安全性

ONTAP Technical Reports

NetApp
January 23, 2026

目錄

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。

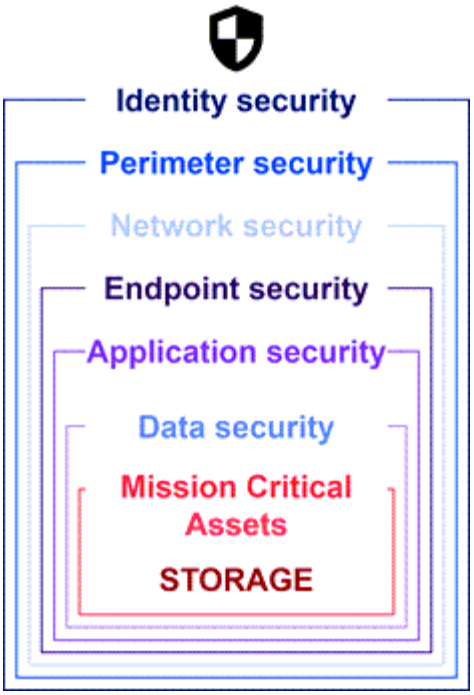
組織必須從周邊、網路、身分識別、應用程式、以及資料位於儲存層級的位置、查看整個安全狀態、並保護這些層級的安全。在現今的威脅環境中、在儲存層採用以資料為中心的網路保護方法是至關重要的。雖然沒有任何單一解決方案能阻擋所有攻擊、但使用包括合作夥伴關係和第三方在內的解決方案組合、可提供分層防禦。

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。

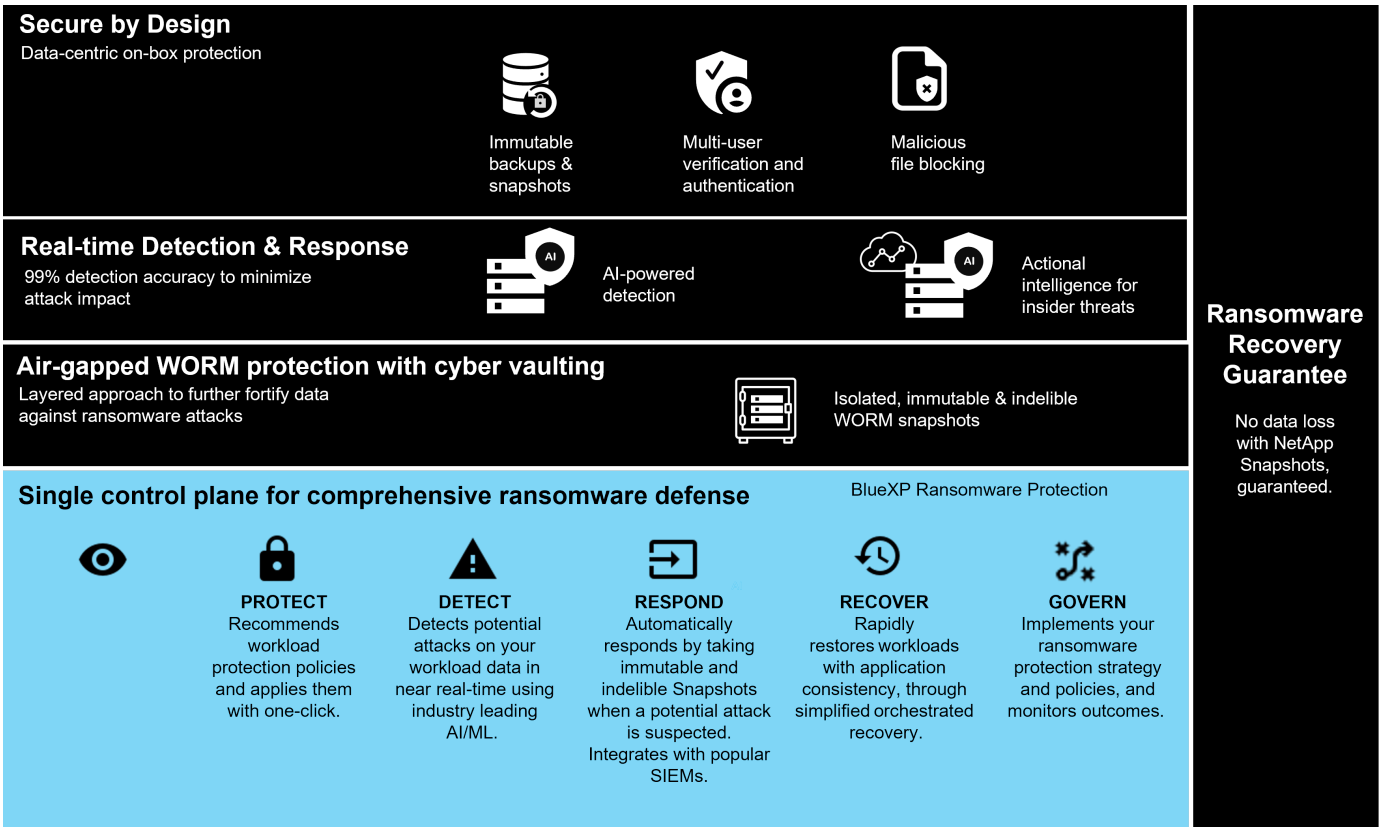
資料層的勒索軟體保護

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"

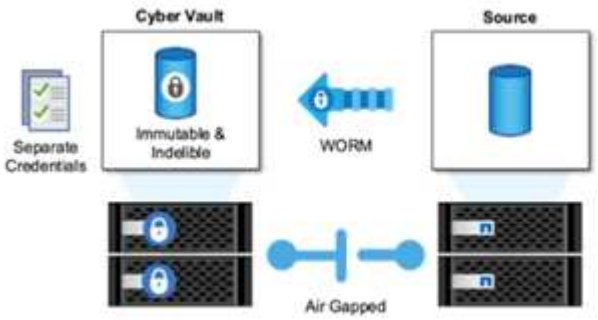
在 **ONTAP** 中使用網路資料傳輸技術，提供空中綁帶式 **WORM** 保護

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。

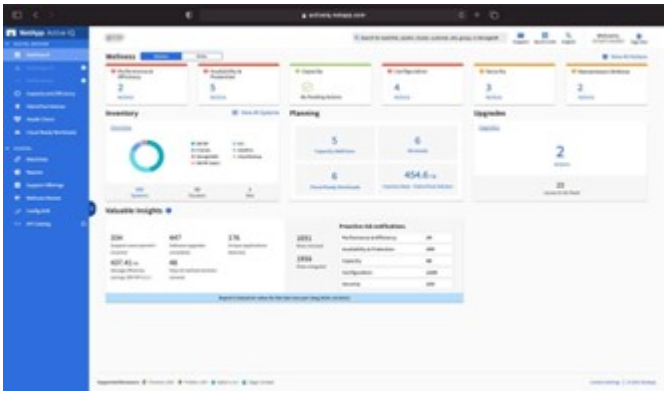
深入瞭解

- "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。

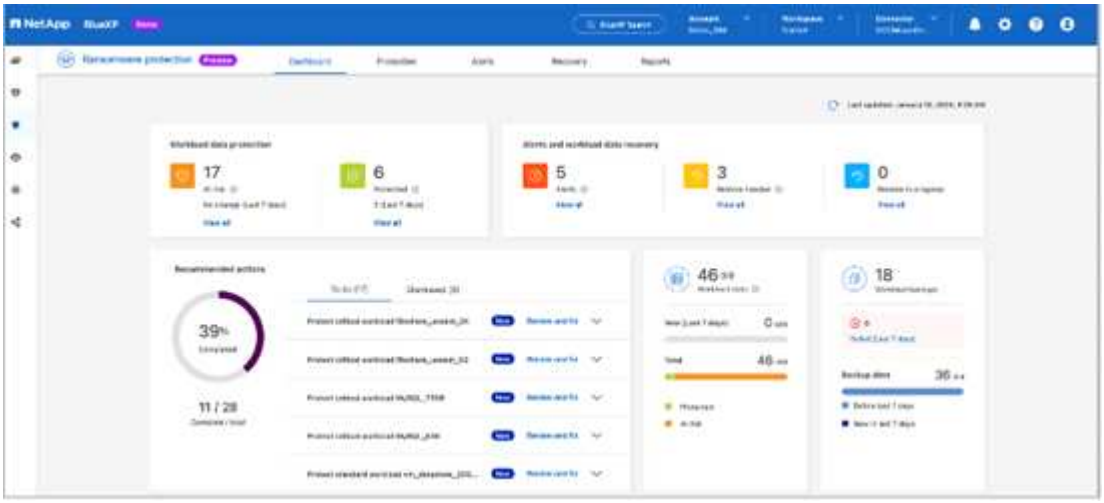
若要查看勒索軟體的保護措施，請參閱"數位顧問"。

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 。

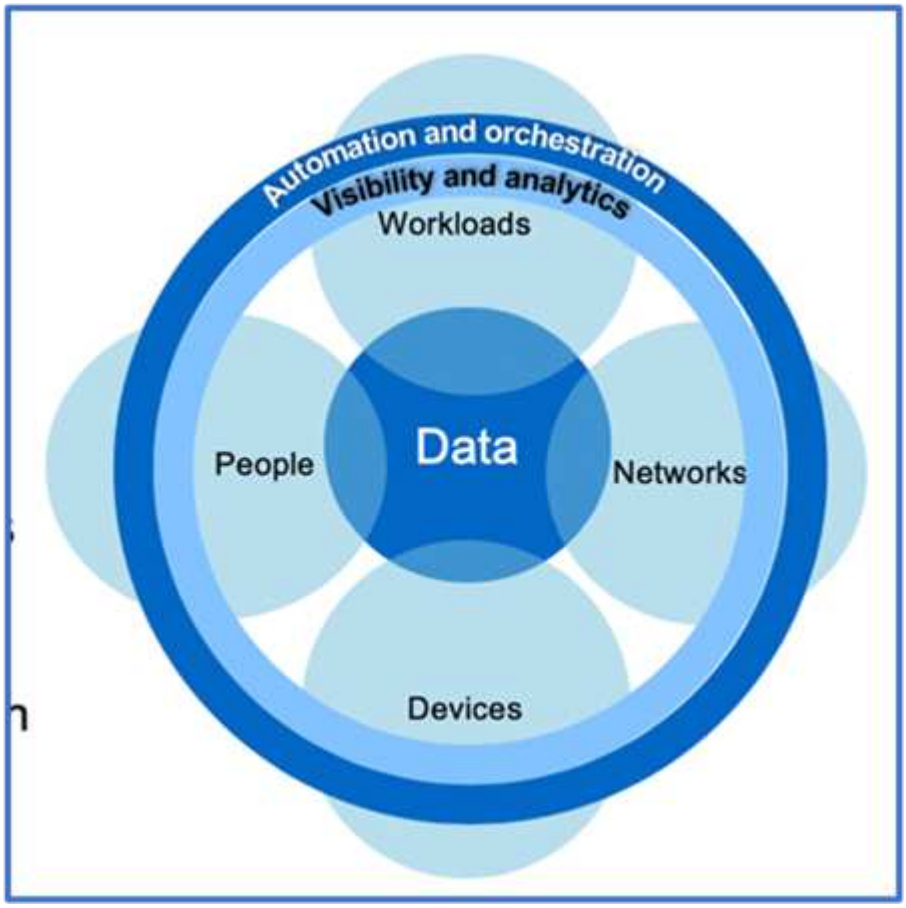
安全資源

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。

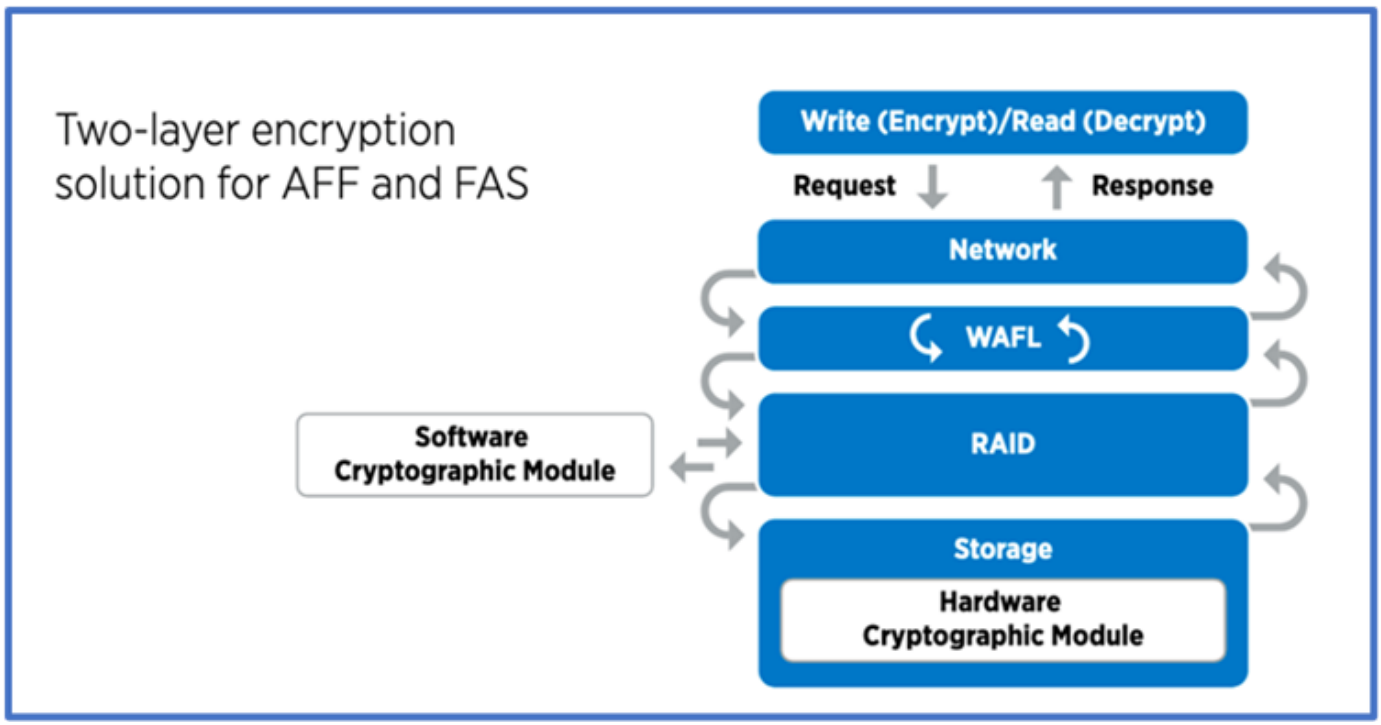
對靜止資料和正在傳輸的資料使用加密

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。

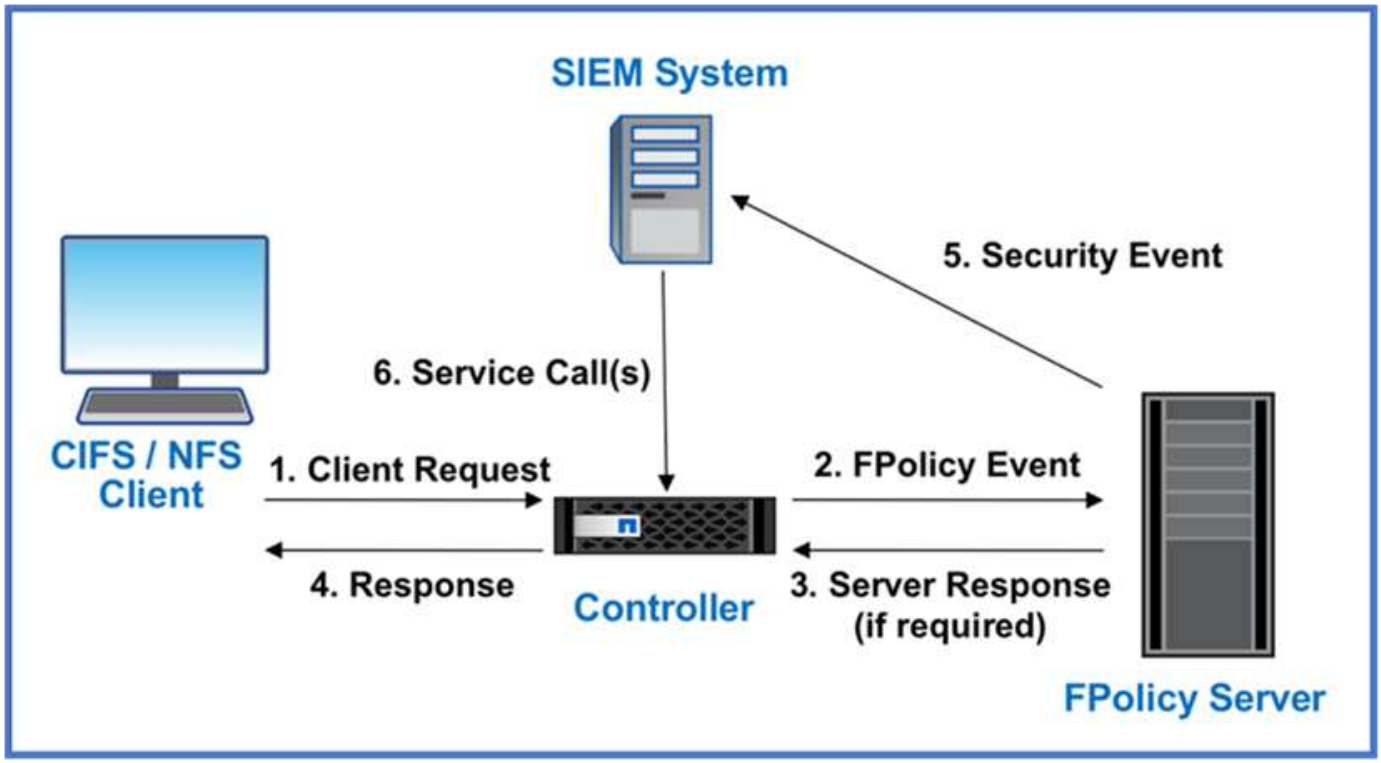
資料傳輸中加密

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 。

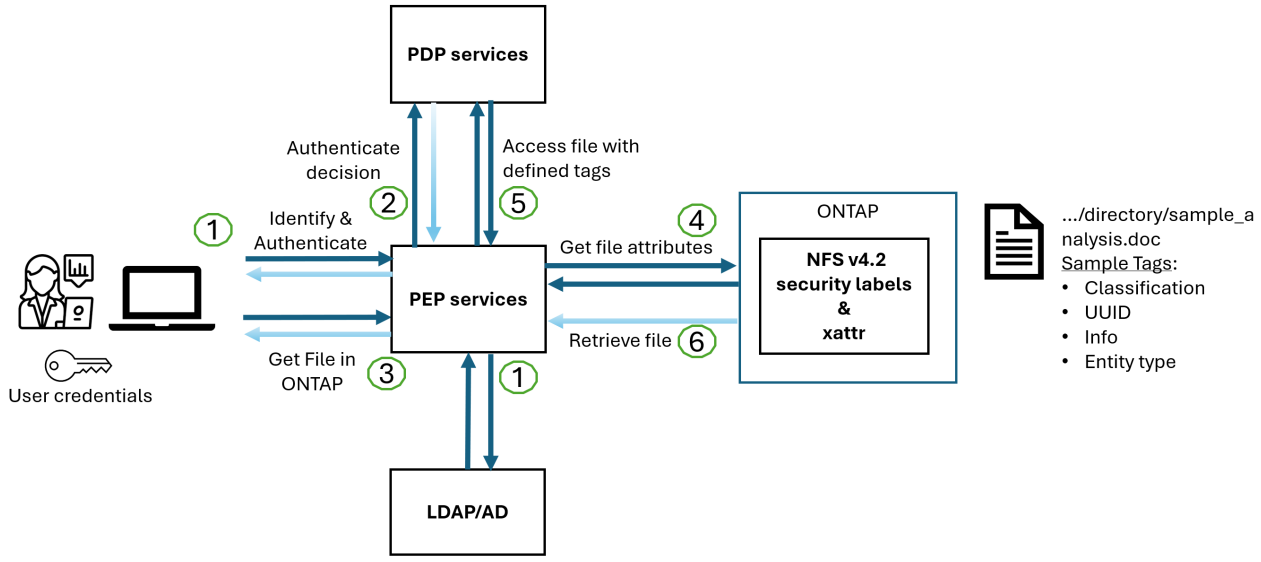
2. 然後， PDP 會根據已建立的 ABAC 原則來評估此要求。

   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	<pre>[
	  {
	  "value": "USA"
	  }
	]</pre>

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

dissemTos	<pre>{
	  "value": "DoD"
	}</pre>

二合一組織	<pre>{
	  "value": "DoD"
	}</pre>

entityType	<pre>{
	  "value": "GOV"
	}</pre>

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"