ONTAP 技術報告

ONTAP Technical Reports

NetApp
February 23, 2026

目錄

ONTAP 技術報告

ONTAP 及應用程式與資料庫技術報告

ONTAP 是許多企業應用程式與資料庫技術的資料管理與資料保護基礎。下列技術報告提供 NetApp 針對 Microsoft SQL Server 、 MySQL 、 Oracle 、 PostgreSQL 、 SAP HANA 及 Epic 的建議實務做法與實作程序指引。

Microsoft SQL Server

SQL Server 是 Microsoft 資料平台的基礎、無論是在內部部署或雲端、都能以記憶體內建技術提供關鍵任務效能、並更快洞悉任何資料。

"Microsoft SQL Server with ONTAP 的最佳實務做法"瞭解儲存管理員和資料庫管理員如何在 ONTAP 儲存設備上成功部署 Microsoft SQL Server 。

> 本文件取代先前發佈的技術報告 _TR-4590 ： Microsoft SQL Server 與 ONTAP 的最佳實務做法指南。 _

"TR-4976 ： NetApp AFF A 系列和 C 系列系統上的虛擬化 Microsoft SQL Server 效能"
瞭解使用 NetApp AFF A 系列和 C 系列系統的 Microsoft SQL Server 效能特性、以及如何根據工作負載選擇正確系統的指引。

"TR-4714 ：使用 SnapCenter 的 Microsoft SQL Server 最佳實務做法"
立即瞭解如何使用 SnapCenter 技術在 ONTAP 儲存設備上成功部署 Microsoft SQL Server 、以保護資料。

MySQL

本文檔介紹了配置要求，並提供了有關在 ONTAP 上部署 MySQL 的調整和存儲配置的指導。

"NetApp ONTAP 最佳實務做法的 MySQL 資料庫"MySQL 及其變種（包括 MariaDB 和 Percona ）廣泛用於許多企業應用程式。這些應用程式涵蓋全球社群網站和大量的經濟應用系統、以及包含數千個資料庫執行個體的中小企業代管系統。瞭解在 ONTAP 上部署 MySQL 的組態需求、以及調整與儲存組態的相關指引。

> 本文件取代先前發佈的技術報告 _TR-4722 ： NetApp ONTAP 最佳實務做法的 MySQL 資料庫。 _

Oracle

ONTAP 專為 Oracle 資料庫所設計。數十年來、 ONTAP 已針對關聯式資料庫 I/O 的獨特需求進行最佳化、並特別建立多項 ONTAP 功能、以滿足 Oracle 資料庫的需求、甚至是 Oracle Inc. 本身的要求。

"ONTAP 上的 Oracle 資料庫"瞭解可讓儲存管理員和資料庫管理員在 ONTAP 儲存設備上成功部署 Oracle 的建議實務做法。

"使用 ONTAP 保護 Oracle 資料"瞭解可讓儲存管理員和資料庫管理員在 ONTAP 儲存設備上成功備份、恢復、複寫及提供災難恢復給 Oracle 的建議實務做法。

"使用 ONTAP 進行 Oracle 災難恢復"瞭解在 MetroCluster 和 SnapMirror 業務持續運作上操作 Oracle 資料庫的建議實務做法、測試程序及其他考量。

"將 Oracle 資料庫移轉至 ONTAP 儲存系統"瞭解規劃移轉策略的整體考量、進行資料移動的三個不同層級、並詳細說明一些可用的各種程序。

以上連結的文件取代了先前發佈的技術報告 _TR-3633 ： ONTAP 上的 Oracle 資料庫； TR-4591 ： Oracle 資料保護：備份、還原、複寫； TR-4592 ： MetroCluster 上的 Oracle ；以及 TR-4534 ：將 Oracle 資料庫移轉至 NetApp 儲存系統

"TR-4969 ： AFF A 系列和 C 系列上的 Oracle 資料庫效能"
ONTAP 是功能強大的資料管理平台、具備內嵌壓縮、不中斷硬體升級、以及從外部儲存陣列匯入 LUN 的原生功能。最多可將 24 個節點叢集在一起、同時透過網路檔案系統（ NFS ）、伺服器訊息區（ SMB ）、 iSCSI 、光纖通道（ FC ）和非揮發性記憶體高速（ NVMe ）傳輸協定來提供資料。此外、 Snapshot 技術是建立數萬個線上備份和完整運作資料庫複本的基礎。除了豐富的 ONTAP 功能集之外、還有各式各樣的使用者需求、包括資料庫大小、效能需求和資料保護需求。瞭解使用 AFF 儲存系統（包括 A 系列和 C 系列）的裸機資料庫效能、其中涵蓋兩種 AFF 選項之間的最大值和實際差異。

"TR-4971 ： AFF A 系列和 C 系列上的虛擬化 Oracle 資料庫效能"
ONTAP 是功能強大的資料管理平台、具備內嵌壓縮、不中斷硬體升級、以及從外部儲存陣列匯入 LUN 的原生功能。最多可將 24 個節點叢集在一起、同時透過網路檔案系統（ NFS ）、伺服器訊息區（ SMB ）、 iSCSI 、光纖通道（ FC ）和非揮發性記憶體高速（ NVMe ）傳輸協定來提供資料。此外、 Snapshot 技術是建立數萬個線上備份和完整運作資料庫複本的基礎。除了豐富的 ONTAP 功能集之外、還有各式各樣的使用者需求、包括資料庫大小、效能需求和資料保護需求。瞭解使用 AFF 儲存系統（包括 A 系列和 C 系列）的虛擬化資料庫效能、其中涵蓋兩種 AFF 選項之間的最大值和實際差異。

"TR-4695 ：使用 FabricPool 進行資料庫儲存分層"
瞭解 FabricPool 的優點和組態選項、包括 Oracle 關聯式資料庫管理系統（ RDBMS ）。

"TR-4899 ： Oracle 資料庫透明化應用程式容錯移轉、採用 SnapMirror 主動式同步" SnapMirror 主動式同步（前身為 SM-BC ）和 Oracle Real Application Cluster （ RAC ）可在發生站台中斷和真正災難時、提供透明的應用程式容錯移轉（ TAF ）和持續性。瞭解 AFF 儲存陣列的組態指南和建議實務做法、其中 SnapMirror Active Sync 是 Oracle RAC 的儲存元件。

"TR-4876 ：採用 ONTAP 解決方案和部署最佳實務做法的 Oracle 多租戶"
瞭解解決方案建議的實務做法、瞭解如何使用 ONTAP 儲存設備來配置、管理及保護 Oracle 多租戶資料庫、以充分發揮 Oracle 多租戶資料庫的效益、以及 ONTAP 軟體的功能。

PostgreSQL

PostgreSQL 隨附的變種包括 PostgreSQL 、 PostgreSQL Plus 和 EDBS PostgreSQL 進階伺服器（ EPAS ）。PostgreSQL 通常部署為多層應用程式的後端資料庫。NetApp ONTAP 是執行 PostgreSQL 資料庫的絕佳選擇、可確保其可靠性、高效能及高效率的資料管理功能。

"ONTAP 最佳實務做法的 PostgreSQL 資料庫"PostgreSQL 隨附的變種包括 PostgreSQL 、 PostgreSQL Plus 和 EDBS PostgreSQL 進階伺服器（ EPAS ）。PostgreSQL 通常部署為多層應用程式的後端資料庫。它受一般中介軟體套件的支援（例如 PHP 、 Java 、 Python 、 Tcl/Tk 、 ODBC 、 和 JDBC)，過去一直是開放原始碼資料庫管理系統的熱門選擇。瞭解在 ONTAP 上部署 PostgreSQL 的組態需求、以及調整與儲存組態的相關指引。

本文件取代先前發表的技術報告 _TR-4770 ： ONTAP 最佳實務做法的 PostgreSQL 資料庫。

SAP HANA

"ONTAP 上的 SAP HANA 資料庫解決方案"設定、管理及自動化 SAP 解決方案的最佳實務做法、請參閱 NetApp SAP 解決方案頁面。

致勝

"EPIC on ONTAP 最佳實務做法"瞭解在內部部署和雲端部署 Epic 的最佳實務做法、同時符合在 ONTAP 上適當部署的組態標準的指南。

本文件取代先前發表的技術報告 _TR-3923 ： Epic 的 NetApp 最佳實務做法。

營運不中斷技術報告

NetApp 提供多種解決方案、可在應用程式和資料上線時進行合理化、以符合成本效益的方式改善效能。資料保護、複寫及持續可用度： ONTAP 資料管理可透過設定 IT 原則管理來簡化資料保護作業、同時透過 MetroCluster 和 SnapMirror 主動式同步提供業務連續性。

這些技術報告會針對和產品文件進行擴充 "ONTAP SnapMirror 主動同步" "ONTAP MetroCluster" 。

SnapMirror 主動式同步（前身為 SM-BC ）

"TR-4878 ： SnapMirror 主動同步" SnapMirror 主動式同步是一種持續可用的儲存解決方案、具備應用程式層級的精細度、適用於在 AFF 或所有 SAN 陣列（ ASA ）儲存系統上執行的 ONTAP 、以滿足最關鍵業務應用程式的 RPO 0 和 RTO 0 需求。

MetroCluster

"TR-4705 ： NetApp MetroCluster 解決方案架構與設計"
本文件說明 ONTAP 中 MetroCluster 功能的高階架構和設計概念。

知識產權**MetroCluster**

"TR-4689 ： NetApp MetroCluster IP"MetroCluster 是適用於在 FAS 和 AFF 系統上執行的 ONTAP 的持續可用儲存解決方案。MetroCluster IP 是採用乙太網路型後端儲存架構的最新進化產品。MetroCluster IP 提供高度備援的組態、以滿足最關鍵業務應用程式的需求。MetroCluster IP 包含在 ONTAP 中、可為使用 ONTAP 儲存設備的用戶端和伺服器提供 NAS 和 SAN 連線。

部分**FC MetroCluster**

"TR-4375 ： NetApp MetroCluster FC"MetroCluster 為任務關鍵型應用程式提供跨地理區分離資料中心的持續資料可用度。瞭解 MetroCluster FC 建議實務做法、設計決策及支援的組態。

ONTAP 資料保護與災難恢復技術報告

SnapMirror 是一款經濟實惠、易於使用的統一複製解決方案、適用於整個資料架構。它可透過LAN或WAN高速複寫資料。您可以在虛擬和傳統環境中、為業務關鍵應用程式（例如 Microsoft Exchange 、 Microsoft SQL Server 和 Oracle ）提供高資料可用度和快速資料複寫功能。當您將資料複寫到一或多個 ONTAP 儲存系統、並持續更新次要資料時、您的資料會保持在最新狀態、並隨時可供您使用。不需要外部複寫伺服器。

這些技術報告會針對產品文件進行擴充"ONTAP 資料保護與災難恢復"。

SnapMirror

SnapMirror 非同步

"TR-4015 ： SnapMirror 非同步組態和最佳實務做法"瞭解設定 SnapMirror 非同步（ SM-A ）磁碟區複寫，一致性群組和儲存虛擬機器（ SVM 災難恢復）的建議實務做法。

"TR-4678 ：資料保護與備份 ONTAP FlexGroup 磁碟區"
瞭解 FlexGroup 磁碟區的建議資料保護與備份。主題包括 Snapshot 複本、 SnapMirror 及其他資料保護與備份解決方案。

SnapMirror同步

"TR-4733 ： SnapMirror 同步組態和最佳實務做法"瞭解設定 SnapMirror 同步（ SM-S ）複寫的建議做法。

SnapMirror 三資料中心災難恢復

"TR-4832 ：使用 NetApp SnapMirror for ONTAP 9.7 進行三個資料中心災難恢復"瞭解使用 ONTAP SnapMirror 技術進行複寫的三個資料中心災難恢復組態。

應用程式與基礎架構搭配 SnapMirror

"TR-4900 ： VMware Site Recovery Manager 與 ONTAP" ONTAP 自 2002 年引進現代化資料中心以來、一直是 VMware vSphere 環境的領先儲存解決方案、並持續新增創新功能、以簡化管理、同時降低成本。瞭解 VMware 領先業界的災難恢復（ DR ）軟體 VMware Site Recovery Manager （ SRM ）推薦的 ONTAP 解決方案、包括最新產品資訊和建議實務做法、以簡化部署、降低風險並簡化後續管理。

ONTAP 網路保存庫

"ONTAP 網路保存庫"NetApp 的 ONTAP 型網路資料保險箱為組織提供全方位且靈活的解決方案、以保護最重要的資料資產。ONTAP 運用邏輯氣帶和強大的強化方法、讓您建立安全、隔離的儲存環境、以因應不斷演變的網路威脅。透過 ONTAP 、您可以確保資料的機密性、完整性和可用度、同時維持儲存基礎架構的敏捷度和效率。

ONTAP FlexCache 與 FlexGroup Volume 技術報告

NetApp NAS 解決方案可簡化資料管理、協助您跟上成長腳步、同時最佳化成本。ONTAP NAS 解決方案可在統一化架構中提供不中斷營運、獲證實的效率和無縫擴充能力。採用 ONTAP 技術的橫向擴充 NAS 運用龐大的 ONTAP 生態系統、擁有重大的創新商機和願景、可推動未來的創新。

這些技術報告會針對和產品文件進行擴充 "ONTAP FlexCache Volume" "ONTAP FlexGroup Volume" 。

FlexCache

"TR-4743：FlexCache 《不ONTAP 實的"
FlexCache 是一種快取技術、可在相同或不同的 ONTAP 叢集上建立磁碟區的稀疏可寫入複本。它可以讓資料和檔案更接近使用者、以更小的佔用空間來加快處理量。瞭解如何使用 FlexCache 、建議的實務做法、限制及設計與實作考量。

FlexCache 回寫

"FlexCache 回寫" FlexCache 回寫是 ONTAP 9.15.1 推出的另一種寫入快取的作業模式。回寫功能可將寫入內容提交至快取的穩定儲存設備、並將其確認給用戶端、而無需等待資料傳送至原始伺服器。資料會以非同步方式重新排清回來源。因此、全球分散式檔案系統可讓寫入作業以接近本機的速度執行特定工作負載和環境、提供顯著的效能效益。

資料量FlexGroup

"TR-4571a ： FlexGroup 十大最佳實務做法"
本技術報告是 TR-4571 的精簡版： NetApp ONTAP FlexGroup Volume 快速使用的最佳實務做法與實作指南。

"TR-4557 ： NetApp ONTAP FlexGroup Volume - 技術概觀"
瞭解 FlexGroup Volume （ ONTAP 橫向擴充 NAS 容器）、它將近乎無限的容量與中繼資料繁重工作負載中可預測的低延遲效能融合在一起。

"TR-4571 ： NetApp ONTAP FlexGroup Volume 最佳實務做法與實作指南"
瞭解 FlexGroup Volume 、建議實務做法和實作秘訣。FlexGroup Volume 是 ONTAP 橫向擴充 NAS 容器的演進、可在中繼資料繁重的工作負載中、將幾乎無限的容量與可預測的低延遲效能混合在一起。

"TR-4678 ： FlexGroup 磁碟區的資料保護與備份"
瞭解 FlexGroup 磁碟區的資料保護與備份、包括 Snapshot 複本、 SnapMirror 及其他資料保護與備份解決方案。

ONTAP NAS 技術報告

NetApp NAS 解決方案可簡化資料管理、協助您跟上成長腳步、同時最佳化成本。ONTAP NAS 解決方案可在統一化架構中提供不中斷營運、效率和無縫擴充性。採用 NetApp ONTAP 技術的橫向擴充 NAS 運用龐大的 ONTAP 生態系統、擁有重大的創新商機和願景、可推動未來的創新。

這些技術報告會針對和產品文件進行擴充 "ONTAP NAS 儲存管理" "ONTAP S3 儲存管理" 。

NFS

"TR-4067 ： ONTAP 最佳實務做法與實作指南中的 NFS"
瞭解 ONTAP 中 NFS 的基本概念、支援資訊、組態秘訣及建議實務做法。

"TR-4962 ： NFSv4.2 延伸屬性"
瞭解如何在 ONTAP 9.12.1 及更新版本中啟用及使用 NFSv4.2 延伸屬性。

中小企業

"TR-4740 ： SMB 3.0 多通道"
Microsoft 在 SMB 3.0 傳輸協定中引進多通道、其目標是藉由解決 SMB1 和 SMB2 的效能和可靠性限制、來改善 SMB3 傳輸協定。瞭解 ONTAP 的多重通路功能、包括其功能、建議實務做法和效能測試結果。

多重傳輸協定

"TR-4887 ： ONTAP 中的多重傳輸協定 NAS 總覽與最佳實務做法"
瞭解多重傳輸協定 NAS 存取如何在 ONTAP 中運作、以及多重傳輸協定環境的建議實務做法。

SS3 ONTAP

"TR-4814 ： ONTAP 最佳實務做法中的 S3" 瞭解將 Amazon Simple Storage Service （ S3 ）與 ONTAP 軟體搭配使用的建議實務做法，以及將 ONTAP 作為物件存放區與原生 S3 應用程式搭配使用的功能和組態，或作為 FabricPool 的分層目的地。

名稱服務

"TR-4523 ： ONTAP 中的 DNS 負載平衡"
瞭解如何設定 ONTAP 以搭配 DNS 負載平衡方法使用、包括 ONTAP 中的 DNS 、各種組態方法、以及建議的實務做法。

"TR-4668 ：名稱服務最佳實務做法指南"
瞭解在 ONTAP 中實作網路附加儲存（ NAS ）解決方案（例如 CIFS/SMB 和 NFS ）時的建議實務做法、限制和考量。

"TR-4835 ：如何在 ONTAP 多重傳輸協定 NAS 身分識別管理中設定 LDAP"
瞭解如何在 ONTAP 中設定適用於多重傳輸協定 NAS 的輕量型目錄存取傳輸協定（ LDAP ）身分識別管理。

NAS 安全性

"TR-4616：ONTAP NFS Kerberos in Sf2"
瞭解 ONTAP 中的 NFS Kerberos 、包括 Active Directory 和 Red Hat Enterprise Linux （ RHEL ）用戶端的組態步驟。

ONTAP 網路技術報告

ONTAP 提供各種不同的網路功能和組態、以滿足最嚴苛的橫向擴充應用程式需求。公司可以利用網路功能和功能、建立可靠且安全的資料存取。

這些技術報告會針對產品文件進行擴充"ONTAP 網路管理"。

"TR-4949 ：在資料中心使用 ONTAP 的 BGP/VIP"
瞭解如何在 ONTAP 中快速部署基本 BGP 組態。

ONTAP SAN 技術報告

ONTAP SAN 儲存設備提供簡化的 SAN 體驗，可為貴組織的關鍵任務資料庫和其他 SAN 工作負載提供高可用度。ONTAP SAN 與 Oracle 、 SAP 和 Microsoft SQL Server 資料庫整合了同級最佳的資料服務、加上 VMware 和其他領先業界的 Hypervisor 、可為企業資料庫應用程式提供更快的價值實現時間。

這些技術報告會針對產品文件進行擴充"ONTAP SAN 儲存管理"。

"TR-4080 ： ONTAP 中現代 SAN 的最佳實務做法"
瞭解 ONTAP 中的區塊傳輸協定、以及建議實務做法。

"TR-4684 ：使用 NVMe over Fabrics （ NVMe of ）實作及設定現代化 SAN"
瞭解如何實作和設定 NVMe over Fabrics 傳輸（ NVMe over Fibre Channel 和 NVMe over TCP ）。主題包括設計、實作、組態、管理準則和建議實務做法、以使用 NVMe 通訊協定和傳輸來建置高可用度、高效能的現代化 SAN 解決方案。

"TR-4968 ： NetApp All SAN 陣列資料可用度與完整性"
瞭解 All SAN 陣列系統的各種資料保護與資料完整性功能如何運作、以達到最長的應用程式正常運作時間、以及設計、實作及管理 SAN 網路的建議實務做法。

"現代化的 SAN 雲端連線 Flash 解決方案"
此 NetApp 驗證架構已由 NetApp 、 VMware 和 Broadcom 共同設計與驗證。它使用最新的 Brocade 、 Emulex 和 VMware vSphere 技術解決方案、搭配 NetApp All Flash 儲存設備、為企業級 SAN 儲存設備和資料保護樹立新標準、創造卓越的商業價值。

安全性

ONTAP 安全技術報告

ONTAP 持續進化、安全性是解決方案不可或缺的一部分。最新版的 ONTAP 包含許多新的安全功能、這些功能對貴組織來說非常重要、可以保護其資料在混合雲中的安全性、防止勒索軟體攻擊、並遵循業界建議的實務做法。這些新功能也能協助貴組織邁向 Zero Trust 模式。

這些技術報告會針對產品文件進行擴充"ONTAP 安全性與資料加密"。

ONTAP 網路保存庫

"ONTAP 網路保存庫"NetApp 的 ONTAP 型網路資料保險箱為組織提供全方位且靈活的解決方案、以保護最重要的資料資產。ONTAP 運用邏輯氣帶和強大的強化方法、讓您建立安全、隔離的儲存環境、以因應不斷演變的網路威脅。透過 ONTAP 、您可以確保資料的機密性、完整性和可用度、同時維持儲存基礎架構的敏捷度和效率。

勒索軟體

"TR-4572 ：勒索軟體的 NetApp 解決方案" 瞭解勒索軟體如何進化、以及如何利用 NetApp 解決方案來識別攻擊、防止擴散、並儘快恢復。本文件所提供的指引與解決方案旨在協助組織擁有網路彈性解決方案、同時符合其規定的資訊系統機密性、完整性及可用度安全目標。

"TR-4526 ：使用 NetApp SnapLock 的符合 WORM 儲存設備"
許多企業都仰賴一次寫入、多次讀取（ WORM ）資料儲存設備來滿足法規遵循要求、或只是在資料保護策略中新增另一層。瞭解如何將 ONTAP 的 WORM 解決方案 SnapLock 整合至需要 WORM 資料儲存的環境。

零信任

"NetApp 與 Zero Trust" 零信任傳統上是一種以網路為中心的方法、用於建構微核心和周邊（ MCAP ）、以控制區段閘道的方式來保護資料、服務、應用程式或資產。ONTAP 採用以資料為中心的 Zero Trust 方法、讓儲存管理系統成為區段閘道、以保護及監控客戶資料的存取。特別是、 FPolicy Zero Trust 引擎和 FPolicy 合作夥伴生態系統成為控制中心、可深入瞭解正常和異常的資料存取模式、並識別內部威脅。

多因素驗證

"TR-4647 ： ONTAP 最佳實務做法與實作指南中的多因素驗證"
瞭解 ONTAP 的多因素驗證功能、以便使用 System Manager 、 Active IQ Unified Manager 和 ONTAP 安全 Shell （ SSH ） CLI 驗證進行管理存取。

"TR-4717 ：使用通用存取卡進行 ONTAP SSH 驗證"
瞭解如何搭配 ActivClient 軟體、設定及測試協力廠商 SSH 用戶端、以便在 ONTAP 中設定 ONTAP 儲存管理員時、透過儲存在通用存取卡（ CAC ）上的公開金鑰來驗證其身分。

多租戶

"TR-4160 ： ONTAP 中的安全多租戶共享"
瞭解如何在 ONTAP 中使用儲存 VM 實作安全的多租戶共享、包括設計考量和建議實務做法。

標準

"TR-4401 ： PCI-DSS 4.0 和 ONTAP"
瞭解如何根據 PCI DSS 4.0 標準驗證系統、並符合您套用至 NetApp ONTAP 系統的控制項要求。

屬性型存取控制

"使用 ONTAP 進行屬性型存取控制"瞭解如何設定 NFSv4.2 安全性標籤和延伸屬性（ xATT ），以支援角色型存取控制（ RBAC ）和屬性型存取控制（ ABAC ），這是根據使用者，資源和環境屬性來定義權限的授權策略。

NetApp 勒索軟體解決方案

勒索軟體和 **NetApp** 的保護產品組合

勒索軟體仍是 2024 年組織造成營運中斷的最重大威脅之一。根據 "Sophos State of 勒索軟體 2024"、勒索軟體攻擊影響了 72% 的受訪對象。勒索軟體攻擊已進化成更精密且目標明確、威脅行動者運用人工智慧等先進技術、將其影響和利潤最大化。

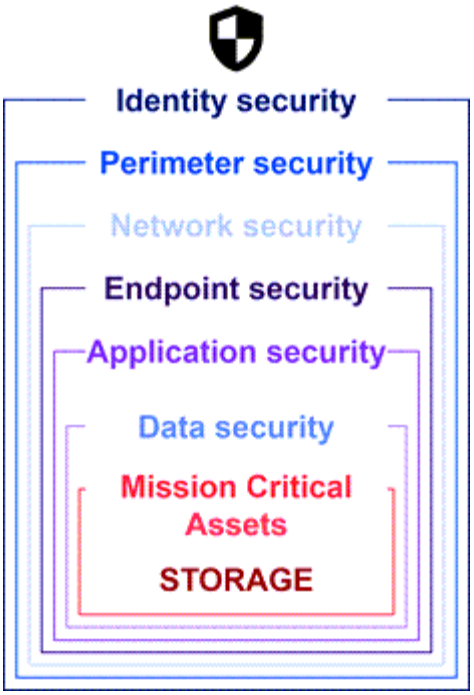
組織必須從周邊、網路、身分識別、應用程式、以及資料位於儲存層級的位置、查看整個安全狀態、並保護這些層級的安全。在現今的威脅環境中、在儲存層採用以資料為中心的網路保護方法是至關重要的。雖然沒有任何單一解決方案能阻擋所有攻擊、但使用包括合作夥伴關係和第三方在內的解決方案組合、可提供分層防禦。

NetApp 產品組合提供各種有效的工具來進行可見度、偵測和補救、協助您及早發現勒索軟體、防止散播、並在必要時快速恢復、以避免代價高昂的停機時間。傳統的分層防禦解決方案依然盛行、第三方和合作夥伴的可見度與偵測解決方案也同樣如此。有效的補救措施仍是回應任何威脅的關鍵部分。運用不可變的 NetApp Snapshot 技術和 SnapLock 邏輯空空缺解決方案的獨特產業方法、是一項產業差異化優勢、也是勒索軟體補救功能的最佳實務做法。

> 自 2024 年 7 月起，技術報告（ _TR-4572 ： NetApp 勒索軟體保護）的內容（先前以 PDF 格式發佈）可在 docs.netapp.com 上取得。

資料是主要目標

網路犯罪者越來越直接鎖定資料、以辨識其價值。雖然周邊、網路和應用程式的安全性都很重要、但卻可以略過這些安全性。儲存層著重於保護資料來源、提供關鍵的最後防線。存取正式作業資料、加密或使其無法存取、是勒索軟體攻擊的目標。為了達到目標、攻擊者必須已經破解組織目前部署的現有防禦措施、從周邊環境到應用程式安全性。



可惜、許多組織並未充分利用資料層的安全功能。這就是 NetApp 勒索軟體保護產品組合的其中一項、可在最後一道防線上保護您的安全。

勒索軟體的實際成本

贖金本身並不是對企業造成最大的金錢影響。雖然這筆款項並不微不足道、但與遭受勒索軟體事件的停機成本相比、這筆款項卻很微不足道。

贖金付款只是處理勒索軟體事件時的一項回收成本要素。根據該 "2024 Sophos State of 勒索軟體"報告、 2024 年企業組織申報的勒索軟體攻擊平均回收成本為 2.73 萬美元、比 2023 年報告的 1.82 萬美元增加將近 100 萬美元。對於高度依賴 IT 可用度的組織、例如電子商務、股票交易和醫療保健、成本可能高出 10 倍以上。

網路保險成本也持續攀升、因為受到保險公司勒索軟體攻擊的可能性非常大。

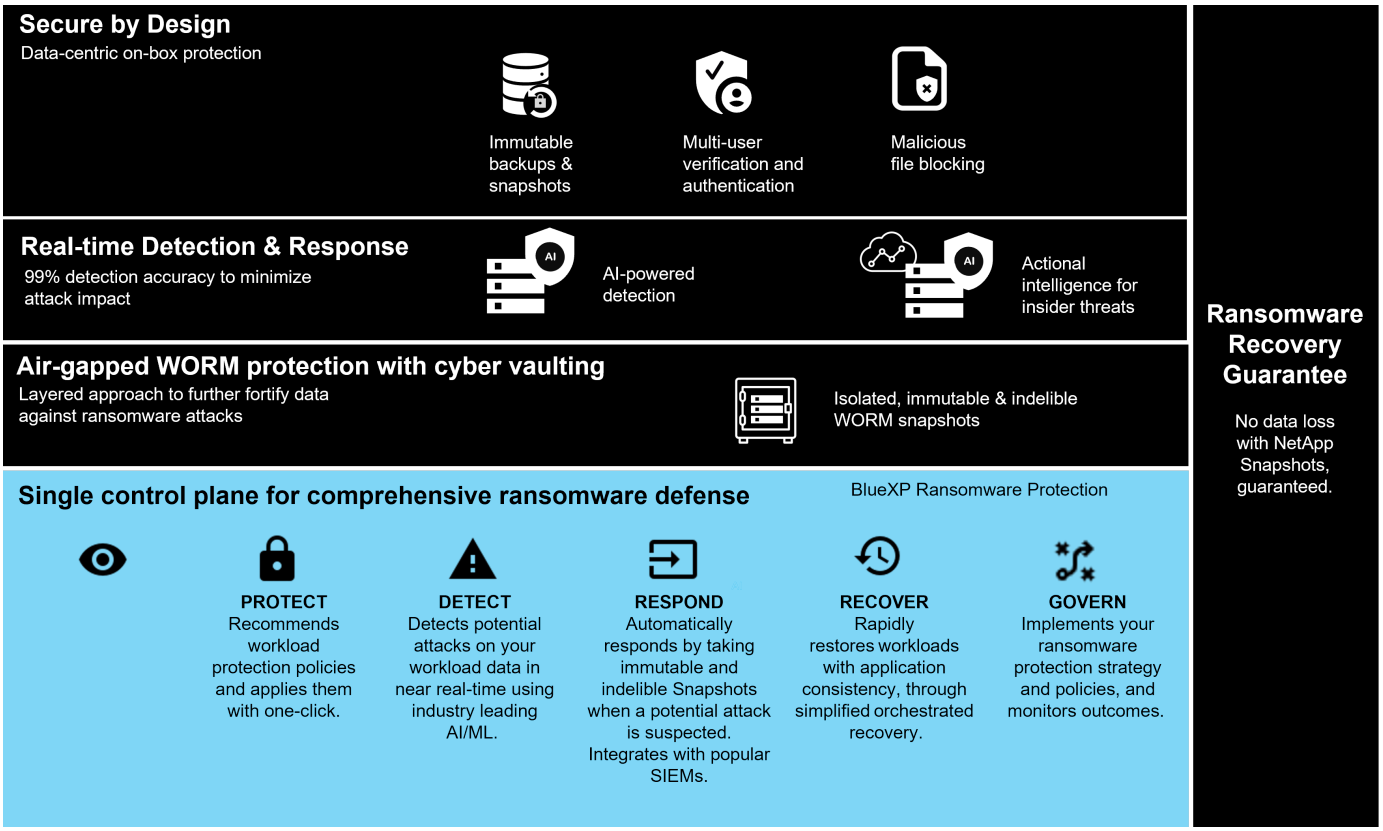
資料層的勒索軟體保護

NetApp 瞭解您的安全態勢、從邊界到儲存層的資料所在、都是在整個組織中的廣泛且深入的。您的安全堆疊十分複雜、應該能在技術堆疊的每個層級提供安全性。

資料層的即時保護更為重要、而且有獨特的需求。為了有效運作、此層的解決方案必須提供以下關鍵屬性：

- * 設計上的安全性 * 可將成功攻擊的機率降至最低
- * 即時偵測與回應 * 、將成功攻擊的影響降到最低
- * 空中綁定 WORM 保護 * 可隔離關鍵資料備份
- * 單一控制飛機 * 提供全面的勒索軟體防禦

NetApp 可以提供所有這些功能、甚至更多功能。



NetApp 的勒索軟體保護產品組合

NetApp "內建勒索軟體保護"為您的關鍵資料提供即時、強大、多面向的防禦功能。先進的 AI 驅動偵測演算法是其核心、可持續監控資料模式、以 99% 的準確度迅速識別可能的勒索軟體威脅。快速回應攻擊可讓我們的儲存設備快速建立資料快照、並保護複本的安全、確保快速恢復。

為了進一步強化資料、 NetApp 的"網路拖運"功能會將資料隔離在邏輯空氣間隙中。透過保護關鍵資料、我們可確保快速的業務持續運作。

NetApp"NetApp勒索軟體防護"透過單一控制平面智慧協調和執行端到端以工作負載為中心的勒索軟體防禦，減輕營運負擔，因此您只需單擊即可識別和保護處於危險中的關鍵工作負載數據，準確、自動地檢測和響應以限制潛在攻擊的影響，並在幾分鐘內（而不是幾天內）恢復工作負載，保護您寶貴的工作負載數據並最大限度地減少代價高昂的中斷。

身為內建的原生 ONTAP 解決方案，可保護未經授權存取您的資料，"多重管理驗證（ MAV ）"並具備一組強大的功能，可確保刪除磁碟區，建立其他管理使用者或刪除快照等作業，只有在至少有第二位指定管理員核准之後才能執行。如此可防止遭到入侵、惡意或缺乏經驗的系統管理員進行不必要的變更或刪除資料。在刪除快照之前，您可以視需要設定任意數量的指定管理員核准者。

NetApp ONTAP 解決了 "多因素驗證（ MFA ）"在系統管理器中基於 Web 和 SSH CLI 驗證的要求。

NetApp 的勒索軟體保護功能可在不斷演變的威脅環境中、讓您高枕無憂。其全方位方法不僅能抵禦目前的勒索軟體變種、也能因應新興威脅、為您的資料基礎架構提供長期安全性。

瞭解其他保護選項

- "數位顧問勒索軟體保護"

- "Data Infrastructure Insights儲存工作負載安全"
- "FPolicy"
- "SnapLock 和防竄改快照"

勒索軟體恢復保證

NetApp 保證在發生勒索軟體攻擊時還原快照資料。我們保證：如果我們無法協助您還原快照資料、我們會做對的。新購買的 AFF A 系列、 AFF C 系列、 ASA 和 FAS 系統均提供保證。

深入瞭解

- "恢復保證服務說明"
- "勒索軟體恢復保證部落格"。

相關資訊

- "NetApp 支援網站資源頁面"
- "NetApp 產品安全性"

SnapLock 和防竄改快照可保護勒索軟體

SnapLock 是 NetApp Snap Ar武庫 中的重要武器之一、它在防範勒索軟體威脅方面已獲證實相當有效。SnapLock 可防止未經授權的資料刪除、提供額外的安全層級、確保即使發生惡意攻擊、關鍵資料仍能保持完整且可存取。

符合法規**SnapLock**

SnapLock Compliance （ SLC ）為您的資料提供不可磨滅的保護。即使系統管理員嘗試重新初始化陣列、 SLC 也會禁止刪除資料。與其他競爭產品不同、 SnapLock Compliance 不易透過這些產品的支援團隊而遭受社會工程駭客攻擊。受 SnapLock Compliance Volume 保護的資料可在資料到達到期日之前恢復。

若要啟用 SnapLock 、"ONTAP One"則需要授權。

深入瞭解

- "SnapLock 文件"

防竄改快照

防竄改 Snapshot （ TPS ）複本提供了一種方便且快速的方法、可保護資料免受惡意行為的侵害。與 SnapLock Compliance 不同的是、 TPS 通常用於主要系統、使用者可以在確定的時間內保護資料、並將資料留在本機以進行快速恢復、或不需要將資料從主要系統複寫。TPS 使用 SnapLock 技術，即使 ONTAP 管理員使用相同的 SnapLock 保留到期期間，也無法刪除主快照。即使磁碟區未啟用 SnapLock ，也無法刪除快照，不過快照的性質與 SnapLock Compliance 磁碟區的性質並不相同。

若要使快照防竄改，"ONTAP One"必須取得授權。

深入瞭解

- "鎖定快照以防止勒索軟體攻擊"。

FPolicy 檔案封鎖

FPolicy 可防止不想要的檔案儲存在企業級儲存設備上。FPolicy 也可讓您封鎖已知的勒索軟體副檔名。使用者仍擁有主資料夾的完整存取權限、但 FPolicy 不允許使用者儲存管理員標記為封鎖的檔案。無論這些檔案是 MP3 檔案或已知的勒索軟體副檔名、都沒問題。

使用 **FPolicy** 原生模式封鎖惡意檔案

NetApp FPolicy 原生模式（名稱的進化、檔案原則）是檔案副檔名封鎖架構、可讓您封鎖不想要的檔案副檔名、使其無法進入您的環境。這是 ONTAP 十多年來的一部分、在協助您防範勒索軟體方面非常有用。這款 Zero Trust 引擎非常實用、因為除了存取控制清單（ ACL ）權限之外、您還能獲得額外的安全措施。

在ONTAP系統管理器和NetApp Console中，有超過 3000 個檔案副檔名的清單可供參考。

某些擴充功能在您的環境中可能是合法的、而封鎖這些擴充功能可能會導致非預期的問題。在設定原生 FPolicy 之前、請先建立適合您環境的清單。

所有 ONTAP 授權均包含 FPolicy 原生模式。

深入瞭解

- "部落格：對抗勒索軟體：第三部分： ONTAP FPolicy 、另一個強大的原生（又稱為免費）工具"

使用 **FPolicy** 外部模式啟用使用者和實體行為分析（ **UEBA** ）

FPolicy 外部模式是檔案活動通知和控制架構、可提供檔案和使用者活動的可見度。外部解決方案可使用這些通知來執行 AI 型分析、以偵測惡意行為。

也可以將 FPolicy 外部模式設定為等待 FPolicy 伺服器核准、再允許特定活動通過。這樣的多個原則可在叢集上進行設定、提供您極大的彈性。

如果設定為提供核准、 FPolicy 伺服器必須回應 FPolicy 要求；否則、儲存系統效能可能會受到負面影響。

FPolicy 外部模式包含在"所有 ONTAP 授權"中。

深入瞭解

- "部落格：對抗勒索軟體：第四部分：使用 FPolicy 外部模式的 UBA 和 ONTAP 。"

Data Infrastructure Insights儲存工作負載安全

儲存工作負載安全性 (SWS) 是NetAppData Infrastructure Insights的功能，可大幅增強ONTAP環境的安全態勢、可恢復性和責任感。 SWS 採用以使用者為中心的方法，追蹤環境中每個經過驗證的使用者的所有檔案活動。它使用高級分析為每個使用者建立正常和季節性的存取模式。這些模式用於快速識別可疑行為，而無需勒索軟體簽名。

當 SWS 偵測到潛在的勒索軟體或資料刪除時，它可以採取自動措施，例如：

- 拍攝受影響磁碟區的快照。

- 封鎖疑似惡意活動的使用者帳戶和 IP 位址。
- 傳送警示給管理員。

由於 SWS 可以採取自動化行動來快速阻止內部威脅、並追蹤每個檔案活動、因此從勒索軟體事件中恢復的過程更簡單、更快。內建進階稽核和鑑識工具、使用者可以立即查看哪些磁碟區和檔案受到攻擊、攻擊來自哪個使用者帳戶、以及執行了哪些惡意動作。自動快照可減輕損害並加速檔案還原。

ONTAP 的自主勒索軟體保護（ ARP ）所發出的警示也會顯示在 SWS 中、為同時使用 ARP 和 SWS 的客戶提供單一介面、以防止勒索軟體攻擊。

深入瞭解

- "NetAppData Infrastructure Insights"

NetApp ONTAP 內建的內建 AI 型偵測與回應功能

隨著勒索軟體威脅越來越複雜、您的防禦機制也越來越複雜。NetApp 的自動勒索軟體保護（ ARP ）是由 AI 提供、內建於 ONTAP 的智慧型異常偵測功能。開啟此功能、為您的網路恢復能力增添另一層防禦。

ARP 和 ARP/AI 可透過 ONTAP 內建管理介面、系統管理員進行設定、並以每個磁碟區為基礎啟用。

自主勒索軟體保護（Arp）

自主勒索軟體保護（ ARP ）是自 9.10.1 起的另一個原生內建 ONTAP 解決方案、從 NAS 儲存磁碟區工作負載檔案活動和資料 Entropy 來自動偵測潛在的勒索軟體。ARP 為系統管理員提供即時偵測、洞見和資料還原點、提供前所未有的隨裝即用勒索軟體偵測功能。

對於支援 ARP 的 ONTAP 9 ． 15.1 版和更早版本、 ARP 會以學習模式開始學習一般工作負載資料活動。對於大多數環境而言、這可能需要七天的時間。學習模式完成後、 ARP 會自動切換至使用中模式、並開始尋找可能是勒索軟體的異常工作負載活動。

如果偵測到異常活動，就會立即擷取自動快照，以最少受感染資料的方式，盡可能提供最接近攻擊時間的還原點。同時、系統會產生自動警示（可設定）、讓系統管理員能夠查看異常的檔案活動、以便判斷該活動是否確實是惡意活動、並採取適當的行動。

如果活動是預期的工作負載、管理員可以輕鬆地將其標示為誤判。ARP 會將這項變更視為正常的工作負載活動、不再將其標示為潛在的未來攻擊。

若要啟用 ARP 、"ONTAP One"需要授權。

深入瞭解

- "自主勒索軟體保護"

自主勒索軟體保護 /AI （ ARP/AI ）

ARP/AI 在 ONTAP 9 15.1 中推出技術預覽、將 NAS 儲存系統的隨裝即時偵測功能帶入更高層級。全新 AI 驅動的偵測技術已針對超過一百萬個檔案和各種已知的勒索軟體攻擊進行訓練。除了 ARP 中使用的訊號之外、ARP/AI 也會偵測標頭加密。AI 電源和額外訊號可讓 ARP/AI 提供超過 99% 的偵測準確度。SE Labs 已驗證這項功能、這是一項可給予 ARP/AI 最高 AAA 評等的測試實驗室。

由於模型持續在雲端進行訓練、因此 ARP/AI 不需要學習模式。它會在開啟時作用。持續訓練也意味著 ARP/AI 一律會在發生新的勒索軟體攻擊類型時加以驗證。ARP/AI 也隨附自動更新功能、可為所有客戶提供新參數、讓勒索軟體偵測功能保持在最新狀態。ARP 的所有其他偵測、洞見和資料恢復點功能、都會保留給 ARP/AI 。

若要啟用 ARP/AI 、"ONTAP One"需要授權。

深入瞭解

- "部落格： NetApp 的 AI 即時勒索軟體偵測解決方案達到 AAA 評等"

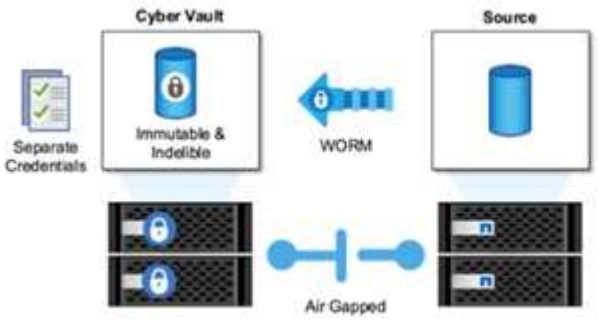
在 ONTAP 中使用網路資料傳輸技術，提供空中綁帶式 WORM 保護

NetApp 的網路資料保險箱方法是專為邏輯上無線網路資料保險箱所打造的參考架構。這種方法利用安全強化和法規遵循技術（例如 SnapLock ）來實現不可改變和難以磨滅的快照。

使用 SnapLock Compliance 進行網路鏈接、並在邏輯上造成空氣落差

攻擊者越來越傾向於破壞備份複本、在某些情況下甚至加密這些複本。因此網路安全產業中有許多人建議將氣隙備份作為整體網路恢復策略的一部分。

問題在於傳統的空缺（磁帶和離線媒體）可能會大幅增加還原時間、進而增加停機時間和整體相關成本。即使採用更現代化的方法來解決空缺問題、也可能是問題所在。例如、如果備份資料保險箱暫時開啟以接收新的備份複本、然後中斷與主要資料的網路連線、再次「無線搭接」、攻擊者就可以利用暫時的開啟。在連線上線期間、攻擊者可能會攻擊以破壞或破壞資料。這類組態通常也會增加不必要的複雜度。邏輯氣隙是傳統或現代氣隙的絕佳替代品、因為它有相同的安全保護原則、同時保持備份在線上。有了 NetApp ，您就能解決磁帶或磁碟氣在邏輯氣帶上的複雜性，這可以透過不可變的快照和 NetApp SnapLock Compliance 來達成。



NetApp 在 10 多年前推出 SnapLock 功能、以因應資料法規遵循的要求、例如健康保險可攜性與責任法案（ HIPAA ）、沙賓法案（ arbanes-Oxlei ）及其他法規資料規則。您也可以將主要快照儲存至 SnapLock 磁碟區，以便將複本歸入 WORM ，避免刪除。有兩個 SnapLock 授權版本： SnapLock Compliance 和 SnapLock

Enterprise 。為了保護勒索軟體， NetApp 建議您使用 SnapLock Compliance ，因為您可以設定特定的保留期間，在這段期間內，即使是由 ONTAP 管理員或 NetApp 支援人員鎖定或刪除快照，也無法刪除快照。

深入瞭解

- "部落格： ONTAP 網路資料保險箱總覽"

防竄改快照

雖然利用 SnapLock Compliance 作為邏輯空空缺口，可提供終極保護，防止攻擊者刪除備份複本，但您必須使用 SnapVault 將快照移至啟用 SnapLock 的次要磁碟區。因此、許多客戶都會在整個網路的次要儲存設備上部署此組態。相較於在主要儲存設備上還原主要 Volume Snapshot ，還原時間可能會較長。

從 ONTAP 9.12.1 開始，防竄改快照可為主儲存設備和主磁碟區上的快照提供近乎 SnapLock Compliance 層級的保護。不需要使用 SnapVault 將快照儲存至次要 SnapLoced Volume 。防竄改快照使用 SnapLock 技術，即使是由完整的 ONTAP 管理員使用相同的 SnapLock 保留期限，也能防止主快照遭到刪除。這可加快還原時間，並能以防竄改，受保護的傳統 SnapLock Compliance 資料保險箱快照來備份 FlexClone 磁碟區。

SnapLock Compliance 與防竄改快照之間的主要差異在於，如果 SnapLock Compliance 磁碟區存在尚未達到到期日的拱形快照，則 SnapLock Compliance 不允許初始化和清除 ONTAP 陣列。為了防止快照竄改，需要 SnapLock Compliance 授權。

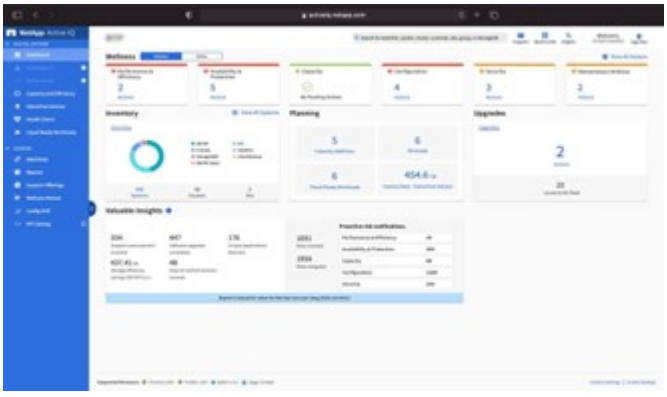
深入瞭解

- "鎖定快照以防止勒索軟體攻擊"

數位顧問勒索軟體保護

Digital Advisor 由 Active IQ 提供支援，可簡化 NetApp 儲存設備的主動式維護和最佳化，並提供可據以行動的智慧資訊，以實現最佳資料管理。它利用我們高度多樣化的已安裝基礎設備的遙測資料，運用先進的 AI 和 ML 技術，發掘降低風險並提升儲存環境效能和效率的機會。

不僅能 "NetApp 數位顧問" "消除安全漏洞"提供協助、還能提供專為保護免受勒索軟體攻擊而提供的深入見解與指引。專屬的健康卡片會顯示所需的行動和所解決的風險、因此您可以確保系統符合這些最佳實務建議。



在勒索軟體「國防健康」頁面上追蹤的風險和行動包括下列（以及更多）：

- Volume Snapshot 數低，降低了勒索軟體的潛在保護。
- FPolicy 未針對所有針對 NAS 傳輸協定設定的儲存虛擬機器（ SVM ）啟用。

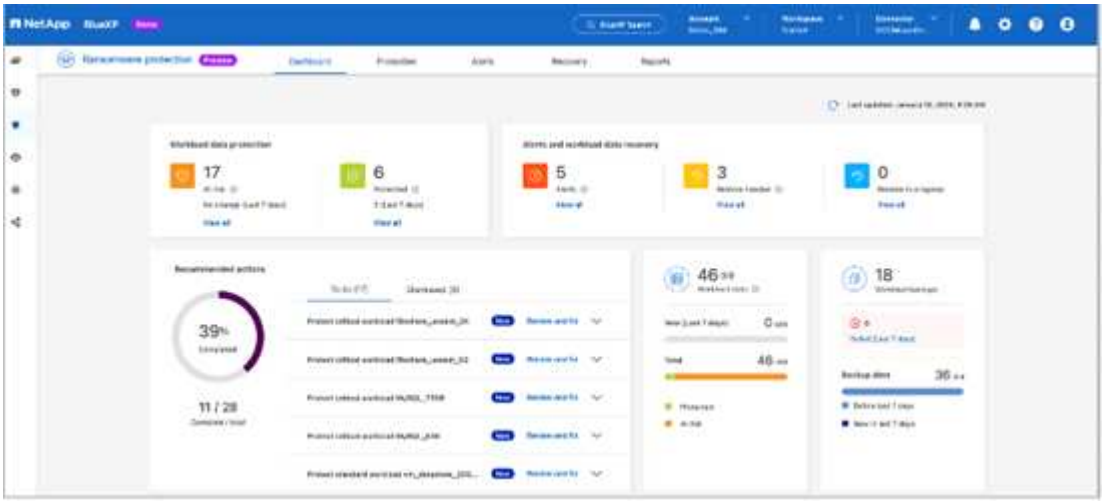
若要查看勒索軟體的保護措施，請參閱"數位顧問"。

NetApp勒索軟體防護提供全面的復原能力

儘早偵測勒索軟體非常重要，這樣才能防止其傳播並避免代價高昂的停機。然而，有效的勒索軟體偵測策略應該包含多層保護。 NetApp 的勒索軟體防護採用綜合方法，包括使用NetApp Console擴展到資料服務的即時、機上功能以及用於網路保管的隔離、分層解決方案。

NetApp勒索軟體防護

NetApp Console是一個單一控制平面，可以智慧地協調全面的、以工作負載為中心的勒索軟體防禦。 NetApp勒索軟體防護匯集了ONTAP強大的網路彈性功能（例如 ARP、FPolicy 和防篡改快照）以及NetApp資料服務（例如NetApp Backup and Recovery）。它還添加了自動化工作流程的建議和指導，以透過單一 UI 提供端到端防禦。它在工作負載層級運行，以確保運行您業務的應用程式受到保護，並且在受到攻擊時可以盡快恢復。



客戶效益：

- 輔助勒索軟體準備工作可減少營運成本並提高效率
- 以 AI / ML 為動力的異常狀況偵測功能可提供更高的準確度、並更快地因應風險
- 引導式應用程式一致的還原可讓您更輕鬆地在幾分鐘內恢復工作負載

"NetApp勒索軟體防護"使得這些 NIST 功能更容易實現：

- 自動 * 探索 * 並優先處理 NetApp 儲存設備中的資料 * 、重點放在最重要的應用程式型工作負載 * 上。
- * 一鍵保護 * 、可執行工作負載最高的資料備份、不可變更、安全組態、惡意檔案封鎖及不同的安全網域。
- * 使用 * 次世代 AI 型異常偵測、 * 盡可能 * 快速 * 精確偵測 * 勒索軟體。 *
- 自動化回應與工作流程、並與頂尖 * SIEM 與 XDR 解決方案整合。 *
- 使用簡化的 * 協調式恢復 * 來快速恢復資料、以加速應用程式正常運作時間。
- 實施勒索軟體保護 * 策略 * 和 * 政策 * 、以及 * 監控成果 * 。

NetApp 與 Zero Trust

NetApp 與 Zero Trust

零信任傳統上是一種以網路為中心的方法、用於建構微核心和周邊（ MCAP ）、以控制區段閘道的方式來保護資料、服務、應用程式或資產。NetApp ONTAP 採用以資料為中心的 Zero Trust 方法、將儲存管理系統變成區段閘道、以保護及監控客戶資料的存取。特別是、 FPolicy Zero Trust 引擎和 FPolicy 合作夥伴生態系統成為控制中心、可深入瞭解正常和異常的資料存取模式、並識別內部威脅。

自 2024 年 7 月起，技術報告 _TR-4829 的內容： NetApp 與 Zero Trust ：啟用以資料為中心的 Zero Trust 模式 _ ，此模式先前以 PDF 格式發佈，可在 docs.netapp.com 取得。

資料是貴組織最重要的資產。根據 2022 年的資料外洩、內部威脅是 18% 資料外洩的原因 "Verizon 資料外洩調查報告"。組織可以利用 NetApp ONTAP 資料管理軟體、針對資料部署領先業界的 Zero Trust 控管措施、提高警覺性。

什麼是 **Zero Trust** ？

Zero Trust 模式是由 John Kindervag 在 Forrester Research 首次開發。它從內到外都能實現網路安全性、而非從外到外。 「內到外零信任」方法可識別微核心和周邊（ MCAP ）。MCAP 是資料、服務、應用程式和資產的內部定義、可透過一套完整的控制功能加以保護。安全外部邊界的概念已經過時。受信任且允許透過周邊環境成功驗證的實體、可能會使組織容易遭受攻擊。根據定義、內部人員已經在安全的邊界內。員工、承包商和合作夥伴都是內部人員、他們必須能夠在組織基礎架構中執行職務時、以適當的控管方式運作。

零信任被視為一項技術、可在 2019 年 9 月向 DoD 提供承諾 "FY19-23 DoD 數位現代化策略"。它將 Zero Trust 定義為「一種網路安全策略、可在整個架構內嵌安全性、以阻止資料外洩。這種以資料為中心的安全模式消除了受信任或不受信任的網路、裝置、角色或程序的概念、並移轉到多屬性型信任層級、以在最低權限存取概念下啟用驗證和授權原則。實作零信任需要重新思考我們如何使用現有基礎架構，以更簡單，更有效率的方式設計安全性，同時實現不受阻礙的作業。」

2020 年 8 月、 NIST 發佈 "Special Pub 800-207 Zero Trust Architecture" （ ZTA ）。ZTA 著重於保護資源、而非網路區段、因為網路位置不再被視為資源安全狀態的主要元件。資源是資料和運算。ZTA 策略適用於企業網路架構設計師。ZTA 引進了一些來自 Forrester 原創概念的新術語。稱為原則決策點（ PDP ）和原則執行點（ PEP ）的保護機制、類似於 Forrester 分割閘道。ZTA 推出四種部署模式：

- 裝置代理程式或閘道型部署
- 以飛地為基礎的部署（有點類似於 Forrester MCAP ）
- 資源入口網站型部署
- 裝置應用程式沙箱

就本文件而言、我們使用 Forrester Research 的概念和術語、而非 NIST ZTA 。

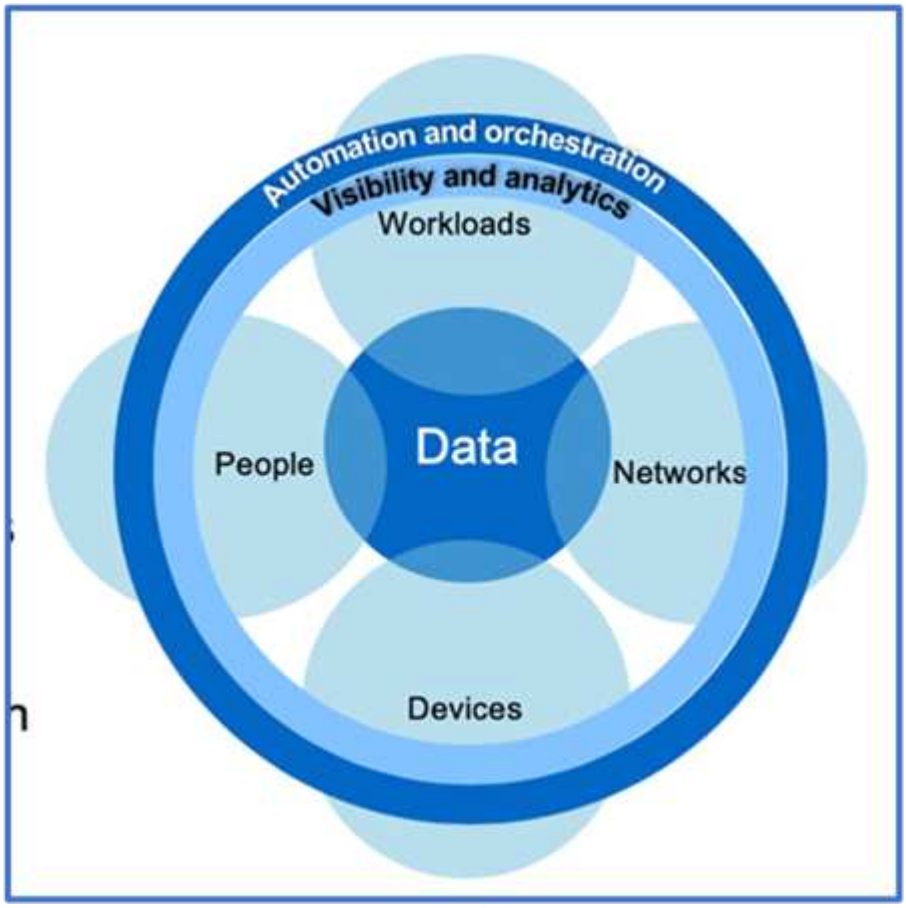
安全資源

有關報告漏洞和事件、 NetApp 安全響應和客戶機密性的信息，請參閱 "NetApp 安全入口網站"。

使用 **ONTAP** 架構以資料為中心的零信任方法

Zero Trust 網路是以資料為中心的方法所定義、其中的安全控管措施應盡可能接近資料。ONTAP 的功能搭配 NetApp FPolicy 合作夥伴生態系統、可為以資料為中心的零信任模式提供必要的控制。

ONTAP 是 NetApp 提供的安全性豐富的資料管理軟體、而 FPolicy Zero Trust Engine 則是領先業界的 ONTAP 功能、可提供精細的檔案型事件通知介面。NetApp FPolicy 合作夥伴可以使用此介面、在 ONTAP 中提供更多資料存取的照明。



建構 **Zero Trust** 資料導向的 **MCAP**

若要架構以資料為中心的 Zero Trust MCAP 、請遵循下列步驟：

1. 識別所有組織資料的位置。
2. 將資料分類。
3. 安全地處理不再需要的資料。
4. 瞭解哪些角色應該能夠存取資料分類。
5. 應用最低權限原則來強制執行存取控制。
6. 使用多因素驗證來進行管理存取和資料存取。
7. 對靜止資料和正在傳輸的資料使用加密。

8. 監控並記錄所有存取。
9. 警示可疑的存取或行為。

識別所有組織資料的位置

ONTAP 的 FPolicy 功能搭配 FPolicy 合作夥伴的 NetApp 聯盟合作夥伴生態系統、可讓您識別貴組織資料的存在位置、以及哪些人可以存取。這是透過使用者行為分析來完成、可識別資料存取模式是否有效。「監控」和「記錄所有存取」中會討論使用者行為分析的更多詳細資料。如果您不瞭解資料的位置和存取權、使用者行為分析可以提供基準、以根據經驗觀察來建立分類和原則。

將資料分類

在零信任模型的術語中，資料分類涉及有毒資料的識別。有毒資料是不適合在組織外部暴露的敏感資料。洩漏有毒資料可能會違反法規合規性並損害組織的聲譽。在監管合規方面，有毒數據包括持卡人數據 "支付卡產業資料安全標準（PCI-DSS）"，歐盟的個人數據 "一般資料保護規範（ GDPR ）"或醫療保健數據 "健康保險可攜性與責任法案（ HIPAA ）"。您可以使用NetApp "NetApp Data Classification" （以前稱為 Cloud Data Sense），一款人工智慧驅動的工具包，可自動掃描、分析和分類您的資料。

安全地處理不再需要的資料

將組織的資料分類之後、您可能會發現有些資料不再需要或與組織的功能相關。保留不必要的資料是一項責任、應刪除此類資料。如需加密清除資料的進階機制、請參閱「靜止資料加密」中的安全清除說明。

瞭解哪些角色應該擁有資料分類的存取權、並運用最低權限原則來強制執行存取控制

對應對敏感資料的存取權、並套用最低權限原則、意味著只有組織中的人員才能存取執行工作所需的資料。此過程涉及基於角色的訪問控制 ("RBAC")，適用於數據訪問和管理訪問。

有了 ONTAP 、儲存虛擬機器（ SVM ）可用來區隔 ONTAP 叢集內租戶的組織資料存取。RBAC 可套用至資料存取、以及對 SVM 的管理存取。您也可以在叢集管理層級套用 RBAC 。

除了 RBAC 之外、您也可以使用 ONTAP "多重管理驗證" （ MAV ）來要求一或多個系統管理員核准或等命令 `volume delete` `volume snapshot delete`。啟用MAV之後、修改或停用MAV需要MAV管理員核准。

另一種保護快照的方法是使用 ONTAP "Snapshot 鎖定"。Snapshot 鎖定是一種 SnapLock 功能，可在磁碟區快照原則上以手動或自動方式呈現快照，並保留一段時間。Snapshot 鎖定也稱為防竄改快照鎖定。快照鎖定的目的是防止惡意或不受信任的系統管理員刪除主要和次要 ONTAP 系統上的快照。可在主要系統上快速恢復鎖定的快照，以還原遭勒索軟體毀損的磁碟區。

使用多因素驗證來進行管理存取和資料存取

除了叢集管理 RBAC 之外、 "多因素驗證（ MFA ）" 也可部署以進行 ONTAP Web 管理存取和安全 Shell （ SSH ）命令列存取。美國公共部門組織或必須遵守 PCI-DSS 的組織、都必須使用 MFA 來進行管理存取。MFA 讓攻擊者無法僅使用使用者名稱和密碼來危害帳戶。MFA 需要兩個以上的驗證因素。雙因素驗證的範例是使用者擁有的東西、例如私密金鑰、以及使用者知道的東西、例如密碼。安全聲明標記語言（ SAML） 2.0 可讓管理網路存取 ONTAP 系統管理員或 ActiveIQ Unified Manager 。SSH 命令列存取使用連結的雙因素驗證搭配公開金鑰和密碼。

您可以使用 ONTAP 中的身分識別與存取管理功能、透過 API 控制使用者和機器存取：

- 使用者：
  - * 驗證與授權。 *透過適用於 SMB 和 NFS 的 NAS 傳輸協定功能。

- * 稽核 *存取與事件的系統記錄。CIFS 通訊協定的詳細稽核記錄、以測試驗證和授權原則。精細精細的 FPolicy 稽核檔案層級的詳細 NAS 存取。

- 裝置：
  - * 驗證。 *用於 API 存取的憑證型驗證。
  - * 授權。 *預設或自訂角色型存取控制（ RBAC ）。
  - * 稽核 *系統記錄所採取的所有行動。

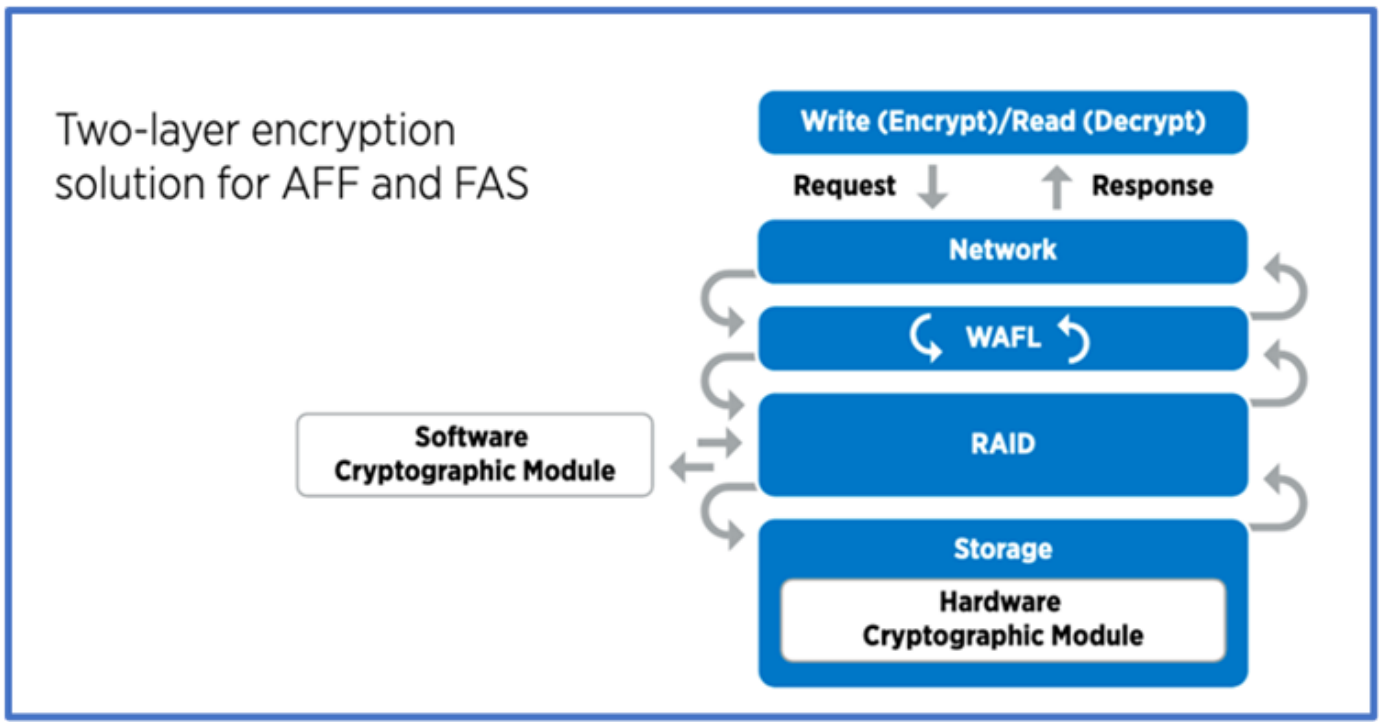
對靜止資料和正在傳輸的資料使用加密

靜態資料加密

每天都有新的要求、可在組織重新調整磁碟機用途、退回故障磁碟機、或透過銷售或交易方式升級到較大磁碟機時、降低儲存系統風險和基礎架構漏洞。 身為資料的管理員和操作者、儲存工程師必須在資料的整個生命週期內、安全地管理及維護資料。 "NetApp 儲存加密（ NSE ） ；#44 ； NetApp Volume 加密（ NVE ） ；#44 ；以及 NetApp Aggregate 加密" 協助您隨時加密所有資料、無論資料是否有毒、而且不會影響日常作業。 "NSE" 是 ONTAP 硬體 "靜態資料" 解決方案、使用 FIPS 140-2 第 2 級驗證的自我加密磁碟機。 "NVE 和 NAE" 是使用的 ONTAP 軟體 "靜態資料" 解決方案 "FIPS 140-2 第 1 級驗證 NetApp 密碼編譯模組"。有了 NVE 和 NAE 、硬碟或固態硬碟都可用於靜態資料加密。此外、 NSE 磁碟機也可用於提供原生的分層加密解決方案、提供加密備援和額外的安全性。如果有一層被破壞、則第二層仍會保護資料安全。這些功能讓 ONTAP 成為 "Quantum 就緒加密"的理想選擇。

NVE 也提供一項稱為的功能 "安全清除" 、可在將敏感檔案寫入非機密磁碟區時、以密碼方式移除資料外洩的有毒資料。

可將 "內建金鑰管理程式（OKM）"內建於 ONTAP 的金鑰管理員或協力廠商搭配 NSE 和 NVE 使用、以安全地儲存金鑰 "已核准" "外部金鑰管理員" 資料。



如上圖所示、可結合硬體和軟體型加密。這項功能可讓您 "將 ONTAP 驗證為 NSA 的商業解決方案、以供分類方案使用" 儲存重要機密資料。

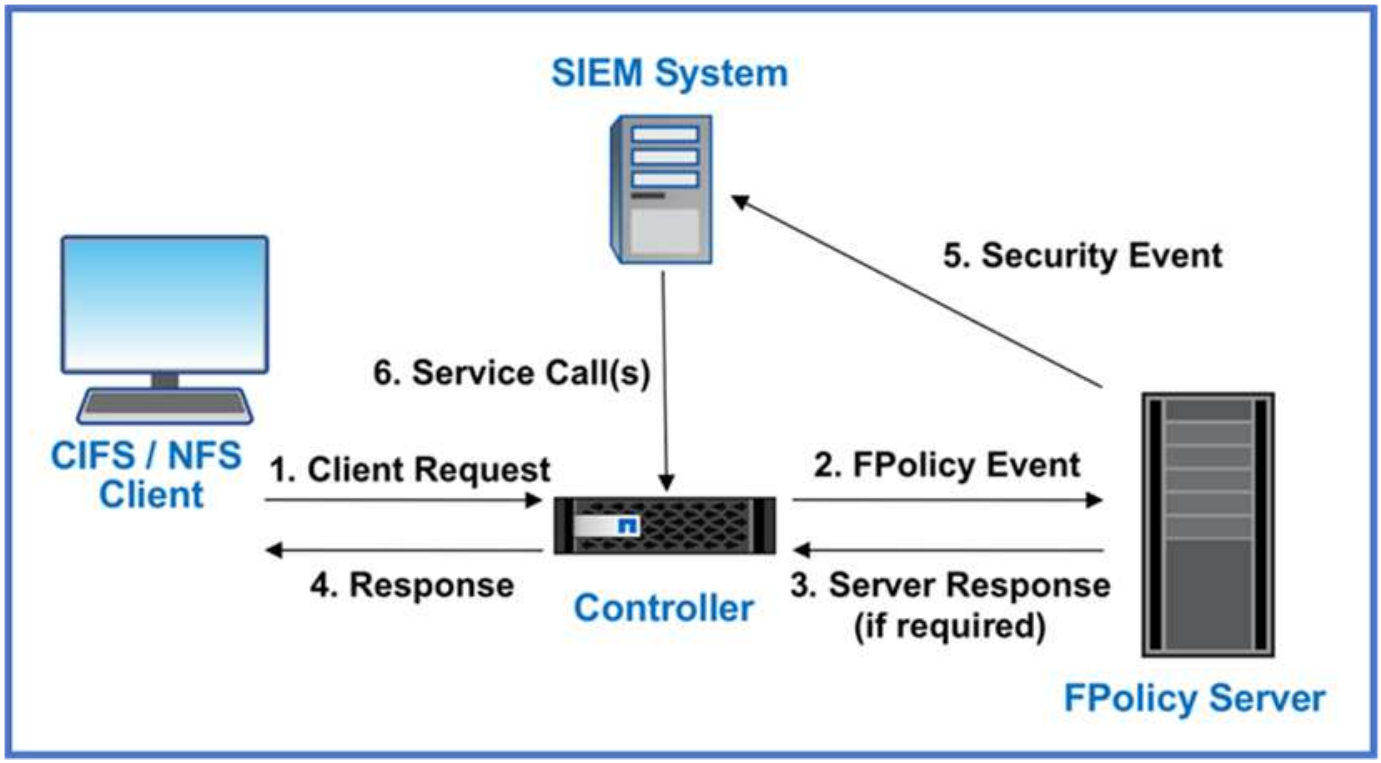
資料傳輸中加密

ONTAP 資料傳輸加密功能可保護使用者資料存取和控制面板存取。使用者資料存取可透過 SMB 3.0 加密來加密 Microsoft CIFS 共用存取、或透過 krb5P for NFS Kerberos 5 來加密。使用 CIFS 、 NFS 和 iSCSI 也可以加密使用者資料存取 "IPsec" 。控制平面存取是以傳輸層安全性（ TLS ）加密。ONTAP 提供"FIPS"控制平面存取的法規遵循模式，可啟用 FIPS 核准的演算法，並停用未經 FIPS 核准的演算法。資料複寫是使用加密 "叢集對等加密"的。這可為 ONTAP SnapVault 和 SnapMirror 技術提供加密。

監控並記錄所有存取

建立 RBAC 原則之後、您必須部署主動監控、稽核及警示。NetApp ONTAP 的 FPolicy Zero Trust Engine 搭配提供資料導向的 Zero "NetApp FPolicy 合作夥伴生態系統"Trust 模式所需的控制功能。NetApp ONTAP 是安全性豐富的資料管理軟體、 "FPolicy" 是領先業界的 ONTAP 功能、可提供精細的檔案型事件通知介面。NetApp FPolicy 合作夥伴可以使用此介面、在 ONTAP 中提供更多資料存取的照明。ONTAP 的 FPolicy 功能搭配 FPolicy 合作夥伴的 NetApp 聯盟合作夥伴生態系統、可讓您識別組織資料的存在位置、以及哪些人可以存取。這是透過使用者行為分析來完成、可識別資料存取模式是否有效。使用者行為分析可用於警示異常或可疑的資料存取、而這種存取方式不符合正常模式、並在必要時採取行動拒絕存取。

FPolicy 合作夥伴正從使用者行為分析轉向機器學習（ ML ）和人工智慧（ AI ）、以提高事件的逼真度、減少誤報（如果有）。所有事件都應記錄到 Syslog 伺服器或安全資訊與事件管理（ SIEM ）系統、而此系統也可以採用 ML 和 AI 。



NetApp 的 "DII 儲存工作負載安全"利用雲端和本地ONTAP儲存系統上的 FPolicy 介面和使用者行為分析，為您提供惡意使用者行為的即時警報。儲存工作負載安全性透過先進的機器學習和異常檢測保護組織資料不被惡意或受感染的使用者濫用。儲存工作負載安全性可以識別勒索軟體攻擊或其他惡意行為，呼叫快照並隔離惡意使用者。儲存工作負載安全性還具有取證功能，可以詳細查看使用者和實體活動。儲存工作負載安全性是NetAppData Infrastructure Insights的一部分。

除了儲存工作負載安全性之外、 ONTAP 還具備內建的勒索軟體偵測功能、稱為 "自主勒索軟體保護" （ ARP ）。ARP 會使用機器學習來判斷異常檔案活動是否表示勒索軟體攻擊正在進行中，並叫用快照並向系統管理員發出警示。儲存工作負載安全性與 ONTAP 整合、可接收 ARP 事件、並提供額外的分析和自動回應層。

如需有關本程序中所述命令"ONTAP 命令參照"的詳細資訊，請參閱。

ONTAP 外部的 NetApp 安全性自動化與協調控制

自動化功能可讓您以最少的人力協助來執行程序或程序。自動化功能可讓組織將 Zero Trust 部署規模擴充至遠超出手動程序的範圍、以抵禦同樣自動化的誤報活動。

Ansible 是開放原始碼軟體資源配置、組態管理及應用程式部署工具。它可以在許多類似 Unix 的系統上執行、而且可以同時設定類似 Unix 的系統和 Microsoft Windows 。其中包含自己的宣告語言、可用來描述系統組態。Ansible 由 Michael DeHaan 撰寫、並於 2015 年由 Red Hat 收購。Ansible 是無代理程式、可透過 SSH 或 Windows 遠端管理（允許遠端執行 PowerShell ）進行遠端連線以執行工作。NetApp 開發的不只是、還 "150 個適用於 ONTAP 軟體的 Ansible 模組"能進一步整合 Ansible 自動化架構。適用於 NetApp 的 Ansible 模組提供一組指示、說明如何定義所需的狀態、並將其轉送至目標 NetApp 環境。模組的設計可支援設定授權、建立集合體和儲存虛擬機器、建立磁碟區、以及還原快照等工作。Ansible 角色 "發表於 GitHub" 專屬於 NetApp DoD 統一化功能（ UC ）部署指南。

使用者可以利用可用模組庫輕鬆開發 Ansible 教戰手冊，並根據自己的應用程式和業務需求自訂這些手冊，以自動化日常工作。在撰寫教戰手冊之後、您可以執行該手冊來執行指定的工作、這樣可以節省時間並提高生產力。NetApp 已建立並共用範例教戰手冊、可直接使用或根據您的需求自訂。

Data Infrastructure Insights是一種基礎設施監控工具，可讓您了解完整的基礎架構。透過Data Infrastructure Insights，您可以監控、排除故障並最佳化所有資源，包括公有雲實例和私有資料中心。Data Infrastructure Insights可以將平均解決時間縮短 90%，並防止 80% 的雲端問題影響最終用戶。它還可以平均降低 33% 的雲端基礎設施成本，並透過使用可操作的情報來保護您的資料來減少您受到內部威脅的風險。Data Infrastructure Insights的儲存工作負載安全功能支援透過 AI 和 ML 進行使用者行為分析，以便在因內部威脅而出現異常使用者行為時發出警報。對於ONTAP，儲存工作負載安全使用零信任 FPolicy 引擎。

Zero Trust 與混合雲部署

NetApp是混合雲的資料權威。NetApp提供了多種選項，可透過 Amazon Web Services (AWS)、Microsoft Azure、Google Cloud 和其他領先的雲端供應商將內部部署資料管理系統擴展到混合雲。NetApp混合雲端解決方案支援與本機ONTAP系統和ONTAP Select軟體定義儲存相同的零信任安全控制。

您可以使用適用於 AWS（FSxN）、Google Cloud（GCNV）和適用於 Microsoft Azure 的Azure NetApp Files 的企業級雲端原生檔案服務，輕鬆擴展公有雲的容量，而不受典型的資本支出限制。這些雲端資料服務非常適合分析和 DevOps 等資料密集型工作負載，它將NetApp的彈性按需儲存即服務與ONTAP資料管理結合在一起，形成一個完全託管的產品。

ONTAP借助NetApp SnapMirror資料複製軟體，支援在本機ONTAP系統與 AWS、Google Cloud 或 Azure 儲存環境之間移動資料。

屬性型存取控制

使用 ONTAP 進行屬性型存取控制

從 9.12.1 開始，您可以使用 NFSv4.2 安全性標籤和延伸屬性（ xATT ）來設定 ONTAP ，以支援具有屬性和屬性型存取控制（ ABAC ）的角色型存取控制（ RBAC ）。

ABAC 是根據使用者屬性，資源屬性和環境條件來定義權限的授權策略。ONTAP 與 NFS v4.2 安全性標籤和 xATTs 的整合符合 NIST 標準的 ABAC 解決方案，如 NIST 特別出版品 800-162 所述。

您可以使用 NFS v4.2 安全性標籤和 xatts 來指派檔案使用者定義的屬性和標籤。ONTAP 可與 ABAC 導向的身分識別與存取管理軟體整合，以根據這些屬性和標籤，強制執行精細的檔案和資料夾存取控制原則。

相關資訊

- "使用 ONTAP 的 ABAC 方法"
- "NetApp ONTAP 中的 NFS ：最佳實務做法與實作指南"

ONTAP 中的屬性型存取控制（ ABAC ）方法

ONTAP 提供數種方法，可用於達成檔案層級屬性型存取控制（ ABAC ），包括 NFS v4.2 安全性標籤和使用 NFS 的延伸屬性（ xATT ）。

NFS v4.2 安全性標籤

從 ONTAP 9.9.1 開始，支援名為 NFS 的 NFS v4.2 功能。

NFS v4.2 安全性標籤是一種使用 SELinux 標籤和強制存取控制（ MAC ）來管理精細檔案和資料夾存取的方法。這些 MAC 標籤會與檔案和資料夾一起儲存，並與 UNIX 權限和 NFS v4.x ACL 搭配使用。

支援 NFS v4.2 安全性標籤，表示 ONTAP 現在能辨識及瞭解 NFS 用戶端的 SELinux 標籤設定。RFC-7204 涵蓋 NFS v4.2 安全性標籤。

NFS v4.2 安全性標籤的使用案例包括：

- 虛擬機器（ VM ）映像的 Mac 標籤
- 公共部門的資料安全性分類（秘密，機密和其他分類）
- 安全法規遵循
- 無磁碟Linux

啟用NFS v4.2安全性標籤

您可以使用下列命令來啟用或停用 NFS v4.2 安全性標籤（需要進階權限）：

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

如"ONTAP 命令參照"需詳細 `vserver nfs modify`資訊，請參閱。

NFS v4.2 安全性標籤的強制模式

從 ONTAP 9.9.1 開始， ONTAP 支援下列強制模式：

- * 有限伺服器模式 * ： ONTAP 無法強制執行標籤，但可以儲存及傳輸標籤。

  變更 MAC 標籤的能力由用戶端來強制執行。

- * 來賓模式 * ：如果用戶端未標示 NFS 感知（ v4.1 或更低版本），則 MAC 標籤不會傳輸。

ONTAP 目前不支援「完整模式」（儲存及強制執行 MAC 標籤）。

NFS v4.2 安全性標籤範例

以下組態範例示範使用 Red Hat Enterprise Linux 9.3 （ Plow ）版本的概念。

根據 John R. Smith 的認證建立的使用者 `jrsmith`擁有下列 Privileges 帳戶：

- 使用者名稱 = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

有兩種角色：系統管理員帳戶是具有權限的使用者和使用者， `jrsmith`如下列 MLS Privileges 表所述：

使用者	角色	類型	層級
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

在此範例環境中，使用者 `jrsmith`**可以存取層級為的** `s3`**檔案** `s0`。我們可以加強現有的安全性分類，如下所述，以確保系統管理員無法存取使用者專屬的資料。

- S0 = 權限管理使用者資料
- S0 = 未分類資料
- S1 = 機密
- S2 = 機密資料
- S3 = 重要機密資料

以 **MCS** 為例的 **NFS v4.2** 安全性標籤

除了多層安全（ MLS ）之外，另一項稱為「多類別安全（ MCS ）」的功能可讓您定義專案等類別。

NFS 安全性標籤	價值
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

延伸屬性（ **xatts** ）

從 ONTAP 9.12.1 開始， ONTAP 支援 xatts 。 xatts 允許中繼資料與系統所提供的檔案和目錄相關聯，例如存取控制清單（ ACL ）或使用者定義的屬性。

若要實作 xattis ，您可以在 Linux 中使用 `setfattr`和 `getfattr`命令列公用程式。這些工具提供了一種強大的方法來管理檔案和目錄的其他中繼資料。請謹慎使用，因為不當使用可能導致非預期行為或安全問題。請務必參閱

`setfattr`和 `getfattr`手冊頁或其他可靠的文件，以取得詳細的使用說明。

在 ONTAP 檔案系統上啟用 xattis 時，使用者可以設定，修改及擷取檔案上的任意屬性。這些屬性可用來儲存標準檔案屬性集未擷取之檔案的其他資訊，例如存取控制資訊。

在 ONTAP 中使用 xattis 有幾項要求和限制：

- Red Hat Enterprise Linux 8.4 或更新版本
- Ubuntu 22.04或更新版本
- 每個檔案最多可有 128 個 xatts
- xattr 金鑰限制為 255 個位元組
- 組合金鑰或值大小為每個 xattr 1,229 位元組
- 目錄和檔案可以有 xattis
- 若要設定和擷取 xatts ， `w`或必須為使用者和群組啟用寫入模式位元

在使用者命名空間內使用 Xatts ，不會對 ONTAP 本身具有任何內在意義。而是由與檔案系統互動的用戶端應用程式來決定及管理其實際應用程式。

xattr 使用案例範例：

- 記錄負責建立檔案的應用程式名稱
- 保留取得檔案的電子郵件訊息參考資料
- 建立分類架構以組織檔案物件
- 使用檔案原始下載來源的 URL 來標示檔案

用於管理 **xattis** 的命令

- `setfattr`設定檔案或目錄的延伸屬性：

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  命令範例：

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr`擷取特定延伸屬性的值，或列出檔案或目錄的所有延伸屬性：

  特定屬性：
  ```
  getfattr -n <attribute_name> <file or directory name>
  ```

  所有屬性：
  ```
  getfattr <file or directory name>
  ```

  命令範例：

```
getfattr -n user.comment example.txt
```

xattr 金鑰值配對範例

下表顯示兩個 xattr 金鑰值配對範例：

xattr	價值
user.digitalIdentifier	CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US
user.countryOfAffiliations	USA

使用者對 xattis 的 ACE 權限

存取控制項目（ ACE ）是 ACL 中的元件，可定義授予個別使用者或特定資源（例如檔案或目錄）使用者群組的存取權限。每個 ACE 都會指定允許或拒絕的存取類型，並與特定的安全性主體（使用者或群組身分識別）相關聯。

xattis 需要存取控制項目（ **ACE** ）

- Retrieve xattr ：使用者讀取檔案或目錄的延伸屬性所需的權限。「 R 」表示需要讀取權限。
- 設定 xattis ：修改或設定延伸屬性所需的權限。「 A 」，「 w 」和「 T 」代表不同的權限範例，例如附加，寫入及與 xatts 相關的特定權限。
- 檔案：使用者需要附加，寫入及可能與 xattis 相關的特殊權限，才能設定延伸屬性。
- 目錄：設定延伸屬性需要特定的權限「 T 」。

檔案類型	擷取 **xattr**	設定 **xattis**
檔案	R	A ， w ， T
目錄	R	T

與 **ABAC** 身分識別與存取控制軟體整合

為了充分發揮 ABAC 的功能， ONTAP 可以與 ABAC 導向的身分識別與存取管理軟體整合。

在 ABAC 系統中，政策執行點（ PEP ）和政策決策點（ PDP ）扮演著重要角色。PEP 負責強制執行存取控制原則，而 PDP 則根據原則決定是否授予或拒絕存取。

在實際的設定中，組織會混合使用 NFS 安全性標籤和 xattis 。這些資料用於代表各種中繼資料，包括分類，安全性，應用程式和內容，這些都是做出 ABAC 決策的重要工具。例如， xattis 可用於儲存 PDp 用於其決策程序的資源屬性。可以定義屬性來代表檔案的分類層級（例如，「未分類」，「機密」，「秘密」或「最高機密」）。然後， PDP 可以利用此屬性來強制執行原則，限制使用者只能存取其分類層級等於或低於淨空層級的檔案。

本內容假設客戶的身分識別，驗證和存取服務至少包含一個 PEP 和一個可作為存取檔案系統中介的 PDP 。

ABAC 流程範例

1. 使用者向系統存取 PEP 提供認證（例如， PKI ， OAuth ， SAML ），並從 PDP 取得結果。

   PEP 的角色是攔截使用者的存取要求，並將其轉送至 PDP 。

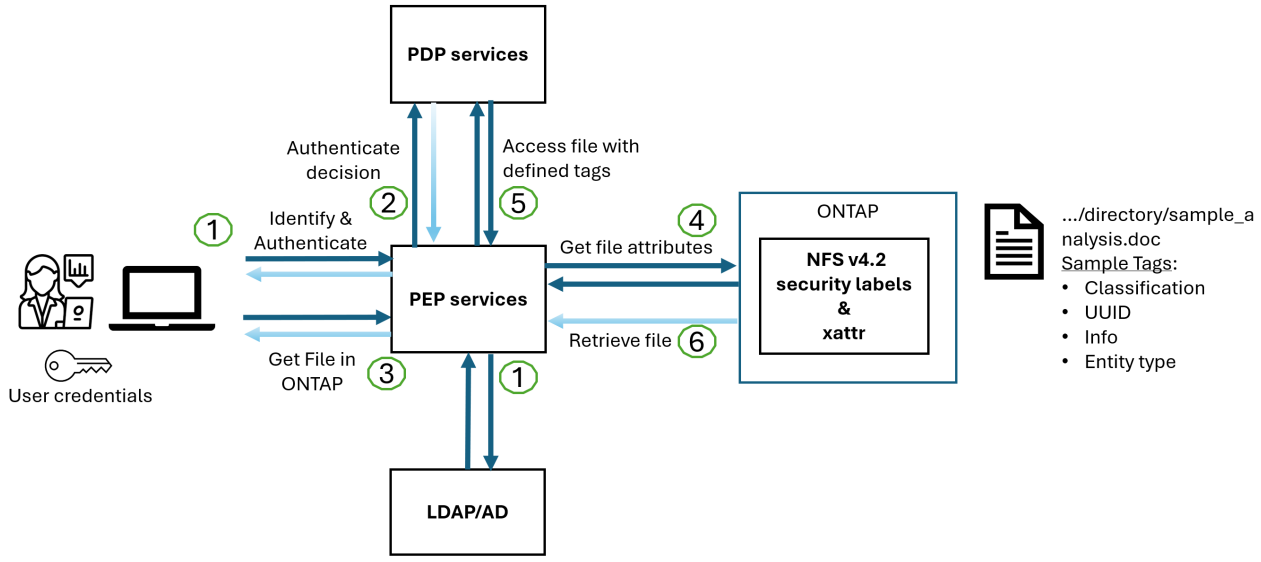
2. 然後， PDP 會根據已建立的 ABAC 原則來評估此要求。

   這些原則會考量與使用者，相關資源及周邊環境相關的各種屬性。根據這些原則， PDP 會決定是否允許存取，然後將此決定傳回給 PEP 。

   PDP 為 PEP 提供強制政策。然後，根據 PDP 的決定， PEP 會強制執行此決定，授予或拒絕使用者的存取要求。

3. 成功要求後，使用者會要求儲存在 ONTAP （例如 AFF ， AFF C ）中的檔案。
4. 如果申請成功，則 PEP 會從文件中取得精細的存取控制標籤。
5. PEP 根據該使用者的認證要求使用者的原則。
6. 如果使用者有權存取檔案，且可讓使用者擷取檔案，則 PEP 會根據原則和標籤做出決定。

實際存取可能是使用權杖來完成。



ONTAP 複製與 **SnapMirror**

ONTAP 的複製和 SnapMirror 技術旨在提供高效可靠的資料複寫和複製功能，確保檔案資料的所有層面（包括 xatts ）都會隨檔案一起保留和傳輸。 xattis 非常重要，因為它們會儲存與檔案相關的額外中繼資料，例如安全標籤，存取控制資訊和使用者定義的資料，這些資料對於維護檔案的內容和完整性非常重要。

使用 ONTAP 的 FlexClone 技術複製磁碟區時，會建立磁碟區的完全可寫入複本。這項複製程序既即時又節省空間，而且包含所有檔案資料和中繼資料，可確保完整複寫 xattis 。同樣地， SnapMirror 也能確保資料鏡射到具

有完全逼真度的次要系統。這包括 xattis ，對於仰賴此中繼資料才能正常運作的應用程式而言，這是非常重要的。

NetApp ONTAP 在複製和複寫作業中納入 xattis ，可確保完整的資料集及其所有特性，在主要和次要儲存系統中均可用且一致。對於需要一致的資料保護，快速恢復，以及遵守法規遵循與法規標準的組織而言，這種全方位的資料管理方法非常重要。它也能簡化不同環境（無論是內部部署或雲端環境）的資料管理，讓使用者確信在這些程序中，資料完整且不會遭到竄改。

NFS v4.2 安全性標籤有中定義的注意事項NFS v4.2 安全性標籤。

稽核標籤變更

稽核對 xattis 或 NFS 安全性標籤所做的變更，是檔案系統管理與安全性的關鍵層面。標準檔案系統稽核工具可監控及記錄檔案系統的所有變更，包括修改 xattis 和安全性標籤。

在 Linux 環境中， `auditd`常駐程式通常用於建立檔案系統事件的稽核。它可讓系統管理員設定規則，以監控與 `xattr` 變更相關的特定系統呼叫，例如 `setxattr`，`lsetxattr`以及 `fsetxattr`設定屬性和 `removexattr`，`lremovexattr`以及 `fremovexattr`移除屬性。

ONTAP FPolicy 提供強大的架構，可即時監控及控制檔案作業，進而擴充這些功能。FPolicy 可設定為支援各種 xattr 事件，提供對檔案作業的精細控制，以及強制執行全方位資料管理原則的能力。

對於使用 xattis 的使用者，尤其是在 NFS v3 和 NFS v4 環境中，僅支援特定的檔案作業和篩選器組合來進行監控。以下是 NFS v3 和 NFS v4 檔案存取事件的 FPolicy 監控支援檔案作業和篩選器組合清單：

支援的檔案作業	支援的篩選器
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

setattr 作業的 **auditd** 記錄片段範例：

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

"ONTAP FPolicy"為使用 xatts 的使用者提供一層可見度和控制權，這對於維護檔案系統的完整性和安全性至關重要。利用 FPolicy 的進階監控功能，組織可以確保追蹤，稽核 xatts 的所有變更，並符合其安全性與法規遵循標準。這種主動式檔案系統管理方法，是為何強烈建議任何想要加強資料治理和保護策略的組織採用 ONTAP FPolicy 的原因。

控制資料存取的範例

以下儲存在 John R. Smith 的 PKI 認證書中的資料項目範例，說明如何將 NetApp 方法套用至檔案，並提供精細的存取控制。

這些範例僅供說明用途，客戶有責任判斷與 NFS v4.2 安全性標籤和 xatts 相關的中繼資料。為了簡化更新和保留標籤的作業，我們省略了相關詳細資料。

- 範例 PKI 憑證值 *

金鑰	價值
entitySecurityMark	T:S01 = 未分類

資訊	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

規格	" 職稱 "
UUID	b4111349-7875-4115-AD30-0928565f2e15

金鑰	價值

管理組織	{
	"value": "DoD"
	}

簡報	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

公民身分	{
	"value": "US"
	}

餘隙	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

金鑰	價值

國家分支機構	[
	  {
	  "value": "USA"
	  }
	]

數位識別碼	{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}

dissemTos	{
	  "value": "DoD"
	}

二合一組織	{
	  "value": "DoD"
	}

entityType	{
	  "value": "GOV"
	}

金鑰	價值

fineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

這些 PKI 授權可顯示 John R. Smith 的存取詳細資料，包括依資料類型和歸屬來存取。

在 IC-TDF 中繼資料與檔案分開儲存的情況下， NetApp 主張額外提供一層精細的存取控制。這包括在目錄層級儲存存取控制資訊，以及與每個檔案相關聯。例如，請考慮連結至檔案的下列標記：

- NFS v4.2 安全性標籤：用於做出安全性決策
- xattis ：提供與檔案及組織方案需求相關的補充資訊

下列金鑰值配對是中繼資料的範例，可儲存為 xatts ，並提供檔案建立者及相關安全性分類的詳細資訊。用戶端應用程式可以利用這項中繼資料來做出明智的存取決策，並根據組織標準和要求來組織檔案。

xattr 鍵值對的範例 *

金鑰	價值
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

金鑰	價值

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

金鑰	價值
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

相關資訊

- "NetApp ONTAP 中的 NFS ：最佳實務做法與實作指南"
- "ONTAP 命令參照"
- 徵求意見（ RFC ）
  - "RFC 7204 ：標籤 NFS 的需求"
  - "RFC 2203 ： RPCSEC_GSS 傳輸協定規格"
  - "RFC 3530 ：網路檔案系統（ NFS ）第 4 版傳輸協定"

強化安全性

ONTAP 安全強化指南

這些技術報告提供如何強化 NetApp ONTAP 及其他 NetApp 產品的指引。

這些技術報告會針對產品文件進行擴充"ONTAP 安全性與資料加密"。

強化指南

"TR-4569 ： NetApp ONTAP 安全強化指南" 瞭解如何設定 NetApp ONTAP 、以協助組織達成資訊系統機密性、完整性和可用度等規定的安全目標。

"適用於 VMware vSphere 的 ONTAP 工具安全性強化指南" 瞭解如何為 VMware vSphere 設定 ONTAP 工具、以協助組織達成資訊系統機密性、完整性和可用度等規定的安全目標。

"TR-4957 ： NetApp SnapCenter 安全強化指南"
瞭解如何設定 NetApp SnapCenter 軟體、以協助組織達成資訊系統機密性、完整性和可用度等規定的安全目標。

"TR-4963：安全強化指南： NetApp Backup and Recovery"了解如何設定NetApp Cloud Backup for Applications，以協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。

"TR-4943 ： NetApp Active IQ Unified Manager 安全強化指南"
瞭解如何設定 NetApp Active IQ Unified Manager 、以協助組織達成資訊系統機密性、完整性和可用度等規定的安全目標。

"TR-4945 ： NetApp Manageability SDK 的安全強化指南"
瞭解如何設定 NetApp Manageability SDK （ NMSDK ）、以協助組織達成資訊系統機密性、完整性和可用度的規定安全目標。

"MetroCluster tiebreaker 主機和資料庫的安全性強化指南"瞭解如何設定 NetApp MetroCluster tiebreaker 主機和資料庫、以協助組織達成資訊系統機密性、完整性和可用度的規定安全目標。

ONTAP 安全強化準則

ONTAP 安全強化概述

ONTAP 提供一系列控制功能、可強化業界領先的資料管理軟體 ONTAP 儲存作業系統。使用 ONTAP 的指引和組態設定、協助貴組織達成資訊系統機密性、完整性和可用度等規定的安全目標。

目前威脅情勢的演變、為組織帶來獨特的挑戰、以保護其最寶貴的資產：資料與資訊。我們所面臨的先進動態威脅和弱點越來越精密。系統管理員必須主動處理資料和資訊的安全性、再加上潛在入侵者混淆和偵查技術的效率提高。

自 2024 年 7 月起，技術報告 _TR-4569 ： ONTAP 安全強化指南（先前以 PDF 格式發佈）的內容可在 docs.netapp.com 取得。

ONTAP 映像驗證

ONTAP 提供各種機制、確保 ONTAP 映像在升級和開機時有效。

升級映像驗證

程式碼簽章可協助驗證透過不中斷營運的映像更新或自動不中斷營運的映像更新、 CLI 或 ONTAP API 所安裝的 ONTAP 映像是由 NetApp 真正製作、且未遭竄改。升級映像驗證已在 ONTAP 9.3 中推出。

此功能是 ONTAP 升級或還原的無接觸安全性增強功能。除了選擇性地驗證頂層簽章之外、使用者不應採取任何不同的 `image.tgz` 做法。

開機時間映像驗證

從 ONTAP 9.4 開始、統一化可延伸韌體介面（ UEFI ）安全開機已啟用 NetApp AFF A800 、 AFF A220 、 FAS2750 和 FAS2720 系統、以及採用 UEFI BIOS 的後續新一代系統。

開機期間、開機載入器會驗證安全開機金鑰的白名單資料庫、以及與載入的每個模組相關聯的簽名。每個模組都經過驗證並載入之後、開機程序會繼續 ONTAP 初始化。如果任何模組的簽章驗證失敗、系統會重新開機。

這些項目適用於 ONTAP 映像和平台 BIOS 。

本機儲存管理員帳戶

ONTAP 角色，應用程式和驗證

ONTAP 讓注重安全性的企業能夠透過不同的登入應用程式和方法、對不同的管理員提供精細的存取。這有助於客戶建立以資料為中心的零信任模式。

這些角色可供管理員和儲存虛擬機器管理員使用。指定登入應用程式方法和登入驗證方法。

角色

透過角色型存取控制（ RBAC ）、使用者只能存取其工作角色和功能所需的系統和選項。ONTAP 中的 RBAC 解決方案可將使用者的系統管理存取權限限制為其定義角色所授予的層級、讓系統管理員能夠依指派的角色來管理使用者。ONTAP 提供數個預先定義的角色。操作員和管理員可以建立、修改或刪除自訂存取控制角色、也可以指定特定角色的帳戶限制。

叢集管理員的預先定義角色

此角色…	具有此存取層級…	至下列命令或命令目錄
`admin`	全部	所有命令目錄(`DEFAULT`)
`admin-no-fsa`（從 ONTAP 9.12.1 開始提供）	讀取/寫入	• 所有命令目錄(`DEFAULT`) • `security login rest-role` • `security login role`

唯讀	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	無
volume file show-disk-usage	autosupport	全部
• set • system node autosupport	無	所有其他命令目錄(DEFAULT)
backup	全部	vserver services ndmp
唯讀	volume	無
所有其他命令目錄(DEFAULT)	readonly	全部
• security login password 僅用於管理自己的使用者帳戶本機密碼和金鑰資訊 • set	無	security

唯讀	所有其他命令目錄(DEFAULT)	none

`autosupport`角色會指派給預先定義的帳戶， AutoSupport OnDemand 會 `autosupport`使用該帳戶。ONTAP 可防止您修改或刪除 `autosupport`帳戶。ONTAP 也會防止您將角色指派 `autosupport`給其他使用者帳戶。

儲存虛擬機器（ **SVM** ）管理員的預先定義角色

角色名稱	功能
vsadmin	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、但磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 執行 SnapLock 作業、但特權刪除除外 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務： DNS 、 LDAP 和 NIS • 監控工作 • 監控網路連線和網路介面 • 監控 SVM 的健全狀況
vsadmin-volume	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、但磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務： DNS 、 LDAP 和 NIS • 監控網路介面 • 監控 SVM 的健全狀況

vsadmin-protocol	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務： DNS 、 LDAP 和 NIS • 管理LUN • 監控網路介面 • 監控 SVM 的健全狀況
vsadmin-backup	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理 NDMP 作業 • 將還原的磁碟區設為讀取 / 寫入 • 管理 SnapMirror 關係和快照 • 檢視磁碟區和網路資訊
vsadmin-snaplock	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、但磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 執行 SnapLock 作業、包括特權刪除 • 設定通訊協定： NFS 和 SMB • 設定服務： DNS 、 LDAP 和 NIS • 監控工作 • 監控網路連線和網路介面
vsadmin-readonly	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 監控 SVM 的健全狀況 • 監控網路介面 • 檢視磁碟區和 LUN • 檢視服務與通訊協定

應用程式方法

應用程式方法會指定登入方法的存取類型。可能的值包括 `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, 和 `telnet`。

設定此參數可 `service-processor` 授予使用者對服務處理器的存取權。當此參數設為 `service-processor`時、參數必須設為、 `-authentication-method password` 因為服務處理器僅支援 `password` 驗證。SVM 使用者帳戶無法存取服務處理器。因此，當此參數設為時，操作員和管理員無法使用 `-vserver` 此參數 `service-processor`。

要進一步限制對的訪問 `service-processor` ，請使用命令 `system service-processor ssh add-allowed-addresses`。此命令 `system service-processor api-service` 可用於更新組態和憑證。

基於安全考量、依預設會停用 Telnet 和遠端 Shell （ RSH ）、因為 NetApp 建議使用安全 Shell （ SSH ）來進行安全遠端存取。如果需要 Telnet 或 RSH 、或是有獨特的需求、則必須啟用這些功能。

此 `security protocol modify` 命令會修改現有的 RSH 和 Telnet 叢集範圍組態。在叢集中啟用 RSH 和 Telnet 、方法是將啟用欄位設定為 `true`。

驗證方法

驗證方法參數指定用於登入的驗證方法。

驗證方法	說明
`cert`	SSL 憑證驗證
`community`	SNMP 社群字串
`domain`	Active Directory 驗證
`nsswitch`	LDAP 或 NIS 驗證
`password`	密碼
`publickey`	公開金鑰驗證
`usm`	SNMP 使用者安全模式

由於傳輸協定安全性弱點、不建議使用 NIS 。

從 ONTAP 9.3 開始、連結式雙因素驗證可用於使用和做為兩種驗證方法的本機 SSH `admin` 帳戶 `publickey password`。除了命令中的欄位之外 `-authentication-method` `security login` 、還新增了一個名為的新欄位 `-second-authentication-method`。 `publickey`或 `password` 可以指定為 `-authentication-method` 或 `-second-authentication-method`。不過、在 SSH 驗證期間、訂單一律 `publickey` 採用部分驗證、接著是完整驗證的密碼提示。

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

從 ONTAP 9.4 開始、 `nsswitch` 可以用做第二種驗證方法 `publickey`。

從 ONTAP 9.12.1 開始、 FIDO2 也可用於使用 YubiKey 硬體驗證裝置或其他 FIDO2 相容裝置進行 SSH 驗證。

從 ONTAP 9.13.1 開始：

- `domain` 帳戶可以用作第二種驗證方法 `publickey`。
- 時間型一次性密碼 (`totp`）是由演算法所產生的暫時密碼、該演算法會使用目前時間作為第二種驗證方法的驗證因素之一。

- SSH 公開金鑰和憑證均支援公開金鑰撤銷、這些憑證將在 SSH 期間檢查是否到期 / 撤銷。

如需 ONTAP System Manager 、 Active IQ Unified Manager 和 SSH 的多因素驗證（ MFA ）詳細資訊、請參閱 "TR-4647 ： ONTAP 9 中的多因素驗證"。

預設管理帳戶

應限制管理帳戶、因為系統管理員的角色可以使用所有應用程式進行存取。診斷帳戶可存取系統 Shell 、且應僅保留給技術支援人員、以執行疑難排解工作。

有兩個預設的系統管理帳戶： `admin` 和 `diag`。

孤立帳戶是一種主要的安全媒介、通常會導致弱點、包括權限升級。這些是不必要且未使用的帳戶、保留在使用者帳戶儲存庫中。這些帳戶主要是從未使用過的預設帳戶、或從未更新或變更過密碼的帳戶。為了解決此問題、ONTAP 支援移除和重新命名帳戶。

您無法刪除或重新命名內建帳戶。如果管理員刪除了帳戶，系統重新啟動後，該內建帳戶將會重新建立。*NetApp 建議*使用 lock 指令鎖定任何不需要的內建帳戶。

雖然孤立帳戶是重要的安全問題，但 **NetApp** 強烈建議 測試從本機帳戶庫中刪除帳戶的影響。

列出本機帳戶

若要列出本機帳戶、請執行 `security login show` 命令。

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1
                              Authentication              Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------ -----------
admin            console     password  admin             no     no
admin            http        password  admin             no     no
admin            ontapi      password  admin             no     no
admin            service-processor password admin        no     no
admin            ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
6 entries were displayed.
```

設定診斷（診斷）帳戶密碼

您的儲存系統會隨附一個名為的診斷帳戶 `diag` 。您可以使用 `diag` 帳戶執行中的疑難排解工作 `systemshell`。 `diag`帳戶是唯一可用於通過特權命令訪問 `systemshell` 的帳戶 `diag systemshell`。

systemshell 和相關 `diag` 帳戶是為了低層級的診斷目的而設計。他們的存取權限需要診斷權限層級、且僅保留在技術支援人員的指引下使用、以執行疑難排解工作。帳戶和都不是 `diag systemshell` 用於一般管理用途。

開始之前

在存取之前 `systemshell`、您必須使用命令設定 `diag` 帳戶密碼 `security login password`。您應該使用強式密碼原則、並定期變更 `diag` 密碼。

步驟

1. 設定 `diag` 帳戶使用者密碼：

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

多管理員驗證

從 ONTAP 9.11.1 開始，您可以使用多重管理驗證（ MAV ），只有在指定管理員核准後，才能執行某些作業，例如刪除磁碟區或快照。如此可防止遭到入侵、惡意或缺乏經驗的系統管理員進行不必要的變更或刪除資料。

設定 MAV 包含下列項目：

- "建立一個或多個管理員核准群組"。
- "啟用多重管理驗證功能"。
- "新增或修改規則"。

在初始設定之後、只有 MAV 核准群組（ MAV 管理員）中的管理員可以修改這些元素。

啟用 MAV 時、完成每項受保護的作業需要三個步驟：

1. 當使用者啟動作業時，會"已產生要求"出現一個。
2. 在執行之前，所需的數量爲"MAV 管理員必須核准"。

3. 核准後、使用者即完成作業。

MAV 不適用於需要大量自動化的磁碟區或工作流程、因為每項自動化工作都需要先獲得核准、才能完成作業。如果您想要同時使用自動化和 MAV 、 NetApp 建議您針對特定的 MAV 作業使用查詢。例如、您只能將 MAV 規則套用 `volume delete` 至不涉及自動化的磁碟區、而且可以使用特定的命名方案來指定這些磁碟區。

有關 MAV 的詳細信息，請參閱 "ONTAP 多管理驗證文件"。

Snapshot 鎖定

Snapshot 鎖定是一種 SnapLock 功能，可在磁碟區快照原則上以手動或自動方式呈現快照，並保留一段時間。快照鎖定的目的是防止惡意或不受信任的系統管理員刪除主要或次要 ONTAP 系統上的快照。

ONTAP 9.12.1 引進快照鎖定功能。Snapshot 鎖定也稱為防竄改快照鎖定。雖然它需要 SnapLock 授權和法規遵循時鐘的初始化，但快照鎖定與 SnapLock Compliance 或 SnapLock Enterprise 無關。沒有值得信賴的儲存管理員、就像 SnapLock Enterprise 一樣、它也無法保護基礎實體儲存基礎架構、就像 SnapLock Compliance 一樣。這是對次要系統的 SnapVauling 快照的改善。可在主要系統上快速恢復鎖定的快照，以還原遭勒索軟體毀損的磁碟區。

如需詳細資訊，請參閱"Snapshot 鎖定文件"。

設定憑證型 **API** 存取

除了用於 REST API 或 NetApp Manageability SDK API 存取 ONTAP 的使用者 ID 和密碼驗證之外、還必須使用憑證型驗證。

作為 REST API 憑證型驗證的替代方案、請使用 "OAuth 2.0 權杖型驗證"。）

您可以在 ONTAP 上產生並安裝自我簽署的憑證、如下列步驟所述。

步驟

1. 使用 Openssl 執行下列命令來產生憑證：

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
............................+++
writing new private key to 'test.key'
```

此命令會產生一個名為的公開憑證 `test.pem` 和一個名為的私密金鑰 `key.out`。一般名稱 CN 對應於 ONTAP 使用者 ID 。

2. 在 ONTAP 中以隱私權增強郵件（ pem ）格式安裝公開憑證內容、方法是執行下列命令、並在出現提示時貼上憑證內容：

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. 啟用 ONTAP 以允許透過 SSL 存取用戶端、並定義 API 存取的使用者 ID 。

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

在下列範例中、使用者 ID `cert_user` 現在已啟用、可使用憑證驗證的 API 存取。使用簡單的 Manageability SDK Python 指令碼 `cert_user` 來顯示 ONTAP 版本、如下所示：

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

指令碼的輸出會顯示 ONTAP 版本。

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. 若要使用 ONTAP REST API 執行憑證型驗證、請完成下列步驟：
   a. 在 ONTAP 中、定義 http 存取的使用者 ID ：

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

   b. 在您的 Linux 用戶端上、執行下列命令來產生 ONTAP 版本做為輸出：

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

更多資訊

- "憑證型驗證、搭配 NetApp Manageability SDK for ONTAP"。

REST API 的 ONTAP OAuth 2.0 權杖型驗證

除了憑證型驗證之外、您也可以使用 OAuth 2.0 權杖型驗證來進行 REST API 。

從 ONTAP 9.14.1 開始、您可以選擇使用開放授權（ OAuth 2.0 ）架構來控制對 ONTAP 叢集的存取。您可以使用任何 ONTAP 管理介面（包括 ONTAP CLI 、系統管理員和 REST API ）來設定此功能。不過、 OAuth 2.0 授權和存取控制決策只能在用戶端使用 REST API 存取 ONTAP 時套用。

OAuth 2.0 Token 取代使用者帳戶驗證的密碼。

如需使用 OAuth 2.0 的詳細資訊，請參閱 "使用 OAuth 2.0 驗證和授權的 ONTAP 文件"。

有效的安全態勢遵循既定的組織原則、準則、以及適用於組織的任何治理或標準。這些需求的範例包括使用者名稱存留期、密碼長度要求、字元需求、以及這類帳戶的儲存。ONTAP 解決方案提供解決這些安全性架構的功能。

新的本機帳戶功能

為了支援組織的使用者帳戶原則、準則或標準、包括治理、 ONTAP 支援下列功能：

- 設定密碼原則以強制執行最小位數、小寫字元或大寫字元數
- 登入嘗試失敗後需要延遲
- 定義帳戶非使用中限制
- 使用者帳戶過期
- 顯示密碼過期警告訊息
- 登入無效的通知

可設定的設定是使用安全登入角色組態修改命令來管理。

支援 **SHA-512**

為了加強密碼安全性、 ONTAP 9 支援 SHA-2 密碼雜湊功能、並預設使用 SHA-512 來雜湊新建立或變更的密碼。操作員和管理員也可以視需要過期或鎖定帳戶。

在升級至 ONTAP 9.0 或更新版本之後、具有未變更密碼的現有 ONTAP 9 使用者帳戶會繼續使用 MD5 雜湊功能。不過、 NetApp 強烈建議使用者變更密碼、以移轉至更安全的 SHA-512 解決方案。

密碼雜湊功能可讓您執行下列工作：

- 顯示符合指定雜湊功能的使用者帳戶：

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- 使使用指定雜湊功能（例如、 MD5 ）的帳戶過期、強制使用者在下一次登入時變更其密碼：

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- 使用使用指定雜湊功能的密碼鎖定帳戶。

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

叢集管理 SVM 中的內部使用者無法辨識密碼雜湊功能 `autosupport` 。此問題只是表面問題。雜湊功能未知、因為此內部使用者預設沒有設定的密碼。

  - 若要檢視使用者的密碼雜湊功能 `autosupport` 、請執行下列命令：

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                    Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

  - 若要設定密碼雜湊功能（預設值： SHA512 ）、請執行下列命令：

```
::> security login password -username autosupport
```

無論密碼設定為何、都沒有關係。

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

密碼參數

ONTAP 解決方案支援密碼參數、可滿足及支援組織原則需求與準則。

從 9.14.1 開始，密碼的複雜度和鎖定規則增加，僅適用於新安裝的 ONTAP 。

所有密碼都必須與使用者名稱不同。

屬性	說明	預設	範圍
username-minlength	需要使用者名稱長度下限	3	3-16
username-alphanum	使用者名稱英數字元	已停用	啟用 / 停用
passwd-minlength	所需的密碼長度下限	8	3-64
passwd-alphanum	密碼英數字元	已啟用	啟用 / 停用
passwd-min-special-chars	密碼中所需的最少特殊字元數	0	0-64
passwd-expiry-time	密碼過期時間（以天為單位）	無限制、這表示密碼永遠不會過期	不受限制 0 = 現在到期
require-initial-passwd-update	首次登入時需要初始密碼更新	已停用	啟用 / 停用 允許透過主控台或 SSH 進行變更
max-failed-login-attempts	失敗嘗試次數上限	0 、請勿鎖定帳戶	-
lockout-duration	最長鎖定期間（以天為單位）	預設值為 0 、表示帳戶已鎖定一天	-
disallowed-reuse	不允許最後 N 個密碼	6	最小值為 6

屬性	說明	預設	範圍
change-delay	密碼變更之間的延遲（以天為單位）	0	-
delay-after-failed-login	每次登入嘗試失敗後的延遲（以秒為單位）	4	-
passwd-min-lowercase-chars	密碼中所需的最小小寫字母字元數	0 、不需要小寫字元	0-64
passwd-min-uppercase-chars	所需的大寫字母字元數下限	0 、不需要大寫字元	0-64
passwd-min-digits	密碼中所需的最小位數	0 、不需要數字	0-64
passwd-expiry-warn-time	在密碼過期前顯示警告訊息（以天為單位）	無限制、這表示永遠不會警告密碼過期	0 、這表示每次成功登入時、都會警告使用者密碼過期
account-expiry-time	帳戶在 N 天內過期	無限、這表示帳戶永遠不會過期	帳戶過期時間必須大於帳戶非使用中限制
account-inactive-limit	帳戶過期前的最長閒置時間（以天為單位）	無限、這表示非使用中帳戶永遠不會過期	帳戶非使用中限制必須小於帳戶到期時間

範例

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                        Vserver: cluster1
                                      Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                         Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

系統管理方法

這些是強化 ONTAP 系統管理的重要參數。

命令列存取

建立安全的系統存取權、是維護安全解決方案的重要一環。最常見的命令列存取選項是 SSH 、 Telnet 和 RSH 。其中、 SSH 是最安全、業界標準的遠端命令列存取最佳實務做法。NetApp 強烈建議使用 SSH 命令列存取 ONTAP 解決方案。

SSH 組態

此 `security ssh show` 命令會顯示叢集和 SVM 的 SSH 金鑰交換演算法、加密演算法和 MAC 演算法組態。金鑰交換方法使用這些演算法和密碼來指定一次性工作階段金鑰的產生方式、以進行加密和驗證、以及伺服器驗證的執行方式。

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

登入橫幅

登入橫幅可讓組織向任何營運者、管理員甚至是誤解者展示可接受使用的條款與條件、並指出哪些人可以存取系統。此方法有助於建立對系統存取與使用的期望。命令會 `security login banner modify` 修改登入橫幅。登入橫幅會在 SSH 和主控台裝置登入程序中的驗證步驟之前顯示。橫幅文字必須使用雙引號（"""）、如下例所示。

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

登入橫幅參數

參數	說明
`vserver`	使用此參數以修改後的橫幅指定 SVM 。使用叢集管理 SVM 的名稱來修改叢集層級訊息。叢集層級的訊息會作為未定義訊息的資料 SVM 的預設值。
`message`	此選用參數可用於指定登入橫幅訊息。如果叢集已設定登入橫幅訊息、則所有資料 SVM 也會使用叢集登入橫幅。設定資料 SVM 的登入橫幅會覆寫叢集登入橫幅的顯示。若要重設資料 SVM 登入橫幅以使用叢集登入橫幅、請將此參數與值 "-" 一起使用。 如果您使用此參數、登入橫幅不得包含換行（也稱為行尾 [EOLS] 或換行符號）。若要以新行輸入登入橫幅訊息、請勿指定任何參數。系統會提示您以互動方式輸入訊息。以互動方式輸入的訊息可以包含新行。 非 ASCII 字元必須使用 Unicode UTF-8 。
`uri`	`(ftp
http):///(hostname	IPv4` 使用此參數指定登入橫幅下載來源的 URI 。 訊息長度不得超過 2048 位元組。非ASCII字元必須以UNICODE UTF-8格式提供。

當日訊息

命令會 `security login motd modify` 更新當天的訊息（ MOTD ）。

MOTD 有兩種類別：叢集層級 MOTD 和資料 SVM 層級 MOTD 。登入資料 SVM 叢集 Shell 的使用者可能會看到兩則訊息：叢集層級 MOTD 、以及該 SVM 的 SVM 層級 MOTD 。

叢集管理員可視需要個別啟用或停用每個 SVM 上的叢集層級 MOTD 。如果叢集管理員停用 SVM 的叢集層級 MOTD 、則登入 SVM 的使用者不會看到叢集層級的訊息。只有叢集管理員才能啟用或停用叢集層級的訊息。

MOTD 參數	說明
Vserver	使用此參數可指定修改 MOTD 的 SVM 。使用叢集管理 SVM 的名稱來修改叢集層級訊息。

MOTD 參數	說明
訊息	此選用參數可用於指定訊息。如果您使用此參數、則 MOTD 不能包含換行。如果您未指定參數以外的任何參數 `-vserver` 、系統會提示您以互動方式輸入訊息。以互動方式輸入的訊息可以包含新行。非ASCII字元必須以UNICODE UTF-8格式提供。訊息可以包含使用下列轉義序列動態產生的內容： • `\\` - 單一反彈字元 • `\b` - 無輸出（僅支援與 Linux 相容） • `\C` - 叢集名稱 • `\d` - 登入節點上設定的目前日期 • `\t` - 登入節點上設定的目前時間 • `\I` - 傳入 LIF IP 位址（列印主控台以供 `console` 登入） • `\l` - 登入裝置名稱（列印登入主控台 `console` ） • `\L` - 使用者在叢集中任何節點上的上次登入 • `\m` - 機器架構 • `\n` - 節點或資料 SVM 名稱 • `\N` - 登入的使用者名稱 • `\o` - 與 \O 相同提供Linux相容性。 • `\O` - 節點的 DNS 網域名稱。請注意、輸出取決於網路組態、可能是空的。 • `\r` - 軟體版本編號 • `\s` - 作業系統名稱 • `\u` - 本機節點上的作用中叢集 Shell 工作階段數目。對於叢集管理：所有叢集Shell使用者。針對資料 SVM 管理：僅適用於該資料 SVM 的作用中工作階段。 • `\U` - 與相同 `\u`、但有 `user` 或 `users` 附加 • `\v` - 有效的叢集版本字串 • `\W` - 跨叢集的作用中工作階段、供登入的使用者使用 (`who`)

如需在 ONTAP 中設定當日訊息的詳細資訊，請參閱 "當日訊息上的 ONTAP 文件"。

CLI 工作階段逾時

預設 CLI 工作階段逾時為 30 分鐘。逾時對於防止過時的工作階段和工作階段工作階段暫存是很重要的。

使用 `system timeout show` 命令檢視目前的 CLI 工作階段逾時。若要設定逾時值、請使用 `system timeout modify -timeout <minutes>` 命令。

透過 NetApp ONTAP 系統管理員存取網路

如果 ONTAP 管理員偏好使用圖形化介面而非 CLI 來存取和管理叢集、請使用 NetApp ONTAP 系統管理員。ONTAP 隨附 Web 服務、預設為啟用、並可使用瀏覽器存取。如果使用 DNS 、 IPv4 或 IPv6 位址、請將瀏

覽器指向主機名稱（透過 `https://cluster-management-LIF`）。

如果叢集使用自我簽署的數位憑證、瀏覽器可能會顯示警告、指出該憑證不受信任。您可以確認繼續存取的風險、或在叢集上安裝憑證授權單位（ CA ）簽署的數位憑證、以進行伺服器驗證。

從 ONTAP 9.3 開始、安全聲明標記語言（ SAML ）驗證是 ONTAP 系統管理員的選項。

ONTAP 系統管理員的 SAML 驗證

SAML 2.0 是廣泛採用的產業標準、可讓任何符合 SAML 標準的第三方身分識別供應商（ IDP ）、使用企業所選擇的 IDP 所特有的機制來執行 MFA 、並做為單一登入（ SSO ）的來源。

SAML 規格中定義了三種角色：主體、 IDP 和服務供應商。在 ONTAP 實作中、主要是叢集管理員透過 ONTAP 系統管理員或 NetApp Active IQ Unified Manager 存取 ONTAP 。IDP 是第三方 IDP 軟體。從 ONTAP 9.3 開始、支援 Microsoft Active Directory 聯合服務（ ADFS ）和開放原始碼 Shibboleth IDP 。從 ONTAP 9.12.1 開始、 Cisco 雙核心支援 IDP 。服務供應商是 ONTAP 系統管理員或 Active IQ Unified Manager 網路應用程式所使用的 ONTAP 內建 SAML 功能。

與 SSH 雙因素組態程序不同的是、啟動 SAML 驗證之後、 ONTAP 系統管理員或 ONTAP 服務處理器存取需要所有現有系統管理員透過 SAML IDP 進行驗證。叢集使用者帳戶無需變更。啟用 SAML 驗證時、會將的新驗證方法新 `saml` 增至具有與應用程式管理員角色的現有使用者 `http ontapi` 。

啟用 SAML 驗證之後、需要 SAML IDP 存取的其他新帳戶應在 ONTAP 中定義、並以系統管理員角色及和應用程式的 SAML 驗證方法定義 `http ontapi` 。如果在某個時間點停用 SAML 驗證、則這些新帳戶需要 `password` 以和應用程式的管理員角色來定義驗證方法、並將應用程式新增至 ONTAP 系統管理員以 `http ontapi console` 進行本機 ONTAP 驗證。

啟用 SAML IDP 之後、 IDP 會使用 IDP 可用的方法（例如輕量型目錄存取傳輸協定（ LDAP ）、 Active Directory （ AD ）、 Kerberos 、密碼等）來執行 ONTAP 系統管理員存取的驗證。可用的方法對 IDP 是唯一的。在 ONTAP 中設定的帳戶必須具有對應至 IDP 驗證方法的使用者 ID 。

已通過 NetApp 驗證的 IDP 為 Microsoft ADFS 、 Cisco Duo 和開放原始碼 Shibboleth IDP 。

從 ONTAP 9.14.1 開始、 Cisco 雙核心可作為 SSH 的第二個驗證因素。

如需更多關於 MFA for ONTAP System Manager 、 Active IQ Unified Manager 和 SSH 的資訊、請參閱 "TR-4647 ： ONTAP 9 中的多因素驗證"。

ONTAP System Manager 洞見

從 ONTAP 9.11.1 開始、 ONTAP 系統管理員提供深入見解、協助叢集管理員簡化日常工作。安全性洞見是以本技術報告的建議為基礎。

Security Insight	決心
已啟用 Telnet	NetApp建議使用安全Shell（SSH）進行安全遠端存取。
已啟用遠端 Shell （ RSH ）	NetApp 建議使用 SSH 進行安全的遠端存取。
AutoSupport 使用的是不安全的傳輸協定	AutoSupport 未設定為透過連結： HTTPS 傳送。
叢集層級的叢集上未設定登入橫幅	如果未針對叢集設定登入橫幅、則會發出警告。
SSH 使用不安全的密碼	如果 SSH 使用不安全的密碼、則會發出警告。

Security Insight	決心
設定的 NTP 伺服器太少	如果設定的 NTP 伺服器數量少於三個、則會發出警告。
預設管理使用者未鎖定	如果不使用任何預設的系統管理帳戶（ admin 或 diag ）登入系統管理員、而且這些帳戶未鎖定、建議您將其鎖定。
勒索軟體防禦：磁碟區沒有 Snapshot 原則	一個或多個磁碟區未附加適當的 Snapshot 原則。
勒索軟體防禦：停用 Snapshot 自動刪除	已為一或多個磁碟區設定 Snapshot 自動刪除。
磁碟區並未受到勒索軟體攻擊的監控	多個磁碟區支援自動勒索軟體保護，但尚未設定。
SVM 並未設定為自動勒索軟體保護	多個 SVM 支援自動勒索軟體保護，但尚未設定。
未設定原生 FPolicy	未針對 NAS SVM 設定 FPolicy 。
啟用自動勒索軟體保護作用中模式	數個磁碟區已完成其學習模式、您可以開啟作用中模式
停用全域 FIPS 140-2 規範	未啟用全域 FIPS 140-2 規範。
未設定叢集以接收通知	電子郵件、 Webhooks 或 SNMP traphosts 未設定為接收通知。

如需 ONTAP System Manager 深入分析的詳細資訊，請參閱 "ONTAP System Manager Insights 文件"。

System Manager 工作階段逾時

您可以變更 System Manager 工作階段閒置逾時。預設的閒置逾時為 30 分鐘。逾時對於防止過時的工作階段和工作階段暫存是很重要的。

如果已設定 SAML ，則閒置逾時會由 IDP 上的設定控制。

步驟

1. 選擇*叢集>設定*。
2. 在 **UI settings** 中，選擇 。
3. 在 * 閒置逾時 * 方塊中，輸入介於 2 到 180 之間的分鐘值，或輸入「 0 」以停用逾時。
4. 選擇*保存*。

ONTAP 自主勒索軟體保護

為了輔助使用者對儲存工作負載安全性的行為分析， ONTAP 自主勒索軟體保護會分析大量工作負載和 Entropy ，以偵測勒索軟體，並在懷疑有攻擊時擷取快照並通知管理員。

除了使用外部 FPolicy 使用者行為分析 (UBA) 結合NetApp Data Infrastructure Insights Storage Workload Security 和NetApp FPolicy 合作夥伴生態系統進行勒索軟體偵測和預防之外， ONTAP 9.10.1 還引入了自主勒索軟體防護。 ONTAP自主勒索軟體防護使用內建的機上機器學習 (ML) 功能，可查看大量工作負載活動和資料熵來自動偵測勒索軟體。它監控與 UBA 不同的活動，以便能夠偵測到 UBA 無法偵測到的攻擊。

如需此功能的詳細資訊、請參閱"NetApp 勒索軟體解決方案"或"ONTAP 自主勒索軟體保護文件"。

儲存管理系統稽核

將 ONTAP 事件卸載到遠端系統記錄伺服器、確保事件稽核的完整性。此伺服器可能是像 Splunk 這樣的安全性資訊事件管理系統。

傳送系統記錄

從支援與可用度的角度來看、記錄與稽核資訊對組織來說是非常寶貴的。此外、記錄（ Syslog ）和稽核報告和輸出中所包含的資訊和詳細資料、通常都是敏感的性質。為了維持安全控管和狀態、組織必須以安全的方式管理記錄和稽核資料。

若要將資料外洩的範圍或佔用空間限制在單一系統或解決方案、就必須卸載syslog資訊。因此、NetApp建議將系統記錄資訊安全地卸載到安全的儲存或保留位置。

建立記錄轉送目的地

使用 `cluster log-forwarding create` 命令建立記錄轉送目的地以進行遠端記錄。

參數

使用下列參數來設定 `cluster log-forwarding create` 命令：

- * 目的地主機 *此名稱是要將記錄轉送到的伺服器的主機名稱或 IPv4 或 IPv6 位址。

```
-destination <Remote InetAddress>
```

- * 目的地連接埠。 *這是目的地伺服器接聽的連接埠。

```
[-port <integer>]
```

- * 記錄轉送通訊協定。 *此傳輸協定用於傳送訊息至目的地。

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  記錄轉送通訊協定可以使用下列其中一個值：

  - `udp-unencrypted`。沒有安全性的使用者資料包傳輸協定。
  - `tcp-unencrypted`。無安全性的 TCP 。
  - `tcp-encrypted`。傳輸層安全性（ TLS ）的 TCP 。

- * 驗證目的地伺服器身分識別。 *當此參數設為 true 時、會驗證其憑證、以驗證記錄轉送目的地的身分識別。只有在通訊協定欄位中選取值時、才能將值設為 true `tcpencrypted` 。

```
[-verify-server \{true|false}]
```

- * 系統記錄工具。 *此值是用於轉送記錄的 Syslog 功能。

```
[-facility <Syslog Facility>]
```

- * 跳過連線測試。 *通常、 `cluster log-forwarding create` 命令會傳送網際網路控制訊息傳輸協定（ ICMP ） ping 來檢查目的地是否可連線、如果無法連線則會失敗。將此值設定為 `true` 略過 ping 檢查、以便在無法到達目的地時設定目的地。

```
[-force [true]]
```

NetApp 建議您使用 `cluster log-forwarding` 命令強制連線至某種 `-tcp-encrypted` 類型。

事件通知

保護離開系統的資訊和資料、對於維護和管理系統的安全狀態至關重要。ONTAP 解決方案所產生的事件、提供豐富的解決方案所遇到的問題、處理的資訊等資訊。這些資料的活力、突顯了以安全的方式管理及移轉資料的必要性。

命令會 `event notification create` 將事件篩選器定義的一組事件的新通知傳送至一或多個通知目的地。下列範例說明事件通知組態和 `event notification show` 命令、該命令會顯示設定的事件通知篩選器和目的地。

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

ONTAP 中的儲存加密

為了在磁碟遭竊、退回或重新規劃用途時保護敏感資料、請使用硬體型 NetApp 儲存加密或軟體型 NetApp Volume 加密 /NetApp Aggregate 加密。這兩種機制均已通過 FIPS 140-2 驗證、若將硬體型機制搭配軟體型機制使用、則解決方案符合商業解決方案分類（ CSfC ）方案的資格。它可在硬體和軟體層、為機密和機密資料提供強化的安全保護。

當磁碟遭竊、退回或重新使用時、靜止資料加密對於保護敏感資料非常重要。

ONTAP 9 有三種符合聯邦資訊處理標準（ FIPS ） 140-2 標準的靜態資料加密解決方案：

- NetApp 儲存加密（ NSE ）是使用自我加密磁碟機的硬體解決方案。
- NetApp Volume Encryption （ NVE ）是一種軟體解決方案、可加密任何磁碟機類型上的任何資料磁碟區、

並為每個磁碟區啟用唯一的金鑰。

- NetApp Aggregate Encryption （ NAE ）是一種軟體解決方案、可加密任何磁碟機類型上的任何資料磁碟區、並為每個集合啟用唯一金鑰。

NSE 、 NVE 和 NAE 可以使用外部金鑰管理或內建金鑰管理程式（ OKM ）。使用 NSE 、 NVE 和 NAE 不會影響 ONTAP 儲存效率功能。不過、 NVE 磁碟區會排除在 Aggregate 重複資料刪除之外。Nae Volume 參與並受益於 Aggregate 重複資料刪除技術。

OKM 為 NSE 、 NVE 或 NAE 的靜態資料提供獨立加密解決方案。

NVE 、 NAE 和 OKM 使用 ONTAP CryptoMod.CryptoModis會列在CMVP FIPS 140-2驗證模組清單中。請參閱。 "FIPS 140-2 Cert# 4144"

若要開始 OKM 組態、請使用 `security key-manager onboard enable` 命令。若要設定外部金鑰管理互通性通訊協定（ KMIP ）金鑰管理員、請使用 `security key-manager external enable` 命令。從 ONTAP 9.6 開始、外部金鑰管理員可支援多處佔用。使用此 `-vserver <vserver name>` 參數為特定 SVM 啟用外部金鑰管理。在 9.6 之前、 `security key-manager setup` 命令用於設定 OKM 和外部金鑰管理員。為了進行內建金鑰管理、此組態會引導操作員或管理員完成複雜密碼設定、以及設定 OKM 的其他參數。

以下範例提供部分組態：

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode` 的「真」選項 `security key-manager setup` 、要求使用者在重新開機後輸入複雜密碼。對於 ONTAP 9.6 及更新版本、命令語法為 `security key-manager onboard enable -cc-mode-enabled yes`。

從 ONTAP 9.4 開始、您可以使用 `secure-purge` 具有進階權限的功能、在啟用 NVE 的磁碟區上不中斷地「清理」資料。清理加密磁碟區上的資料可確保無法從實體媒體恢復資料。以下命令可安全地清除 SVM VS1 上 vol1 上刪除的檔案：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

從 ONTAP 9.7 開始、如果有 VE 授權、設定 OKM 或外部金鑰管理員、且不使用 NSE 、則預設會啟用 NAE 和 NVE 。根據預設、 NAE 集合體上會建立 Nae Volume 、而非 NAE 集合體預設會建立 NVE Volume 。您可以輸入下列命令來覆寫：

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

從 ONTAP 9.6 開始、您可以使用 SVM 範圍來設定叢集中資料 SVM 的外部金鑰管理。這最適合多租戶環境、其中每個租戶使用不同的 SVM （或 SVM 組）來提供資料。只有特定租戶的SVM管理員可以存取該租戶的金鑰。如需詳細資訊、請參閱 "在 ONTAP 9.6 及更新版本中啟用外部金鑰管理" ONTAP 文件中的。

從 ONTAP 9.11.1 開始，您可以在 SVM 上指定主要和次要金鑰伺服器，以設定與叢集式外部金鑰管理伺服器的連線。如需詳細資訊、請參閱 "設定叢集式外部金鑰伺服器" ONTAP 文件中的。

從 ONTAP 9.13.1 開始，您可以在系統管理員中設定外部金鑰管理伺服器。如需詳細資訊、請參閱 "管理外部金鑰管理員" ONTAP 文件中的。

資料複寫加密

為了補充靜態資料加密，您可以使用 TLS 和預共用金鑰對叢集之間的 ONTAP 資料複製流量進行加密，金鑰可以是 SnapMirror、SnapVault 或 FlexCache。

當複寫資料以進行災難恢復、快取或備份時、您必須在從ONTAP 一個叢集傳輸到另一個叢集的過程中、透過線路來保護資料。這樣做可防止惡意攔截式攻擊、攻擊正在傳輸的敏感資料。

從 ONTAP 9.6 開始，叢集對等加密為 ONTAP 資料複製功能（例如 SnapMirror、SnapVault 和 FlexCache）提供 TLS 1.2 AES-256 GCM 加密支援。加密是透過兩個叢集對等體之間的預共用金鑰（PSK）來設定的。

從 ONTAP 9.15.1 開始，叢集對等加密為 ONTAP 資料複製功能（例如 SnapMirror、SnapVault 和 FlexCache）提供 TLS 1.3 AES-256 GCM 加密支援。加密是透過兩個叢集對等體之間的預共用金鑰（PSK）來設定的。

使用 NSE、NVE 和 NAE 等技術保護靜態資料的客戶，也可以透過升級到 ONTAP 9.6 或更高版本來使用叢集對等加密，從而實現端對端資料加密。

叢集對等連線會對叢集對等節點之間的所有資料進行加密。例如，使用 SnapMirror 時，所有對等連線資訊以及來源叢集對等節點和目標叢集對等節點之間的所有 SnapMirror 關係都會被加密。啟用叢集對等連線加密後，您無法在叢集對等節點之間傳送明文資料。

從 ONTAP 9.6 開始，新建立的叢集對等關係預設會啟用加密。若要在 ONTAP 9.6 之前建立的叢集對等關係上

啟用加密，您必須將來源叢集和目的地叢集升級至 9.6。此外，您還必須使用 `cluster peer modify` 命令將來源叢集對等端點和目的地叢集對等端點都變更為使用叢集對等加密。

您可以按照以下範例所示、將現有的對等關係轉換為在 ONTAP 9.6 中使用叢集對等加密：

```
On the destination cluster peer:

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the source cluster peer:

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

IPsec 資料傳輸中加密

使用 NetApp 儲存加密（ NSE ）或 NetApp Volume Encryption （ NVE ）和叢集對等加密（叢集對等加密）等靜態資料加密技術來進行資料複寫流量的客戶、現在可以升級至 ONTAP 9.8 或更新版本並使用、在用戶端和儲存設備之間使用端點對端加密 IPsec ：IPsec 提供 NFS 或 SMB/CIFS 加密的替代方案、也是 iSCSI 流量唯一的傳輸中加密選項。

在某些情況下、可能需要保護透過有線（或在線中）傳輸至 ONTAP SVM 的所有用戶端資料。如此可防止在敏感資料傳輸期間對其進行重播和惡意攔截式攻擊。

從 ONTAP 9.8 開始、網際網路傳輸協定安全性（ IPsec ）可為用戶端和 ONTAP SVM 之間的所有 IP 流量提供端點對端點加密支援。所有IP流量的IPsec資料加密包括NFS、iSCSI及SMB/CIFS傳輸協定。IPsec為iSCSI流量提供唯一的傳輸加密選項。

透過網路提供 NFS 加密是 IPsec 的主要使用案例之一。在 ONTAP 9.8 之前， NFS 有線加密需要設定和組態 Kerberos ，才能使用 krb5p 來加密執行中的 NFS 資料。在每個客戶環境中、這並不總是簡單或容易達成的。

使用 NetApp 儲存加密（ NSE ）或 NetApp Volume Encryption （ NVE ）和叢集對等加密（叢集對等加密）等靜態資料加密技術來進行資料複寫流量的客戶、現在可以升級至 ONTAP 9.8 或更新版本並使用、在用戶端和儲存設備之間使用端點對端加密 IPsec ：

IPsec 是一項 IETF 標準。ONTAP 在傳輸模式中使用 IPsec 。它也運用網際網路金鑰交換（ IKE ）傳輸協定第 2 版、使用預先共用金鑰（ PSK ）在用戶端與 ONTAP 之間、以 IPv4 或 IPv6 來交涉金鑰資料。根據預設、 IPsec 使用 Suite B AES-GCM 256 位元加密。也支援採用 256 位元加密的 Suite B AES-GMAC256 和 AES-CBC256 。

雖然必須在叢集上啟用 IPsec 功能、但它會透過使用安全性原則資料庫（ SPD ）項目、套用至個別 SVM IP 位址。原則（ SPD ）項目包含用戶端 IP 位址（遠端 IP 子網路）、 SVM IP 位址（本機 IP 子網路）、要使用的加密密碼套件、以及透過 IKEv2 驗證和建立 IPsec 連線所需的預先共用密碼（ PSK ）。除了 IPsec 原則項目之

外、用戶端必須使用相同的資訊（本機和遠端 IP 、 PSK 和密碼套件）進行設定、才能透過 IPsec 連線傳輸流量。從 ONTAP 9.10.1 開始、新增 IPsec 憑證驗證支援。這會移除 IPsec 原則限制、並啟用 Windows 作業系統對 IPsec 的支援。

如果用戶端和 SVM IP 位址之間有防火牆、則必須允許 ESP 和 UDP （連接埠 500 和 4500 ）傳輸協定（輸入）和輸出（輸出））、讓 IKEv2 交涉成功、從而允許 IPsec 傳輸。

對於 NetApp SnapMirror 和叢集對等流量加密、仍建議透過 IPsec 使用叢集對等加密（ CPe ）、以確保有線傳輸的安全。對於這些工作負載而言、 CPE 的效能比 IPsec 更好。您不需要 IPsec 的授權、也不需要任何匯入或匯出限制。

您可以在叢集上啟用 IPsec 、並為單一用戶端和單一 SVM IP 位址建立 SPD 項目、如下列範例所示：

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

相關資訊

"準備在 ONTAP 網路上使用 IP 安全性"

ONTAP 中的 FIPS 模式和 TLS 與 SSL 管理

FIPS 140-2 標準指定安全系統中密碼模組的安全需求、以保護電腦和電信系統中的機密資訊。FIPS 140-2 標準會套用至加密模組、而非產品、架構、資料或生態系統。密碼編譯模組是執行 NIST 核准安全功能的特定元件（硬體、軟體、韌體或三者的組合）。

啟用 FIPS 140-2 規範會影響其他系統、以及 ONTAP 9 內部和外部的通訊。NetApp 強烈建議在具有主控台存取權的非正式作業系統上測試這些設定。

從 ONTAP 9.11.1 和 TLS 1.3 支援開始、您可以驗證 FIPS 140-3 。

FIPS 組態適用於 ONTAP 和平台 BMC 。

NetApp ONTAP 的 FIPS 模式組態

NetApp ONTAP 具有 FIPS 模式組態、可在控制面板中產生新增的安全層級：

- 從 ONTAP 9.11.1 開始，當啟用 FIPS 140-2 規範模式時，會停用 TLSv1 ， TLSv1.1 和 SSLv3 ，而且只有 TSLv1.2 和 TSLv1.3 會保持啟用狀態。它會影響ONTAP 到其他內部和外部的系統和通訊、而這些系統和通訊則是來自於19。如果您啟用FIPS 140-2規範模式、然後停用、則TLSv1、TLSv1.1及SSLv3會維持停用狀態。視先前的組態而定、TLSv1.2或TLSSv1.3仍會保持啟用狀態。
- 對於 9.11.1 之前的 ONTAP 版本、啟用 FIPS 140-2 規範模式時、 TLSv1 和 SSLv3 都會停用、而且只有 TLSv1.1 和 TLSv1.2 會保持啟用狀態。啟用FIPS 140-2相容模式時、無法同時啟用TLSv1和SSLv3

。ONTAP如果您啟用FIPS 140-2規範模式、然後停用該模式、則TLSv1和SSLv3仍會維持停用狀態、但根據先前的組態、TLSv1.2或同時啟用TLSv1.1和TLSv1.2。

- "NetApp 密碼編譯安全模組（ NCSM ）"已通過 FIPS 140-2 第 1 級驗證、可提供軟體型法規遵循。

NIST 已提交 FIPS-140-3 標準、而 NCSM 將會進行 FIPS-140-2 和 FIPS-140-3 驗證。所有 FIPS 140-2 驗證將於 2026 年 9 月 21 日移至歷史狀態、這是新憑證提交的最後一天之後的五年。

啟用 **FIPS-140-2** 和 **FIPS-140-3** 法規遵循模式

從 ONTAP 9 開始、您可以針對叢集範圍的控制平面介面啟用 FIPS-140-2 和 FIPS-140-3 規範模式。

- "啟用 FIPS"
- "檢視 FIPS 狀態"

FIPS 啟用與通訊協定

此 `security config modify`命令可讓您修改現有的叢集範圍安全性組態。如果您啟用 FIPS 相容模式、叢集會自動僅選取 TLS 通訊協定。

- 使用此 `-supported-protocols` 參數可在 FIPS 模式之外、自行納入或排除 TLS 通訊協定。根據預設，FIPS 模式會停用，且會啟用 TLSv1.3 （從 ONTAP 9.11.1 開始）和 TLSv1.2 通訊協定。
- 先前的 ONTAP 版本預設啟用下列 TLS 通訊協定：
  - TLSv1.1 （從 ONTAP 9.12.1 開始預設為停用）
  - TLSv1 （從 ONTAP 9.8 開始預設為停用）
- 為了回溯相容性、 ONTAP 支援在停用 FIPS 模式時、將 SSLv3 新增至支援的通訊協定清單。

FIPS 啟用與加密

- 使用此 `-supported-cipher-suites` 參數僅設定進階加密標準（ AES ）或 AES 和 3DES 。
- 您可以透過指定來停用弱式密碼 `!RC4`、例如 RC4 。依預設，支援的密碼設定為 `ALL:!LOW:!aNULL:!EXP:!eNULL`。此設定表示所有支援的通訊協定加密套件都已啟用、但使用 64 位元或 56 位元加密演算法且不驗證、無加密、無匯出及低加密密碼套件的加密套件除外。
- 選取對應選取的傳輸協定所提供的加密套件。無效的組態可能會導致某些功能無法正常運作。
- 如需正確的加密字串語法、請參閱 "密碼頁面"開啟 OpenSSL （由 OpenSSL 軟體基礎所發佈）。從 ONTAP 9.9.1 及更新版本開始、您不再需要在修改安全性組態之後手動重新啟動所有節點。

SSH 和 **TLS** 安全強化

ONTAP 9 的 SSH 管理需要 OpenSSH 用戶端 5.7 或更新版本。SSH 用戶端必須與省略曲線數位簽章演算法（ ECDSA ）公開金鑰演算法交涉、才能成功連線。

若要強化 TLS 安全性、請僅啟用 TLS 1.2 、並使用能夠完全轉送機密（ PFS ）的加密套件。PFS 是一種金鑰交換方法、搭配 TLS 1.2 等加密通訊協定使用時、可協助防止攻擊者解密用戶端和伺服器之間的所有網路工作階段。

啟用支援 **TLSv1.2** 和 **PFS** 的加密套件

若要僅啟用 TLS 1.2 和 PFS 功能的加密套件、請使用 `security config modify`進階權限層級的命令。

> ⓘ 在變更 SSL 介面組態之前、請確定用戶端在連線至 ONTAP 時支援加密者 DHE 和 ECDHE 、以維持與 ONTAP 的連線。

範例

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

請針對每個提示進行確認 `y` 。如需 PFS 的詳細資訊，請參閱本 "NetApp部落格"。

相關資訊

"聯邦資訊處理標準（ FIPS ）出版 140"

建立 **CA** 簽署的數位憑證

對於許多組織而言、用於 ONTAP 網路存取的自我簽署數位憑證不符合其資訊安全原則。在正式作業系統上、安裝 CA 簽署的數位憑證以用於驗證叢集或 SVM 作為 SSL 伺服器、是 NetApp 的最佳做法。

您可以使用命令來產生憑證簽署要求（ CSR ）、並使用 `security certificate generate-csr` `security certificate install` 命令來安裝您從 CA 收到的憑證。

步驟

1. 若要建立由組織 CA 簽署的數位憑證、請執行下列步驟：
   a. 產生 CSR 。
   b. 請遵循貴組織的程序、使用組織 CA 的 CSR 申請數位憑證。例如、使用 Microsoft Active Directory 憑證服務 Web 介面、前往 `<CA_server_name>/certsrv` 並要求憑證。
   c. 在 ONTAP 中安裝數位憑證。

線上憑證狀態傳輸協定

線上憑證狀態傳輸協定（ OCSP ）可讓使用 TLS 通訊的 ONTAP 應用程式（例如 LDAP 或 TLS ）在啟用 OCSP 時接收數位憑證狀態。應用程式會收到簽署的回應、表示要求的憑證為「良好」、「已撤銷」或「未知」。

OCSP 可在不需要憑證撤銷清單（ CRL ）的情況下、判斷數位憑證的目前狀態。

根據預設、OCSP憑證狀態檢查會停用。您可以使用命令開啟 `security config ocsp enable -app` `name`**應用程式名稱**、 `autosupport` `audit_log`、 `fabricpool`、 `ems`、、、 `kmip` `ldap_ad` `ldap_nis_namemap`、或 `all`。此命令需要進階權限層級。

SSHv2 管理

此命令會 `security ssh modify` 以您指定的組態設定取代叢集或 SVM 的 SSH 金鑰交換演算法、加密演算法或 MAC 演算法的現有組態。

NetApp 建議：

- 使用密碼進行使用者工作階段。
- 使用公開金鑰存取機器。

支援的密碼與金鑰交換

密碼	金鑰交換
AES256-ctr	Diffie-Hellman-group-exchange — sha 256 （SHA-2）
aes192-ctr	Diffie-Hellman-group-exchange — sha 1 （SHA-1）
AES128/ctr	Diffie-Hellman-group14-sha （SHA-1）
AES256-CBC	Diffie-Hellman-group1-sha （SHA-1）
aes192-CBC	-
AES128/CBC	-
AES128/GCM	-
AES256-GCM	-
3DES-CBC	-

支援的 **AES** 和 **3DES** 對稱加密

ONTAP 也支援下列類型的 AES 和 3DES 對稱加密（也稱為加密）：

- HMAC-sha1
- HMAC-sha1-96
- HMAC-MD5
- HMAC-MD5-96
- HMAC-ripemd160
- umac-64
- umac-64
- umac-128
- HMAC-SHA2-256
- HMAC-SHA2-512
- HMAC-sha1-ETM
- HMAC-sha1-96-ETM
- HMAC-SHA2-256-ETM

- HMAC-SHA2-512-ETM
- HMAC-MD5-ETM
- HMAC-MD5-96-ETM
- HMAC-ripemd160-ETM
- umac-64/ETM
- umac-128/ETM

SSH 管理組態適用於 ONTAP 和平台 BMC 。

NetApp AutoSupport

ONTAP 的 AutoSupport 功能可讓您主動監控系統健全狀況、並自動傳送訊息和詳細資料給 NetApp 技術支援、貴組織的內部支援團隊或支援合作夥伴。根據預設、第一次設定儲存系統時、會啟用傳送給 NetApp 技術支援的 AutoSupport 訊息。此外、 AutoSupport 會在啟用後 24 小時、開始傳送訊息給 NetApp 技術支援。此 24 小時期間是可設定的。若要利用與組織內部支援團隊的通訊、必須完成郵件主機組態。

只有叢集管理員可以執行 AutoSupport 管理（組態）。SVM 管理員無法存取 AutoSupport 。可停用此功能。AutoSupport不過、 NetApp 建議您啟用此功能、因為如果儲存系統發生問題、 AutoSupport 有助於加速問題識別與解決。根據預設、即使您停用 AutoSupport 、系統仍會收集 AutoSupport 資訊並將其儲存在本機。

如需 AutoSupport 訊息的詳細資訊、包括各種訊息所包含的內容、以及傳送不同類型訊息的位置、請參閱 "NetApp 數位顧問" 文件。

AutoSupport 訊息包含敏感資料、包括但不限於下列項目：

- 記錄檔
- 與特定子系統相關的內容相關資料
- 組態與狀態資料
- 效能資料

AutoSupport 支援傳輸通訊協定的 HTTPS 和 SMTP 。由於資訊內容敏感、NetApp強烈建議使用HTTPS作為預設傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸協定、以將資訊傳送給NetApp支援部門。AutoSupport AutoSupport

此外、您應該運用 `system node autosupport modify` 命令來指定 AutoSupport 資料的目標（例如 NetApp 技術支援、組織內部營運或合作夥伴）。此命令也可讓您指定要傳送的特定 AutoSupport 詳細資料（例如效能資料、記錄檔等）。

若要完全停用 AutoSupport 、請使用 `system node autosupport modify -state disable` 命令。

網路時間傳輸協定

雖然 ONTAP 可讓您手動設定叢集上的時區、日期和時間、但您必須設定網路時間傳輸協定（ NTP ）伺服器、使叢集時間至少與三個外部 NTP 伺服器同步。

當叢集時間不準確時、可能會發生問題。雖然 ONTAP 可讓您手動設定叢集上的時區、日期和時間、但您必須設

定網路時間傳輸協定（ NTP ）伺服器、使叢集時間與外部 NTP 伺服器同步。

從使用S25 9.5開始ONTAP 、您可以使用對稱驗證來設定NTP伺服器。

您最多可以使用命令建立 10 個外部 NTP 伺服器的關聯 `cluster time-service ntp server create` 。為了提供備援和時間服務品質、您應將至少三部外部NTP伺服器與叢集建立關聯。

如需 ONTAP 中 NTP 組態的詳細資訊、請參閱 "管理叢集時間（僅限叢集管理員）"。

NAS 檔案系統本機帳戶（ CIFS 工作群組）

工作群組用戶端驗證可為 ONTAP 解決方案提供額外的安全層級、且與傳統的網域驗證狀態一致。使用 `vserver cifs session show` 命令可顯示許多與狀態相關的詳細資料、包括 IP 資訊、驗證機制、傳輸協定版本和驗證類型。

從 ONTAP 9 開始、您可以在具有 CIFS 用戶端的工作群組中、使用本機定義的使用者和群組來驗證伺服器的 CIFS 伺服器。工作群組用戶端驗證可為 ONTAP 解決方案提供額外的安全層級、且與傳統的網域驗證狀態一致。若要設定 CIFS 伺服器、請使用 `vserver cifs create` 命令。建立 CIFS 伺服器之後、您可以將其加入 CIFS 網域、或加入工作群組。若要加入工作群組、請使用 `-workgroup` 參數。以下是組態範例：

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

工作群組模式中的 CIFS 伺服器僅支援 Windows NT LAN Manager （ NTLM ）驗證、不支援 Kerberos 驗證。

NetApp 建議將 NTLM 驗證功能搭配 CIFS 工作群組使用、以維持組織的安全狀態。為了驗證 CIFS 安全狀態、NetApp 建議使用 `vserver cifs session show` 命令來顯示許多與狀態相關的詳細資料、包括 IP 資訊、驗證機制、傳輸協定版本和驗證類型。

NAS 檔案系統稽核

NAS 檔案系統在現今的威脅環境中佔用更多資源、因此稽核功能對於支援可見度至關重要。

安全需要驗證。ONTAP 提供更全面的解決方案稽核事件和詳細資訊。由於 NAS 文件系統在當今的威脅情勢中佔據越來越大的地位，因此審計功能對於提升可見度至關重要。由於 ONTAP 的審計功能改進，CIFS 審計詳細資訊比以往任何時候都更加豐富。關鍵詳細資訊（包括以下內容）會隨建立的事件一起記錄：

- 檔案、資料夾及共用存取
- 建立、修改或刪除的檔案
- 成功的檔案讀取存取
- 嘗試讀取或寫入檔案失敗
- 資料夾權限變更

建立稽核組態

您必須啟用 CIFS 稽核、才能產生稽核事件。使用 `vserver audit create` 命令建立稽核組態。根據預設、稽核記錄會根據大小使用旋轉方法。如果在「旋轉參數」欄位中指定、您可以使用時間型旋轉選項。其他記錄稽核輪調組態詳細資料包括輪調排程、輪調限制、一週的輪調天數、以及輪調大小。下列文字提供範例組態，描述稽核組態，使用每月的時間輪換，排定在每週的所有日期 12 ： 30 進行。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

CIFS 稽核事件

CIFS 稽核事件如下：

- * 檔案共用 * ：使用相關命令新增、修改或刪除 CIFS 網路共用時、會產生稽核事件 `vserver cifs share` 。
- * 稽核原則變更 * ：使用相關命令停用、啟用或修改稽核原則時，會產生稽核事件 `vserver audit` 。
- * 使用者帳戶 * ：建立或刪除本機 CIFS 或 UNIX 使用者時、會產生稽核事件；啟用、停用或修改本機使用者帳戶；或重設或變更密碼。此事件使用 `vserver cifs users-and-groups local-group` 命令或相關 `vserver services name-service unix-user` 命令。
- * 安全性群組 * ：使用命令或相關命令建立或刪除本機 CIFS 或 UNIX 安全性群組時、會產生稽核事件 `vserver cifs users-and-groups local-group` `vserver services name-service unix-group` 。
- * 授權原則變更 * ：使用命令授與或撤銷 CIFS 使用者或 CIFS 群組的權限時、會產生稽核事件 `vserver cifs users-and-groups privilege` 。

這項功能是以系統稽核功能為基礎、可讓系統管理員從資料使用者的角度來檢閱系統允許和執行的項目。

REST API 對 **NAS** 稽核的影響

ONTAP 包括管理員帳戶使用 REST API 存取及操作 SMB/CIFS 或 NFS 檔案的能力。雖然 REST API 只能由 ONTAP 管理員執行、 REST API 命令卻會略過系統 NAS 稽核記錄。此外、 ONTAP 系統管理員也可以在使用 REST API 時略過檔案權限。不過、系統命令記錄檔會擷取系統管理員對檔案執行 REST API 的動作。

建立無存取權限 **REST API** 角色

您可以建立無法透過 REST 存取 ONTAP 磁碟區的 REST API 角色、以防止 ONTAP 管理員使用 REST API 進行檔案存取。若要配置此角色、請完成下列步驟。

/api/storage/volumes REST API 的用途不僅限於檔案存取。System Manager 和其他圖形使用者介面也使用它來建立、檢視和修改磁碟區。

步驟

1. 建立新的 REST 角色、此角色無法存取儲存磁碟區、但具有所有其他 REST API 存取權。

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. 將系統管理員帳戶指派給您在上一個步驟中建立的新 REST API 角色。

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

如果您想阻止內置 ONTAP 羣集管理員帳戶使用 REST API 進行文件訪問，則需要先 "建立新的系統管理員帳戶、並停用或刪除內建帳戶"執行。

設定並啟用 **CIFS SMB** 簽署與封裝

您可以設定及啟用 SMB 簽署、以確保儲存系統與用戶端之間的流量不會受到重播或攔截式攻擊的影響、進而保護資料架構的安全性。SMB 簽署可驗證 SMB 訊息是否具有有效的簽章、以保護其安全。

關於這項工作

檔案系統和架構的常見威脅模式、在於 SMB 傳輸協定。為了解決這個問題、 ONTAP 9 解決方案採用業界標準的 SMB 簽署與密封。SMB 簽署可確保儲存系統與用戶端之間的流量不會因為重播或攔截式攻擊而受到影響、進而保護資料架構的安全性。驗證 SMB 訊息是否有有效的簽章、即可完成此作業。

雖然 SMB 簽署依預設為停用、以提高效能、但 NetApp 強烈建議您啟用此功能。此外、 ONTAP 解決方案支援 SMB 加密、也稱為密封。這種方法可讓資料以每個共享區的方式安全傳輸。預設會停用SMB加密。不過、 NetApp 建議您啟用 SMB 加密。

現在 SMB 2.0 及更新版本均支援 LDAP 簽署和封裝。簽署（防止竄改）和密封（加密）可在 SVM 和 Active Directory 伺服器之間實現安全通訊。SMB 3.0 及更新版本均支援加速 AES 新指令（ Intel AES NI ）加密。Intel AES NI 可改善 AES 演算法、並透過支援的處理器系列來加速資料加密。

步驟

1. 若要設定及啟用 SMB 簽署，請使用 `vserver cifs security modify` 命令並確認 `-is-signing-required` 參數已設定為 `true`。請參閱下列組態範例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. 若要設定及啟用 SMB 密封與加密，請使用 `vserver cifs security modify` 命令並確認 `-is-smb-encryption-required` 參數已設定為 `true`。請參閱下列組態範例：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

NFS 安全性

匯出規則是匯出原則的功能要素。匯出規則會根據您設定的特定參數、比對磁碟區的用戶端存取要求、以決定如何處理用戶端存取要求。匯出原則必須包含至少一個匯出規則、才能允許存取用戶端。如果匯出原則包含多個規則、則會依照規則在匯出原則中的顯示順序來處理這些規則。

存取控制是維持安全狀態的核心。因此、 ONTAP 使用匯出原則功能、將 NFS Volume 存取限制在符合特定參數的用戶端。匯出原則包含一或多個匯出規則、可處理每個用戶端存取要求。匯出原則會與每個磁碟區相關聯、以設定用戶端對磁碟區的存取。此程序的結果會決定是否授予或拒絕用戶端（使用拒絕權限的訊息）對磁碟區的存取權。此程序也會決定提供給磁碟區的存取層級。

> 具有匯出規則的匯出原則必須存在於 SVM 上、用戶端才能存取資料。SVM 可以包含多個匯出原則。

規則順序由規則索引編號決定。如果規則符合用戶端、則會使用該規則的權限、而不會處理其他規則。如果沒有符合的規則、用戶端就會被拒絕存取。

匯出規則會套用下列準則來決定用戶端存取權限：

- 傳送要求的用戶端所使用的檔案存取傳輸協定（例如 NFSv4 或 SMB ）
- 用戶端識別碼（例如主機名稱或 IP 位址）
- 用戶端用來驗證的安全性類型（例如 Kerberos v5 、 NTLM 或 AUTH_SYS ）

如果規則指定多個準則、且用戶端不符合其中一或多個準則、則規則將不適用。

匯出原則範例包含具有下列參數的匯出規則：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

安全性類型決定用戶端接收的存取層級。這三種存取層級分別為唯讀、讀寫及超級使用者（適用於具有使用者 ID 的用戶端 0）。由於會依此順序評估由安全性類型所決定的存取層級、因此您必須遵守列出的規則：

匯出規則中存取層級參數的規則

讓用戶端取得下列存取層級	這些存取參數必須符合用戶端的安全性類型
一般使用者唯讀	唯讀(`-rorule`)
一般使用者讀寫	只讀(`-rorule`）和讀寫(`-rwrule`（ read — write ）
超級使用者唯讀	唯讀(`-rorule`）和 `-superuser`
超級使用者讀寫	只讀(`-rorule`）(`-rwrule`和讀寫） `-superuser`

以下是這三種存取參數的有效安全類型：

- 任何
- 無
- 永不

這些安全性類型不適用於 `-superuser` 下列參數：

- krb5
- NTLM
- 系統

存取參數結果規則

如果用戶端的安全類型 ...	然後 ...
符合存取參數中指定的安全性類型。	用戶端會以自己的使用者 ID 接收該層級的存取權。
與指定的安全類型不匹配，但訪問參數包括選項 `none`。	用戶端會接收該層級的存取權、並接收使用參數所指定之使用者 ID 的匿名使用者 `-anon` 。
與指定的安全類型不匹配，訪問參數不包括選項 `none`。	用戶端無法接收該層級的任何存取權。 此限制不適用於 `-superuser` 參數、因為即使未指定、此參數也一律包含無。

Kerberos 5 和 **Krb5p**

從 ONTAP 9 開始、支援使用隱私權服務（ krb5p ）進行 Kerberos 5 驗證。krbp5 驗證模式是安全的、使用校驗和來加密用戶端和伺服器之間的所有流量、可防止資料竄改和窺探。ONTAP 解決方案支援 Kerberos 的 128 位元和 256 位元 AES 加密。隱私權服務包括驗證所接收資料的完整性、驗證使用者、以及在傳輸前加密資料。

krb5p 選項最常出現在匯出原則功能中、其設定為加密選項。krb5p 驗證方法可用作驗證參數、如下列範例所示：

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

啟用輕量型目錄存取傳輸協定簽署與密封

支援簽署和封裝、以在查詢 LDAP 伺服器時提供工作階段安全性。此方法可替代 LDAP over TLS 工作階段安全性。

簽署可確認使用秘密金鑰技術的 LDAP 有效負載資料完整性。「密封」會加密LDAP有效負載資料、以避免以純文字傳輸敏感資訊。SVM 上的工作階段安全性設定對應於 LDAP 伺服器上可用的設定。依預設、 LDAP 簽署和密封會停用。

步驟

1. 若要啟用此功能、請使用參數執行 `vserver cifs security modify` 命令 `session-security-for-ad-ldap` 。

   LDAP 安全功能選項：

   - * 無 * ：預設、無簽署或密封
   - * 簽署 * ：簽署 LDAP 流量
   - * 認證標章 * ：簽署及加密 LDAP 流量

   > ⓘ 符號和認證標章參數是累積的、表示如果使用簽署選項、結果是 LDAP 加上簽署。不過、如果使用密封選項、結果會同時是簽署和密封。此外、如果未指定此命令的參數、則預設值為無。

   以下是組態範例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

建立及使用 **NetApp FPolicy**

您可以建立及使用 FPolicy 、這是 ONTAP 解決方案的基礎架構元件、可讓合作夥伴應用程式監控及設定檔案存取權限。其中一個功能更強大的應用程式是儲存工作負載安全、這是 NetApp SaaS 應用程式、可在混合雲環境中集中可見度及控制所有企業資料存取、確保安全性與法規遵循目標得以達成。

存取控制是一項重要的安全概念。可見度和回應檔案存取和檔案作業的能力、對於維持您的安全狀態至關重要。為了提供檔案的可見度和存取控制、 ONTAP 解決方案使用 NetApp FPolicy 功能。

檔案原則可以根據檔案類型來設定。FPolicy 決定儲存系統如何處理個別用戶端系統的要求、以執行建立、開啟、重新命名及刪除等作業。從 ONTAP 9 開始、 FPolicy 檔案存取通知架構就會透過篩選控制和恢復功能來增

強、以避免短暫的網路中斷。

步驟

1. 若要使用 FPolicy 功能、您必須先使用命令建立 FPolicy 原則 `vserver fpolicy policy create` 。

   此外、如果您使用 FPolicy 來查看和收集事件、請使用此 `-events` 參數。ONTAP 提供的額外精細度可讓您篩選及存取控制的使用者名稱層級。若要使用使用者名稱來控制權限和存取、請指定 `-privilege-user-name` 參數。

   下列文字提供 FPolicy 建立範例：

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. 建立 FPolicy 原則之後、您必須使用命令加以啟用 `vserver fpolicy enable` 。此命令也會設定 FPolicy 項目的優先順序或順序。

   FPolicy 順序很重要、因為如果多個原則已訂閱相同的檔案存取事件、則順序會指示存取的授與或拒絕順序。

   下列文字提供啟用 FPolicy 原則和使用命令驗證組態的範例組態 `vserver fpolicy show` ：

   ```
   cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
   vs2_pol -sequence-number 5

   cluster1::> vserver fpolicy show
   Vserver                 Policy Name                     Sequence  Status
   Engine
   ----------------------- ------------------------------ --------  -------
   -------
   vs1.example.com         vs1_pol
   vs2.example.com         vs2_pol
    external
   2 entries were displayed.
   ```

FPolicy 增強功能

ONTAP 9 包括以下各節所述的 FPolicy 增強功能。

篩選控制項

新的篩選器可用於 `SetAttr` 和移除目錄活動的通知。

如果以非同步模式運作的FPolicy伺服器發生網路中斷、則中斷期間產生的FPolicy通知會儲存在儲存節點上。當FPolicy伺服器重新連線時、系統會警示已儲存的通知、並從儲存節點擷取通知。在停機期間可儲存通知的時間長度可設定為10分鐘。

ONTAP 中 LIF 角色的安全特性

LIF 是 IP 位址或全球連接埠名稱（ WWPN ）、具有相關特性、例如角色、主連接埠、主節點、容錯移轉至的連接埠清單、以及防火牆原則。您可以在叢集透過網路傳送和接收通訊的連接埠上設定LIF。瞭解每個 LIF 角色的安全性特性非常重要。

LIF 角色

LIF 角色可以是：

- * Data LIF* ：與 SVM 相關的 LIF 、用於與用戶端通訊。
- * 叢集 LIF* ： LIF 用於在叢集中的節點之間傳輸叢集內的流量。
- * 節點管理 LIF* ：提供專用 IP 位址的 LIF 、用於管理叢集中的特定節點。
- * 叢集管理 LIF* ：為整個叢集提供單一管理介面的 LIF 。
- * 叢集間 LIF* ：用於跨叢集通訊、備份及複寫的 LIF 。

每個 LIF 角色的安全特性

	Data LIF	叢集 LIF	節點管理 LIF	叢集管理LIF	叢集間 LIF
需要私有 IP 子網路？	否	是的	否	否	否
需要安全的網路？	否	是的	否	否	是的
預設防火牆原則	非常嚴格	完全開放	中	中	非常嚴格
防火牆是否可自訂？	是的	否	是的	是的	是的

- 由於叢集 LIF 完全開啟、而且沒有可設定的防火牆原則、因此它必須位於安全隔離網路上的私有 IP 子網路上。
- LIF 角色絕不應暴露在網際網路上。

要了解有關保護 LIF 的更多信息，請參閱 "設定lifs的防火牆原則"。本頁面也提供了從ONTAP 9.10.1 開始的 LIF 服務策略的詳細資訊。

要了解有關如何建立新服務策略的更多信息，請參閱 `network interface service-policy create` 命令 "命令參考。"

傳輸協定與連接埠安全性

除了執行隨裝即用的安全作業和功能外、解決方案的強化還必須包括隨裝即用的安全機制。利用其他基礎架構裝置（例如防火牆、入侵防禦系統（ IPS ）和其他安全裝置）來篩選和限制對 ONTAP 的存取、是建立和維持嚴苛安全狀態的有效方法。此資訊是篩選及限

制環境及其資源存取的關鍵元件。

常用的通訊協定和連接埠

服務	連接埠/傳輸協定	說明
SSH	22/TCP	SSH 登入
telnet	23/TCP	遠端登入
Domain	53/TCP	網域名稱伺服器
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	遠端程序呼叫
NTP	123/UDP	網路時間傳輸協定
msrpc	135/TCP	Microsoft 遠端程序呼叫
Netbios-name	137/TCP 137/UDP	NetBios 名稱服務
netbios-ssn	139/TCP	NetBios 服務工作階段
SNMP	161/UDP	SNMP
HTTPS	443/TCP	安全連結： http
microsoft-ds	445/TCP	Microsoft 目錄服務
IPsec	500/UDP	網際網路傳輸協定安全性
mount	635/UDP	NFS 掛載
named	953/UDP	名稱精靈
NFS	2049/UDP 2049/TCP	NFS 伺服器精靈
nrv	2050/TCP	NetApp 遠端 Volume 傳輸協定
iscsi	3260/TCP	iSCSI目標連接埠
Lockd	4045/TCP 4045/UDP	NFS 鎖定精靈
NFS	4046/TCP	NFS mountd 傳輸協定
acp-proto	4046/UDP	會計傳輸協定
rquotad	4049/UDP	NFS rquotad 傳輸協定
krb524	4444/UDP	Kerberos 524.
IPsec	4500/UDP	網際網路傳輸協定安全性
acp	5125/UDP 5133/UDP 544/TCP	磁碟的替代控制連接埠

服務	連接埠/傳輸協定	說明
Mdns	5353/UDP	多點傳送DNS
HTTPS	5986/UDP	HTTPS 連接埠：正在接聽二進位傳輸協定
TELNET	8023/TCP	節點範圍 Telnet
HTTPS	8443/TCP	7MTT GUI 工具、透過連結： HTTPS
RSH	8514/TCP	節點範圍 RSH
KMIP	9877/TCP	KMIP 用戶端連接埠（僅限內部本機主機）
ndmp	10000/TCP	NDMP
cifs 見證連接埠	40001/TCP	CIFS 見證連接埠
TLS	50000/TCP	傳輸層安全性
Iscsi	65200/TCP	iSCSI 連接埠
SSH	65502/TCP	安全Shell
vsun	65503/TCP	Vsun

NetApp 內部連接埠

連接埠/傳輸協定	說明
900	NetApp 叢集 RPC
902	NetApp 叢集 RPC
904	NetApp 叢集 RPC
905	NetApp 叢集 RPC
910	NetApp 叢集 RPC
911	NetApp 叢集 RPC
913	NetApp 叢集 RPC
914	NetApp 叢集 RPC
915	NetApp 叢集 RPC
918	NetApp 叢集 RPC
920	NetApp 叢集 RPC
921	NetApp 叢集 RPC
924	NetApp 叢集 RPC
925	NetApp 叢集 RPC
927	NetApp 叢集 RPC
928	NetApp 叢集 RPC
929	NetApp 叢集 RPC
931	NetApp 叢集 RPC

連接埠/傳輸協定	說明
932	NetApp 叢集 RPC
933	NetApp 叢集 RPC
934	NetApp 叢集 RPC
935	NetApp 叢集 RPC
936	NetApp 叢集 RPC
937	NetApp 叢集 RPC
939	NetApp 叢集 RPC
940	NetApp 叢集 RPC
951	NetApp 叢集 RPC
954	NetApp 叢集 RPC
955	NetApp 叢集 RPC
956	NetApp 叢集 RPC
958	NetApp 叢集 RPC
961	NetApp 叢集 RPC
963	NetApp 叢集 RPC
964	NetApp 叢集 RPC
966	NetApp 叢集 RPC
967	NetApp 叢集 RPC
7810	NetApp 叢集 RPC
7811	NetApp 叢集 RPC
7812	NetApp 叢集 RPC
7813	NetApp 叢集 RPC
7814	NetApp 叢集 RPC
7815	NetApp 叢集 RPC
7816	NetApp 叢集 RPC
7817	NetApp 叢集 RPC
7818	NetApp 叢集 RPC
7819	NetApp 叢集 RPC
7820	NetApp 叢集 RPC
7821	NetApp 叢集 RPC
7822	NetApp 叢集 RPC
7823	NetApp 叢集 RPC
7824	NetApp 叢集 RPC

ONTAP SnapCenter 技術報告

SnapCenter 提供統一化的平台、可實現應用程式一致的資料保護與複製管理。SnapCenter 透過應用程式整合式工作流程、簡化備份、還原及複製生命週期管理。SnapCenter 運用儲存型資料管理功能、可提升效能與可用度、並縮短測試與開發時間。

這些技術報告會針對產品文件進行擴充"SnapCenter"。

SnapCenter for Oracle

"TR-4700 ：適用於 Oracle 資料庫的 SnapCenter 外掛程式最佳實務做法"
NetApp SnapCenter 是一套統一且可擴充的平台、可提供 Oracle 一致的資料保護功能、透過集中化的控制與監督功能、將複雜的作業自動化。瞭解使用 SnapCenter 部署 Oracle 資料庫的建議實務做法。

"TR-4964 ：使用 SnapCenter 服務備份、還原及複製 Oracle 資料庫"瞭解如何設定 SnapCenter 服務來備份，還原及複製部署至 Amazon FSX 的 Oracle 資料庫，以供 ONTAP 儲存設備和 EC2 運算執行個體使用。SnapCenter 服務雖然設定和使用容易得多、但透過 SnapCenter 介面提供主要功能。

SnapCenter for Microsoft SQL Server

"TR-4714 ：使用 NetApp SnapCenter 的 Microsoft SQL Server 最佳實務做法"
瞭解如何使用 SnapCenter 在 NetApp 儲存設備上成功部署 Microsoft SQL Server 以保護資料。

SnapCenter for Microsoft Exchange Server

"TR-4681 ：使用 NetApp SnapCenter 的 Microsoft Exchange Server 最佳實務做法"
瞭解如何使用 SnapCenter 在 NetApp 儲存設備上成功部署 Microsoft Exchange Server 以保護資料。

SnapCenter for SAP HANA

"TR-4614：SAP HANA備份與還原SnapCenter 功能搭配使用"SnapCenter 是一個統一且可擴充的平台，可為 SAP HANA 及其他資料庫提供應用程式一致的資料保護。支援集中控制和監督、同時委派使用者管理應用程式專屬的備份、還原和複製工作的能力。SnapCenter藉助SnapCenter 於功能強大的功能、資料庫和儲存管理員只需學習單一工具、即可管理各種應用程式和資料庫的備份、還原和複製作業。

"TR-4926：適用於NetApp ONTAP 的Amazon FSX上的SAP HANA - SnapCenter 利用NetApp進行備份與還原"
瞭解 Amazon FSX for NetApp ONTAP 和 SnapCenter 上的 SAP HANA 資料保護建議實務做法。主題包括 SnapCenter 概念、組態建議和作業工作流程、包括組態、備份作業、 以及還原與還原作業。

"TR-4667 ：利用 SnapCenter 將 SAP HANA 系統複製與複製作業自動化"SnapCenter 儲存複製和靈活定義複製前和複製後作業的選項，可讓 SAP 基礎管理員加速和自動化 SAP 系統複製，複製或重新整理作業。立即瞭解在任何主要或次要儲存設備上選擇任何 SnapCenter Snapshot 備份的選項、可讓您解決最重要的使用案例、包括邏輯毀損、災難恢復測試或 SAP QA 系統的重新整理。

"TR-4719 ： SAP HANA 系統複寫備份與還原、採用 SnapCenter 技術"
瞭解 SnapCenter 技術和 SAP HANA 外掛程式如何在 SAP HANA 系統複製環境中用於備份與還原。

"TR-4667 ：利用 SnapCenter 將 SAP HANA 系統複製與複製作業自動化"在儲存層上建立應用程式一致的 NetApp Snapshot 備份，是系統複本和系統複製作業的基礎。儲存型Snapshot備份是使用SnapCenter 適用於SAP HANA的NetApp還原外掛程式和SAP HANA資料庫提供的介面來建立。此功能可在SAP HANA備份目錄中登錄Snapshot備份、以便將備份用於還原與還原、以及複製作業。SnapCenter

SnapCenter 強化指南

"TR-4957 ： NetApp SnapCenter 安全強化指南"
瞭解如何設定 SnapCenter 、以協助組織達成資訊系統機密性、完整性和可用度等規定的安全目標。

ONTAP 分層技術報告

有了 FabricPool 資料分層解決方案、企業的 Flash 系統整體使用者體驗就能改善、同時避免重新架構應用程式以提高儲存效率的難題。FabricPool 可減少系統環境的儲存佔用空間及相關成本。作用中資料仍保留在高效能 SSD 上。非使用中資料會分層化為低成本物件儲存、同時保留儲存效率。

這些技術報告會針對產品文件進行擴充"ONTAP FabricPool"。

"TR-4598：FabricPool 最佳實務做法"
瞭解 FabricPool 的功能、需求、實作及建議實務做法。

"TR-4826 ： NetApp FabricPool with StorageGRID 推薦指南"
瞭解部署 StorageGRID 並將其調整為 ONTAP 元件 FabricPool 容量層的建議實務做法。本文件也涵蓋使用 StorageGRID 時的核心功能、需求、實作及建議實務做法。

"TR-4695 ：使用 NetApp FabricPool 進行資料庫儲存分層"
瞭解 FabricPool 的優點和組態選項、包括 Oracle 關聯式資料庫管理系統（ RDBMS ）。

ONTAP 虛擬化技術報告

NetApp 虛擬化解決方案可協助您從伺服器獲得最大價值。有了以突破性的高效能 ONTAP Flash 系統為基礎的回應性虛擬伺服器基礎架構、您就能更快存取資料。精細的虛擬基礎架構可在不中斷多 PB 資料的情況下進行擴充、提供您共享存取多個工作負載所需的效能。ONTAP 透過關鍵合作夥伴關係、部署指南、應用程式整合及優異設計、協助簡化及降低虛擬伺服器基礎架構部署的複雜度。ONTAP 針對內部部署和雲端環境的健全虛擬化環境、提供許多建議的實務做法和解決方案。

這些技術報告會針對產品文件進行擴充"VMware vSphere適用的工具ONTAP"。

"TR-4597：VMware vSphere ONTAP for VMware"ONTAP 在將近 20 年來一直是 VMware vSphere 環境的領先儲存解決方案，並持續新增創新功能來簡化管理，同時降低成本。本文件介紹適用於 vSphere 的 ONTAP 解決方案、包括最新的產品資訊和建議實務做法、以簡化部署、降低風險並簡化管理。

"TR-4400 ：採用 NetApp ONTAP 的 VMware vSphere 虛擬磁碟區（ vVols ）"ONTAP 在過去二十多年來一直是 VMware vSphere 環境的領先儲存解決方案，並持續新增創新功能來簡化管理，同時降低成本。本文件涵蓋適用於 VMware vSphere 虛擬磁碟區（ VVols ）的 ONTAP 功能、包括最新的產品資訊和使用案例、以及建議的實務做法和其他資訊、可簡化部署並減少錯誤。

"TR-4900 ： VMware Site Recovery Manager 與 NetApp ONTAP" ONTAP 自 2002 年引進現代化資料中心以來、一直是 VMware vSphere 環境的領先儲存解決方案、並持續新增創新功能、以簡化管理、同時降低成本。本文件將介紹 VMware 領先業界的災難恢復（ DR ）軟體 VMware Site Recovery Manager （ SRM ） ONTAP 解決方案、包括最新產品資訊和建議實務做法、以簡化部署、降低風險並簡化後續管理。

"介紹自動化功能以利ONTAP 實現VMware及vSphere"自 VMware ESX 第一天開始，自動化是管理 VMware 環境不可或缺的一環。能夠以程式碼形式部署基礎架構、並將實務做法延伸至私有雲端作業、有助於減輕對擴充性、靈活度、自我配置及效率的顧慮。本文件介紹自動化 ONTAP 和 VMware vSphere 環境的 ONTAP 解決方案。

"WP-7353 ：適用於 VMware vSphere 的 ONTAP 工具 - 產品安全性"本文件說明保護 ONTAP 工具的技術與技術，以保護 VMware vSphere 9.X 免受產品環境中現有和新興威脅的影響。

"WP-7355 ： SnapCenter 外掛程式 VMware vSphere - 產品安全性"本文件說明用於保護 NetApp SnapCenter Plug-in for VMware vSphere 4.X 免受產品環境中現有和新興威脅的技術與技術。

"TR-4568 ：適用於 Windows Server 的 NetApp 部署準則和儲存最佳實務做法"Microsoft Windows Server 是企業級作業系統，涵蓋網路，安全性，虛擬化，雲端，虛擬桌面基礎架構，存取保護，資訊保護， Web 服務，應用程式平台基礎架構等。本文件著重於 Microsoft Windows 、特別著重於 Hyper-V 虛擬化技術、包括最新產品資訊和建議實務做法、以簡化部署、降低風險及簡化管理。

法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

版權

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp 、 Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

"https://www.netapp.com/company/legal/trademarks/"

專利

如需最新的 NetApp 擁有專利清單、請參閱：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隱私權政策

"https://www.netapp.com/company/legal/privacy-policy/"

開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

ONTAP

"ONTAP 9.16.1 注意事項" "ONTAP 9.16.0 注意事項" "ONTAP 9.15.1 注意事項" "ONTAP 9.15.0 注意事項" "ONTAP 9.14.1 注意事項" "ONTAP 9.14.0 注意事項" "ONTAP 9.13.1 注意事項" "關於此功能的注意事項ONTAP 9.12.1.1" "關於此功能的注意事項ONTAP 9.12.0" "ONTAP 9.11.1 注意事項" "關於本產品的注意事項ONTAP 9.10.1" "ONTAP 9.10.0 注意事項" "關於此功能的注意事項ONTAP" "關於本產品的注意事項ONTAP 9.8" "關於產品的注意ONTAP 事項9.7" "關於此功能的注意事項ONTAP" "關於本產品的注意事項ONTAP" "關於產品的注意事項ONTAP 9.4" "關於本產品的注意事項ONTAP" "關於此功能的注意事項ONTAP 9.2" "關於此產品的注意事項ONTAP"

適用於 **MetroCluster IP** 組態的 **ONTAP Mediator**

"9.9.1 MetroCluster IP 組態的 ONTAP Mediator 注意事項" "9.8 適用於 MetroCluster IP 組態的 ONTAP Mediator 注意事項" "9.7 適用於 MetroCluster IP 組態的 ONTAP Mediator 注意事項"