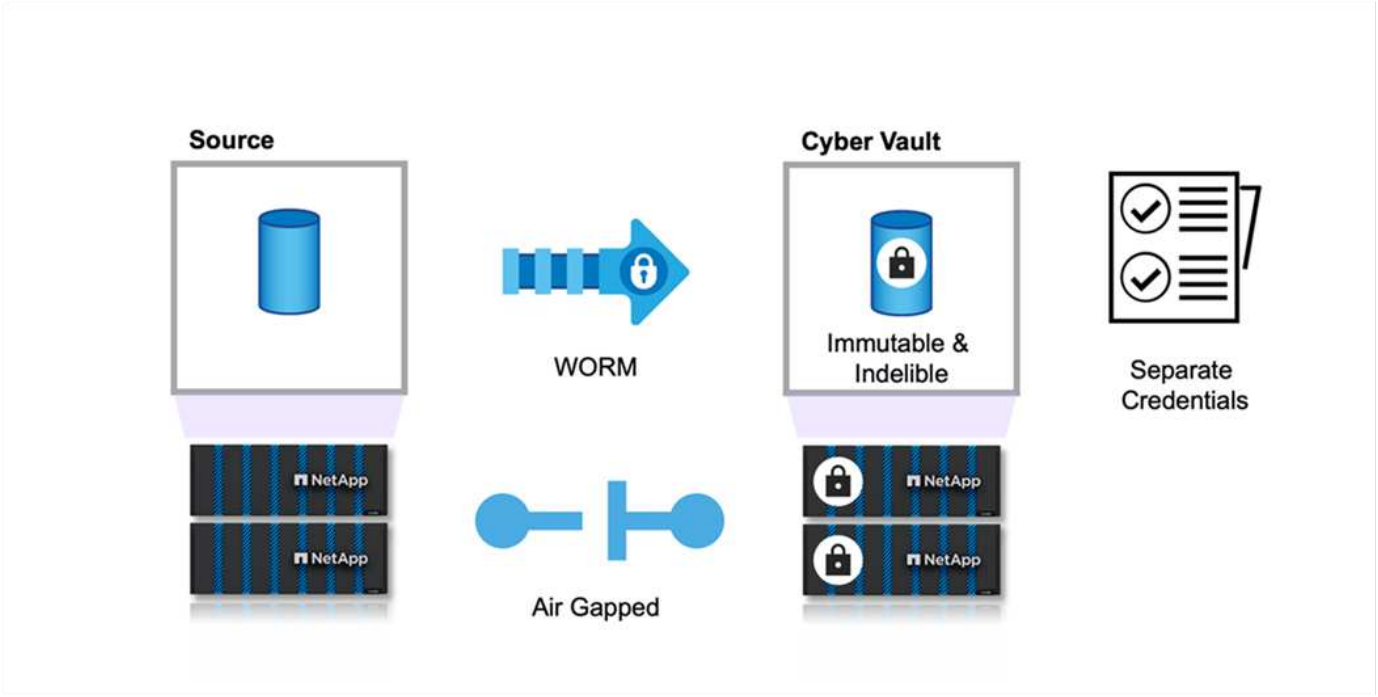
Übersicht über ONTAP Cyber Vault mit PowerShell

In der heutigen digitalen Landschaft ist der Schutz der kritischen Datenbestände eines Unternehmens nicht nur eine bewährte Methode, sondern eine geschäftliche Notwendigkeit. Cyberbedrohungen entwickeln sich in beispiellosem Tempo und herkömmliche Datenschutzmaßnahmen reichen nicht mehr aus, um vertrauliche Informationen zu schützen. Hier kommt ein Cyber-Tresor ins Spiel. Die hochmoderne ONTAP -basierte Lösung von NetApp kombiniert fortschrittliche Air-Gapping-Techniken mit robusten Datenschutzmaßnahmen, um eine undurchdringliche Barriere gegen Cyber-Bedrohungen zu schaffen. Durch die Isolierung der wertvollsten Daten mithilfe sicherer Härtungstechnologie minimiert ein Cyber-Tresor die Angriffsfläche, sodass die wichtigsten Daten vertraulich, intakt und bei Bedarf sofort verfügbar bleiben.

Ein Cyber-Tresor ist eine sichere Speichereinrichtung, die aus mehreren Schutzebenen besteht, beispielsweise Firewalls, Netzwerken und Speicher. Diese Komponenten schützen wichtige Wiederherstellungsdaten, die für wichtige Geschäftsvorgänge erforderlich sind. Die Komponenten des Cyber-Tresors werden gemäß der Tresorrichtlinie regelmäßig mit den wesentlichen Produktionsdaten synchronisiert, bleiben ansonsten jedoch unzugänglich. Diese isolierte und getrennte Einrichtung stellt sicher, dass im Falle eines Cyberangriffs, der die Produktionsumgebung gefährdet, eine zuverlässige und endgültige Wiederherstellung problemlos aus dem Cyber-Tresor durchgeführt werden kann.

NetApp ermöglicht die einfache Erstellung eines Air Gap für Cyber Vault durch Konfiguration des Netzwerks, Deaktivierung von LIFs, Aktualisierung der Firewall-Regeln und Isolierung des Systems von externen Netzwerken und dem Internet. Dieser robuste Ansatz trennt das System effektiv von externen Netzwerken und dem Internet und bietet so einen beispiellosen Schutz vor Cyberangriffen aus der Ferne und unbefugten Zugriffsversuchen, wodurch das System immun gegen netzwerkbasierte Bedrohungen und Eindringlinge wird.

In Kombination mit dem SnapLock Compliance Schutz können Daten nicht geändert oder gelöscht werden, nicht einmal von ONTAP Administratoren oder dem NetApp Support. SnapLock wird regelmäßig auf die Einhaltung der SEC- und FINRA-Vorschriften geprüft, um sicherzustellen, dass die Datenausfallsicherheit diesen strengen WORM- und Datenaufbewahrungsvorschriften der Bankenbranche entspricht. NetApp ist der einzige Enterprise-Speicher, der von der NSA CSfC für die Speicherung streng geheimer Daten validiert wurde.



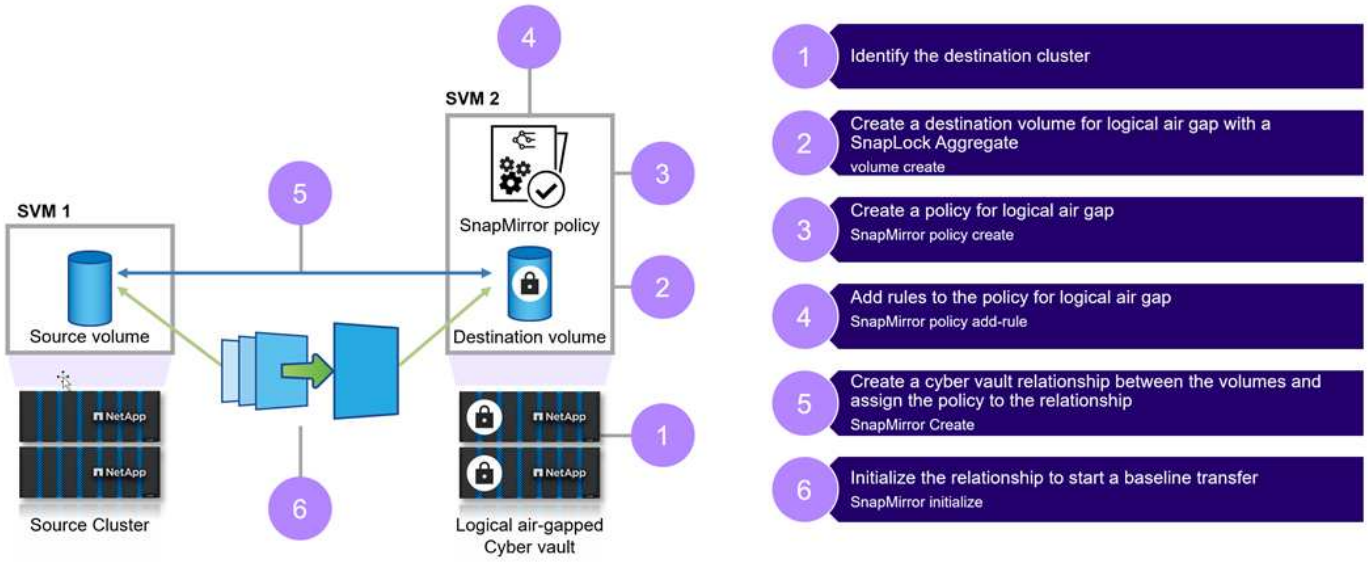
Dieses Dokument beschreibt die automatisierte Konfiguration des Cyber Vault von NetApp für den lokalen ONTAP -Speicher auf einem anderen dafür vorgesehenen ONTAP -Speicher mit unveränderlichen Snapshots, die eine zusätzliche Schutzebene vor zunehmenden Cyberangriffen für eine schnelle Wiederherstellung bieten. Als Teil dieser Architektur wird die gesamte Konfiguration gemäß den Best Practices von ONTAP angewendet. Der letzte Abschnitt enthält Anweisungen zur Durchführung einer Wiederherstellung im Falle eines Angriffs.

Dieselbe Lösung ist anwendbar, um den vorgesehenen Cyber-Tresor in AWS mit FSx ONTAP zu erstellen.

Allgemeine Schritte zum Erstellen eines ONTAP Cyber Vault

- Peering-Beziehung erstellen
  - Der Produktionsstandort, der ONTAP -Speicher verwendet, ist mit dem dafür vorgesehenen Cyber Vault ONTAP -Speicher verbunden
- SnapLock Compliance Volume erstellen
- Richten Sie die SnapMirror -Beziehung und die Regel zum Festlegen des Etiketts ein
  - SnapMirror -Beziehung und entsprechende Zeitpläne sind konfiguriert
- Legen Sie Aufbewahrungszeiten fest, bevor Sie die SnapMirror -Übertragung (Tresor) starten
  - Auf die kopierten Daten wird eine Aufbewahrungssperre angewendet, die die Daten zusätzlich vor Insidern oder Datenfehlern schützt. Dadurch können die Daten nicht vor Ablauf der Aufbewahrungsfrist gelöscht werden
  - Organisationen können diese Daten je nach Bedarf einige Wochen/Monate lang aufbewahren
- Initialisieren Sie die SnapMirror -Beziehung basierend auf Beschriftungen
  - Das anfängliche Seeding und die inkrementelle Übertragung erfolgen basierend auf dem SnapMirror Zeitplan
  - Die Daten sind durch SnapLock Konformität geschützt (unveränderlich und unlöschbar) und stehen für die Wiederherstellung zur Verfügung.

- Implementieren Sie strenge Datenübertragungskontrollen
  - Der Cyber-Tresor wird für einen begrenzten Zeitraum mit Daten vom Produktionsstandort freigeschaltet und mit den Daten im Tresor synchronisiert. Sobald die Übertragung abgeschlossen ist, wird die Verbindung getrennt, geschlossen und wieder gesperrt
- Schnelle Genesung
  - Wenn die primäre Produktionsumgebung betroffen ist, werden die Daten aus dem Cyber-Tresor sicher in die ursprüngliche Produktionsumgebung oder in eine andere ausgewählte Umgebung zurückgeführt.



Lösungskomponenten

NetApp ONTAP mit 9.15.1 auf Quell- und Zielclustern.

ONTAP One: Die All-in-One-Lizenz von NetApp ONTAP.

Von der ONTAP One-Lizenz genutzte Funktionen:

- SnapLock Compliance
- SnapMirror
- Multi-Admin-Verifizierung
- Alle Härtungsfunktionen von ONTAP
- Separate RBAC-Anmeldeinformationen für Cyber Vault

Alle einheitlichen physischen Arrays von ONTAP können für einen Cyber-Tresor verwendet werden. Die kostengünstigsten und idealsten Plattformen für diesen Zweck sind jedoch die kapazitätsbasierten Flash-Systeme der AFF C-Serie und die Hybrid-Flash-Systeme von FAS . Bitte konsultieren Sie die"Dimensionierung des ONTAP Cyber Vault" zur Größenberatung.

ONTAP Cyber Vault-Erstellung mit PowerShell

Bei Air-Gapping-Backups mit herkömmlichen Methoden müssen Platz geschaffen und das primäre und sekundäre Medium physisch getrennt werden. Durch die Verlagerung der Medien an einen anderen Standort und/oder die Trennung der Verbindung haben

böswillige Akteure keinen Zugriff auf die Daten. Dies schützt die Daten, kann jedoch zu längeren Wiederherstellungszeiten führen. Mit SnapLock Compliance ist keine physische Trennung erforderlich. SnapLock Compliance schützt die im Tresor gespeicherten Snapshots zu bestimmten Zeitpunkten und schreibgeschützten Kopien. Das Ergebnis sind Daten, die schnell zugänglich, vor Löschung geschützt bzw. unauslöschlich und vor Änderungen geschützt bzw. unveränderlich sind.

Voraussetzungen

Bevor Sie mit den Schritten im nächsten Abschnitt dieses Dokuments beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Auf dem Quellcluster muss ONTAP 9 oder höher ausgeführt werden.
- Die Quell- und Zielaggregate müssen 64-Bit sein.
- Die Quell- und Zielcluster müssen per Peering verbunden sein.
- Die Quell- und Ziel-SVMs müssen per Peering verbunden sein.
- Stellen Sie sicher, dass die Cluster-Peering-Verschlüsselung aktiviert ist.

Das Einrichten von Datenübertragungen zu einem ONTAP Cyber Vault erfordert mehrere Schritte. Konfigurieren Sie auf dem primären Volume eine Snapshot-Richtlinie, die angibt, welche Kopien wann erstellt werden sollen. Verwenden Sie dazu entsprechende Zeitpläne und weisen Sie Bezeichnungen zu, um anzugeben, welche Kopien von SnapVault übertragen werden sollen. Auf dem sekundären Server muss eine SnapMirror -Richtlinie erstellt werden, die die Bezeichnungen der zu übertragenden Snapshot-Kopien angibt und wie viele dieser Kopien im Cyber-Tresor aufbewahrt werden sollen. Nachdem Sie diese Richtlinien konfiguriert haben, erstellen Sie die SnapVault -Beziehung und legen Sie einen Übertragungsplan fest.

In diesem Dokument wird davon ausgegangen, dass der primäre Speicher und der vorgesehene ONTAP Cyber Vault bereits eingerichtet und konfiguriert sind.

Der Cyber-Vault-Cluster kann sich im selben oder einem anderen Rechenzentrum wie die Quelldaten befinden.

Schritte zum Erstellen eines ONTAP Cyber Vault

1. Verwenden Sie die ONTAP CLI oder den System Manager, um die Compliance-Uhr zu initialisieren.
2. Erstellen Sie ein Datenschutzvolume mit aktivierter SnapLock Konformität.
3. Verwenden Sie den Befehl „SnapMirror erstellen“, um SnapVault Datenschutzbeziehungen zu erstellen.
4. Legen Sie den standardmäßigen Aufbewahrungszeitraum für die SnapLock Compliance für das Zielvolume fest.

Die Standardaufbewahrung ist „Auf Minimum einstellen“. Einem SnapLock -Volume, das ein Tresorziel ist, ist eine Standardaufbewahrungsdauer zugewiesen. Der Wert für diesen Zeitraum ist zunächst auf mindestens 0 Jahre und höchstens 100 Jahre eingestellt (ab ONTAP 9.10.1). Bei früheren ONTAP Versionen liegt der Wert zwischen 0 und 70.) für SnapLock Compliance Volumes. Jede NetApp Snapshot-Kopie wird zunächst mit dieser Standardaufbewahrungsdauer festgeschrieben. Die Aufbewahrungsfrist kann bei Bedarf später verlängert, jedoch nie verkürzt werden. Weitere Informationen finden Sie unter "Übersicht über die eingestellte Aufbewahrungsdauer" .

Das oben Genannte umfasst manuelle Schritte. Sicherheitsexperten raten zur Automatisierung des Prozesses, um eine manuelle Verwaltung zu vermeiden, die eine große Fehlerquote mit sich bringt. Unten finden Sie den Codeausschnitt, der die Voraussetzungen und die Konfiguration der SnapLock -Konformität und Initialisierung der Uhr vollständig automatisiert.

Hier ist ein PowerShell-Codebeispiel zum Initialisieren der ONTAP Compliance-Uhr.

```
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
    }
}
```

Hier ist ein PowerShell-Codebeispiel zum Konfigurieren eines ONTAP Cyber Vault.

```
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. Sobald die oben genannten Schritte abgeschlossen sind, ist der Air-Gap-Cyber-Tresor mit SnapLock Compliance und SnapVault bereit.

Vor der Übertragung von Snapshot-Daten in den Cyber Vault muss die SnapVault -Beziehung initialisiert werden. Zuvor ist jedoch eine Sicherheitshärtung erforderlich, um den Tresor zu sichern.

ONTAP Cyber Vault-Härtung mit PowerShell

Der ONTAP Cyber Vault bietet im Vergleich zu herkömmlichen Lösungen eine bessere Widerstandsfähigkeit gegen Cyberangriffe. Beim Entwurf einer Architektur zur Verbesserung der Sicherheit ist es von entscheidender Bedeutung, Maßnahmen zur Verringerung der Angriffsfläche zu berücksichtigen. Dies kann durch verschiedene Methoden erreicht werden, beispielsweise durch die Implementierung gehärteter Kennwortrichtlinien, die Aktivierung von RBAC, das Sperren von Standardbenutzerkonten, die Konfiguration von Firewalls und die Nutzung von Genehmigungsabläufen für alle Änderungen am Tresorsystem. Darüber hinaus kann die Einschränkung von Netzwerkzugriffsprotokollen auf bestimmte IP-Adressen dazu beitragen, potenzielle Sicherheitslücken zu begrenzen.

ONTAP bietet eine Reihe von Steuerelementen, mit denen der ONTAP Speicher gehärtet werden kann. Verwenden Sie die"Anleitungen und Konfigurationseinstellungen für ONTAP" um Organisationen dabei zu helfen, vorgeschriebene Sicherheitsziele hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen zu erreichen.

Best Practices zur Härtung

Manuelle Schritte

1. Erstellen Sie einen bestimmten Benutzer mit vordefinierter und benutzerdefinierter Administratorrolle.
2. Erstellen Sie einen neuen IP-Bereich, um den Netzwerkverkehr zu isolieren.
3. Erstellen Sie eine neue SVM im neuen IP-Bereich.
4. Stellen Sie sicher, dass die Firewall-Routing-Richtlinien richtig konfiguriert sind und dass alle Regeln regelmäßig überprüft und bei Bedarf aktualisiert werden.

ONTAP CLI oder über Automatisierungsskript

1. Schützen Sie die Administration mit Multi-Admin-Verifizierung (MAV) zusätzlich zur Multi-Faktor-Authentifizierung (MFA) und erhöhen Sie so die Sicherheit des administrativen Zugriffs auf die Datenspeicher-VM.
2. Aktivieren Sie die Verschlüsselung für Standarddaten während der Übertragung zwischen Clustern.
3. Sichern Sie SSH mit einer starken Verschlüsselungsmethode und erzwingen Sie sichere Passwörter.
4. Aktivieren Sie globales FIPS.
5. Telnet und Remote Shell (RSH) sollten deaktiviert sein.
6. Standard-Administratorkonto sperren.
7. Deaktivieren Sie Daten-LIFs und sichern Sie Remote-Zugriffspunkte.
8. Deaktivieren und entfernen Sie nicht verwendete oder überflüssige Protokolle und Dienste.
9. Verschlüsseln Sie den Netzwerkverkehr.
10. Verwenden Sie beim Einrichten von Superuser- und Administratorrollen das Prinzip der geringsten Privilegien.
11. Beschränken Sie HTTPS und SSH von bestimmten IP-Adressen mithilfe der Option „Zulässige IPs“.
12. Beenden Sie die Replikation und setzen Sie sie basierend auf dem Übertragungsplan fort.

Die Punkte 1–4 erfordern manuelle Eingriffe wie die Festlegung eines isolierten Netzwerks, die Trennung des IP-Bereichs usw. und müssen im Voraus durchgeführt werden. Detaillierte Informationen zur Konfiguration der Härtung finden Sie im"Leitfaden zur ONTAP -Sicherheitshärtung" . Der Rest kann zur einfachen Bereitstellung und Überwachung problemlos automatisiert werden. Das Ziel dieses orchestrierten Ansatzes besteht darin, einen Mechanismus zur Automatisierung der Härtungsschritte bereitzustellen, um den Vault-Controller zukunftssicher zu machen. Der Zeitraum, in dem die Cyber-Vault-Air-Gap geöffnet ist, ist so kurz wie möglich. SnapVault nutzt die „Incremental Forever“-Technologie, die nur die Änderungen seit der letzten Aktualisierung in den Cyber-Tresor verschiebt und so die Zeit minimiert, die der Cyber-Tresor geöffnet bleiben muss. Um den Arbeitsablauf weiter zu optimieren, wird die Öffnung des Cyber-Tresors mit dem Replikationszeitplan koordiniert, um das kleinstmögliche Verbindungsfenster sicherzustellen.

Hier ist ein PowerShell-Codebeispiel zum Härten eines ONTAP -Controllers.

```
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
    }
}
```

ONTAP Cyber Vault-Validierung mit PowerShell

Ein robuster Cyber-Tresor sollte einem ausgeklügelten Angriff standhalten können, selbst wenn der Angreifer über Anmeldeinformationen verfügt, um mit erhöhten Berechtigungen auf die Umgebung zuzugreifen.

Sobald die Regeln eingerichtet sind, schlägt ein Versuch fehl (vorausgesetzt, der Angreifer konnte irgendwie eindringen), einen Snapshot auf der Tresorseite zu löschen. Gleiches gilt für alle Härtungseinstellungen, indem Sie die erforderlichen Einschränkungen vornehmen und das System absichern.

PowerShell-Codebeispiel zur Validierung der Konfiguration auf Zeitplanbasis.

```
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
    }
}
```

Dieser Screenshot zeigt, dass auf dem Vault-Controller keine Verbindungen bestehen.

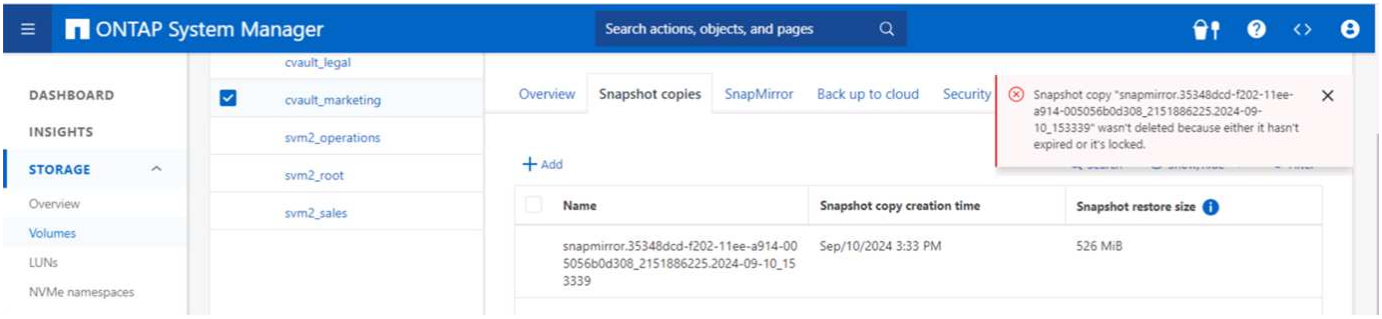
```
cluster2::> network connections  listening show
This table is currently empty.

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

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

cluster2::>
```

Dieser Screenshot zeigt, dass die Snapshots nicht manipuliert werden können.



Führen Sie die folgenden Schritte aus, um die Air-Gapping-Funktionalität zu validieren und zu bestätigen:

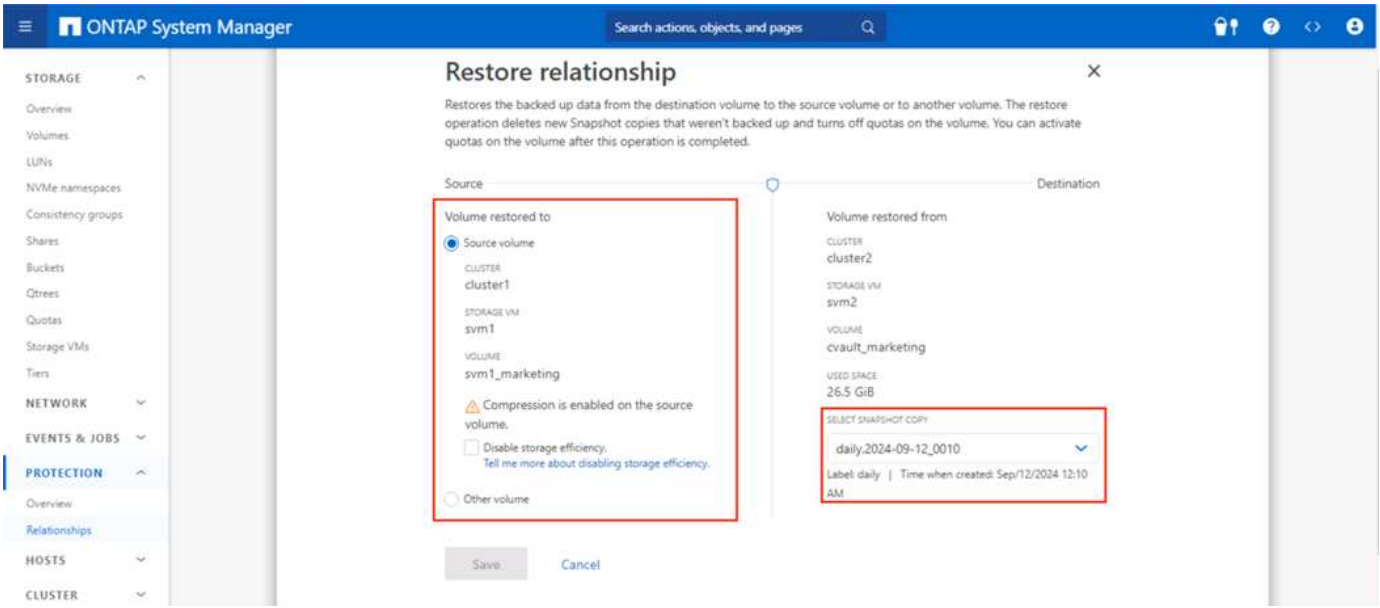
- Testen Sie die Netzwerkisolationsfunktionen und die Möglichkeit, eine Verbindung stillzulegen, wenn keine Daten übertragen werden.
- Stellen Sie sicher, dass auf die Verwaltungsschnittstelle von keiner Entität außer den zulässigen IP-Adressen zugegriffen werden kann.
- Überprüfen Sie, ob die Multi-Admin-Überprüfung vorhanden ist, um eine zusätzliche Genehmigungsebene bereitzustellen.
- Überprüfen Sie die Zugriffsmöglichkeit über CLI und REST-API
- Lösen Sie von der Quelle aus einen Übertragungsvorgang zum Tresor aus und stellen Sie sicher, dass die im Tresor gespeicherte Kopie nicht geändert werden kann.
- Versuchen Sie, die unveränderlichen Snapshot-Kopien zu löschen, die in den Tresor übertragen werden.
- Versuchen Sie, die Aufbewahrungsdauer durch Manipulation der Systemuhr zu ändern.

ONTAP Cyber Vault-Datenwiederherstellung

Wenn Daten im Produktionsrechenzentrum zerstört werden, können die Daten aus dem Cyber-Tresor sicher in der gewählten Umgebung wiederhergestellt werden. Anders als bei einer physisch luftgekapselten Lösung wird der luftgekapselte ONTAP Cyber Vault mithilfe nativer ONTAP -Funktionen wie SnapLock Compliance und SnapMirror erstellt. Das Ergebnis ist ein Wiederherstellungsprozess, der sowohl schnell als auch einfach durchzuführen ist.

Im Falle eines Ransomware-Angriffs und der Notwendigkeit einer Wiederherstellung aus dem Cyber-Tresor ist

der Wiederherstellungsprozess einfach und unkompliziert, da die im Cyber-Tresor gespeicherten Snapshot-Kopien zur Wiederherstellung der verschlüsselten Daten verwendet werden.



Wenn die Anforderung darin besteht, eine schnellere Methode bereitzustellen, um Daten bei Bedarf wieder online zu bringen, um die Daten für die Wiederherstellung schnell zu validieren, zu isolieren und zu analysieren. Dies lässt sich leicht erreichen, indem Sie FlexClone verwenden und die Option „Snaplock-Typ“ auf „Nicht-Snaplock-Typ“ einstellen.

Ab ONTAP 9.13.1 kann eine gesperrte Snapshot-Kopie auf dem Ziel SnapLock Volume einer SnapLock Vault-Beziehung sofort wiederhergestellt werden, indem ein FlexClone mit der Snaplock-Typ-Option „Nicht-Snaplock“ erstellt wird. Geben Sie beim Ausführen des Vorgangs zum Erstellen eines Volume-Klons die Snapshot-Kopie als „übergeordneten Snapshot“ an. Weitere Informationen zum Erstellen eines FlexClone -Volumes mit einem SnapLock -Typ"Hier."

Durch das Üben von Wiederherstellungsverfahren aus dem Cyber-Tresor wird sichergestellt, dass die richtigen Schritte zum Herstellen einer Verbindung mit dem Cyber-Tresor und zum Abrufen von Daten eingerichtet werden. Die Planung und Prüfung des Verfahrens ist für jede Wiederherstellung nach einem Cyberangriff von entscheidender Bedeutung.

Weitere Überlegungen

Beim Entwerfen und Bereitstellen eines ONTAP -basierten Cyber-Tresors sind zusätzliche Überlegungen anzustellen.

Überlegungen zur Kapazitätsdimensionierung

Die Menge an Speicherplatz, die für ein ONTAP Cyber Vault-Zielvolume erforderlich ist, hängt von einer Reihe von Faktoren ab. Der wichtigste davon ist die Änderungsrate der Daten im Quellvolume. Sowohl der Sicherungszeitplan als auch der Snapshot-Zeitplan auf dem Zielvolume wirken sich auf die Datenträgernutzung auf dem Zielvolume aus, und die Änderungsrate auf dem Quellvolume ist wahrscheinlich nicht konstant. Es empfiehlt sich, einen Puffer an zusätzlicher Speicherkapazität bereitzustellen, der über den erforderlichen Wert hinausgeht, um zukünftigen Änderungen im Endbenutzer- oder Anwendungsverhalten Rechnung zu tragen.

Um die Größe einer Beziehung für eine einmonatige Aufbewahrung in ONTAP festzulegen, müssen die Speicheranforderungen anhand mehrerer Faktoren berechnet werden, darunter die Größe des primären Datensatzes, die Datenänderungsrate (tägliche Änderungsrate) und die Einsparungen durch Deduplizierung und Komprimierung (falls zutreffend).

Hier ist die schrittweise Vorgehensweise:

Der erste Schritt besteht darin, die Größe des/der Quellvolumes/-volumes zu kennen, das/die Sie mit dem Cyber Vault schützen. Dies ist die Basisdatenmenge, die zunächst zum Cyber-Vault-Ziel repliziert wird. Schätzen Sie als Nächstes die tägliche Änderungsrate für den Datensatz. Dies ist der Prozentsatz der Daten, der sich täglich ändert. Es ist entscheidend, ein gutes Verständnis dafür zu haben, wie dynamisch Ihre Daten sind.

Beispiel:

- Größe des primären Datensatzes = 5 TB
- Tägliche Änderungsrate = 5 % (0,05)
- Deduplizierungs- und Komprimierungseffizienz = 50 % (0,50)

Lassen Sie uns nun die Berechnung durchgehen:

- Berechnen Sie die tägliche Datenänderungsrate:

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

- Berechnen Sie die gesamten geänderten Daten für 30 Tage:

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

- Berechnen Sie den insgesamt erforderlichen Speicher:

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

- Einsparungen durch Deduplizierung und Komprimierung anwenden:

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

Zusammenfassung des Speicherbedarfs

- Ohne Effizienz: Es wären **12,5 TB** erforderlich, um 30 Tage der Cyber-Vault-Daten zu speichern.
- Bei 50 % Effizienz: Nach Deduplizierung und Komprimierung wären **6,25 TB** Speicherplatz erforderlich.

Snapshot-Kopien können aufgrund von Metadaten zusätzlichen Aufwand verursachen, dieser ist jedoch normalerweise geringfügig.

Wenn mehrere Sicherungen pro Tag durchgeführt werden, passen Sie die Berechnung an die Anzahl der täglich erstellten Snapshot-Kopien an.

Berücksichtigen Sie das Datenwachstum im Laufe der Zeit, um sicherzustellen, dass die Dimensionierung zukunftssicher ist.

Auswirkungen auf die Leistung der Primärquelle

Da es sich bei der Datenübertragung um einen Pull-Vorgang handelt, können die Auswirkungen auf die Leistung des Primärspeichers je nach Arbeitslast, Datenvolumen und Häufigkeit der Sicherungen variieren. Die Gesamtauswirkungen auf die Leistung des primären Systems sind jedoch im Allgemeinen moderat und beherrschbar, da die Datenübertragung darauf ausgelegt ist, Datenschutz- und Sicherungsaufgaben auf das Cyber-Vault-Speichersystem auszulagern. Während der anfänglichen Einrichtung der Beziehung und der ersten vollständigen Sicherung wird eine erhebliche Datenmenge vom primären System auf das Cyber-Vault-System (das SnapLock Compliance Volume) übertragen. Dies kann zu erhöhtem Netzwerkverkehr und einer erhöhten E/A-Last auf dem primären System führen. Sobald die erste vollständige Sicherung abgeschlossen ist, muss ONTAP nur noch Blöcke verfolgen und übertragen, die sich seit der letzten Sicherung geändert haben. Dies führt zu einer wesentlich geringeren E/A-Last im Vergleich zur ursprünglichen Replikation. Inkrementelle Updates sind effizient und haben nur minimale Auswirkungen auf die Leistung des Primärspeichers. Der Tresorprozess läuft im Hintergrund, wodurch die Wahrscheinlichkeit von Störungen der Produktionsarbeitslasten des primären Systems verringert wird.

- Indem Sie sicherstellen, dass das Speichersystem über genügend Ressourcen (CPU, Speicher und IOPs) verfügt, um die zusätzliche Last zu bewältigen, können Sie die Auswirkungen auf die Leistung abmildern.

Konfigurieren, Analysieren, Cron-Skript

NetApp hat eine"einzelnes Skript, das heruntergeladen werden kann" und wird zum Konfigurieren, Überprüfen und Planen von Cyber-Vault-Beziehungen verwendet.

Was dieses Skript macht

- Cluster-Peering
- SVM-Peering
- DP-Volume-Erstellung
- SnapMirror -Beziehung und Initialisierung
- Härten Sie das für den Cyber Vault verwendete ONTAP -System
- Beenden und Fortsetzen der Beziehung basierend auf dem Übertragungsplan
- Überprüfen Sie die Sicherheitseinstellungen regelmäßig und erstellen Sie einen Bericht, der etwaige Anomalien aufzeigt.

So verwenden Sie dieses Skript

"Laden Sie das Skript herunter"und um das Skript zu verwenden, folgen Sie einfach den folgenden Schritten:

- Starten Sie Windows PowerShell als Administrator.
- Navigieren Sie zu dem Verzeichnis, das das Skript enthält.
- Führen Sie das Skript mit `.\` Syntax zusammen mit den erforderlichen Parametern

> Bitte stellen Sie sicher, dass alle Informationen eingegeben wurden. Beim ersten Ausführen (Konfigurationsmodus) werden Anmeldeinformationen sowohl für das Produktions- als auch für das neue Cyber-Vault-System abgefragt. Anschließend werden die SVM-Peerings (falls nicht vorhanden), die Volumes und der SnapMirror zwischen dem System erstellt und initialisiert.

Der Cron-Modus kann verwendet werden, um die Ruhephase und Wiederaufnahme der Datenübertragung zu planen.

Betriebsarten

Das Automatisierungsskript bietet 3 Ausführungsmodi: `configure` , `analyze` Und `cron` .

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

- Konfigurieren – Führt die Validierungsprüfungen durch und konfiguriert das System als Air-Gap.
- Analysieren – Automatisierte Überwachungs- und Berichtsfunktion zum Senden von Informationen zu Anomalien und verdächtigen Aktivitäten an Überwachungsgruppen, um sicherzustellen, dass die Konfigurationen nicht abweichen.
- Cron – Um eine getrennte Infrastruktur zu ermöglichen, automatisiert der Cron-Modus die Deaktivierung des LIF und legt die Übertragungsbeziehung still.

Die Übertragung der Daten in diesen ausgewählten Volumes dauert je nach Systemleistung und Datenmenge einige Zeit.

```
./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"
```

Fazit zur ONTAP Cyber Vault PowerShell-Lösung

Durch die Nutzung von Air-Gapping mit den robusten Härtungsmethoden von ONTAP ermöglicht NetApp Ihnen die Erstellung einer sicheren, isolierten Speicherumgebung, die widerstandsfähig gegen sich entwickelnde Cyberbedrohungen ist. All dies wird erreicht, während die Agilität und Effizienz der vorhandenen Speicherinfrastruktur erhalten bleibt. Dieser sichere Zugriff ermöglicht es Unternehmen, ihre strengen Sicherheits- und Betriebszeitziele mit minimalen Änderungen an ihrem bestehenden Personal-, Prozess- und Technologierahmen zu erreichen.

ONTAP Cyber Vault verwendet native Funktionen in ONTAP und bietet einen einfachen Ansatz für zusätzlichen Schutz, um unveränderliche und unlöschbare Kopien Ihrer Daten zu erstellen. Durch die Ergänzung der allgemeinen Sicherheitslage um den ONTAP basierten Cyber Vault von NetApp ergeben sich folgende Vorteile:

- Erstellen Sie eine Umgebung, die von den Produktions- und Backup-Netzwerken getrennt und nicht verbunden ist, und beschränken Sie den Benutzerzugriff darauf.