Erstellen, Aushärten und Validieren eines ONTAP-Cybervells mit PowerShell

NetApp Solutions

NetApp
December 19, 2024

Inhalt

Erstellen, Aushärten und Validieren eines ONTAP-Cybervells mit PowerShell

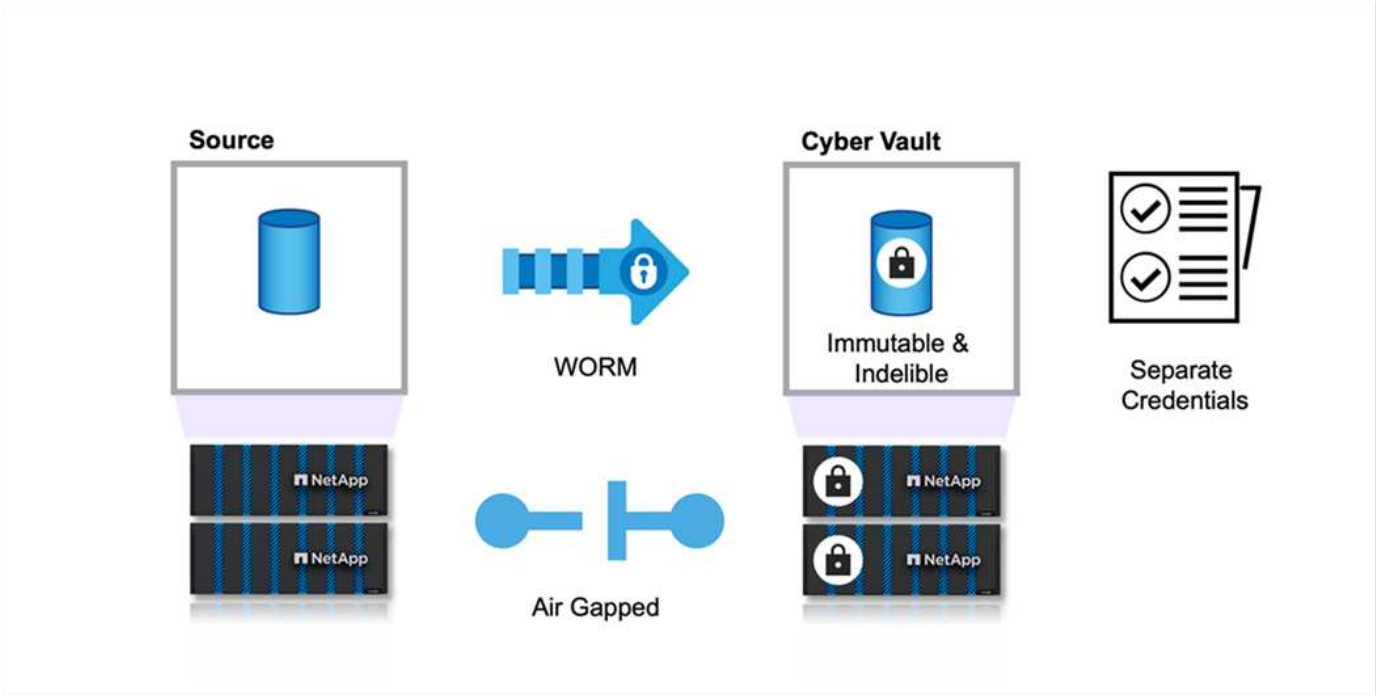
Übersicht über ONTAP Cyber-Vault mit PowerShell

In der heutigen digitalen Landschaft ist der Schutz der kritischen Datenbestände eines Unternehmens nicht nur eine Best Practice, sondern ein Geschäftsziel. Cyberbedrohungen entwickeln sich mit einem beispiellosen Tempo weiter und herkömmliche Datensicherungsmaßnahmen reichen nicht mehr aus, um sensible Daten zu schützen. Hier kommt ein Cyber-Vault ins Spiel. Die innovative ONTAP-basierte Lösung von NetApp kombiniert fortschrittliche Air-Gating-Techniken mit robusten Datenschutzmaßnahmen, um eine undurchdringliche Barriere gegen Cyber-Bedrohungen zu schaffen. Durch die Isolierung der wertvollsten Daten mithilfe einer sicheren Härtetechnologie minimiert ein Cyber-Vault die Angriffsfläche. Dadurch bleiben die kritischsten Daten vertraulich, intakt und jederzeit verfügbar, wenn sie benötigt werden.

Ein Cyber-Vault ist eine sichere Storage-Einrichtung, die aus mehreren Schutzebenen wie Firewalls, Networking und Storage besteht. Diese Komponenten sichern wichtige Recovery-Daten, die für wichtige Geschäftsabläufe erforderlich sind. Die Komponenten des Cyber-Tresors synchronisieren sich regelmäßig mit den wesentlichen Produktionsdaten auf der Grundlage der Tresorrichtlinie, bleiben aber ansonsten unzugänglich. Dieses isolierte und getrennte Setup stellt sicher, dass im Falle eines Cyberangriffs, der die Produktionsumgebung beeinträchtigt, eine zuverlässige und endgültige Wiederherstellung problemlos vom Cyber-Vault aus durchgeführt werden kann.

NetApp ermöglicht die einfache Erstellung eines Air Gap für Cyber-Vault, indem es das Netzwerk konfiguriert, LIFs deaktiviert, Firewall-Regeln aktualisiert und das System von externen Netzwerken und dem Internet isoliert. Dieser robuste Ansatz trennt das System effektiv von externen Netzwerken und dem Internet und bietet so einen unvergleichlichen Schutz vor Cyber-Angriffen und unberechtigten Zugriffsversuchen, wodurch das System gegen netzwerkbasierte Bedrohungen und Angriffe immun wird.

In Kombination mit SnapLock Compliance-Schutz können Daten nicht einmal von ONTAP-Administratoren oder dem NetApp-Support geändert oder gelöscht werden. SnapLock wird regelmäßig gegen die SEC- und FINRA-Vorschriften geprüft, um sicherzustellen, dass die Ausfallsicherheit der Daten diesen anspruchsvollen WORM- und Datenaufbewahrungsvorschriften der Bankbranche entspricht. NetApp ist der einzige Enterprise Storage, der von NSA CSfC für die Speicherung von streng geheimen Daten validiert wurde.



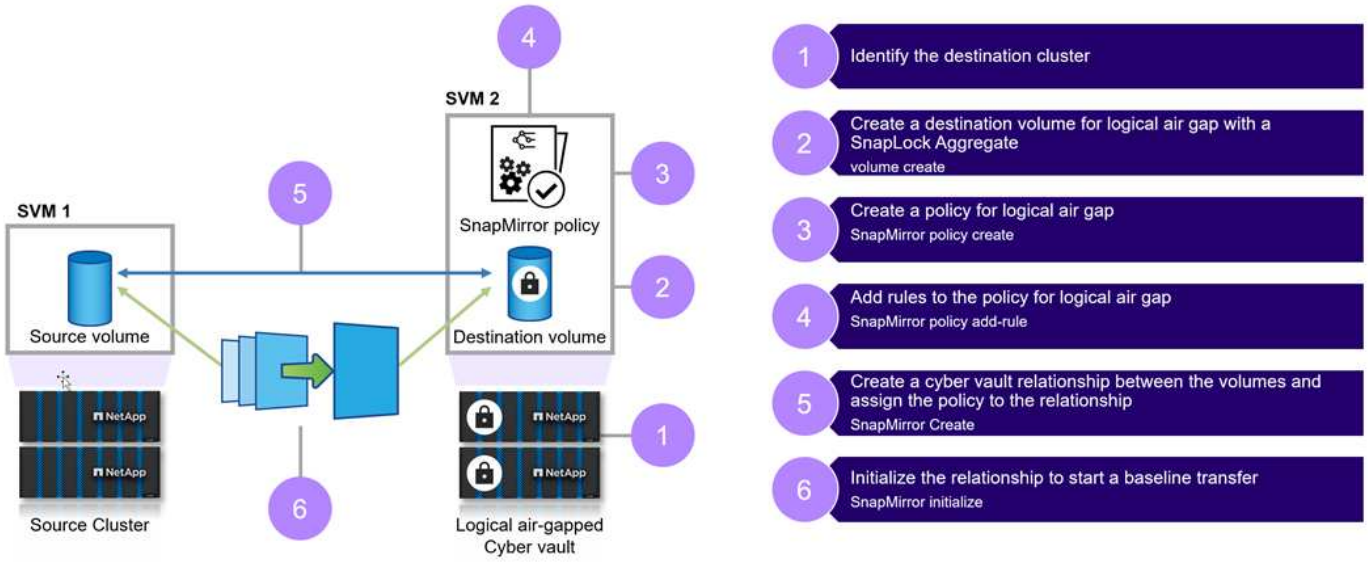
In diesem Dokument wird die automatisierte Konfiguration des NetApp Cyber Vault für lokalen ONTAP Storage in einem anderen designierten ONTAP Storage mit unveränderlichen Snapshots beschrieben, die eine zusätzliche Schutzschicht vor zunehmenden Cyberangriffen für eine schnelle Recovery hinzufügen. Als Teil dieser Architektur wird die gesamte Konfiguration gemäß den ONTAP Best Practices angewendet. Der letzte Abschnitt enthält Anweisungen zur Durchführung einer Wiederherstellung im Falle eines Angriffs.

Dieselbe Lösung kann mithilfe von FSX ONTAP für die Erstellung des designierten Cyber-Vault in AWS angewendet werden.

Grundlegende Schritte zur Erstellung eines ONTAP-Cyber-Vault

- Peering-Beziehung erstellen
  - Der Produktionsstandort mit ONTAP-Storage wird mit designiertem Cyber-Vault ONTAP-Storage verbunden
- Erstellen Sie ein SnapLock Compliance Volume
- SnapMirror-Beziehung und -Regel einrichten, um die Bezeichnung festzulegen
  - Die SnapMirror-Beziehung und entsprechende Zeitpläne sind konfiguriert
- Legen Sie Retentions fest, bevor Sie die SnapMirror (Vault)-Übertragung starten
  - Auf die kopierten Daten wird eine Aufbewahrungs-Lock angewendet, wodurch die Daten noch vor Insider- oder Datenfehlern verhindert werden. Damit können die Daten nicht vor Ablauf der Aufbewahrungsfrist gelöscht werden
  - Unternehmen können diese Daten je nach Anforderung mehrere Wochen/Monate lang aufbewahren
- Initialisieren Sie die SnapMirror-Beziehung auf Basis von Labels
  - Das erste Seeding und der inkrementelle, immerwährende Transfer erfolgen basierend auf dem SnapMirror-Zeitplan
  - Daten sind mit SnapLock Compliance geschützt (unveränderlich und unlöschbar) und stehen für die Recovery zur Verfügung

- Implementieren strenger Kontrollen für den Datentransfer
  - Cyber-Vault wird für einen begrenzten Zeitraum mit Daten vom Produktionsstandort entsperrt und mit den Daten im Vault synchronisiert. Nach Abschluss der Übertragung wird die Verbindung getrennt, geschlossen und wieder gesperrt
- Schnelle Recovery
  - Wenn die Primärdaten am Produktionsstandort beeinträchtigt werden, werden die Daten des Cyber-Vault sicher in die ursprüngliche Produktionsumgebung oder in eine andere gewählte Umgebung wiederhergestellt



Lösungskomponenten

NetApp ONTAP mit Ausführung 9.15.1 auf Quell- und Ziel-Clustern.

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

Funktionen, die mit der ONTAP One Lizenz verwendet werden:

- SnapLock-Compliance
- SnapMirror
- Überprüfung durch mehrere Administratoren
- Alle Härtungsmöglichkeiten offengelegt von ONTAP
- Separate Anmeldedaten für RBAC für Cyber-Vault

Alle einheitlichen physischen ONTAP Arrays können für eine Cyber-Vault eingesetzt werden. Kapazitätsbasierte Flash-Systeme der AFF C-Serie und FAS Hybrid-Flash-Systeme sind dafür die kostengünstigsten, idealen Plattformen. "Dimensionierung von ONTAP Cyber-Vaults"Informationen zur Dimensionierung finden Sie im.

Erstellung von ONTAP Cyber-Vaults mit PowerShell

Air-Gap-Backups, die herkömmliche Methoden verwenden, erfordern die Schaffung von Speicherplatz und die physische Trennung des primären und sekundären Mediums.

Durch Verlagerung der Medien an einen anderen Standort und/oder durch Trennung der Konnektivität haben schlechte Akteure keinen Zugriff auf die Daten. So sind die Daten geschützt, können aber zu langsameren Recovery-Zeiten führen. Mit SnapLock Compliance ist keine physische Trennung erforderlich. SnapLock Compliance sichert die archivierten, zeitpunktgenauen, schreibgeschützten Snapshot Kopien. Die damit gespeicherten Daten sind schnell zugänglich, sicher vor Löschung und nicht löschbar und sicher vor Veränderung oder unveränderbar.

Voraussetzungen

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

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

Die Einrichtung von Datentransfers zu einem ONTAP-Cyber-Vault erfordert mehrere Schritte. Konfigurieren Sie auf dem primären Volume eine Snapshot-Richtlinie, die angibt, welche Kopien erstellt werden sollen, und wann sie mithilfe der entsprechenden Zeitpläne erstellt werden sollen. Außerdem weisen Sie Etiketten zu, um festzulegen, welche Kopien von SnapVault übertragen werden sollen. Auf dem sekundären Server muss eine SnapMirror-Richtlinie erstellt werden, in der die Labels der zu übertragenden Snapshot Kopien angegeben sind und wie viele dieser Kopien im Cyber-Vault aufbewahrt werden sollen. Nach der Konfiguration dieser Richtlinien erstellen Sie die SnapVault Beziehung und legen einen Übertragungszeitplan fest.

Bei diesem Dokument wird davon ausgegangen, dass der primäre Storage und der designierte Cyber-Vault von ONTAP bereits eingerichtet und konfiguriert sind.

Cyber-Vault-Cluster können sich im gleichen oder anderen Datacenter wie die Quelldaten befinden.

Schritte zum Erstellen einer ONTAP-Cyber-Vault

1. Verwenden Sie die ONTAP CLI oder System Manager, um die Compliance-Uhr zu initialisieren.
2. Erstellen Sie ein Datensicherungs-Volume mit aktivierter SnapLock Compliance.
3. Verwenden Sie den Befehl SnapMirror create, um SnapVault Datensicherungsbeziehungen zu erstellen.
4. Legen Sie den SnapLock Compliance-Standardaufbewahrungszeitraum für das Ziel-Volume fest.

Die standardmäßige Aufbewahrung ist „auf Minimum gesetzt“. Einem SnapLock-Volume, das ein Vault-Ziel ist, ist ein Standardaufbewahrungszeitraum zugewiesen. Der Wert für diesen Zeitraum wird zunächst auf mindestens 0 Jahre und maximal 100 Jahre (beginnend mit ONTAP 9.10.1) festgelegt. Bei älteren ONTAP Versionen beträgt der Wert 0 - 70.) für SnapLock Compliance Volumes. Jede NetApp Snapshot-Kopie wird zunächst mit diesem standardmäßigen Aufbewahrungszeitraum festgelegt. Die Aufbewahrungsfrist kann bei Bedarf später verlängert, aber nie verkürzt werden. Weitere Informationen finden Sie unter "Aufbewahrungszeit einstellen".

Die oben genannten Schritte umfassen manuelle Schritte. Sicherheitsexperten raten, den Prozess zu automatisieren, um ein manuelles Management zu vermeiden, was zu einer großen Fehlerspanne führt. Unten ist der Code-Snippet, der die Voraussetzungen und die Konfiguration von SnapLock Compliance und die Initialisierung der Uhr vollständig automatisiert.

Hier ist ein PowerShell-Codebeispiel für die Initialisierung 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-Code-Beispiel zur Konfiguration eines Cyber-Vaults für 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. Sobald die oben genannten Schritte abgeschlossen sind, ist ein Cyber-Vault mit Air-Gap-Technologie und SnapLock Compliance und SnapVault bereit.

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

ONTAP Cyber-Vault-Härtung mit PowerShell

Im Vergleich zu herkömmlichen Lösungen bietet die ONTAP Cyber-Vault eine bessere Ausfallsicherheit gegen Cyberangriffe. Bei der Entwicklung einer Architektur zur Erhöhung der Sicherheit ist es von entscheidender Bedeutung, Maßnahmen zur Reduzierung der Angriffsfläche zu berücksichtigen. Dies kann durch verschiedene Methoden erreicht werden, wie z. B. die Implementierung gesicherter Passwortrichtlinien, die Aktivierung von RBAC, die Sperrung von Standardbenutzerkonten, die Konfiguration von Firewalls und die Nutzung von Genehmigungsströmen für Änderungen am Vault-System. Darüber hinaus kann die Einschränkung von Netzwerkzugriffsprotokollen von einer bestimmten IP-Adresse helfen, potenzielle Schwachstellen zu begrenzen.

ONTAP bietet eine Reihe von Kontrollen, die das Absichern des ONTAP-Speichers ermöglichen. Verwenden Sie das"Richtlinien und Konfigurationseinstellungen für ONTAP", um Unternehmen bei der Einhaltung vorgegebener Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen zu unterstützen.

Best Practices optimieren

Manuelle Schritte

1. Erstellen Sie einen bestimmten Benutzer mit einer vordefinierten und benutzerdefinierten Administratorrolle.
2. Erstellen Sie einen neuen IPspace, um den Netzwerkverkehr zu isolieren.
3. Erstellen Sie eine neue SVM im neuen IPspace.
4. Stellen Sie sicher, dass Firewall-Routing-Richtlinien ordnungsgemäß konfiguriert und alle Regeln regelmäßig geprüft und bei Bedarf aktualisiert werden.

ONTAP CLI oder über Automatisierungsskript

1. Schutz der Administration durch MFA (Multi-Admin Verification)
2. Verschlüsselung von Standarddaten „während der Übertragung“ zwischen Clustern aktivieren
3. Sichern Sie SSH mit starker Verschlüsselung und erzwingen Sie sichere Passwörter.
4. Globalen FIPS ermöglichen.
5. Telnet und Remote Shell (RSH) sollten deaktiviert werden.
6. Standard-Administratorkonto sperren.
7. Deaktivieren Sie Daten-LIFs und sichere Remote-Zugriffspunkte.
8. Deaktivieren und entfernen Sie nicht verwendete oder externe Protokolle und Services.
9. Verschlüsseln Sie den Netzwerkverkehr.
10. Verwenden Sie beim Einrichten von Superuser- und Administratorrollen das Prinzip „Least Privilege“.
11. Beschränken Sie HTTPS und SSH von einer bestimmten IP-Adresse mit der zulässigen IP-Option.
12. Legen Sie die Replikation auf der Grundlage des Übertragungszeitplans still und nehmen Sie sie wieder auf.

Die Aufzählungspunkte 1-4 müssen manuell eingreifen, wie z. B. die Benennung eines isolierten Netzwerks, die Trennung des IPspaces usw. und müssen vorher durchgeführt werden. Detaillierte Informationen zur Konfiguration der Härtung finden Sie im "Leitfaden zur ONTAP-Erhöhung der Sicherheit". Der Rest kann leicht automatisiert werden, um eine einfache Bereitstellung und Überwachung zu ermöglichen. Das Ziel dieses orchestrierten Ansatzes besteht darin, einen Mechanismus zur Automatisierung der Härtungsschritte bereitzustellen, um den Vault-Controller zukunftssicher zu machen. Der Zeitrahmen, in dem der Cyber-Vault-Luftspalt offen ist, ist so kurz wie möglich. SnapVault nutzt die Incremental Forever-Technologie, die die Änderungen seit dem letzten Update nur in den Cyber-Vault verschiebt, um so die Zeit zu minimieren, die das Cyber-Vault offen halten muss. Um den Workflow weiter zu optimieren, wird die Cyber-Vault-Eröffnung mit dem Replikationszeitplan abgestimmt, um das kleinste Verbindungsfenster zu gewährleisten.

Hier ist ein PowerShell-Code-Beispiel 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
    }
}
```

Validierung von ONTAP Cyber-Vaults mit PowerShell

Ein robuster Cyber-Vault sollte in der Lage sein, einem anspruchsvollen Angriff standzuhalten, selbst wenn der Angreifer über Anmeldeinformationen verfügt, um mit erhöhten Privileges auf die Umgebung zuzugreifen.

Sobald die Regeln festgelegt sind, schlägt ein Versuch (in der Annahme, dass der Angreifer irgendwie in der Lage war, hereinzukommen) fehl, einen Snapshot auf der Tresorseite zu löschen. Gleiches gilt für alle Härtungseinstellungen, indem die erforderlichen Einschränkungen vorgenommen und das System geschützt werden.

PowerShell Code-Beispiel zur Validierung der Konfiguration nach Zeitplan

```
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 es keine Verbindungen auf dem Vault Controller gibt.

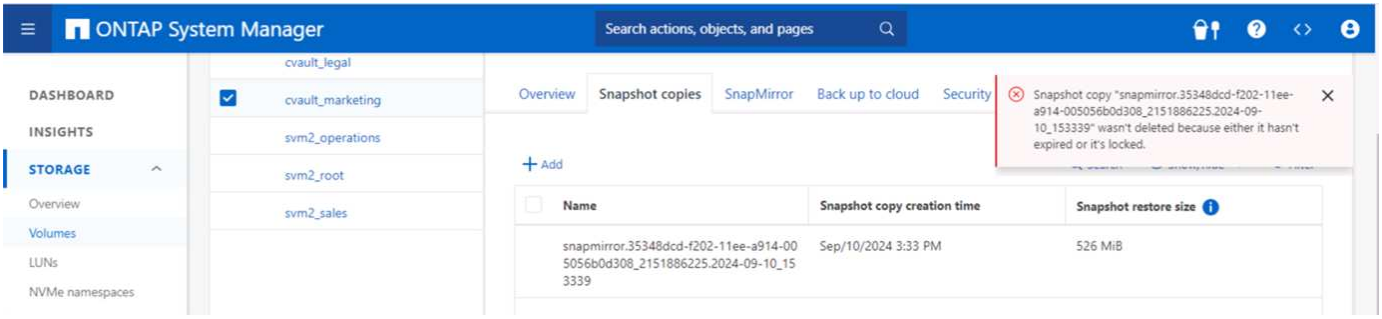
```
cluster2::> network connections  listening show
This table is currently empty.

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 es keine Möglichkeit gibt, die Snapshots zu manipulieren.



Gehen Sie wie folgt vor, um die Air-Gapping-Funktion zu überprüfen und zu bestätigen:

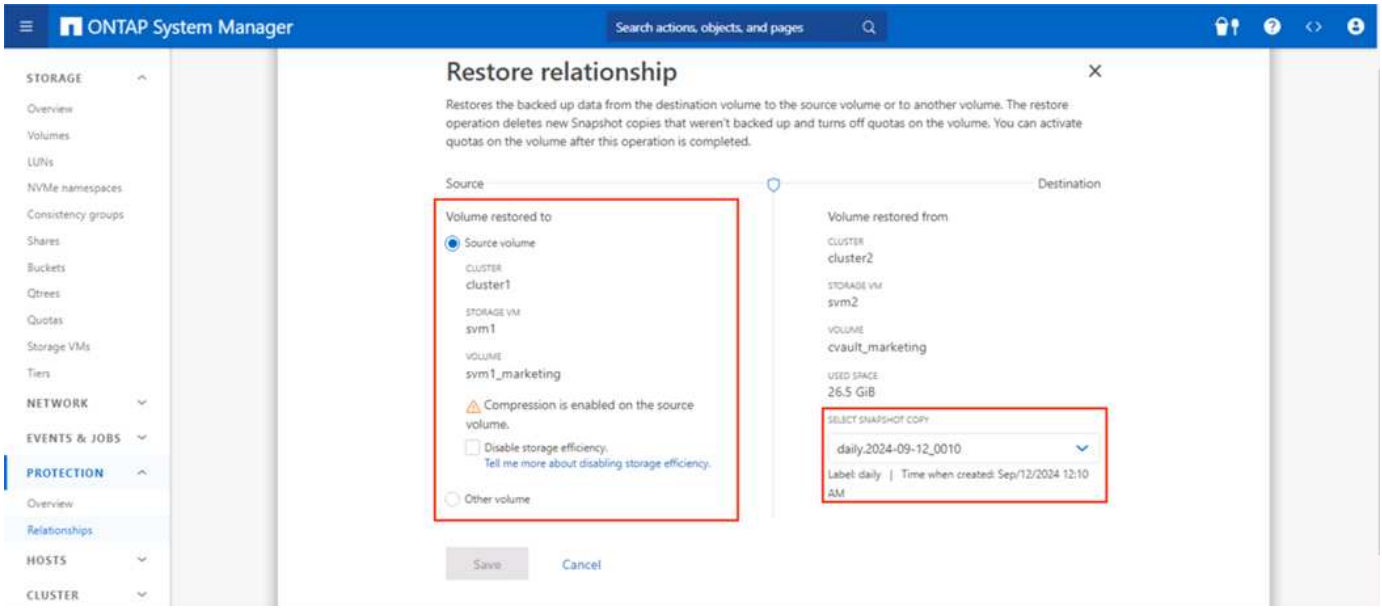
- Testen Sie die Funktionen zur Netzwerkisolation und die Fähigkeit, eine Verbindung stillzulegen, wenn keine Daten übertragen werden.
- Vergewissern Sie sich, dass außer den zulässigen IP-Adressen kein Zugriff auf die Verwaltungsschnittstelle möglich ist.
- Überprüfen Sie, ob eine Multi-Admin-Verifizierung vorhanden ist, um eine zusätzliche Genehmigungsebene bereitzustellen.
- Validieren der Zugriffsmöglichkeiten über CLI und REST API
- Starten Sie von der Quelle aus einen Übertragungsvorgang zum Tresor, und stellen Sie sicher, dass die gewölbte Kopie nicht geändert werden kann.
- Versuchen Sie, die unveränderlichen Snapshot Kopien zu löschen, die in den Vault übertragen werden.
- Versuchen Sie, die Aufbewahrungsfrist zu ändern, indem Sie die Systemuhr manipulieren.

Cyber-Vault-Datenwiederherstellung bei ONTAP

Wenn Daten im Produktions-Datacenter zerstört werden, können die Daten aus dem Cyber-Vault sicher in der gewählten Umgebung wiederhergestellt werden. Im Gegensatz zu einer physisch gezapften Lösung basiert der ONTAP-Cyber-Vault auf nativen ONTAP-Funktionen wie SnapLock Compliance und SnapMirror. Das Ergebnis ist ein Recovery-Prozess, der sowohl schnell als auch einfach auszuführen ist.

Im Falle eines Ransomware-Angriffs und der Notwendigkeit einer Wiederherstellung aus dem Cyber-Vault ist der Recovery-Prozess einfach und einfach, da die in der Cyber-Vault gespeicherten Snapshot-Kopien zur

Wiederherstellung der verschlüsselten Daten verwendet werden.



Wenn es darum geht, bei Bedarf eine schnellere Methode zur Wiederherstellung der Daten bereitzustellen, um die Daten schnell zu validieren, zu isolieren und zu analysieren. Dies kann leicht erreicht werden, indem mit FlexClone die Option SnapLock-type auf nicht-SnapLock-Typ eingestellt wird.

Ab ONTAP 9.13.1 kann die Wiederherstellung einer gesperrten Snapshot Kopie auf dem SnapLock Ziel-Volume in einer SnapLock Vault-Beziehung sofort wiederhergestellt werden, indem eine FlexClone erstellt wird, bei der die Option „nicht-SnapLock“ für den SnapLock-Typ eingestellt ist. Wenn Sie die Klonerstellung des Volumes durchführen, geben Sie die Snapshot Kopie als „Parent-Snapshot“ an. Weitere Informationen zur Erstellung eines FlexClone Volumes mit einem SnapLock-Typ "Hier."

Das Üben von Recovery-Verfahren aus dem Cyber-Vault wird sicherstellen, dass die richtigen Schritte für die Verbindung mit dem Cyber-Vault und Abrufen von Daten eingerichtet werden. Die Planung und das Testen des Verfahrens ist für jede Wiederherstellung während eines Cyber-Angriffs unerlässlich.

Weitere Überlegungen

Beim Design und der Implementierung einer ONTAP-basierten Cyber-Vault müssen noch weitere Überlegungen angestellt werden.

Überlegungen zum Kapazitätsdimensionieren

Die Menge an Speicherplatz, die für ein ONTAP Cyber Vault-Ziel-Volume benötigt wird, hängt von verschiedenen Faktoren ab. Am wichtigsten ist dabei die Änderungsrate der Daten im Quell-Volume. Der Backup-Zeitplan und der Snapshot-Zeitplan auf dem Ziel-Volume wirken sich sowohl auf die Festplattennutzung auf dem Ziel-Volume aus als auch auf die Änderungsrate auf dem Quell-Volume ist wahrscheinlich nicht konstant. Es empfiehlt sich, darüber hinaus einen Puffer an zusätzlicher Storage-Kapazität bereitzustellen, der erforderlich ist, um künftige Änderungen im Verhalten von Endbenutzern oder Applikationen zu berücksichtigen.

Für die Dimensionierung eines Verhältnisses für 1 Monat Aufbewahrung in ONTAP müssen die Storage-

Anforderungen auf Grundlage verschiedener Faktoren berechnet werden, darunter die Größe des primären Datensatzes, die Änderungsrate der Daten (tägliche Änderungsrate) sowie die Einsparungen durch Deduplizierung und Komprimierung (falls zutreffend).

Hier ist der Schritt-für-Schritt-Ansatz:

Der erste Schritt besteht darin, die Größe der Quell-Volumes zu kennen, die Sie mit dem Cyber-Vault schützen. Dies ist die Grundmenge der Daten, die zunächst auf das Cyber-Vault-Ziel repliziert werden. Schätzen Sie als Nächstes die tägliche Änderungsrate für den Datensatz ab. Dies ist der Prozentsatz der Daten, die sich jeden Tag ändern. Dabei ist es entscheidend, die Dynamik der Daten genau zu kennen.

Beispiel:

- Größe des primären Datensatzes = 5 TB
- Tägliche Änderungsrate = 5% (0.05)
- Deduplizierungs- und Komprimierungs-Effizienz = 50 % (0.50)

Lassen Sie uns nun die Berechnung durchgehen:

- Berechnung der täglichen Datenänderungsrate:

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

- Berechnen der geänderten Gesamtdaten für 30 Tage:

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

- Berechnen Sie den insgesamt erforderlichen Storage:

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

- Einsparungen bei Deduplizierung und Komprimierung:

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

Zusammenfassung des Speicherbedarfs

- Ohne Effizienz würde **12,5 TB** erforderlich sein, um 30 Tage Cyber-Vault-Daten zu speichern.
- Bei einer Effizienz von 50 % würde nach Deduplizierung und Komprimierung **6,25 TB** Storage benötigt.

Snapshot-Kopien können durch Metadaten zusätzlichen Overhead haben, dieser Vorgang ist jedoch in der Regel geringfügig.

Wenn pro Tag mehrere Backups erstellt 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 das Sizing zukunftssicher ist.

Performance-Auswirkungen auf Primär-/Quelle

Da es sich bei dem Datentransfer um einen Pull-Vorgang handelt, können die Auswirkungen auf die Performance des primären Storage je nach Workload, Datenvolumen und Häufigkeit von Backups variieren. Die Auswirkungen auf die Performance des primären Systems insgesamt sind jedoch im Allgemeinen moderat und managebar, da der Datentransfer darauf ausgelegt ist, die Datensicherung und Backup-Aufgaben ins Cyber Vault-Storage-System zu verlagern. Beim ersten Beziehungs-Setup und beim ersten kompletten Backup wird eine beträchtliche Menge an Daten vom primären System auf das Cyber Vault-System (das SnapLock Compliance Volume) übertragen. Dies kann zu einem erhöhten Netzwerk-Traffic und einer höheren I/O-Last auf dem primären System führen. Nach Abschluss des ersten vollständigen Backups muss ONTAP nur noch die seit dem letzten Backup geänderten Blöcke nachverfolgen und übertragen. Dies führt zu einer wesentlich geringeren I/O-Last als bei der ersten Replizierung. Inkrementelle Updates sind effizient und haben nur minimale Auswirkungen auf die Performance des primären Storage. Der Vault-Prozess wird im Hintergrund ausgeführt, wodurch das Risiko von Beeinträchtigungen der Produktions-Workloads des primären Systems verringert wird.

- Wenn sichergestellt wird, dass das Storage-System über genügend Ressourcen (CPU, Arbeitsspeicher und IOPS) verfügt, um die zusätzliche Last bewältigen zu können, werden die Auswirkungen auf die Performance verringert.

Konfigurieren, Analysieren, cron-Skript

NetApp hat eine erstellt "Einzelnes Skript, das heruntergeladen werden kann"und verwendet, um Cyber-Vault-Beziehungen zu konfigurieren, zu überprüfen und zu planen.

Was dieses Skript tut

- Cluster-Peering
- SVM-Peering
- Erstellung von DP-Volumes
- SnapMirror Beziehung und Initialisierung
- Das für den Cyber-Vault verwendete ONTAP-System erhärten
- Legen Sie die Beziehung basierend auf dem Transferzeitplan still und setzen Sie sie fort
- Überprüfen Sie die Sicherheitseinstellungen regelmäßig, und erstellen Sie einen Bericht mit Anomalien

So verwenden Sie dieses Skript

"Das Skript herunterladen" 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 mithilfe der `.\` Syntax zusammen mit den erforderlichen Parametern aus

> Stellen Sie sicher, dass alle Informationen eingegeben wurden. Beim ersten Durchlauf (Konfigurationsmodus) fragt er nach Anmeldeinformationen für das Produktions- und das neue Cyber Vault-System. Danach werden die SVM-Peering (falls nicht vorhanden), die Volumes und die SnapMirror zwischen dem System erstellt und initialisiert.

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

Betriebsmodi

Das Automatisierungsskript bietet 3 Modi für die Ausführung - `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 luftgezapft.
- Analyse – automatisierte Überwachungs- und Berichtsfunktion zum Senden von Informationen an Überwachungsgruppen für Anomalien und verdächtige Aktivitäten, um sicherzustellen, dass die Konfigurationen nicht driften.
- Cron - um eine getrennte Infrastruktur zu aktivieren, automatisiert der cron-Modus die Deaktivierung der LIF und stellt die Transferbeziehung still.

Abhängig von der Systemleistung und der Datenmenge benötigen die Daten in diesen ausgewählten Volumes eine Weile.

```
./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 der ONTAP Cyber Vault PowerShell Lösung

Durch die Nutzung von Air-Gap-Technologie mit robusten Härtungsmethoden von ONTAP können Sie mit NetApp eine sichere, isolierte Storage-Umgebung schaffen, die widerstandsfähig gegen neue Cyberbedrohungen ist. All dies geschieht unter Beibehaltung der Flexibilität und Effizienz der vorhandenen Storage-Infrastruktur. Durch diesen sicheren Zugriff können Unternehmen ihre strengen Sicherheits- und Betriebszeitziele erreichen, wobei die bestehenden Mitarbeiter-, Prozess- und

Technologierahmen nur minimal verändert werden.

ONTAP Cyber Vault verwendet native Funktionen in ONTAP. Das ist ein einfacher Ansatz für zusätzlichen Schutz, um unveränderliche und nicht löschbare Kopien Ihrer Daten zu erstellen. Wenn Sie die allgemeine Sicherheitslage um den ONTAP-basierten Cyber-Vault von NetApp erweitern, werden Sie:

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