使用ONTAP Cyber Vault 進行資料保護

NetApp data management solutions

NetApp
January 28, 2026

目錄

使用ONTAP Cyber Vault 進行資料保護

ONTAP Cyber Vault 概述

需要實施網路保險庫的主要驅動威脅是網路攻擊（尤其是勒索軟體和資料外洩）的日益普遍和日益複雜化。"隨著網路釣魚的增多"以及越來越複雜的憑證竊取方法，用於發動勒索軟體攻擊的憑證隨後可用於存取基礎設施系統。在這些情況下，即使是堅固的基礎設施系統也面臨受到攻擊的風險。抵禦系統入侵的唯一方法是將資料保護並隔離在網路保險庫中。

NetApp 基於ONTAP的網路保險庫為組織提供了全面且靈活的解決方案來保護其最關鍵的資料資產。透過利用邏輯隔離和強大的強化方法， ONTAP使您能夠創建安全、隔離的儲存環境，以抵禦不斷演變的網路威脅。透過ONTAP，您可以確保資料的機密性、完整性和可用性，同時保持儲存基礎架構的靈活性和效率。

> 從 2024 年 7 月開始，先前以 PDF 形式發布的技術報告內容已與ONTAP產品文件整合。此外，諸如本文檔之類的新技術報告 (TR) 將不再獲得 TR 編號。

什麼是網路保險庫？

網路保險庫是一種特定的資料保護技術，涉及將關鍵資料儲存在與主要 IT 基礎設施分開的隔離環境中。

「氣隙」、*不可變*和*不可刪除*的資料儲存庫，可免受影響主網路的威脅，例如惡意軟體、勒索軟體甚至內部威脅。網路保險庫可透過*不可變*和*不可磨滅*的快照實現。

使用傳統方法的氣隙備份涉及創建空間並物理分離主媒體和輔助媒體。透過將媒體移出現場和/或切斷連接，不良行為者就無法存取資料。這可以保護數據，但會導致恢復時間變慢。

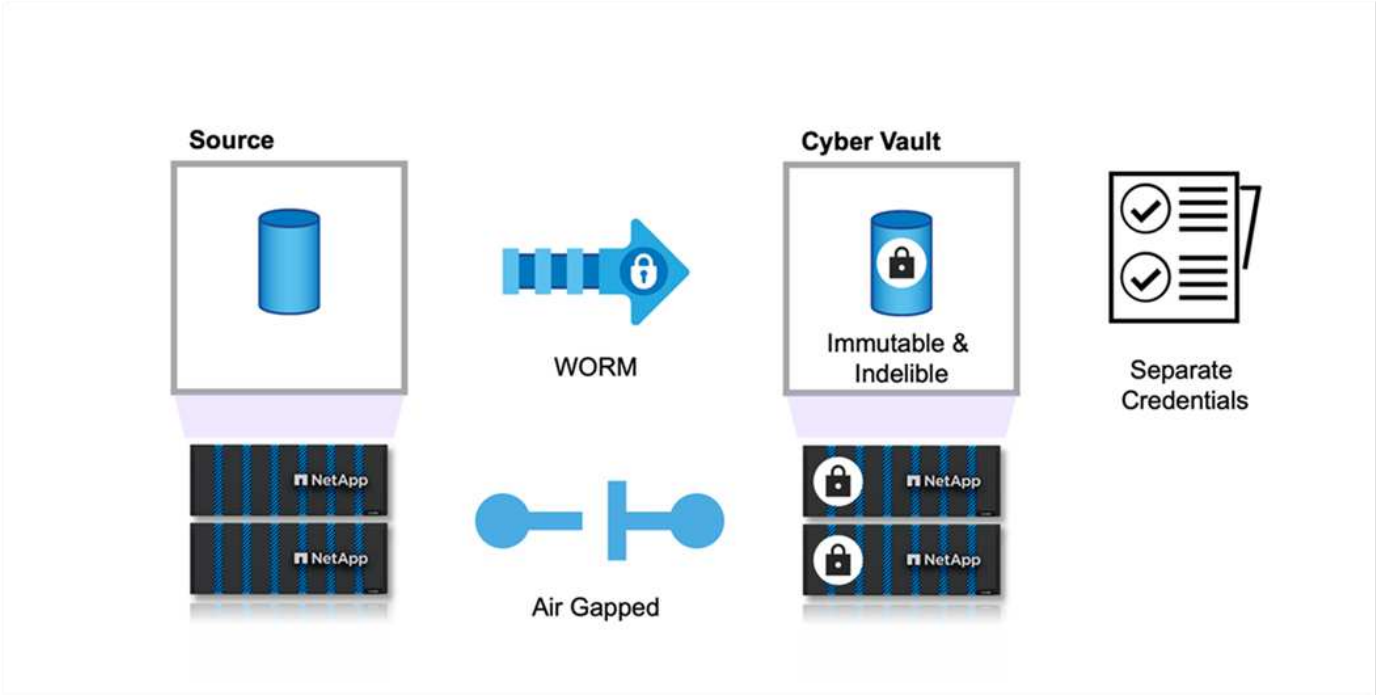
NetApp 的網路保險庫方法

NetApp網路保險庫參考架構的主要功能包括：

- 安全、獨立的儲存基礎架構（例如，隔離儲存系統）
- 資料副本必須毫無例外地*不可變*且*不可刪除*
- 嚴格的存取控制和多因素身份驗證
- 快速資料復原能力

您可以將NetApp儲存與ONTAP結合使用，作為隔離網路保險庫，方法是利用"SnapLock Compliance對 Snapshot 副本進行 WORM 保護"。您可以在 Cyber Vault 上執行所有基本的SnapLock Compliance任務。配置完成後，Cyber vault 磁碟區將自動受到保護，無需手動將 Snapshot 副本提交至 WORM。有關邏輯氣隙的更多信息，請參閱"部落格"

SnapLock Compliance用於遵守銀行和金融法規 SEC 70-a-4(f)、FINRA 4511(c) 和 CFTC 1.31(c)-(d)。該公司已通過 Cohasset Associates 認證，符合這些規定（可根據要求提供審計報告）。透過使用獲得此認證的SnapLock Compliance，您將獲得一種強化的資料隔離機制，世界上最大的金融機構依靠該機制來確保銀行記錄的保留和檢索。



Cyber Vault ONTAP術語

這些是網路保險庫架構中常用的術語。

自主勒索軟體防護 **(ARP)** - 自主勒索軟體防護 (ARP) 功能使用 NAS（NFS 和 SMB）環境中的工作負載分析來主動、即時地偵測並警告可能表明勒索軟體攻擊的異常活動。當懷疑受到攻擊時，ARP 除了現有的計畫 Snapshot 副本保護之外，還會建立新的 Snapshot 副本。有關詳細信息，請參閱"ONTAP關於自主勒索軟體防護的文檔"

氣隙（邏輯） - 您可以利用以下方式將帶有ONTAP的NetApp儲存配置為邏輯氣隙網路保險庫："SnapLock Compliance對 Snapshot 副本進行 WORM 保護"

氣隙（實體） - 實體氣隙系統沒有網路連線。使用磁帶備份，您可以將影像移動到另一個位置。 SnapLock Compliance邏輯氣隙與實體氣隙系統一樣強大。

堡壘主機 - 隔離網路上的專用計算機，配置用於抵禦攻擊。

不可變的 **Snapshot** 副本 - 無法修改的 Snapshot 副本，無一例外（包括支援組織或對儲存系統進行低階格式化的能力）。

不可刪除的 **Snapshot** 副本 - 無法刪除的 Snapshot 副本，無例外（包括支援組織或對儲存系統進行低階格式化的能力）。

防篡改 **Snapshot** 副本 - 防篡改 Snapshot 副本使用SnapLock Compliance時脈功能將 Snapshot 副本鎖定指定時段。任何使用者或NetApp支援人員都無法刪除這些鎖定的快照。如果磁碟區受到勒索軟體攻擊、惡意軟體、駭客、惡意管理員或意外刪除的威脅，您可以使用鎖定的 Snapshot 副本來復原資料。有關詳細信息，請參閱"有關防篡改 Snapshot 副本的ONTAP文檔"

- SnapLock* - SnapLock是一種高效能合規解決方案，適用於使用 WORM 儲存以未修改的形式保留文件以滿足監管和治理目的的組織。有關更多信息，請參閱"有關SnapLock的ONTAP文檔" 。
- SnapMirror* - SnapMirror是一種災難復原複製技術，旨在高效複製資料。 SnapMirror可以為本機或雲端中

的輔助系統建立鏡像（或資料的精確副本）、保管庫（具有較長 Snapshot 副本保留期的資料副本）或兩者。這些副本可用於許多不同的目的，例如災難、雲端爆發或網路保險庫（使用保險庫策略並鎖定保險庫時）。有關詳細信息，請參閱"有關SnapMirror的ONTAP文檔"

- SnapVault* - 在ONTAP 9.3 中， SnapVault已被棄用，取而代之的是使用 vault 或 mirror-vault 政策配置SnapMirror 。這個術語雖然仍在使用，但也已被貶低。有關更多信息，請參閱"有關SnapVault的ONTAP文檔" 。

使用ONTAP調整網路保險庫大小

確定網路保險庫的規模需要了解在給定的恢復時間目標 (RTO) 內需要恢復多少資料。許多因素都會影響到正確設計合適規模的網路保險庫解決方案。在決定網路保險庫的規模時，必須同時考慮效能和容量。

性能大小考慮因素

1. 源平台型號有哪些（FAS v AFF A 系列 v AFF C 系列）？
2. 來源和網路庫之間的頻寬和延遲是多少？
3. 文件大小有多大以及有多少個文件？
4. 您的復原時間目標是什麼？
5. 您需要在 RTO 內恢復多少資料？
6. 網路保險庫將吸收多少個SnapMirror扇入關係？
7. 是否會同時發生單次或多次恢復？
8. 這些多次恢復是否會發生在同一個主伺服器上？
9. 從保管庫恢復期間， SnapMirror是否會複製到保管庫？

尺寸範例

以下是不同網路保險庫配置的範例。

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

容量大小考慮因素

ONTAP Cyber Vault 目標磁碟區所需的磁碟空間量取決於多種因素，其中最重要的是來源磁碟區中資料的變化率。目標磁碟區上的備份計畫和快照計畫都會影響目標磁碟區上的磁碟使用情況，而來源磁碟區上的變更率可能不會保持恆定。最好提供額外的儲存容量緩衝區，以滿足未來最終用戶或應用程式行為變化的需求。

在ONTAP中確定 1 個月保留關係的大小需要根據多種因素計算儲存需求，包括主資料集的大小、資料變化率（

每日變化率）以及重複資料刪除和壓縮節省（如果適用）。

以下是逐步方法：

第一步是了解使用網路保險庫保護的來源磁碟區的大小。這是最初複製到網路保險庫目的地的基本資料量。接下來，估計資料集的每日變化率。這是每天變化的數據百分比。充分了解資料的動態性至關重要。

例如：

- 主資料集大小 = 5TB
- 每日變化率=5%（0.05）
- 重複資料刪除和壓縮效率 = 50% (0.50)

現在，讓我們來看看計算過程：

- 計算每日數據變化率：

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

- 計算30天的總變化數據：

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

- 計算所需的總儲存量：

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

- 應用重複資料刪除和壓縮節省：

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

儲存需求摘要

- 如果效率不高：儲存 30 天的網路保險庫資料將需要 **12.5TB**。
- 效率為 50%：重複資料刪除和壓縮後需要 **6.25TB** 的儲存空間。

> 快照副本可能會因元資料而產生額外的開銷，但這通常很小。

> 如果每天進行多次備份，則根據每天拍攝的 Snapshot 副本數量調整計算。

> 考慮資料隨時間的成長，以確保規模適合未來。

使用ONTAP建立網路保險庫

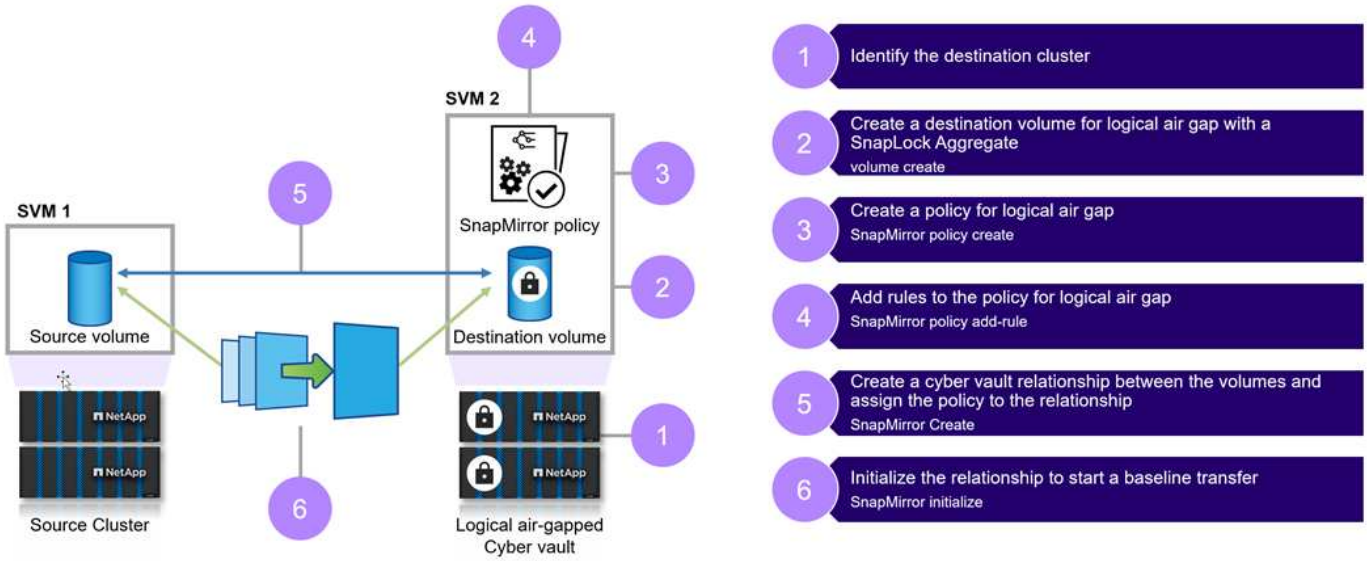
以下步驟將有助於使用ONTAP建立網路保險庫。

開始之前

- 來源叢集必須運行ONTAP 9 或更高版本。
- 來源聚合和目標聚合必須是 64 位元。
- 必須在具有對等 SVM 的對等叢集中建立來源磁碟區和目標磁碟區。有關更多信息，請參閱"集群對等連接"。
- 如果停用磁碟區自動成長，則目標磁碟區上的可用空間必須至少比來源磁碟區上的已使用空間多 5%。

關於此任務

下圖顯示了初始化SnapLock Compliance保險庫關係的過程：



步驟

1. 確定目標陣列將成為接收隔離資料的網路保險庫。
2. 在目標陣列上，準備網路保險庫，"安裝ONTAP One 許可證" ，"初始化合規時鐘" ，如果您使用的是 9.10.1 之前的ONTAP版本，"建立SnapLock Compliance聚合" 。
3. 在目標陣列上，建立 DP 類型的SnapLock Compliance目標磁碟區：

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

4. 從ONTAP 9.10.1 開始， SnapLock和非SnapLock磁碟區可以存在於同一個聚合上；因此，如果您使用ONTAP 9.10.1，則不再需要建立單獨的SnapLock聚合。您使用音量 `-snaplock-type`選項來指定合規性類型。在ONTAP 9.10.1 之前的ONTAP版本中， SnapLock模式、Compliance 是從聚合繼承的。不支援版本靈活的目標磁碟區。目標磁碟區的語言設定必須與來源磁碟區的語言設定相符。

   以下命令將建立一個名為 2 GB 的SnapLock Compliance卷 `dstvolB`在 `SVM2`總體而言 `node01_aggr`：

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

5. 在目標群集上，要建立氣隙，請設定預設保留期，如中所述"設定預設保留期"。作為保管庫目標的SnapLock磁碟區具有指派的預設保留期。此期限的數值最初設定為最短 0 年，最長 100 年（從ONTAP 9.10.1 開始）。對於早期版本的ONTAP ，對於SnapLock Compliance卷，該值為 0 - 70。每個NetApp Snapshot 副本

最初都遵循此預設保留期。必須更改預設保留期。如有需要，保留期可以延長，但絕對不能縮短。有關更多信息，請參閱"設定保留時間概述" 。

> 服務提供者在決定保留期間應考慮客戶的合約結束日期。例如，如果網路保險庫的保留期為 30 天，而客戶的合約在保留期到期之前結束，則網路保險庫中的資料在保留期到期之前不能被刪除。

6. "建立新的複製關係"非SnapLock來源和您在步驟 3 中建立的新SnapLock目標之間。

   此範例使用 XDPDefault 策略建立與目標SnapLock磁碟區 dstvolB 的新SnapMirror關係，以按小時計劃儲存標記為每日和每週的 Snapshot 副本：

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

   "建立自訂複製策略"或"自訂時間表"如果可用的預設值不合適。

7. 在目標 SVM 上，初始化在步驟 5 中建立的SnapVault關係：

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

8. 以下命令初始化 SVM1 上的來源磁碟區 srcvolA 與 SVM2 上的目標磁碟區 dstvolB 之間的關係：

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

9. 關係初始化並處於空閒狀態後，使用目標上的 snapshot show 指令來驗證套用於複製的 Snapshot 副本的SnapLock到期時間。

   此範例列出了磁碟區 dstvolB 上具有SnapMirror標籤和SnapLock到期日的 Snapshot 副本：

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

網路保險庫強化

這些都是強化ONTAP網路保險庫的額外建議。請參閱下面的ONTAP強化指南以取得更多建議和程序。

網路保險庫強化建議

- 隔離網路保險庫的管理平面
- 不要在目標叢集上啟用資料 LIF，因為它們是額外的攻擊媒介
- 在目標叢集上，使用服務策略限制對來源叢集的叢集間 LIF 存取
- 使用服務策略和堡壘主機對目標叢集上的管理 LIF 進行分段，以限制訪問
- 限制從來源叢集到網路保管庫的所有資料流量，僅允許SnapMirror流量所需的連接埠
- 盡可能停用ONTAP中任何不需要的管理存取方法，以減少攻擊面
- 啟用稽核日誌記錄和遠端日誌存儲

- 啟用多重管理員驗證，並要求常規儲存管理員以外的管理員（例如 CISO 員工）進行驗證
- 實施基於角色的存取控制
- 請系統管理員和 ssh 進行多因素管理身份驗證
- 對腳本和 REST API 呼叫使用基於令牌的身份驗證

請參閱"ONTAP強化指南"，"多管理員驗證概述"和"ONTAP多重因素驗證指南"如何完成這些強化步驟。

網路保險庫互通性

ONTAP硬體和軟體可用於建立網路保險庫配置。

ONTAP硬體建議

所有ONTAP統一實體陣列均可用於網路保險庫實作。

- FAS混合儲存提供了最具成本效益的解決方案。
- AFF C 系列提供最高效的耗電量和密度。
- AFF A 系列是效能最高的平台，提供最佳的 RTO。隨著我們最新AFF A 系列的發布，該平台將提供最佳的儲存效率，同時不影響效能。

ONTAP軟體建議

從ONTAP 9.14.1 開始，您可以在SnapMirror關係的SnapMirror政策中為特定SnapMirror標籤指定保留期，以便從來源磁碟區到目標磁碟區複製的 Snapshot 副本保留規則中指定的保留期。如果未指定保留期，則使用目標磁碟區的預設保留期。

從ONTAP 9.13.1 開始，您可以透過建立FlexClone並將 snaplock-type 選項設為“non-snaplock”並在執行磁碟區複製建立操作時將 Snapshot 副本指定為“parent-snapshot”，從而立即恢復SnapLockSnapLock庫關係的目標 SnapLock 磁碟區上的副本鎖定 Snapshot 副本。詳細了解"建立具有SnapLock類型的FlexClone磁碟區" 。

MetroCluster配置

對於MetroCluster配置，您應該注意以下事項：

- 您只能在同步來源 SVM 之間建立SnapVault關係，而不能在同步來源 SVM 和同步目標 SVM 之間建立 SnapVault 關係。
- 您可以建立從同步來源 SVM 上的磁碟區到資料服務 SVM 的SnapVault關係。
- 您可以建立從資料服務 SVM 上的磁碟區到同步來源 SVM 上的 DP 磁碟區的SnapVault關係。

網路保險庫常見問題解答

此常見問題適用於NetApp客戶和合作夥伴。它回答了有關 NetApp 基於ONTAP的網路保險庫參考架構的常見問題。

什麼是NetApp網路保險庫？

網路保險庫是一種特定的資料保護技術，涉及將資料儲存在與主要 IT 基礎設施分開的隔離環境中。

網路保險庫是一個「隔離的」、不可變的、不可磨滅的資料儲存庫，可以免受影響主要資料的威脅，例如惡意軟體、勒索軟體或內部威脅。可以使用不可變的NetApp ONTAP Snapshot 副本實現網路保險庫，並使用NetApp SnapLock Compliance使其不可磨滅。在SnapLock Compliance保護下，資料無法被修改或刪除，即使是ONTAP管理員或NetApp支援人員也無法修改或刪除。

使用傳統方法的氣隙備份涉及創建空間並物理分離主媒體和輔助媒體。網路保險庫的氣隙隔離包括使用標準資料存取網路以外的單獨資料複製網路將 Snapshot 副本複製到不可磨滅的目的地。

除了隔離網路之外，進一步的措施還包括在不需要時停用網路保險庫上的所有資料存取和複製協議。這可以防止目標站點的資料存取或資料外洩。有了SnapLock Compliance，就不需要物理分離。 SnapLock Compliance可保護您儲存的、時間點的、唯讀的 Snapshot 副本，從而實現快速資料恢復，確保資料不會被刪除且無法改變。

NetApp 的網路保險庫方法

NetApp網路保險庫由SnapLock提供支持，為組織提供全面且靈活的解決方案來保護其最關鍵的資料資產。透過利用ONTAP中的強化技術， NetApp讓您能夠建立一個安全、隔離且氣隙封閉的網路保險庫，以抵禦不斷演變的網路威脅。透過NetApp，您可以確保資料的機密性、完整性和可用性，同時保持儲存基礎架構的靈活性和效率。

NetApp網路保險庫參考架構的主要功能包括：

- 安全、獨立的儲存基礎架構（例如，隔離儲存系統）
- 您的資料的備份是不可改變且不可消除的
- 嚴格且獨立的存取控制、多管理員驗證和多因素身份驗證
- 快速資料復原能力

網路保險庫常見問題解答

cyber vault 是NetApp的產品嗎？

不，「網路保險庫」是一個行業通用的術語。 NetApp創建了一個參考架構，讓客戶可以輕鬆建立自己的網路保險庫，並利用數十種ONTAP安全功能來幫助保護他們的資料免受網路威脅。更多資訊請訪問"ONTAP文件站點"。

NetApp的網路保險庫是否只是 LockVault 或SnapVault的另一個名稱？

LockVault 是Data ONTAP 7 模式的功能，在目前版本的ONTAP中不可用。

SnapVault是一個遺留術語，指的是現在透過 SnapMirror 的保險庫策略實現的功能。此策略允許目標保留與來源磁碟區不同數量的 Snapshot 副本。

Cyber vault 將SnapMirror與保險庫策略和SnapLock Compliance結合使用，以建立不可變且不可消除的資料副本。

我可以將哪種**NetApp**硬體用於網路保險庫、 **FAS**、容量快閃記憶體或效能快閃記憶體？

此網路保險庫參考架構適用於整個ONTAP硬體產品組合。客戶可以使用AFF A 系列、 AFF C 系列或FAS平台作為保險庫。基於快閃記憶體的平台將提供最快的恢復時間，而基於磁碟的平台將提供最具成本效益的解決方案。根據要恢復的資料量以及是否同時進行多個恢復，使用基於磁碟的系統（FAS）可能需要幾天到幾週才能完成。請諮詢NetApp或合作夥伴代表，以適當調整網路保險庫解決方案的規模來滿足業務需求。

我可以使用**Cloud Volumes ONTAP**作為網路保險庫來源嗎？

是的，但是使用 CVO 作為來源需要將資料複製到本地網路保險庫目標，因為SnapLock Compliance是ONTAP網路保險庫的要求。從基於超大規模的 CVO 執行個體進行資料複製可能會產生出口費用。

我可以使用**Cloud Volumes ONTAP**作為網路保險庫目標嗎？

Cyber Vault 架構依賴 ONTAP 的SnapLock Compliance 的不可磨滅性，專為本地實施而設計。基於雲端的 Cyber Vault 架構正在接受調查，以便將來發布。

我可以使用**ONTAP Select**作為網路保險庫來源嗎？

是的， ONTAP Select可以用作基於本地硬體的網路保險庫目標的來源。

我可以使用**ONTAP Select**作為網路保險庫目標嗎？

不可以， ONTAP Select不應用作網路保險庫目標，因為它不具備使用SnapLock Compliance 的能力。

NetApp的網路保險庫是否只使用**SnapMirror**？

不是， NetApp網路保險庫架構利用許多ONTAP功能來創建安全、隔離、隔離和強化的資料副本。有關可使用哪些附加技術的更多信息，請參閱下一個問題。

網路保險庫是否使用了其他技術或配置？

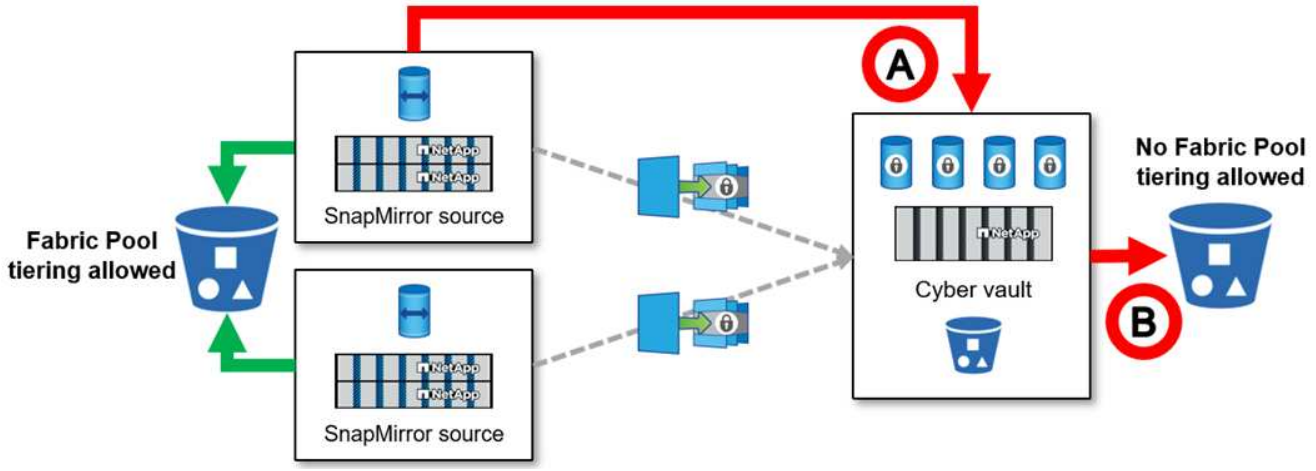
NetApp網路保險庫的基礎是SnapMirror和SnapLock Compliance，但使用其他ONTAP功能（如防篡改 Snapshot 副本、多因素身份驗證 (MFA)、多管理員驗證、基於角色的存取控制以及遠端和本地審計日誌記錄）可提高資料的安全性。

對於網路保險庫來說， **ONTAP Snapshot** 副本為何比其他副本更勝一籌？

ONTAP Snapshot 副本預設是不可變的，並且可以透過SnapLock Compliance使其不可消除。甚至連NetApp支援也無法刪除SnapLock Snapshot 副本。更好的問題是，是什麼讓NetApp網路保險庫比業界其他網路保險庫更好。首先， ONTAP是地球上最安全的存儲，並已獲得 CSfC 驗證，可在硬體和軟體層靜態儲存機密和絕密資料。更多資訊"CSfC 可以在這裡找到"。此外， ONTAP可以在儲存層進行隔離，並由網路保險庫系統控制複製，因此可以在網路保險庫網路內建立隔離。

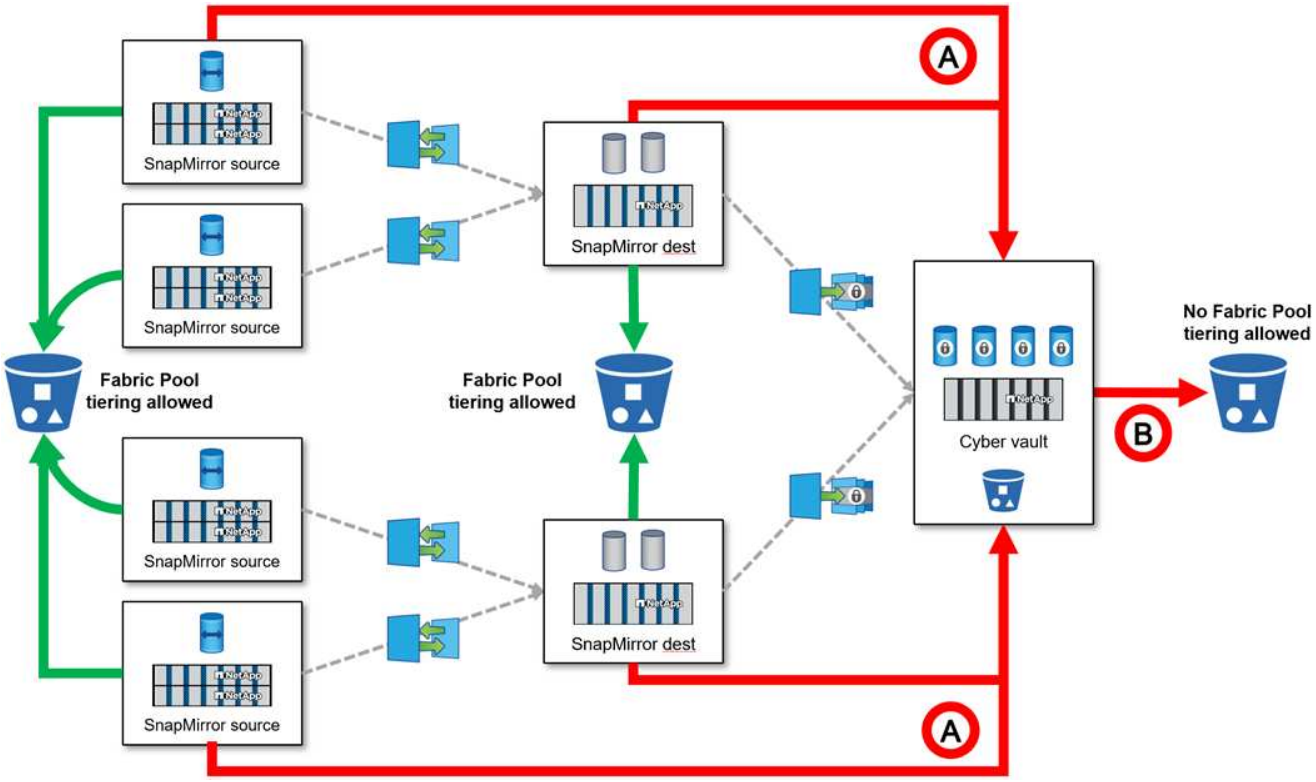
網路保險庫上的磁碟區可以使用**ONTAP Fabric** 池嗎？

不可以，無論策略如何，網路保險庫磁碟區（SnapLock Compliance SnapMirror目標）都不能使用 Fabric Pool 進行分層。



在多種情況下，Fabric 池不能與網路保險庫一起使用。

1. Fabric Pool 冷層*不能*使用網路保險庫叢集。這是因為啟用 S3 協定會使網路保險庫參考架構的安全性失效。此外，用於 Fabric 池的 S3 儲存桶無法受到保護。
2. 由於資料被鎖定在磁碟區中，網路保險庫上的SnapLock Compliance磁碟區*不能*分層到 S3 儲存桶。



ONTAP S3 Worm 可以在網路保險庫中使用嗎？

不，S3 是一種資料存取協議，它使參考架構的安全性無效。

NetApp Cyber Vault 是否在不同的**ONTAP**個性或設定檔上運作？

不，這是一個參考架構。客戶可以使用"參考架構"並建立一個網路保險庫，或可以使用"用於建立、強化和驗證的 PowerShell 腳本"一個網路保險庫。

我可以在網路保險庫中開啟 **NFS**、**SMB** 和 **S3** 等資料協定嗎？

預設情況下，應停用網路保險庫上的資料協定以確保其安全。但是，可以在網路保險庫上啟用資料協定來存取資料以進行復原或在需要時存取資料。這應該是臨時進行的，並在恢復完成後停用。

您可以將現有的**SnapVault**環境轉換為網路保險庫嗎？還是需要重新播種所有內容？

是的。可以採用一個作為SnapMirror目標的系統（具有保管庫策略），停用資料協議，並根據"ONTAP強化指南"，將其隔離在安全的位置，並按照參考架構中的其他程序使其成為網路保險庫，而無需重新播種目的地。

*還有其他問題嗎？ *請發送電子郵件至 ng-cyber-vault@netapp.com 並提出您的問題！我們將回覆您的問題並將其添加到常見問題解答中。

網路保險庫資源

要了解有關此網路保險庫資訊中所述的資訊的更多信息，請參閱以下附加資訊和安全概念。

- "NetApp網路保險庫：多層資料保護解決方案簡介"
- "NetApp以業界首款 AI 驅動的盒內勒索軟體偵測解決方案榮獲 AAA 評級"
- "利用全球最安全的儲存提升網路彈性"
- "ONTAP安全強化指南"
- "NetApp零信任"
- "NetApp網路彈性"
- "NetApp資料保護"
- "使用 CLI 的叢集和 SVM 對等概述"
- "SnapVault歸檔"
- "配置、分析、cron腳本"

使用 **PowerShell** 建立、強化和驗證**ONTAP**網路保管庫

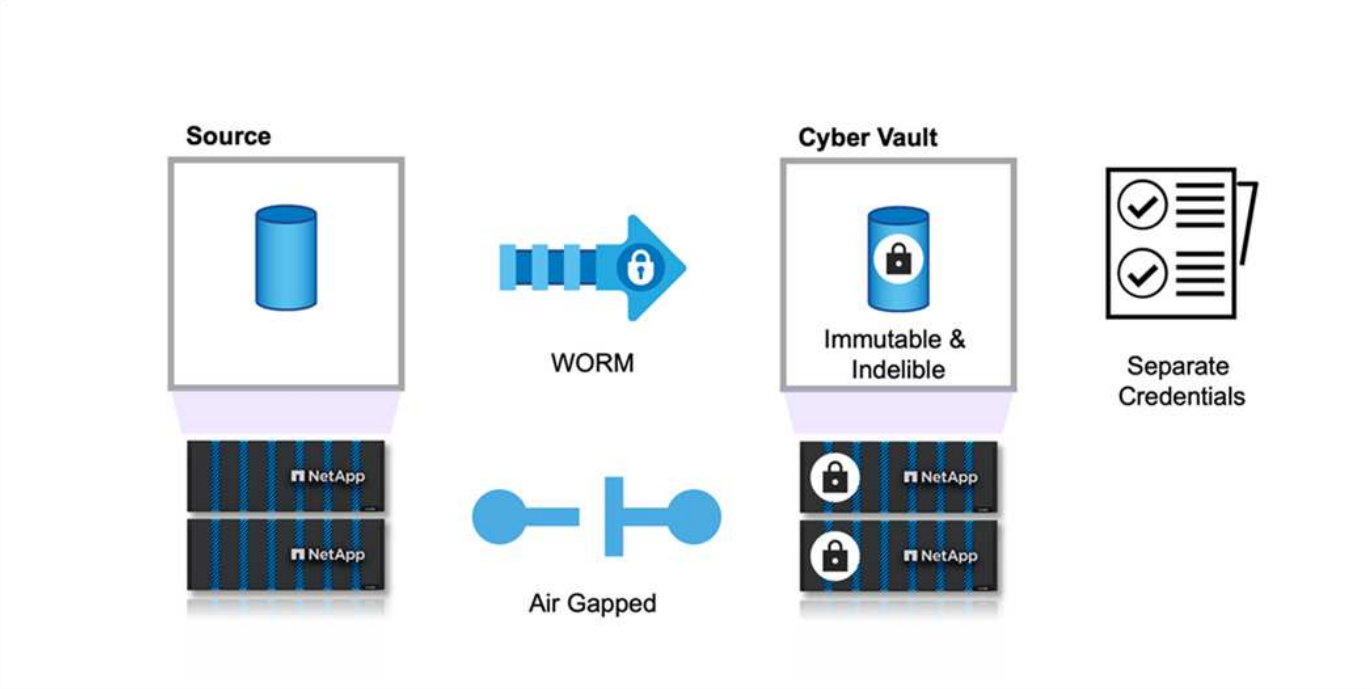
使用 **PowerShell** 的**ONTAP Cyber Vault** 概述

在當今的數位環境中，保護組織的關鍵資料資產不僅是一種最佳實踐，更是業務的當務之急。網路威脅正以前所未有的速度發展，傳統的資料保護措施已不足以確保敏感資訊的安全。這就是網路保險庫的作用所在。 NetApp 基於ONTAP的尖端解決方案將先進的隔離技術與強大的資料保護措施相結合，以創造出抵禦網路威脅的堅不可摧的屏障。透過使用安全強化技術隔離最有價值的數據，網路保險庫可以最大限度地減少攻擊面，從而確保最關鍵的數據在需要時保持機密、完整且隨時可用。

網路保險庫是一種安全的儲存設施，由防火牆、網路和儲存等多層保護組成。這些組件可保護關鍵業務運作所需的重要復原資料。網路保險庫的組件會根據保險庫策略定期與基本生產資料同步，但除此之外仍然無法存取。這種隔離且斷開的設定確保在發生危害生產環境的網路攻擊時，可以輕鬆地從網路保險庫進行可靠的最終恢復。

NetApp透過設定網路、停用 LIF、更新防火牆規則以及將系統與外部網路和網際網路隔離，輕鬆為網路保險庫建立隔離間隙。這種強大的方法有效地將系統與外部網路和互聯網斷開，提供無與倫比的保護，防止遠端網路攻擊和未經授權的存取嘗試，使系統免受基於網路的威脅和入侵。

將此與SnapLock Compliance保護相結合，資料無法被修改或刪除，即使是ONTAP管理員或NetApp支援人員也無法修改或刪除。 SnapLock定期接受 SEC 和 FINRA 法規的審核，確保資料彈性符合銀行業嚴格的 WORM 和資料保留法規。 NetApp是唯一經過 NSA CSfC 驗證可以儲存絕密資料的企業儲存公司。

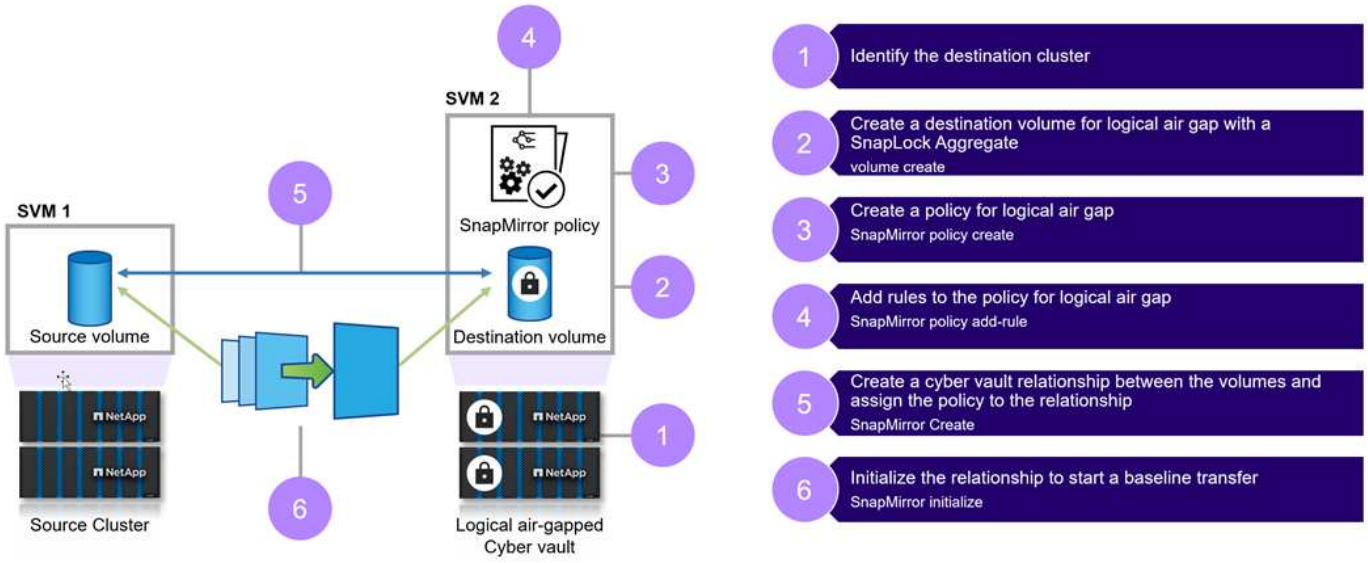


本文檔介紹了 NetApp 的網路保險庫如何從本地ONTAP存儲自動配置到另一個指定的ONTAP存儲，並使用不可變快照增加額外的保護層來防止網路攻擊，從而實現快速恢復。作為此架構的一部分，整個配置均依照ONTAP最佳實務應用。最後一部分介紹了在發生攻擊時執行恢復的說明。

同樣的解決方案也適用於使用 FSx ONTAP在 AWS 中建立指定的網路保險庫。

建立**ONTAP**網路保險庫的高階步驟

- 創建對等關係
  - 使用ONTAP儲存的生產站點與指定的網路保管庫ONTAP儲存對等
- 創建SnapLock Compliance卷
- 設定SnapMirror關係和規則以設定標籤
  - 已配置SnapMirror關係和適當的計劃
- 在啟動SnapMirror （保管庫）傳輸之前設定保留
  - 對複製的資料套用保留鎖，進一步防止資料被任何內部人員竊取或資料故障。使用此功能，在保留期到期之前無法刪除數據
  - 組織可以根據自己的需求將這些數據保存幾週/幾個月
- 根據標籤初始化SnapMirror關係
  - 初始播種和永久增量傳輸根據SnapMirror計劃進行
  - 資料受到SnapLock合規性的保護（不可變且不可刪除），且資料可供恢復
- 實施嚴格的資料傳輸控制
  - 網路保險庫在有限的時間內解鎖，包含來自生產現場的數據，並與保險庫中的數據同步。傳輸完成後，連線中斷、關閉並再次鎖定
- 快速恢復
  - 如果生產站點的主要資料受到影響，則網路保險庫中的資料可以安全地恢復到原始生產環境或其他選定的環境



解決方案組件

NetApp ONTAP在來源叢集和目標叢集上執行 9.15.1。

ONTAP One： NetApp ONTAP 的一體化授權。

ONTAP One 授權所使用的功能：

- SnapLock Compliance
- SnapMirror
- 多管理員驗證
- ONTAP提供的所有增強功能
- 為網路保險庫提供單獨的 RBAC 憑證

所有ONTAP統一實體陣列均可用於網路保險庫，但基於AFF C 系列容量的快閃記憶體系統和FAS混合快閃記憶體系統是實現此目的最具成本效益的理想平台。請諮詢"ONTAP網路保險庫大小調整"以獲得尺寸指導。

使用 **PowerShell** 建立**ONTAP**網路保險庫

使用傳統方法的氣隙備份涉及創建空間並物理分離主媒體和輔助媒體。透過將媒體移出現場和/或切斷連接，不良行為者就無法存取資料。這可以保護數據，但會導致恢復時間變慢。有了SnapLock Compliance，就不需要物理分離。 SnapLock Compliance保護儲存的快照時間點、唯讀副本，讓資料可快速存取、不會被刪除或無法擦除，也不會被修改或無法變更。

先決條件

在開始執行本文檔下一部分中的步驟之前，請確保滿足以下先決條件：

- 來源叢集必須運行ONTAP 9 或更高版本。
- 來源聚合和目標聚合必須是 64 位元。
- 來源集群和目標集群必須對等。
- 來源 SVM 和目標 SVM 必須對等。
- 確保叢集對等加密已啟用。

設定到ONTAP網路保險庫的資料傳輸需要幾個步驟。在主磁碟區上，設定快照策略，使用適當的計畫指定要建立哪些副本以及何時建立這些副本，並指派標籤以指定應由SnapVault傳送哪些副本。在輔助伺服器上，必須建立一個SnapMirror策略，指定要傳輸的 Snapshot 副本的標籤以及應在網路保管庫中保留多少個副本。配置這些策略後，建立SnapVault關係並建立傳輸計劃。

本文檔假設主儲存和指定的ONTAP網路保險庫已經設定和設定。

Cyber vault 叢集可以與來源資料位於相同或不同的資料中心。

建立**ONTAP**網路保險庫的步驟

1. 使用ONTAP CLI 或系統管理員初始化合規時脈。
2. 建立啟用了SnapLock合規性的資料保護磁碟區。
3. 使用SnapMirror create 指令建立SnapVault資料保護關係。
4. 設定目標磁碟區的預設SnapLock Compliance保留期。

預設保留時間為「設定為最小值」。作為保管庫目標的SnapLock磁碟區具有指派的預設保留期。此期限的數值最初設定為最短 0 年，最長 100 年（從ONTAP 9.10.1 開始）。對於早期版本的ONTAP ，對於SnapLock Compliance卷，該值為 0 - 70。每個NetApp Snapshot 副本最初都遵循此預設保留期。如有需要，保留期可以延長，但絕對不能縮短。有關更多信息，請參閱"設定保留時間概述" 。

以上包括手動步驟。安全專家建議將流程自動化，以避免手動管理帶來的巨大錯誤。以下是完全自動化SnapLock合規性的先決條件和配置以及時脈初始化的程式碼片段。

以下是初始化ONTAP合規時脈的 PowerShell 程式碼範例。

```
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
    }
}
```

以下是設定ONTAP網路保險庫的 PowerShell 程式碼範例。

```
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. 完成上述步驟後，使用SnapLock Compliance和SnapVault 的隔離網路保險庫就準備好了。

在將快照資料傳輸到網路保管庫之前，必須初始化SnapVault關係。然而，在此之前，必須進行安全性強化以確保保險庫的安全。

使用 PowerShell 強化ONTAP Cyber Vault

與傳統解決方案相比， ONTAP網路保險庫具有更好的抵禦網路攻擊的能力。在設計增強安全性的架構時，考慮減少攻擊面的措施至關重要。這可以透過各種方法實現，例如實施強化密碼策略、啟用 RBAC、鎖定預設使用者帳戶、配置防火牆以及利用審批流程對保險庫系統進行任何更改。此外，限制特定 IP 位址的網路存取協定有助於限制潛在的漏洞。

ONTAP提供了一組控制措施，可以強化ONTAP儲存。使用"ONTAP的指導和配置設定"幫助組織滿足資訊系統機密性、完整性和可用性的規定安全目標。

強化最佳實踐

手動步驟

1. 建立具有預先定義和自訂管理角色的指定使用者。
2. 建立新的 IP 空間來隔離網路流量。
3. 建立駐留在新 IP 空間中的新 SVM。
4. 確保防火牆路由策略配置正確，並且所有規則都定期審核並根據需要更新。

ONTAP CLI 或透過自動化腳本

1. 除了多因素身份驗證（MFA）之外，還透過多管理員驗證（MAV）來保護管理，從而增強對資料儲存 VM 的管理存取的安全性。
2. 啟用集群之間「傳輸中」的標準資料加密。
3. 使用強加密密碼保護 SSH 並強制使用安全密碼。
4. 啟用全域 FIPS。
5. 應停用 Telnet 和遠端 Shell (RSH)。
6. 鎖定預設管理員帳戶。
7. 停用資料 LIF 並保護遠端存取點。
8. 停用並刪除未使用或多餘的協定和服務。
9. 加密網路流量。
10. 設定超級使用者和管理角色時使用最小特權原則。
11. 使用允許的 IP 選項限制來自特定 IP 位址的 HTTPS 和 SSH。
12. 根據傳輸計劃停止並恢復複製。

項目 1-4 需要手動幹預，例如指定隔離網路、隔離 IP 空間等，並且需要事先執行。有關配置強化的詳細信息，請參閱"ONTAP安全強化指南"。其餘部分可以輕鬆自動化，以便於部署和監控。這種精心設計的方法的目的是提供一種機制來自動化強化步驟，以確保保險庫控制器的未來安全。網路保險庫隔離間隙打開的時間範圍盡可能短。 SnapVault利用永久增量技術，該技術只會將自上次更新以來的變更移至網路保險庫中，從而最大限度地減少網路保險庫必須保持開放的時間。為了進一步優化工作流程，網路保險庫的開放與複製計劃相協調，以確保最小的連接視窗。

以下是用於強化ONTAP控制器的 PowerShell 程式碼範例。

```
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
    }
}
```

使用 PowerShell 驗證ONTAP網路保險庫

強大的網路保險庫應該能夠抵禦複雜的攻擊，即使攻擊者擁有以提升的權限存取環境的憑證。

一旦規則到位，嘗試（假設攻擊者能夠以某種方式進入）刪除保險庫端的快照將會失敗。透過施加必要的限制和保護系統，所有強化設定均適用相同的規定。

PowerShell 程式碼範例，用於按計劃驗證配置。

```
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
    }
}
```

此螢幕截圖顯示保險庫控制器上沒有連線。

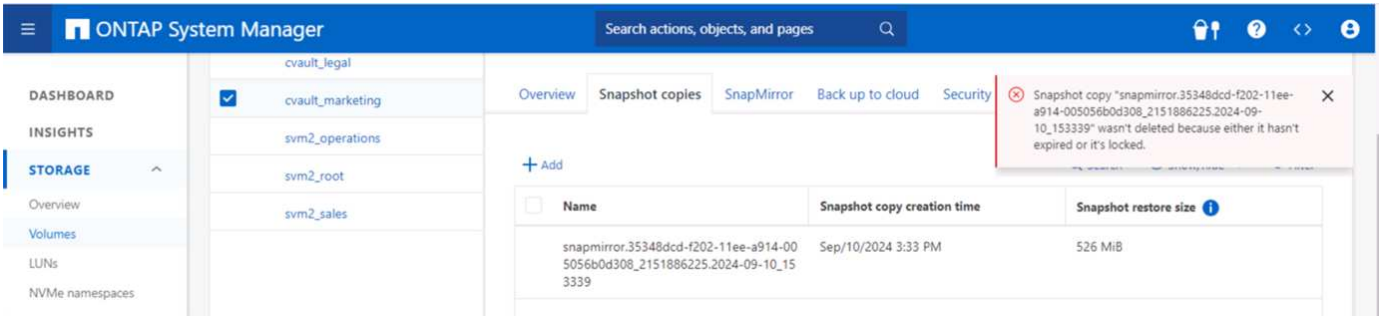
```
cluster2::> network connections  listening show
This table is currently empty.

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

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

cluster2::>
```

該螢幕截圖顯示快照無法被竄改。



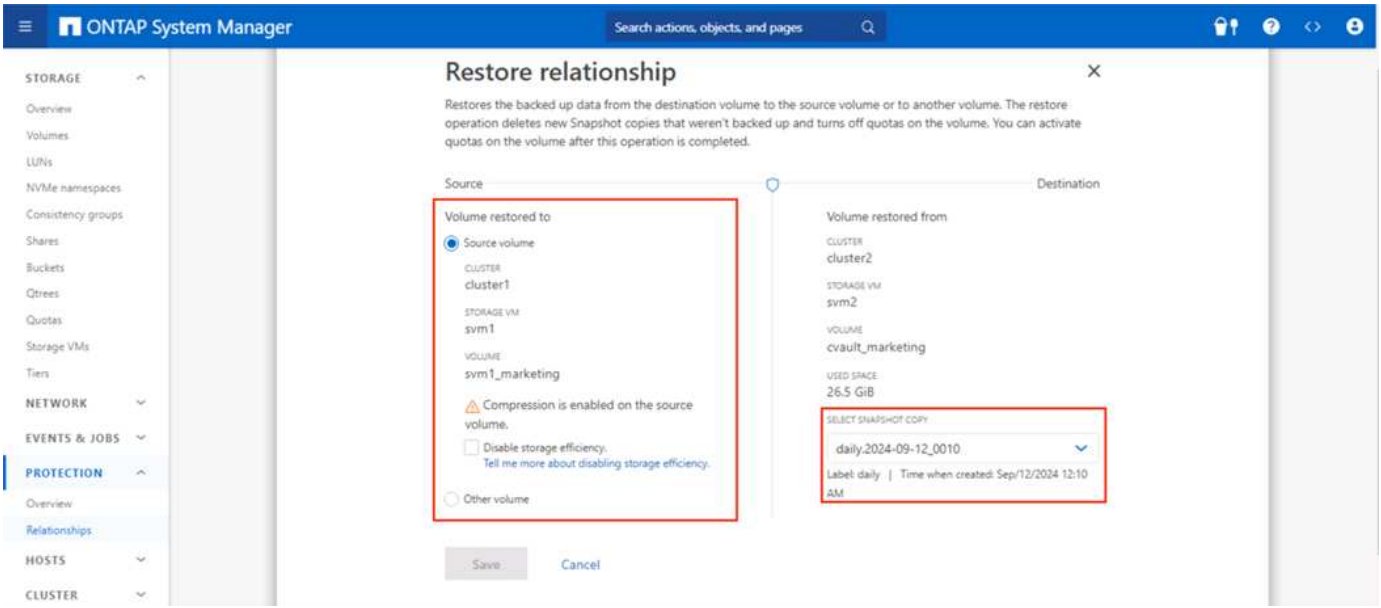
若要驗證並確認氣隙功能，請依照下列步驟操作：

- 測試網路隔離功能以及在未傳輸資料時停止連線的能力。
- 驗證管理介面不能從允許的 IP 位址之外的任何實體存取。
- 驗證多管理員驗證是否到位以提供額外的批准層。
- 驗證透過 CLI 和 REST API 存取的能力
- 從源頭觸發保險庫的傳輸操作，並確保保險庫副本無法被修改。
- 嘗試刪除傳輸到保管庫的不可變快照副本。
- 嘗試透過竄改系統時鐘來修改保留期。

ONTAP網路保險庫資料恢復

如果生產資料中心的資料被破壞，則可以將網路保險庫中的資料安全地恢復到所選環境。與實體隔離解決方案不同，隔離ONTAP網路保險庫是使用SnapLock Compliance和SnapMirror等原生ONTAP功能建構的。結果是恢復過程既快速又易於執行。

如果發生勒索軟體攻擊並需要從網路保險庫中恢復，則恢復過程簡單易行，因為可以使用網路保險庫中儲存的快照副本來恢復加密資料。



如果要求提供更快的方法，在必要時使資料重新上線，以便快速驗證、隔離和分析資料以進行復原。透過使用FlexClone並將 snaplock-type 選項設為非 snaplock 類型，可以輕鬆實現這一點。

從ONTAP 9.13.1 開始，可以透過建立FlexClone並將 snaplock-type 選項設為「non-snaplock」來立即恢復SnapLock保險庫關係的目標SnapLock磁碟區上的鎖定 Snapshot 副本。執行磁碟區複製建立作業時，指定Snapshot副本為「父快照」。有關創建具有SnapLock類型的FlexClone卷的更多信息"這裡。"

實踐網路保險庫的復原程序將確保建立連接到網路保險庫和檢索資料的正確步驟。規劃和測試程序對於網路攻擊事件期間的任何恢復都至關重要。

其他注意事項

在設計和部署基於ONTAP 的網路保險庫時，還需要考慮其他因素。

容量大小考慮因素

ONTAP Cyber Vault 目標磁碟區所需的磁碟空間量取決於多種因素，其中最重要的是來源磁碟區中資料的變化率。目標磁碟區上的備份計畫和快照計畫都會影響目標磁碟區上的磁碟使用情況，而來源磁碟區上的變更率可能不會保持恆定。最好提供額外的儲存容量緩衝區，以滿足未來最終用戶或應用程式行為變化的需求。

在ONTAP中確定 1 個月保留關係的大小需要根據多種因素計算儲存需求，包括主資料集的大小、資料變化率（每日變化率）以及重複資料刪除和壓縮節省（如果適用）。

以下是逐步方法：

第一步是了解使用網路保險庫保護的來源磁碟區的大小。這是最初複製到網路保險庫目的地的基本資料量。接下來，估計資料集的每日變化率。這是每天變化的數據百分比。充分了解資料的動態性至關重要。

例如：

- 主資料集大小 = 5TB
- 每日變化率=5%（0.05）
- 重複資料刪除和壓縮效率 = 50% (0.50)

現在，讓我們來看看計算過程：

- 計算每日數據變化率：

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

- 計算30天的總變化數據：

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

- 計算所需的總儲存量：

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

- 應用重複資料刪除和壓縮節省：

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

儲存需求摘要

- 如果效率不高：儲存 30 天的網路保險庫資料將需要 **12.5TB**。
- 效率為 50%：重複資料刪除和壓縮後需要 **6.25TB** 的儲存空間。

快照副本可能會因元資料而產生額外的開銷，但這通常很小。

如果每天進行多次備份，則根據每天拍攝的 Snapshot 副本數量調整計算。

考慮資料隨時間的成長，以確保規模適合未來。

對主要/源的性能影響

由於資料傳輸是一種拉取操作，因此對主儲存效能的影響可能會因工作負載、資料量和備份頻率而異。然而，由於資料傳輸旨在將資料保護和備份任務卸載到網路保險庫儲存系統，因此對主系統的整體效能影響通常是適度且可控的。在初始關係設定和第一次完整備份期間，大量資料從主系統傳輸到網路保險庫系統（ SnapLock Compliance磁碟區）。這會導致主系統的網路流量和 I/O 負載增加。初始完整備份完成後， ONTAP只需要追蹤並傳輸自上次備份以來發生變化的區塊。與初始複製相比，這會導致 I/O 負載小得多。增量更新效率高，對主儲存效能的影響最小。保險庫進程在後台運行，從而減少了乾擾主系統生產工作負載的可能性。

- 確保儲存系統有足夠的資源（CPU、記憶體和 IOP）來處理額外的負載，從而減輕效能影響。

配置、分析、**cron**腳本

NetApp創建了一個"可以下載的單一腳本"並用於配置、驗證和安排網路保險庫關係。

此腳本的作用

- 集群對等連接
- SVM 對等連接
- DP 磁碟區創建
- SnapMirror關係和初始化
- 強化用於網路保險庫的ONTAP系統
- 根據傳輸計劃暫停和恢復關係
- 定期驗證安全設定並產生顯示任何異常的報告

如何使用此腳本

"下載腳本"要使用該腳本，只需按照以下步驟操作：

- 以管理員身分啟動 Windows PowerShell。
- 導航到包含腳本的目錄。
- 使用執行腳本 `.\`語法以及必需的參數

請確保輸入所有資訊。第一次運行（配置模式）時，它將要求提供生產系統和新網路保險庫系統的憑證。之後，它將在系統之間建立 SVM 對等（如果不存在）、磁碟區和SnapMirror並初始化它們。

Cron 模式可用於安排資料傳輸的靜止和恢復。

操作模式

自動化腳本提供 3 種執行模式 - `configure ， analyze`和 `cron。

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

- 配置 - 執行驗證檢查並將系統配置為隔離。
- 分析－自動監控和報告功能，向監控群組發送異常和可疑活動的訊息，以確保配置不會偏離。
- Cron - 為了啟用斷開連接的基礎設施，cron 模式會自動停用 LIF 並停止傳輸關係。

傳輸選定卷中的資料需要一些時間，具體取決於系統效能和資料量。

```
./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"
```

ONTAP cyber Vault PowerShell 解決方案結論

透過利用ONTAP提供的氣隙和強大的強化方法， NetApp讓您能夠創建一個安全、隔離的儲存環境，以抵禦不斷演進的網路威脅。所有這些都是在保持現有儲存基礎設施的靈活性和效率的同時實現的。這種安全存取使公司能夠以對現有人員、流程和技術框架進行最小限度的改變來實現其嚴格的安全和正常運行時間目標。

ONTAP Cyber Vault 使用ONTAP中的原生功能，是一種簡單的方法，可提供額外的保護，以建立資料的不可變

和不可磨滅的副本。將 NetApp 基於ONTAP的網路保險庫加入整體安全態勢將：

- 創建一個與生產和備份網路分離且斷開的環境，並限制使用者對它的存取。