



開始

NetApp virtualization solutions

NetApp
January 12, 2026

This PDF was generated from <https://docs.netapp.com/zh-tw/netapp-solutions-virtualization/vmware/vmw-getting-started-overview.html> on January 12, 2026. Always check docs.netapp.com for the latest.

目錄

開始	1
核心概念	1
了解適用於 VMware vSphere 的ONTAP	1
了解適用於 VMware 的NetApp平台	4
了解NetApp和 VMware 的混合多雲環境	7
管理工具和解決方案	7
了解如何使用適用ONTAP tools for VMware vSphere管理虛擬機	7
了解如何使用ONTAP和 VMware API 進行管理	8
了解如何使用NetApp Data Infrastructure Insights監控整個基礎架構	9
了解從 VMware vSphere 到ONTAP資料儲存區的虛擬機	10
資料保護解決方案	10
了解如何使用MetroCluster和SnapMirror主動同步保護 VMware 環境	10
了解如何降低 VMware 工作負載的安全性和勒索軟體風險	11
自主防禦 NFS 和 VMFS 勒索軟體	12
備份和災難復原解決方案	19
了解如何使用適用於 VMware vSphere 的SnapCenter插件備份和還原虛擬機	19
了解如何使用NetApp Disaster Recovery進行虛擬機器災難復原	19

開始

核心概念

了解適用於 **VMware vSphere** 的**ONTAP**

NetApp ONTAP 是 VMware vSphere 的領先儲存解決方案，為資料儲存和用戶端連線儲存使用案例提供近二十年的可靠性能。ONTAP 支援 SAN 和 NAS 協議，允許獨立擴展儲存和運算資源，並從主機卸載儲存任務。其優勢包括強大的資料保護、高可用性以及先進的業務連續性功能，如 SnapMirror 和 MetroCluster。

介紹

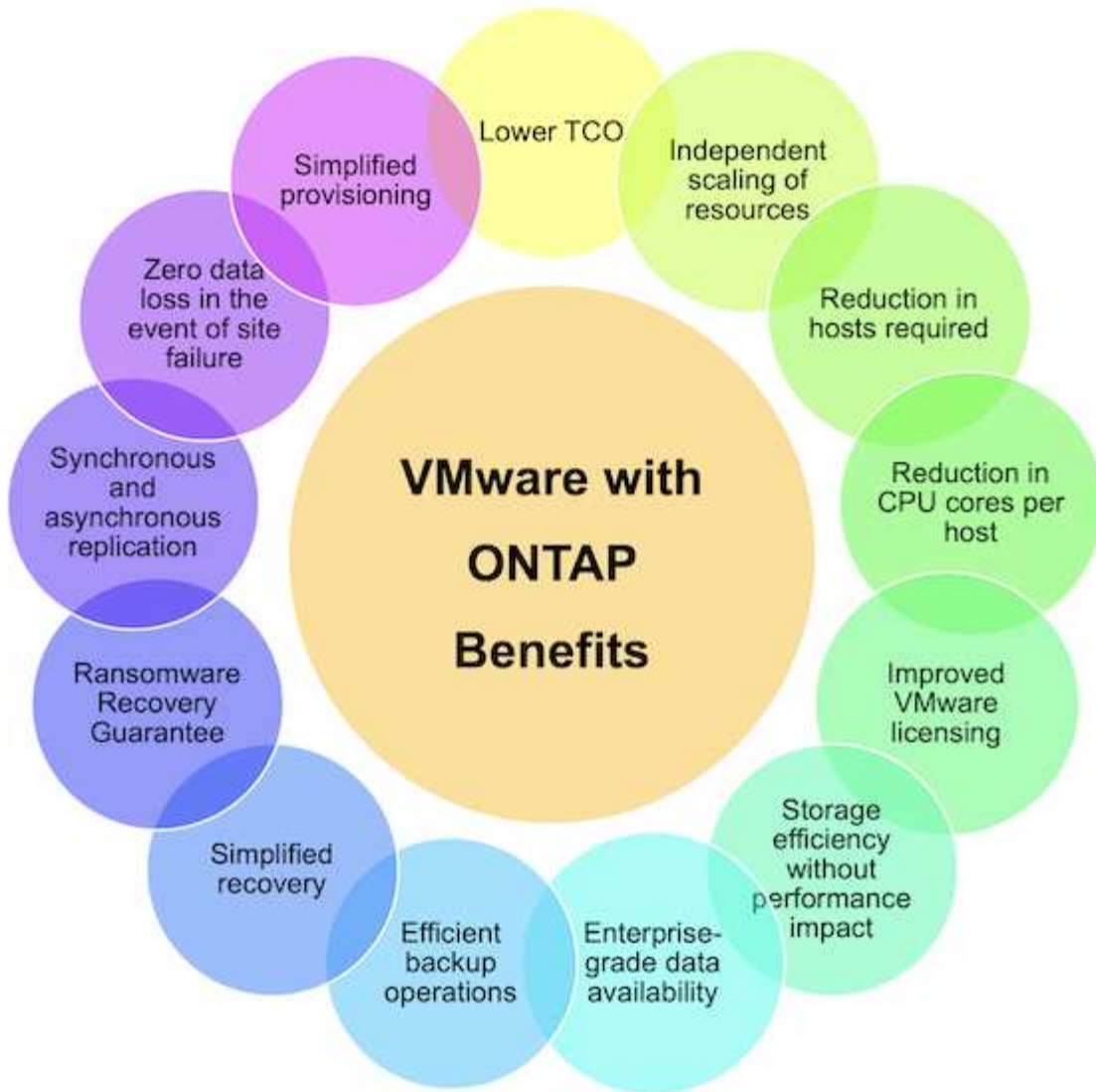
NetApp 持續增加創新功能以簡化儲存管理，同時降低成本並增強對基於 VMware 的整合雲端虛擬基礎架構的信心。此解決方案集合引入了適用於 VMware vSphere Foundation 和 VMware Cloud Foundation 的 ONTAP 產品，包括最新產品資訊和最佳實踐，以簡化部署、降低風險並簡化管理。

有關將 ONTAP 與 VMware vSphere 結合使用的更多信息，請參閱 ["搭載 ONTAP 的 VMware vSphere"](#)。

為什麼選擇 **ONTAP for VMware**

成千上萬的客戶選擇 ONTAP 作為 vSphere 儲存解決方案的原因有很多，例如支援 SAN 和 NAS 協定的統一儲存系統、使用節省空間的快照的強大資料保護功能以及幫助您管理應用程式資料的豐富工具。使用與虛擬機器管理程式分離的儲存系統可讓您卸載許多功能並最大化您對 vSphere 主機系統的投資。這種方法不僅可以確保您的主機資源專注於應用程式工作負載，還可以避免儲存操作對應用程式的隨機效能產生影響。

ONTAP 與 vSphere 結合使用是一種很好的組合，可讓您減少主機硬體和 VMware 軟體的費用。您還可以以較低的成本保護您的資料並保持一致的高效能。由於虛擬化工作負載是移動的，您可以探索使用 Storage vMotion 的不同方法在同一儲存系統上跨 VMFS、NFS 或 vVols 資料儲存移動虛擬機器。



以下是NetApp和 VMware 客戶的主要優勢：

- *第一天以及隨著規模擴大而具有靈活性。*任何架構都可能因各種原因而產生成長的需求。無論效能或容量需求如何變化，或者隨著新主機的添加和網路或結構考慮的出現，選擇一個允許獨立擴展資源的儲存平台至關重要。

借助ONTAP，您可以從所需的容量開始，根據需要增加容量並利用分層功能，而無需添加額外的計算主機。此外，單一ONTAP叢集可與多個工作負載域一起使用，並避免建立儲存孤島。這些好處為組織帶來了顯著的成本節省。

- *將儲存任務卸載到ONTAP。*在典型的 HCI 環境中，主機平台負責運算任務、儲存操作和客戶端的任何網路最佳化。例如，在決定計算節點的硬體需求時需要考慮 CPU 開銷。這種開銷通常很難預先確定範圍，通常被接受為 10-15%，並且取決於工作負載的 I/O 設定檔。此外，考慮記憶體消耗也很重要。記憶體開銷是強制性的，不應為了保持效能而犧牲記憶體開銷。主機可以利用支援 RDMA 的 NIC 來抵消這一點，從而提高網路傳輸效率，但需要額外費用。最後，透過 HCI 平台，儲存效率、RAID 和故障容忍度以及加密等儲存功能由主機處理。

客戶可以利用ONTAP來減輕對主機 CPU 資源的任何不利影響。此策略使主機能夠專注於運算任務，同時允許ONTAP管理 CPU 密集型儲存作業。此策略透過優化儲存效率、加密、快照等來提高整體效能，同時降低整體擁有成本。它不僅可以提高主機效能並減少提供相同工作負載所需的主機數量，還可以減少每個主機所

需的核心數量，從而進一步節省成本。這些節省進一步擴展到節省能源效率、減少冷卻需求、優化授權成本等；所有這些都透過將 CPU 密集型儲存任務卸載到ONTAP並減少對主機處理所有事情的依賴來實現。

- 儲存效率 儘管NetApp是第一個為生產工作負載提供重複資料刪除功能的公司，但這項創新並不是該領域的第一次或最後一次創新。它從快照開始，這是一種節省空間且不會影響效能的資料保護機制，同時結合FlexClone技術，可立即為生產和備份使用製作虛擬機器的讀取/寫入副本。NetApp繼續提供內聯功能，包括重複資料刪除、壓縮和零區塊重複資料刪除，以從昂貴的 SSD 中榨取最多的儲存空間。最近，ONTAP增加了使用壓縮將較小的 I/O 操作和檔案打包到磁碟區塊中的功能。這些功能的結合使客戶看到 VSI 節省高達 5:1，VDI 節省高達 30:1。
- *企業級資料可用性。*對於任何 IT 組織來說，資料保護都是至關重要的。規劃工作負載容錯能力需要仔細考慮，以確保主機負責儲存作業時有足夠數量的節點可用。隨著可容忍的故障數量的增加，對額外主機的需求以及為滿足所需的虛擬機器儲存容量而配置的儲存量也會增加。

ONTAP 的全面可用性功能可確保資料始終可存取、安全且具彈性，使其成為各種規模的 VMware 部署的可靠選擇。利用 VMware 環境中的共享儲存有助於部署較小的 vSphere 集群，簡化設定流程並實現跨集群的儲存共享，增強容錯能力。

ONTAP 的主要可用性功能包括：

- 高可用性 (HA) 架構：ONTAP支援包含叢集部署模型的高可用性架構。
- 自動故障轉移和故障復原：如果發生硬體或軟體故障，ONTAP允許自動故障轉移到備用儲存節點。一旦問題解決，就可以執行故障復原以恢復原始配置，從而最大限度地減少停機時間。
- 內建資料保護：ONTAP包含內建資料保護功能，例如 RAID-DP 和RAID-TEC，它們可提供增強的磁碟故障保護並確保資料完整性和可用性。
- *高效率的備份和復原作業。*除了在發生各種故障時保護資料之外，我們還必須計劃將虛擬機器和工作負載備份作為常規 IT 作業的一部分。快照擷取特定時間點的虛擬機器狀態，包括虛擬機器的磁碟、記憶體和設定。如果出現問題（例如更新失敗、配置變更或成為勒索軟體或病毒攻擊的受害者），管理員可以將虛擬機器恢復到先前的狀態。在為 VMware 環境設計平衡解決方案時，應考慮快照消耗的儲存。

雖然快照是一個重要的工具，但過度依賴基於 VMware 的快照會引發對頻率和保留策略的擔憂。此外，基於 VMware 的快照過多也會降低效能。考慮替代方案非常重要，例如NetApp快照副本和SnapCenter Plug-in for VMware vSphere。SnapCenter利用快照副本，即磁碟區的唯讀、時間點映像，最初與活動檔案系統共用磁碟區塊，不需要額外的空間和最少的儲存空間。這些快照的效能開銷可以忽略不計，僅捕獲自上次快照以來的變化。SnapCenter Plug-in for VMware vSphere利用這些快照為虛擬機器、資料儲存區和 VMDK 提供高效、崩潰一致的備份和還原。這些操作無縫集成，並且不會對 vCenter 環境內的效能產生影響。此外，ONTAP還支援將快照卸載到物件儲存以進行長期保留。

- *整體業務連續性能力。*除了標準的容錯、備份和復原之外，組織還必須為各種情況做好規劃，例如災難、勒索軟體攻擊和資料中心站點遷移。對於基於主機的存儲，解決這些挑戰通常需要依靠一系列第三方解決方案來有效地減輕災難並確保業務連續性。此外，對於網路密集型場景，網路和儲存設備規模不足可能會對效能造成嚴重影響。

ONTAP基於其可用性功能以及備份和復原功能，是 VMware 環境全面業務連續性策略不可或缺的組成部分。組織需要虛擬機器和工作負載在正常和維護作業期間無縫可用，並透過強大的保護和復原功能進行保障，並且能夠利用節省空間且經濟高效的災難復原解決方案。

ONTAP業務連續性的主要功能包括：

- 使用SnapMirror進行資料複製：利用快照副本，SnapMirror可以將資料非同步和同步複製到遠端站點或雲端環境，以實現災難復原
- MetroCluster：ONTAP 的MetroCluster技術可在地理位置分散的站點之間提供同步複製，確保零資料遺

失並在站點發生故障時快速恢復。

- 雲端分層：雲端分層自動識別主儲存上的冷資料（不經常存取的資料）並將其移至雲端或本地端的低成本物件儲存。
- NetApp Disaster Recovery：NetApp Disaster Recovery是一個綜合解決方案，旨在為企業提供強大的災難復原能力，確保在災難發生時實現資料保護、快速復原和業務連續性。

了解適用於 VMware 的NetApp平台

NetApp提供針對 VMware 環境量身打造的平台，包括用於經濟高效儲存的FAS、高效能工作負載的AFF、專用 SAN 部署的ASA以及用於混合和多雲架構的雲端解決方案。這些平台由ONTAP提供支持，支援 VMware Cloud Foundation 和 VMware vSphere。

介紹

這些產品增強了 VMware 管理員的效能、可擴充性和資料管理。此外，ONTAP可在這些平台上使用，提供統一、可擴展且高效的資料管理解決方案，支援各種儲存協定、增強資料保護並最佳化不同工作負載的效能。

NetApp平台的共同優勢

- **VMware 整合**：所有NetApp平台都提供與 VMware 的深度集成，從而提高了儲存環境的效率。內部部署解決方案可利用外掛程式、API、VAAI 和 VASA 來改善整體資料管理，同時提高基礎架構的多功能性。
- ***成本優化和儲存效率**：*利用NetApp儲存可利用重複資料刪除、壓縮和精簡配置等本機效率技術，大幅降低儲存消耗和成本，同時最大限度地提高容量利用率和效能。此外，這些儲存節省還可以減輕運算資源的負擔。
- **統一資料管理**：ONTAP為內部部署和基於雲端的儲存提供單一管理介面，簡化管理並降低複雜性。這允許在本地和雲端環境之間實現無縫的資料移動和管理，為 VMware 工作負載提供靈活性和可擴展性。
- **多協議支援**：ONTAP支援多種儲存協議，包括 NFS、CIFS/SMB、iSCSI、FC 和 NVMe，允許組織在單一平台上整合工作負載或利用專用 SAN 產品，而無需建立資料孤島。
- ***自動化和編排**：*支援 VMware Cloud Foundation Automation（以前稱為 VMware Aria Automation）等自動化工具，並與 Ansible 和其他自動化框架集成，簡化操作並減少管理開銷。
- **安全性**：強大的安全功能，包括靜態和傳輸中加密、安全多租用戶和基於角色的存取控制，確保 VMware 環境保持安全。
- ***適用於 VMware 的ONTAP工具**：* NetApp適用於 VMware 的ONTAP工具提供無縫整合和管理功能，透過統一直觀的介面為 VMware 環境實現高效的儲存配置、資料保護和增強效能。
- *** SnapCenter for VMware vSphere**：* NetApp SnapCenter for VMware vSphere 簡化並集中了 VMware 環境的資料保護、備份和復原作業，確保可靠、有效率地管理虛擬機器資料。
- **高可用性和彈性**：RAID-TEC和 RAID-DP 等功能提供強大的資料保護和高可用性，這對於 VMware 環境至關重要。
- **服務品質 (QoS)**：允許管理員為不同的虛擬機器設定效能保證，確保關鍵工作負載獲得必要的資源。

注意：NetApp雲端解決方案可能具有受雲端供應商限制的功能，但它們對於客戶機連接和本機 NFS 資料儲存的支援仍然非常強大。

NetApp ASA（全 SAN 陣列）優勢

- ***針對 SAN 進行最佳化**：*專為 SAN 工作負載而設計，為依賴區塊儲存的 VMware 環境提供高效能和低延

遲。

- 增強的高可用性：主動-主動控制器和同步複製等功能可確保持續可用性和資料保護。

ASA系列包括 A 系列和 C 系列型號。

NetApp A 系列全 NVMe 快閃記憶體陣列專為高效能工作負載而設計，提供超低延遲和高彈性，使其適用於關鍵任務應用程式。



C 系列 QLC 快閃記憶體陣列針對更高容量的用例，提供快閃記憶體的速度和混合快閃記憶體的經濟性。



儲存協定支援

ASA支援所有標準 SAN 協議，包括 iSCSI、光纖通道 (FC)、乙太網路光纖通道 (FCoE) 和 NVME over fabrics。

iSCSI - NetApp ASA為 iSCSI 提供強大的支持，允許透過 IP 網路對儲存設備進行區塊級存取。它提供與 iSCSI 啟動器的無縫集成，從而實現 iSCSI LUN 的高效配置和管理。ONTAP 的進階功能，例如多路徑、CHAP 驗證和 ALUA 支援。

有關 iSCSI 配置的設計指導，請參閱 ["SAN 配置參考文檔"](#)。

光纖通道 - NetApp ASA為光纖通道 (FC) 提供全面支持，光纖通道是一種常用於儲存區域網路 (SAN) 的高速網路技術。ONTAP與 FC 基礎架構無縫集成，提供可靠、高效的儲存設備區塊級存取。它提供分區、多路徑和結構登入 (FLOGI) 等功能，以優化效能、增強安全性並確保 FC 環境中的無縫連接。

有關光纖通道配置的設計指導，請參閱 ["SAN 配置參考文檔"](#)。

NVMe over Fabrics - NetApp ONTAP和ASA支援 NVMe over fabrics。NVMe/FC 支援透過光纖通道基礎架構使用 NVMe 儲存設備，並透過儲存 IP 網路使用 NVMe/TCP。

有關 NVMe 的設計指導，請參閱 "[NVMe 配置、支援和限制](#)"

雙活技術

NetApp 全快閃 SAN 陣列允許透過兩個控制器實現主動-主動路徑，從而無需主機作業系統等待主動路徑發生故障後再啟動備用路徑。這意味著主機可以利用所有控制器上的所有可用路徑，確保無論系統處於穩定狀態還是正在進行控制器故障轉移操作，活動路徑始終存在。

此外，NetApp ASA 還提供了一項獨特的功能，可大幅提高 SAN 故障轉移的速度。每個控制器不斷地將重要的 LUN 元資料複製到其配對控制器。因此，每個控制器都準備好在其合作夥伴突然發生故障時接管資料服務責任。這種準備是可能的，因為控制器已經擁有開始利用先前由故障控制器管理的驅動器所需的資訊。

透過主動-主動路徑，計劃內和計劃外的接管的 IO 恢復時間均為 2-3 秒。

有關詳細信息，請參閱 "[TR-4968，NetApp 全 SAS 陣列 – NetApp ASA 的資料可用性和完整性](#)"。

詳細資訊請參見 "[NetApp ASA 登入頁面](#)"。

NetApp AFF（全快閃 FAS）優勢

- **極致效能：**利用全快閃儲存提供亞毫秒延遲和高 IOPS，非常適合效能敏感的 VMware 工作負載。
- **持續低延遲：**確保關鍵應用程式和虛擬機器的可預測效能，這對於維護 SLA 至關重要。

有關 NetApp AFF A 系列儲存陣列的更多信息，請參閱 "[NetApp AFF A 系列](#)" 登陸頁。

有關 NetApp C 系列儲存陣列的更多信息，請參閱 "[NetApp AFF C 系列](#)" 登陸頁。

NetApp FAS（光纖連接儲存）優勢

- **統一儲存架構：**支援 SAN（區塊級）和 NAS（檔案級）協議，使其適用於各種 VMware 工作負載。
- **經濟高效：**非常適合需要在效能和成本之間取得平衡的環境，提供 HDD 和 SSD 的組合。

雲端解決方案的優勢

- **雲端原生資料管理：**利用雲端原生產品增強 VMware 工作負載的資料移動性、備份和災難復原。對 VMware 雲端工作負載的原生 NFS 資料儲存支援如下：
 - VMware Cloud on AWS 與 Amazon FSx for NetApp ONTAP
 - 附有 Azure NetApp Files 的 Azure VMware 服務
 - 附有 Google Cloud NetApp Volume 的 Google Cloud VMware Engine -
- **混合雲靈活性：**內部部署和雲端環境之間的無縫集成，為跨多個位置的 VMware 工作負載提供靈活性。

總結

總之，ONTAP 和 NetApp 平台為 VMware 工作負載提供了全面的優勢，增強了效能、可擴充性和資料管理。雖然常見的功能提供了堅實的基礎，但每個平台都提供了針對特定需求的差異化優勢，無論是透過 FAS 實現的經濟高效的儲存、透過 AFF 實現的高效能、透過 ASA 實現的最佳化 SAN 效能，還是透過 NetApp 雲端產品實現的混合雲靈活性。

了解NetApp和 VMware 的混合多雲環境

了解NetApp和 VMware 如何透過將內部基礎架構與公有雲服務整合來簡化混合多雲設置，從而實現工作負載遷移、資源最佳化和跨環境的一致操作。

介紹

這種方法使企業能夠輕鬆遷移工作負載、最佳化資源使用率並在兩個環境中保持一致的操作。

有關 VMware 和NetApp混合雲場景的更多信息，請參閱["NetApp與 VMware 的混合多雲概述"](#)。

NetApp的 VMware 部署場景

本節介紹跨本地端和公有雲的 VMware 環境的各種部署選項。每個雲端供應商都在其各自的公有雲產品中支援 VMware 軟體定義資料中心 (SDDC) 和/或 VMware 雲端基礎 (VCF) 堆疊。

- **VMware 本機部署**

將 VMware 與NetApp儲存體結合使用可提供強大、可擴展且靈活的虛擬化環境。透過將 NetApp 的高階資料管理功能（如重複資料刪除、壓縮和高效快照）與由ONTAP提供支援的適當儲存系統結合，客戶可以選擇適合他們的平台。這種組合可確保虛擬化工作負載的高效能、可靠性和簡化的管理，進而提高整體資料中心的效率。

- **Azure VMware 解決方案**

Azure VMware 解決方案是一種混合雲端服務，可在 Microsoft Azure 公有雲中完全執行 VMware SDDC。Azure VMware 解決方案是完全由 Microsoft 管理和支援的第一方解決方案，並由 VMware 利用 Azure 基礎架構進行了驗證。這意味著，當部署 Azure VMware 解決方案時，客戶可以獲得 VMware 的 ESXi 用於計算虛擬化、vSAN 用於超融合儲存以及 NSX 用於網路和安全，同時利用 Microsoft Azure 的全球影響力、一流的資料中心設施以及靠近豐富的原生 Azure 服務和解決方案生態系統的優勢。

- **AWS 上的 VMware 雲**

VMware Cloud on AWS 將 VMware 的企業級 SDDC 軟體引入 AWS 雲，並優化了對原生 AWS 服務的存取。VMware Cloud on AWS 由 VMware Cloud Foundation 提供支持，整合了 VMware 的運算、儲存和網路虛擬化產品（VMware vSphere、VMware vSAN 和 VMware NSX）以及 VMware vCenter Server 管理，並針對專用、彈性、裸機 AWS 基礎架構上運行進行了最佳化。

- **Google Cloud VMware 引擎**

Google Cloud VMware Engine 是一款基礎架構即服務 (IaaS) 產品，它是基於 Google Cloud 高效能可擴充基礎架構和 VMware Cloud Foundation 堆疊（VMware vSphere、vCenter、vSAN 和 NSX-T）建構。此服務可快速遷移至雲端，將現有 VMware 工作負載從本地環境無縫遷移或擴展到 Google Cloud Platform，無需承擔重構應用程式或重新調整運維的成本、精力或風險。這是一項由 Google 銷售和支援的服務，並與 VMware 密切合作。

管理工具和解決方案

了解如何使用適用ONTAP tools for VMware vSphere管理虛擬機

ONTAP tools for VMware vSphere簡化了使用NetApp儲存的虛擬機器的生命週期管理。管理員可以直接從 vCenter Server 管理存儲，從而簡化操作並增強可擴展性。虛擬儲存控制

台 (VSC)、VASA 提供者和儲存複製適配器 (SRA) 等關鍵元件可最佳化設定、效能監控和災難復原。

介紹

它使管理員能夠直接管理 vCenter Server 內的存儲，並簡化 VMware 環境的儲存和資料管理。VMware vSphere Client 外掛程式工具旨在將外掛功能整合到 vSphere Client 中，而無需在 vCenter Server 內部執行。這提供了插件隔離並支援在大型 vSphere 環境中運行的插件的橫向擴展。

ONTAP 工具元件

- **虛擬儲存控制台 (VSC)** VSC 包括與 vSphere 用戶端整合的介面，您可以在其中新增儲存控制器、設定資料儲存庫、監控資料儲存庫的效能以及檢視和更新 ESXi 主機設定。
- **VASA 提供者** 適用於 ONTAP 的 VMware vSphere APIs for Storage Awareness (VASA) 提供者將有關 VMware vSphere 使用的儲存的資訊傳送至 vCenter Server，從而實現 VMware 虛擬磁碟區 (vVols) 資料儲存的設定、儲存功能設定檔的建立與使用、合規性
- **儲存複製適配器 (SRA)** 啟用並與 VMware Site Recovery Manager (SRM) 一起使用時，SRA 可在發生故障時促進 vCenter Server 資料儲存和虛擬機器的恢復，從而允許配置受保護網站和復原網站以進行災難復原。

有關適用於 VMware 的 NetApp ONTAP 工具的更多信息，請參閱 ["ONTAP tools for VMware vSphere 文檔"](#)。

了解如何使用 ONTAP 和 VMware API 進行管理

ONTAP 和 VMware 提供用於實現儲存和虛擬化平台之間無縫整合和自動化的 API。這使得配置、監控和資料保護得以簡化，從而提高了工作流程的一致性。

介紹

VMware 提供了一系列 API，允許管理員以程式設計方式與各種 VMware 產品和服務進行交互，從而提高作業的效率和一致性。此外，NetApp ONTAP API 提供了一套強大的工具，使管理員能夠自動化、整合和最佳化儲存環境的管理，特別是與 VMware 工作負載結合使用時。這些 API 促進了 ONTAP 儲存系統和 VMware 之間的無縫交互，從而提高了效率、效能和資料保護。

基於 VMware 的 API

- **VMware vSphere API**：vSphere API 是一個綜合性的 API，允許管理員管理和自動化 VMware vSphere 環境。它提供對各種 vSphere 功能的訪問，包括虛擬機器配置、配置、監控和生命週期管理。
- **VMware vCenter Server REST API**：vCenter Server REST API 提供了一個現代化的 RESTful 介面來管理 vCenter Server 及其相關元件。它簡化了自動化以及與其他系統和工具的整合。
- ***VMware Cloud Foundation API**：*VMware 軟體定義資料中心 (SDDC) API 提供對 VMware SDDC 環境中各種元件和服務的程式存取。這些 API 使管理員和開發人員能夠自動化、管理和整合資料中心的不同方面，包括運算、儲存、網路和管理服務。
- ***VMware vSphere 儲存 API - 儲存感知**：*VASA 是一組 API，提供儲存陣列與 vCenter 的集成，以便進行管理。此架構基於多個元件，包括處理 VMware vSphere 和儲存系統之間的通訊的 VASA 提供者。借助 ONTAP，該提供者作為 ONTAP tools for VMware vSphere 的一部分實作。
- ***VMware vSphere 儲存 API - 陣列整合**：*VAAI 是一組支援 VMware vSphere ESXi 主機和儲存設備之間通訊的 API。API 包括一組主機用來將儲存操作卸載到陣列的原始操作。VAAI 可以為儲存密集型任務提供顯著的效能改進。

基於ONTAP的 API

- * NetApp ONTAP REST API：* ONTAP REST API 提供了一個用於管理ONTAP儲存系統的現代 RESTful 介面。它簡化了配置、監控和配置等儲存任務的自動化。它可以輕鬆與 VMware vSphere 和其他 VMware 管理工具集成，從而直接從 VMware 環境實現自動化儲存操作。它支援廣泛的操作，從基本的儲存管理到進階資料保護和複製任務，實現可擴展和靈活的儲存管理。
- * 適用於 VMware vSphere 的ONTAP工具：*ONTAP tools for VMware vSphere是一組用於整合ONTAP和 vSphere 的工具。它實作了 VASA API 框架的提供者功能。ONTAP工具還包括 vCenter 外掛程式、用於 VMware Site Recovery Manager 的儲存複製適配器 (SRA) 以及可用於建立自動化應用程式的 REST API 伺服器。

總結

總之，借助ONTAP API，管理員可以編寫腳本在 VMware 環境中建立和配置資料儲存區，確保快速、一致的儲存配置。此外，它們還可以自動建立、排程和刪除 VMware 虛擬機器的快照，提供高效率的資料保護和復原選項。SnapMirror API 促進了複製關係設定和管理的自動化，確保為 VMware 工作負載提供強大的災難復原解決方案。管理員還可以實施腳本來監控儲存效能指標，並在超出效能閾值時觸發警報或自動操作，確保 VMware 工作負載的最佳儲存效能。透過將ONTAP API 與 VMware API（例如 vSphere 和 vRealize 提供的 API）整合，管理員可以獲得無縫且高度自動化的管理體驗，從而提高其虛擬化基礎架構的整體效率和可靠性。

了解如何使用NetApp Data Infrastructure Insights監控整個基礎架構

NetApp Data Infrastructure Insights（以前稱為Cloud Insights）可監控本機和雲端系統，提供整個 IT 環境（包括 VMware vSphere 和ONTAP儲存系統）的視覺性。它支援跨公共和私有環境的效能追蹤、問題偵測和資源最佳化等功能。

介紹

透過Data Infrastructure Insights，您可以監控、排除故障並優化所有資源，包括公有雲和私有資料中心。

有關Data Infrastructure Insights的更多信息，請參閱["Data Infrastructure Insights文檔"](#)。

Data Infrastructure Insights能力

- Data Infrastructure Insights提供混合多雲監控，讓您可以全端觀察基礎架構和工作負載。
- 異質基礎設施和工作負載的資料收集器，包括 Kubernetes
- 開放 Telegraf 收集器和開放 API，方便集成
- 全面的警報和通知
- 機器學習帶來智慧洞察
- 優化資源利用率
- 內建或可自訂的儀表板，配有高級過濾器，可最大限度地減少顯示噪音，從而回答問題
- 了解ONTAP儲存作業的健康狀況
- 保護您最寶貴的商業資產——數據——免受勒索軟體或資料破壞攻擊

了解從 VMware vSphere 到ONTAP資料儲存區的虛擬機

VMware vSphere 管理員可以透過將工作負載遷移到NetApp ONTAP資料儲存來增強其基礎架構。ONTAP提供虛擬機器感知快照、儲存高效複製和無縫 vMotion 操作，同時支援基於儲存策略的管理 (SPBM)。無論是從 vSAN、傳統儲存遷移，或是實施混合雲部署，ONTAP都能為 VMware 環境提供更高的效能和簡化的儲存作業。

這種遷移實現了無縫整合、改進的資料保護以及管理虛擬化環境的更大靈活性，確保了平穩過渡和最少的停機時間。

用例

在考慮遷移到ONTAP支援的資料儲存時，在來源和目標方面有許多遷移選項。

- 從第三方儲存系統（包括 vSAN）遷移到ONTAP資料儲存。
- 同一 vSphere 叢集中的虛擬機器遷移
- 跨多個 vSphere 叢集遷移虛擬機
- 在同一 SSO 域中跨 vCenter 伺服器遷移虛擬機
- 在不同 SSO 網域中的 vCenter 伺服器之間遷移虛擬機
- 跨資料中心位置遷移虛擬機
- 從第三方儲存系統（包括 vSAN）遷移到ONTAP資料儲存。
- 混合雲環境中虛擬機器的遷移

有關將 VMware 工作負載遷移到ONTAP支援的資料儲存庫的更多信息，請參閱["將虛擬機器遷移到ONTAP資料儲存庫"](#)。

資料保護解決方案

了解如何使用MetroCluster和SnapMirror主動同步保護 VMware 環境

高階業務連續性對於保護 VMware 環境免受域內中斷至關重要。NetApp和 VMware 提供NetApp MetroCluster、SnapMirror active sync 和 VMware vSphere Metro Storage Cluster (vMSC) 等解決方案，以增強工作負載保護並確保高可用性。

介紹

除了產品內建的可用性之外，VMware 和NetApp還提供進階配置，進一步保護分佈在機架、建築物、校園甚至城市等故障域中的工作負載。

NetApp MetroCluster

NetApp MetroCluster使用 NetApp 的高可用性 (HA) 功能來防止控制器故障。MetroCluster還包括SyncMirror技術、按需叢集故障轉移 (CFOD)、硬體冗餘和地理分離，以實現高可用性。SyncMirror在兩個 plex 之間同步鏡像資料：本地 plex 主動提供數據，遠端 plex 作為備用。所有MetroCluster組件（例如控制器、儲存、電纜、交換器和適配器）都具有硬體冗餘。

NetApp SnapMirror主動同步

NetApp SnapMirror主動同步透過 FCP 和 iSCSI SAN 協定提供資料儲存粒度保護，選擇性地保護高優先權工作負載拓樸。與主動-備用MetroCluster不同，它提供對本地和遠端站點的主動-主動存取。從ONTAP 9.15.1 開始，SnapMirror主動同步支援對稱主動/主動功能，允許透過雙向同步複製從受保護 LUN 的兩個副本執行讀寫 I/O 操作。

VMware vSphere Metro 儲存群集

VMware vSphere Metro Storage Cluster (vMSC) 透過主動-主動延伸儲存增強了 VMware HA。此經過認證的配置可保護虛擬機器和容器免受故障影響。這是透過使用延伸儲存概念以及 vSphere 主機叢集來實現的。這些主機分佈在不同的故障域。NetApp MetroCluster和SnapMirror主動同步儲存技術用於提供保護和支援的儲存產品。透過利用 vMSC，NetApp認證的解決方案可跨故障域提供強大且具彈性的 IT 營運。

有關詳細信息，請參閱 ["採用ONTAP 的vSphere Metro 儲存集群"](#)。

了解如何降低 VMware 工作負載的安全性和勒索軟體風險

ONTAP透過加密、快照和進階存取控制增強了 VMware 環境中的安全性和勒索軟體防護，補充了 VMware 的安全功能以保護資料。

介紹

透過在 VMware 環境中利用NetApp ONTAP的進階功能，組織可以確保其資料的完整性、可用性和安全性。

請參閱下文，詳細了解這些技術如何協同工作以提供*安全*和*備份優勢*。

安全和勒索軟體

安全性是虛擬化環境中的首要關注點，而NetApp ONTAP提供了強大的功能來增強 VMware 基礎架構內的安全性。ONTAP為靜態資料和傳輸中的資料提供加密，確保敏感資訊免於未經授權的存取。加密金鑰得到安全管理，並且ONTAP支援基於軟體和基於硬體加密解決方案。透過與 VMware 的安全工具（例如 vSphere 的內建安全功能和第三方安全解決方案）集成，ONTAP有助於建立安全且合規的環境。

勒索軟體防禦

勒索軟體攻擊對組織構成重大威脅，而 VMware 與ONTAP的結合提供了強大的防禦機制。ONTAP 的快照技術允許創建不可變的快照，勒索軟體無法更改或刪除。如果發生攻擊，這些快照可用於快速將受影響的虛擬機器和資料儲存恢復到攻擊前的狀態，從而最大限度地減少停機時間和資料遺失。此外，ONTAP 與安全資訊和事件管理 (SIEM) 系統的整合實現了對可疑活動的主動監控和警報。ONTAP還支援多因素身份驗證 (MFA) 和基於角色的存取控制 (RBAC)，以進一步增強安全性。

勒索軟體恢復保證

NetApp勒索軟體保障為組織提供了強大且可靠的解決方案，以防止勒索軟體攻擊。透過利用NetApp ONTAP的先進功能，組織可以確保其資料的安全性和可用性。此保證讓您安心，因為您知道，如果發生勒索軟體攻擊，資料可以快速有效地恢復，最大限度地減少停機時間、資料遺失和財務影響。對資料安全和彈性的承諾使NetApp成為希望保護其關鍵資產免受不斷演變的網路威脅的組織的理想合作夥伴。

進階安全功能

ONTAP包括進階安全功能，例如安全多租戶（可在多租戶環境中隔離資料和資源）和合規性稽核（可追蹤和記

錄對敏感資料的存取)。這些功能可確保資料安全,並且組織可以證明符合行業法規和標準。

總結

ONTAP 的安全功能(例如加密、不可變快照和進階存取控制)與 VMware 工具的整合提供了對包括勒索軟體在內的網路威脅的強大防禦。ONTAP 對安全多租戶和合規性審計的支援可確保資料保護和法規遵循。

NetApp ONTAP和 VMware 共同提供了用於保護虛擬化環境的全面解決方案,使組織能夠保護資料、最大限度地減少停機時間並保持業務連續性。實施這些技術有助於企業應對現代 IT 挑戰並保護關鍵資產免受不斷演變的安全威脅。

自主防禦 NFS 和 VMFS 勒索軟體

了解NetApp ONTAP 的自主勒索軟體防護 (ARP) 如何使用機器學習來保護 VMware 環境中的 NFS 和 VMFS 資料存儲,提供早期威脅檢測、防篡改快照和快速恢復,以增強虛擬化和雲端工作負載的資料彈性。

概況

勒索軟體威脅正在迅速演變,變得更加複雜和破壞性。傳統的安全措施往往無法保護關鍵資料資產。NetApp ONTAP儲存提供內建安全功能,可主動保護資料。如果發生安全漏洞,ONTAP會提供即時警報和快速復原選項,以減少停機時間並限制資料遺失。ONTAP使客戶能夠保護、恢復和移動其資料和應用程式,從而增強勒索軟體的抵禦能力。

使用案例 – 保護 VMware 虛擬機器及其文件

在 VMware 環境中儘早偵測勒索軟體對於阻止其傳播和最大限度地減少停機時間至關重要。有效的策略是在 ESXi 主機和客戶虛擬機器之間使用多層保護。雖然許多安全控制措施有助於建立強大的防禦,但NetApp ONTAP增加了必要的儲存等級保護措施,進一步加強了保護。

ONTAP 的主要功能包括用於時間點復原的快照技術、由內建機器學習提供支援的自主勒索軟體保護 (ARP)、多重管理員驗證和可保持資料完整性的防篡改快照。這些功能協同作用,增強了勒索軟體的抵禦能力,並在需要時快速恢復。

保護 vSphere 環境和客戶虛擬機器需要採取全面的方法。關鍵措施包括網路分段、部署 EDR/XDR/SIEM 解決方案進行端點監控、及時應用安全更新以及遵循既定的強化指南。每個虛擬機器通常都會執行一個標準作業系統,因此作為多層勒索軟體防禦策略的一部分,安裝和定期更新企業級反惡意軟體解決方案至關重要。

ONTAP如何提供協助

ONTAP透過多層防禦加強資料保護。主要功能包括快照、自主勒索軟體保護 (ARP)、防篡改快照、多重管理員驗證等。本文檔重點介紹 9.17.1 版本中引入的 ARP 增強功能。

您可以在支援 VMware 資料儲存區的 NAS 或 SAN 磁碟區上啟用 ARP。ARP 使用 ONTAP 的內建機器學習來監控工作負載模式和資料熵,自動偵測勒索軟體活動的跡象,並提供智慧、主動的安全層。使用 ONTAP 的 CLI 或系統管理器介面配置每個磁碟區的 ARP。

ARP特性演進

從ONTAP版本 9.10.1 開始,ARP 可用於現有磁碟區或新磁碟區。在ONTAP版本 9.16.1 中,您可以使用系統管理員或 CLI 啟用 ARP。ARP/AI 保護立即生效,無需學習期。在 9.17.1 版本中,ARP 支援 SAN 磁碟區。當您在 SAN 磁碟區上啟用 ARP 時,ARP/AI 會在評估期間持續監控數據,以確定工作負載的適用性並設定最佳偵測

加密閾值。

ARP 內建於ONTAP中，提供與其他ONTAP功能的整合控制和協調。ARP 即時運作，在寫入或讀取資料時進行處理，並快速偵測和回應潛在的勒索軟體攻擊。它會定期建立鎖定快照以及預定的快照，並在未偵測到異常時透過回收快照來智慧地管理快照保留。如果 ARP 偵測到可疑活動，它會將攻擊前拍攝的快照保存較長時間，以確保可靠的復原點。

有關詳細信息，請參閱["ARP 偵測到什麼"](#)。

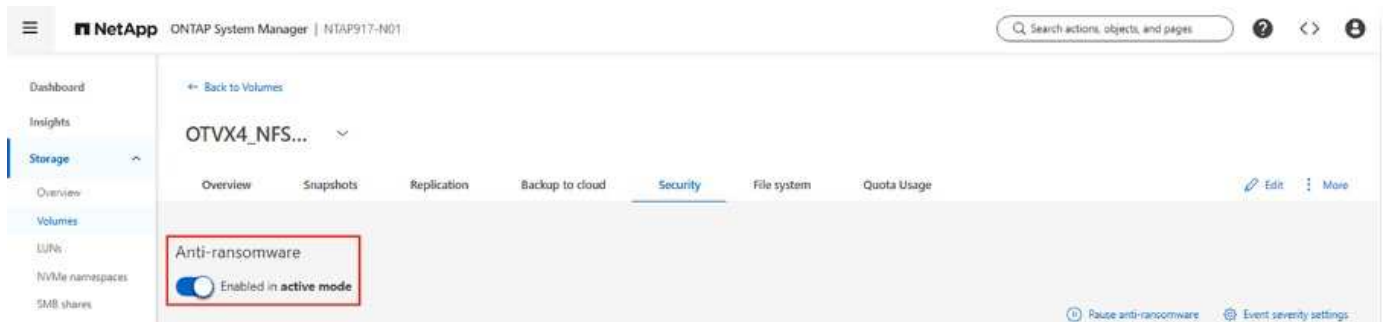


ONTAP ONE 授權包含 ARP 支援。

在 NAS 磁碟區上配置 ARP 並模擬對 VM 的攻擊

了解如何在用於 VMware 資料儲存區的 NAS 和 SAN 磁碟區上啟用NetApp ONTAP自主勒索軟體防護 (ARP)，並模擬勒索軟體攻擊以了解 ARP 如何偵測威脅並促進快速復原。

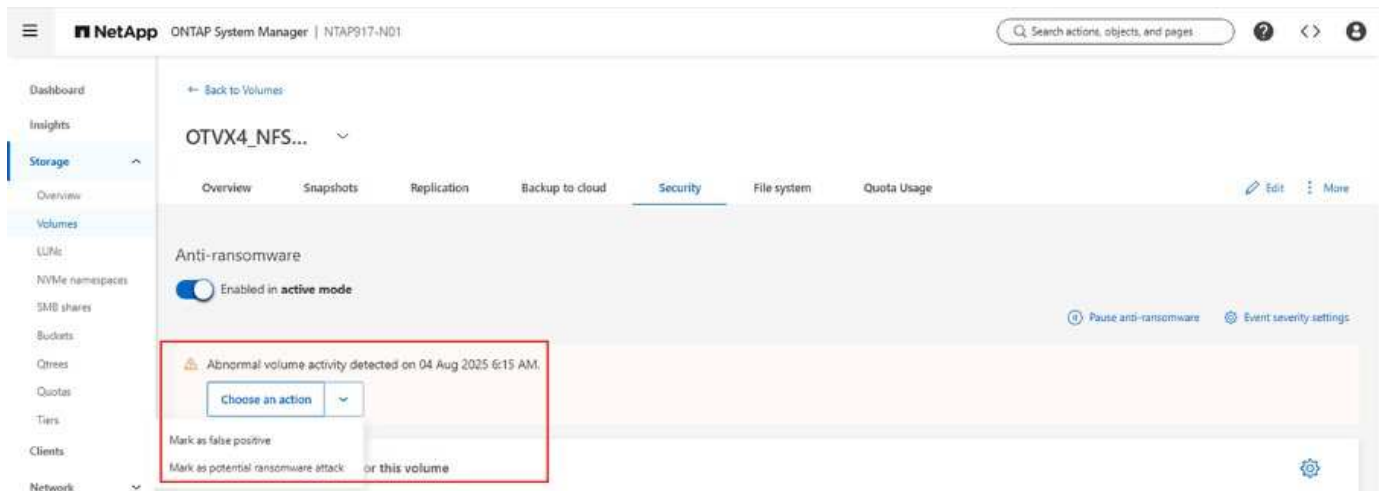
當使用系統管理員或 CLI 在 NAS 磁碟區上啟用 ARP 時，ARP/AI 保護將立即啟用並處於作用中狀態。無需學習期。



在此範例中，使用腳本修改檔案或透過修改檔案副檔名來觸發模擬，以模擬駐留在作為資料儲存附加到 vCenter 的 NFS 磁碟區上的 VM 內的攻擊。

Name	Date modified	Type	Size
Acorn Missouri River.pptx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Moon.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Moon.xls.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Panthers.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pheasant.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pheasant.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pheasant.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pig.pptx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pig.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn River.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn River.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Rosa arkansana.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Rosa arkansana.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Rosa arkansana.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soybean.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soybean.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soybean.xls.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Sun.xls.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tornado.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tornado.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.pptx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Water.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Wheat.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Wheat.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB

如下所示，ARP偵測到了異常活動。



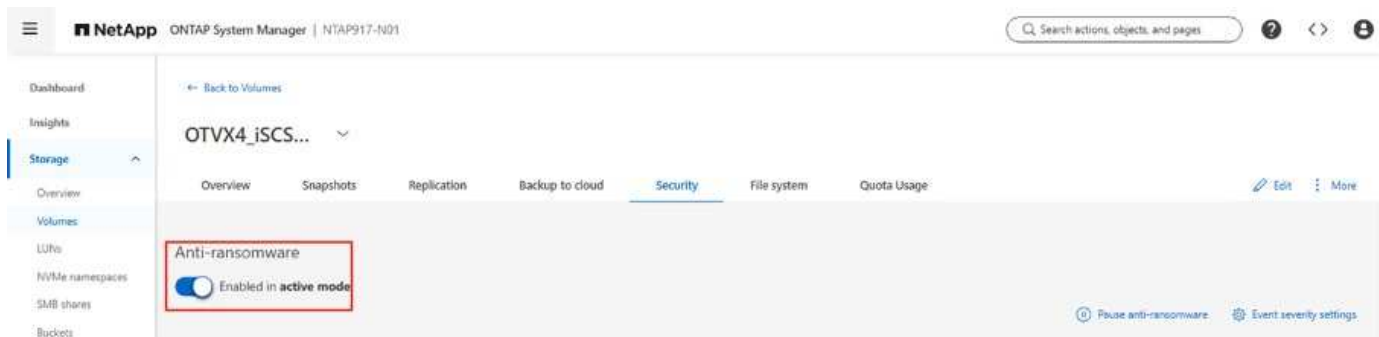
ARP 可提前偵測到攻擊，並能夠從接近攻擊時間的快照中復原資料。若要回滾，請使用事件觸發先前產生的 ARP 定期快照。下面的螢幕截圖顯示了創建的快照：

Anti_ransomware_periodic_backup.2025-08-13_0421	Aug/12/2025 9:21 PM	29 GiB
hourly.2025-08-13_0405	Aug/12/2025 9:05 PM	28.9 GiB
Anti_ransomware_periodic_backup.2025-08-13_0021	Aug/12/2025 5:21 PM	29.1 GiB

有關在用作資料儲存的 NFS 磁碟區上啟用 ARP 並在發生攻擊時復原的詳細指導，請參閱["NFS 儲存的 ARP"](#)。

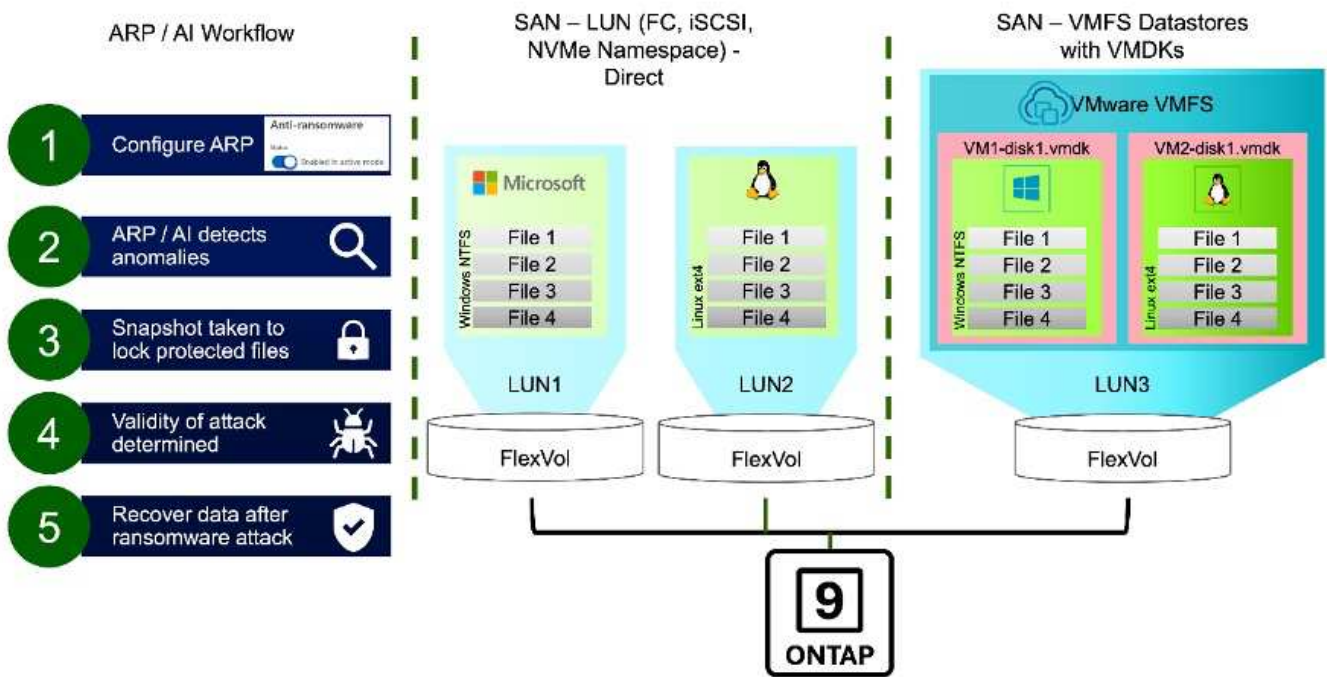
在 SAN 磁碟區上配置 ARP 並模擬對 VM 的攻擊

當在 SAN 磁碟區上啟用 ARP 時，它會從評估階段開始，類似於 NAS 環境中使用的學習模式，然後自動轉換為主動偵測。



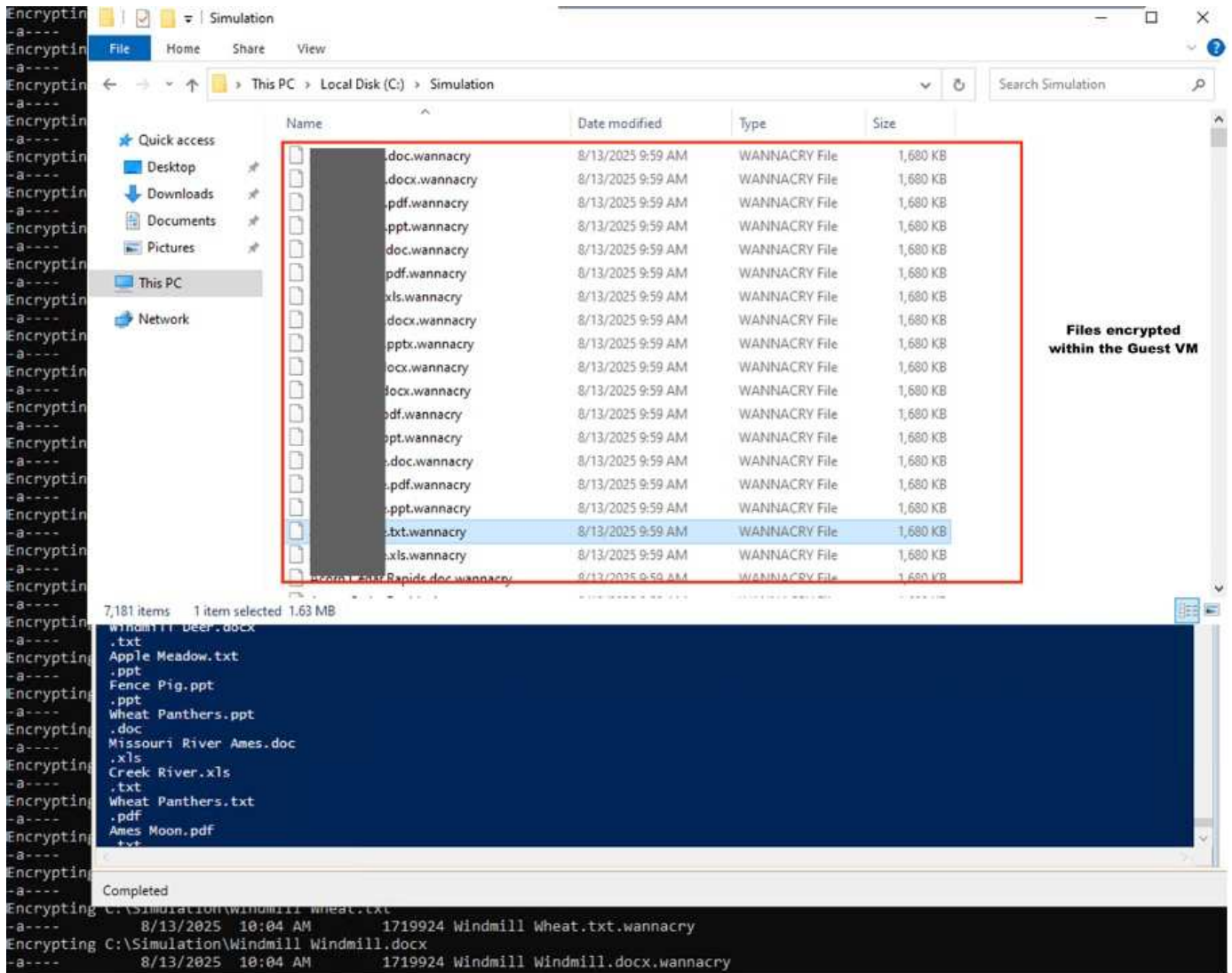
ARP 啟動為期兩到四週的評估期，閾值為 75%，以建立加密行為的基線。可以使用以下方式監控此階段的進度
``security anti-ransomware volume show`` 透過檢查*區塊設備偵測狀態*指令。評估完成後
 ，**Active_suitable_workload** 狀態確認觀察到的熵水準適合持續監控。根據收集的數據，ARP 會自動調整其自適應閾值，以確保準確、靈敏的威脅偵測。根據需求，快照建立間隔可以從預設的 4 小時變更為 1 小時。請謹慎執行此修改。

從ONTAP 9.17.1 開始，NAS 和 SAN 磁碟區都會定期產生 ARP 快照。 ONTAP

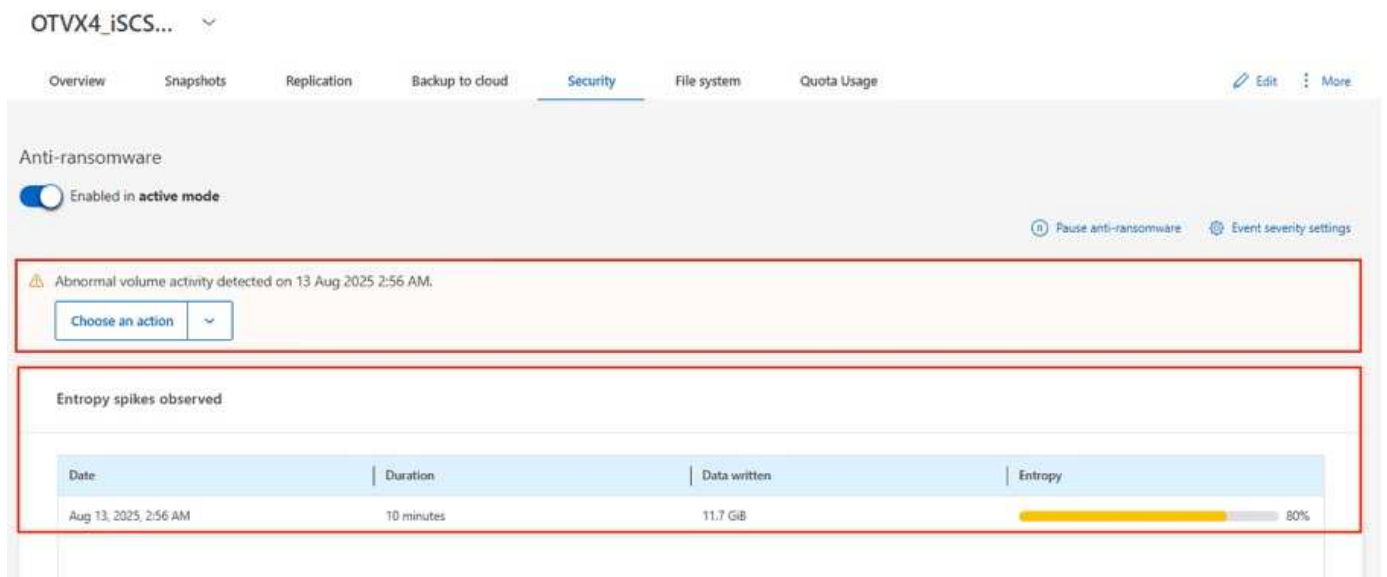


有關詳細信息，請參閱"[SAN 環境和模式類型](#)"

現在是模擬攻擊的時候了。為了示範目的，檔案在基於 iSCSI 的資料儲存體上執行的虛擬機器內進行加密。生成的檔案接近 7000 個，不幸的是，這些檔案受到了勒索軟體攻擊的影響。

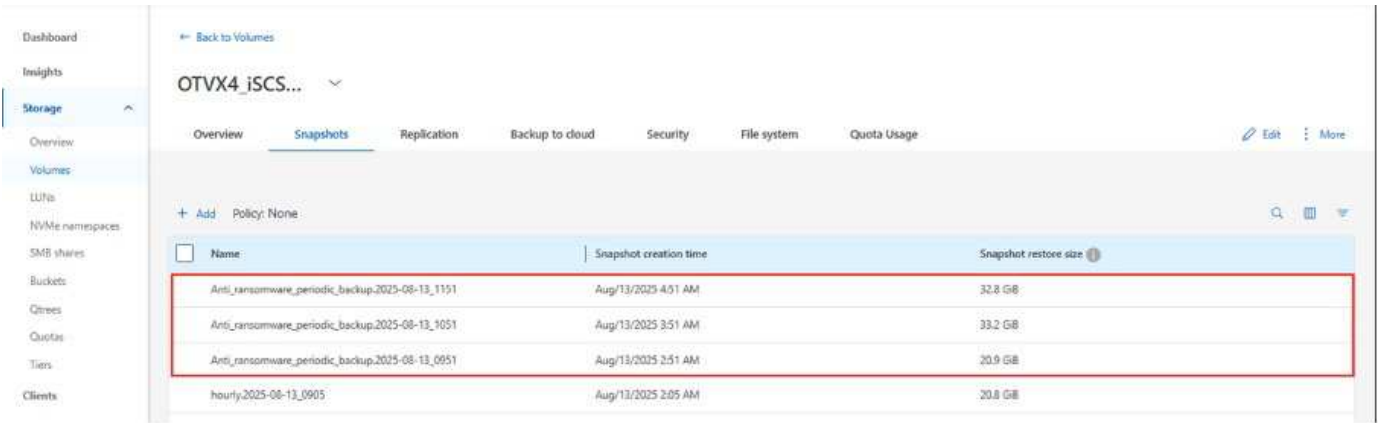


在 10 分鐘內，根據高熵資料偵測到磁碟區上的異常活動，並且 ARP 產生威脅警報，因為它偵測到 VM 內部的熵異常。

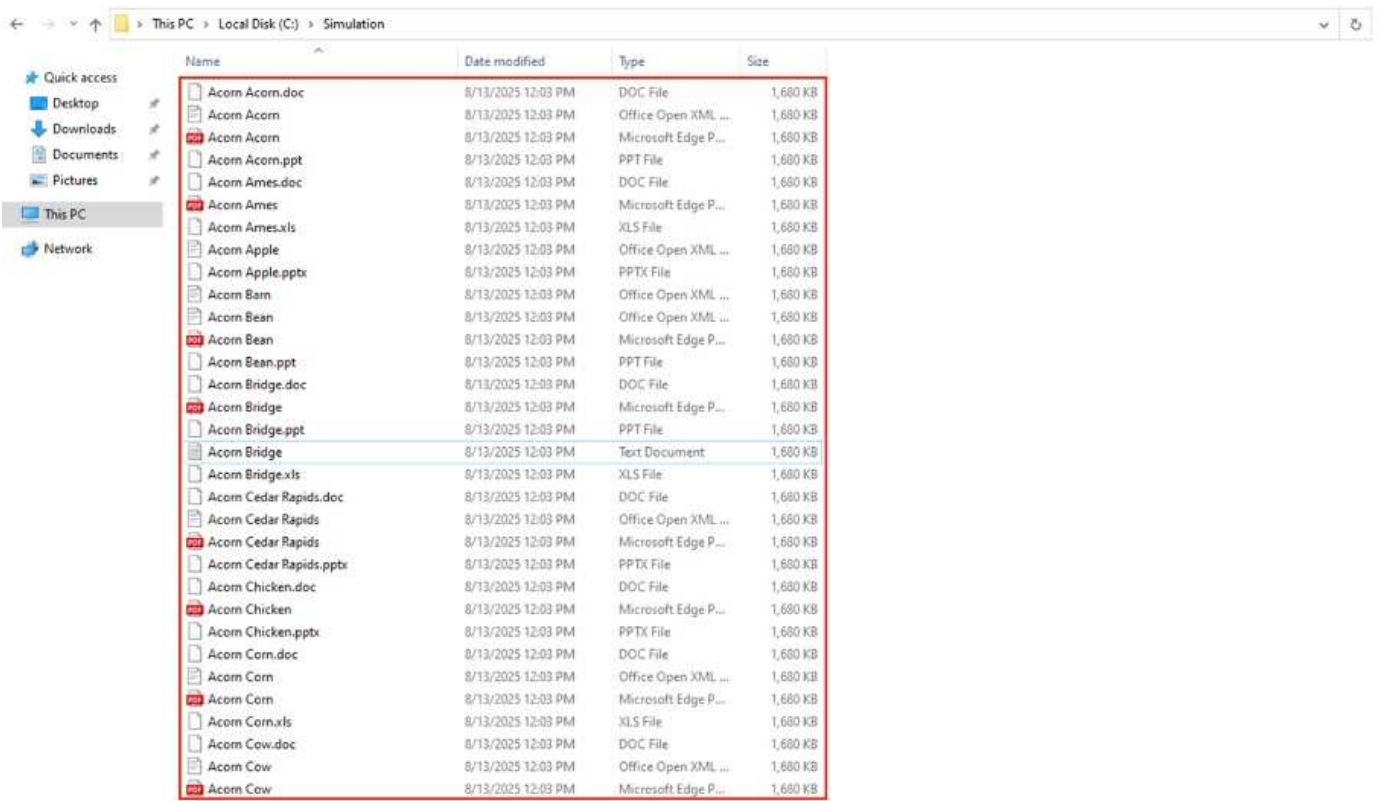


勒索軟體攻擊後恢復虛擬機器及其數據

根據上述步驟確認攻擊後，使用其中一個 ARP 快照或磁碟區的另一個快照來還原資料。



一旦恢復，文件就全部恢復了。



有關詳細指導，請參閱["勒索軟體攻擊後從 ARP 快照恢復數據"](#)

ONTAP作為 VMware 及其他系統的防禦層

只需點擊幾下，企業就可以無縫增強其資料保護策略。 ONTAP採用基於機器學習的先進偵測機制，在 VMware 環境中引入了強大的防禦層。這種智慧保護不僅可提前識別威脅，還可協助在威脅升級之前減輕潛在損害。

此用例不僅適用於 VMware。您可以將相同的原則擴展到任何基於 NAS 或 SAN 的應用程序，以建立多層安全架構。攻擊者被迫穿越多個強化層，大大降低了成功入侵的風險。

ONTAP不僅保護數據，它還能幫助組織在不斷演變的威脅面前保持彈性。

備份和災難復原解決方案

了解如何使用適用於 **VMware vSphere** 的**SnapCenter**插件備份和還原虛擬機

SnapCenter Plug-in for VMware vSphere可對虛擬機器、資料儲存區和 VMDK 檔案實現快速、虛擬機器一致的備份和還原作業。此 VMware 外掛程式與SnapCenter Server 集成，以支援基於應用程式的備份和SnapCenter特定應用程式插件的復原。

文件資源

有關詳細信息，請參閱以下文檔資源。

- ["SnapCenter Plug-in for VMware vSphere文檔"](#)

解決方案資源

請參閱以下 3-2-1 備份解決方案，該方案包含SnapCenter Plug-in for VMware vSphere以及適用於虛擬機器的NetApp備份和復原功能。

技術報告：["使用SnapCenter插件和NetApp Backup and RecoveryVMware 的 3-2-1 資料保護"](#)

Tech ONTAP部落格：["使用SnapCenter插件和NetApp Backup and RecoveryVMware 的 3-2-1 資料保護"](#)

視訊資源

[SnapCenter Plug-in for VMware vSphere- 解決方案先決條件](#)

[SnapCenter Plug-in for VMware vSphere- 部署](#)

[SnapCenter Plug-in for VMware vSphere- 備份工作流程](#)

[SnapCenter Plug-in for VMware vSphere- 還原工作流程](#)

[SnapCenter - SQL 還原工作流程](#)

了解如何使用**NetApp Disaster Recovery**進行虛擬機器災難復原

NetApp Disaster Recovery利用ONTAP儲存自動複製和復原 VMware 虛擬機器。它支援從本機設定還原到 VMware Cloud on AWS，並使用Amazon FSx for NetApp ONTAP或其他本機 VMware 環境。

介紹

成功的計劃和技術組合可確保關鍵資料、應用程式和虛擬機器的保護。DR 的挑戰在於確定適當的保護等級和相關成本。

ONTAP陣列提供內建複製功能，可將磁碟區資料（以及駐留在指定資料儲存 LUN 上的虛擬機器）從一個站點傳輸到另一個站點。NetApp Disaster Recovery與 vSphere 集成，並可自動執行整個工作流程，以便在災難發生時實現無縫故障轉移和故障復原。

有關NetApp Disaster Recovery的更多信息，請參閱["NetApp Disaster Recovery概述"](#)。

注意事項

VMware vSphere 環境中 DR 故障轉移最耗時的部分是在 DR 站點執行清點、註冊、重新配置和啟動虛擬機器所需的步驟。理想的解決方案既具有低 RPO（以分鐘為單位），又具有低 RTO（以分鐘到小時為單位）。DR 解決方案中經常被忽略的一個因素是定期有效地測試 DR 解決方案的能力。

要建立 DR 解決方案，請牢記以下因素：

- 恢復時間目標 (RTO)。RTO 是指企業從災難中復原的速度，或者更具體地說，是執行復原過程以使業務服務再次可用所需的時間。
- 恢復點目標 (RPO)。RPO 是指復原的資料相對於災難發生的時間而言，可供使用的時間。
- 可擴展性和適應性。此因素包括隨著需求的增加而逐步增加儲存資源的能力。

有關可用解決方案的更多技術信息，請參閱：

- ["使用NetApp Disaster Recovery技術為 NFS 資料儲存提供災難復原服務"](#)
- ["使用NetApp Disaster Recovery技術為 VMFS 資料儲存提供災難復原服務"](#)

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。