



NetApp Ransomware Resilience 文檔

NetApp Ransomware Resilience

NetApp
February 27, 2026

目錄

NetApp Ransomware Resilience文檔	1
發行說明	2
NetApp Ransomware Resilience的新功能	2
2026 年 2 月 16 日	2
2026年1月19日	2
2026年1月12日	2
2025年12月8日	3
2025年11月10日	3
2025年10月6日	3
2025年8月12日	4
2025年7月15日	4
2025年6月9日	5
2025年5月13日	6
2025年4月29日	6
2025年4月14日	7
2025年3月10日	7
2024年12月16日	8
2024年11月7日	8
2024年9月30日	9
2024年9月2日	9
2024年8月5日	10
2024年7月1日	10
2024年6月10日	10
2024年5月14日	11
2024年3月5日	13
2023年10月6日	13
NetApp Ransomware Resilience的已知限制	14
準備演習重置選項問題	14
Amazon FSx for NetApp ONTAP限制	14
Azure NetApp Files 限制	14
開始	15
了解NetApp Ransomware Resilience	15
資料層的勒索軟體抵禦能力	15
勒索軟體復原能力可以做什麼	16
使用勒索軟體恢復能力的好處	17
成本	17
授權	18
NetApp Console	18
勒索軟體復原的工作原理	18

支援的備份目標、系統和工作負載資料來源	20
關鍵術語	21
NetApp Ransomware Resilience前提條件	21
支援的系統	22
NetApp Console需求	22
ONTAP 需求	22
資料備份	23
可疑用戶行為要求	23
更新ONTAP系統中的非管理員使用者權限	23
NetApp Ransomware Resilience快速入門	23
設定NetApp Ransomware Resilience	25
準備備份目標	25
設定NetApp Console	25
設定NetApp Ransomware Resilience的許可	26
許可證類型	26
其他許可證	26
試試 Ransomware Resilience 30 天免費試用版	26
透過 AWS Marketplace 訂閱	27
透過 Microsoft Azure Marketplace 訂閱	29
透過 Google Cloud Platform Marketplace 訂閱	31
自帶授權 (BYOL)	33
控制台許可證到期後請更新	34
結束 PAYGO 訂閱	35
更多資訊	35
在 NetApp Ransomware Resilience 中發現並管理工作負載	35
選擇要發現和保護的工作負載	35
發現先前選定的系統新建立的工作負載	37
發現新系統	37
排除工作負載	38
使用勒索軟體彈性	40
存取NetApp Ransomware Resilience	40
在 NetApp Ransomware Resilience 中監控工作負載健全狀況	41
使用儀表板檢視工作負載健全狀況	41
在儀表板上檢視保護建議	43
將保護資料匯出到 CSV 文件	44
存取技術文檔	44
保護和偵測	44
在 NetApp Ransomware Resilience 中檢視保護狀態	45
在 NetApp Ransomware Resilience 中新增備份目的地	47
使用NetApp Ransomware Resilience保護策略保護工作負載	52
設定使用者活動偵測	60

在 NetApp Ransomware Resilience 中管理保護群組	71
使用勒索軟體復原中的 NetApp Data Classification 掃描個人識別資訊	75
回應並恢復	78
在 NetApp Ransomware Resilience 中管理警報	78
透過 NetApp Ransomware Resilience，在勒索軟體攻擊發生後恢復	86
在 NetApp Ransomware Resilience 中進行勒索軟體攻擊準備演練	94
配置勒索軟體攻擊準備演習	94
開始準備演習	97
響應戰備演習警報	97
恢復測試工作負載	99
準備演練後更改警報狀態	100
審查準備演習報告	100
將 NetApp Ransomware Resilience 連接到安全性與事件管理系統 (SIEM)，以進行威脅分析與偵測	101
傳送至 SIEM 的事件資料	101
設定 AWS Security Hub 進行威脅偵測	102
設定 Microsoft Sentinel 進行威脅偵測	102
設定 Splunk Cloud 進行威脅偵測	105
在勒索軟體防禦中連接 SIEM	105
在 NetApp Ransomware Resilience 中下載報告	106
知識和支持	109
註冊以獲得支持	109
支援註冊概述	109
註冊 NetApp Console 以取得 NetApp 支持	109
關聯 NSS 憑證以獲得 Cloud Volumes ONTAP 支持	111
獲取協助	112
獲取雲端提供者文件服務的支持	112
使用自助選項	112
向 NetApp 支援建立案例	113
管理您的支援案例	114
關於 NetApp Ransomware Resilience 的常見問題解答	116
部署	116
使用權	116
互通性	116
工作負載	117
保護策略	118
法律聲明	119
版權	119
商標	119
專利	119
隱私權政策	119
開源	119

NetApp Ransomware Resilience 文檔

發行說明

NetApp Ransomware Resilience的新功能

了解NetApp Ransomware Resilience的新功能。

2026 年 2 月 16 日

Azure NetApp Files 支援

Ransomware Resilience 現已支援 Azure NetApp Files 系統，使您能夠有效率地偵測和應對 Azure NetApp Files 中的勒索軟體威脅。當您發現工作負載時，Ransomware Resilience 現在會呈現 Azure NetApp Files 並在保護儀表中顯示。Ransomware Resilience 對 Azure NetApp Files 的支援僅包括使用快照的偵測和保護策略。對 Azure NetApp Files 的支援目前處於預覽階段。

如需詳細資訊，請參閱 ["了解勒索軟體抵禦能力"](#)。

將使用者從使用者行為警示中排除

NetApp Ransomware Resilience 現已允許您將特定使用者從使用者行為警報中排除。排除受信任的使用者可以防止誤報和不必要的警報。

如需詳細資訊，請參閱 ["將使用者排除在警示範圍之外"](#)。

使用者行為活動的保護群組支援

Ransomware Resilience 防護群組現在支援可疑使用者行為偵測的偵測原則。將勒索軟體防護策略套用至防護群組時，它會在工作負載之間套用原則，簡化網路安全態勢的管理。

如需詳細資訊，請參閱 ["建立保護組"](#)。

2026年1月19日

不支援的捲

Ransomware Resilience 報告現在會在 **Summary** 報告中記錄受支援和不受支援的磁碟區的資訊。使用此資訊可以診斷系統中的磁碟區為何可能不符合勒索軟體防護條件。

有關詳細信息，請參閱 ["下載勒索軟體復原力報告"](#)。

2026年1月12日

將快照複製到ONTAP

Ransomware Resilience 現已支援將快照複製到輔助 ONTAP 網站。使用複製策略的保護群組，您可以為每個工作負載複製到相同或不同的目標位置。您可以建立包含複製功能的勒索軟體防護策略，也可以使用預先定義的策略。

有關詳細信息，請參閱 ["在勒索軟體復原中保護工作負載"](#)。

將工作負載排除在勒索軟體復原能力之外

勒索軟體復原功能現在支援將系統中的特定工作負載從保護範圍和勒索軟體復原儀表中排除。發現工作負載後，您可以將其排除在外；如果您想要添加勒索軟體防護，則可以重新將其包含在內。排除在外的工作負載無需付費。

有關詳細信息，請參閱 ["排除工作負載"](#)。

標記提醒，如正在審核中

勒索軟體復原功能現在允許您將警報標記為「審核中」。使用「審核中」標籤可以提高團隊在對活躍的勒索軟體威脅進行分類和管理時的清晰度。

有關詳細信息，請參閱 ["管理勒索軟體復原能力中的警報"](#)。

2025年12月8日

擴充功能阻止功能已在工作負載層級啟用。

啟用擴充封鎖功能後，現在是在工作負載層級而不是儲存虛擬機器層級啟用此功能。

編輯使用者行為警報狀態

勒索軟體復原功能現在允許您編輯使用者行為警報的狀態。您可以手動關閉和解決警報。

有關詳細信息，請參閱 ["管理勒索軟體復原能力中的警報"](#)。

支援多個控制台代理

勒索軟體復原功能現在支援使用多個控制台代理程式來管理相同系統。

有關控制台代理的更多信息，請參閱 ["建立控制台代理"](#)。

2025年11月10日

此版本包含一般增強與改進。

2025年10月6日

BlueXP ransomware protection 現已升級 **NetApp Ransomware Resilience**

BlueXP ransomware protection 服務已更名為 NetApp Ransomware Resilience。

BlueXP 現在是 **NetApp Console**

NetApp Console 提供企業級跨本地和雲端環境的儲存和資料服務的集中管理，提供即時洞察、更快的工作流程和簡化的管理。

有關更改的詳細信息，請參閱 ["NetApp Console 發行說明"](#)。

資料外洩檢測

勒索軟體復原力包括一種新的檢測機制，只需幾個步驟即可激活，以檢測異常用戶讀取作為資料外洩的早期指標。勒索軟體彈性透過建立歷史基線來收集和分析使用者讀取事件，該基線是根據過去資料得出的預期正常行為的概況。當新用戶活動明顯偏離既定規範（例如意外的閱讀激增與可疑的閱讀模式相結合）時，就會產生警報。勒索軟體復原力包括一個用於偵測可疑讀取模式的 AI 模型。

與儲存層的 ARP 加密偵測不同，勒索軟體彈性 SaaS 服務透過收集 FPolicy 事件來偵測使用者行為異常。



您必須使用新的"[勒索軟體恢復用戶行為管理員](#)和"[勒索軟體恢復用戶行為檢視器](#)"角色來存取可疑用戶行為檢測設定。

有關詳細信息，請參閱"[啟用可疑用戶活動偵測](#)"和"[查看異常用戶行為](#)"。

其他可疑用戶活動檢測

除了資料外洩偵測之外，勒索軟體復原能力還根據觀察到的可疑使用者活動偵測以下警報類型：

- 資料破壞 - 潛在攻擊 - 當檔案刪除的數量超過歷史標準時，會建立具有潛在攻擊嚴重程度的警報。
- 可疑使用者行為 - 潛在攻擊 - 當觀察到類似於勒索軟體攻擊的讀取、重新命名和刪除操作時，會建立嚴重程度為潛在攻擊的警報
- 可疑使用者行為 - 警告 - 當檔案活動（讀取、刪除、重新命名等）的總數超過歷史標準時，將建立嚴重程度為警告的警報

用於資料外洩偵測的新使用者角色

為了管理可疑使用者活動警報，Ransomware Resilience 為控制台組織管理員引入了兩個新角色，以授予對可疑使用者活動偵測的存取權：[Ransomware Resilience 使用者行為管理員](#)和 [Ransomware Resilience 使用者行為檢視器](#)。

您必須是使用者行為管理員才能配置可疑使用者行為設定。勒索軟體復原管理員角色不支援配置可疑使用者行為設定。

有關更多信息，請參閱"[NetApp Ransomware Resilience基於角色的訪問](#)"。

2025年8月12日

此版本包含一般增強與改進。

2025年7月15日

SAN 工作負載支持

此版本包括對BlueXP ransomware protection中的 SAN 工作負載的支援。現在，除了 NFS 和 CIFS 工作負載之外，您還可以保護 SAN 工作負載。

有關詳細信息，請參閱"[BlueXP ransomware protection先決條件](#)"。

改進的工作負載保護

此版本改進了具有其他NetApp工具（如SnapCenter或BlueXP backup and recovery）的快照和備份策略的工作負載的設定過程。在先前的版本中，BlueXP ransomware protection發現了來自其他工具的策略，只允許您更改偵測策略。在這個版本中，您現在可以用BlueXP ransomware protection策略取代快照和備份策略，或繼續使用其他工具中的策略。

有關詳細信息，請參閱["保護工作負載"](#)。

電子郵件通知

如果BlueXP ransomware protection偵測到可能的攻擊，BlueXP通知中會出現通知，並且會向您設定的電子郵件地址發送電子郵件。

電子郵件包含有關嚴重性、受影響的工作負載的信息，以及BlueXP ransomware protection*警報* 標籤中的警報連結。

如果您在BlueXP ransomware protection中配置了安全性和事件管理 (SIEM) 系統，該服務會向您的 SIEM 系統發送警報詳細資訊。

有關詳細信息，請參閱["處理偵測到的勒索軟體警報"](#)。

2025年6月9日

著陸頁更新

此版本包括對BlueXP ransomware protection登陸頁面的更新，使開始免費試用和發現變得更加容易。

準備演習更新

以前，您可以透過模擬對新樣本工作負載的攻擊來執行勒索軟體準備演練。利用此功能，您可以調查模擬攻擊並恢復工作負載。使用此功能來測試警報通知、回應和恢復。根據需要經常運行和安排這些演習。

在此版本中，您可以使用BlueXP ransomware protection儀表板上的新按鈕在測試工作負載上執行勒索軟體準備演練，從而更輕鬆地模擬勒索軟體攻擊、調查其影響並有效地恢復工作負載，所有這些都在受控環境中完成。

現在，除了 NFS 工作負載之外，您還可以在 CIFS (SMB) 工作負載上執行準備情況演練。

有關詳細信息，請參閱 ["進行勒索軟體攻擊準備演習"](#)。

啟用BlueXP classification更新

在BlueXP ransomware protection服務中使用BlueXP classification之前，您需要啟用BlueXP classification來掃描您的資料。將資料分類有助於您找到個人識別資訊 (PII)，這可能會增加安全風險。

您可以在BlueXP ransomware protection中對文件共享工作負載部署BlueXP classification。在*隱私暴露*欄中，選擇*識別暴露*選項。如果您已啟用分類服務，此操作將識別曝光。否則，在此版本中，對話方塊會顯示部署BlueXP classification的選項。選擇*部署*前往BlueXP classification服務登入頁面，您可以在其中部署服務。西

如需詳細資訊、請參閱 ["在雲端部署BlueXP classification"](#)、若要在 BlueXP ransomware protection 中使用服務、請參閱 ["使用BlueXP classification掃描個人識別資訊"](#)。

2025年5月13日

BlueXP ransomware protection中不支援的工作環境報告

在發現工作流程期間，當您將滑鼠懸停在「支援」或「不支援的工作負載」上時，BlueXP ransomware protection會報告更多詳細資訊。這將幫助您了解為什麼您的某些工作負載未被BlueXP ransomware protection服務發現。

服務不支援工作環境的原因有很多，例如，工作環境中的ONTAP版本可能低於所需的版本。當您將滑鼠懸停在未支援的工作環境上時，工具提示會顯示原因。

您可以在初始發現期間查看不受支援的工作環境，也可以在其中下載結果。您也可以從「設定」頁面中的「工作負載發現」選項查看發現的結果。

有關詳細信息，請參閱 ["發現BlueXP ransomware protection中的工作負載"](#)。

2025年4月29日

支援Amazon FSx for NetApp ONTAP

此版本支援Amazon FSx for NetApp ONTAP。此功能可協助您使用BlueXP ransomware protection來保護FSx for ONTAP工作負載。

FSx for ONTAP是一項完全託管的服務，可在雲端提供NetApp ONTAP儲存的強大功能。它提供與您在本機上使用的相同的功能、效能和管理能力，同時具有原生AWS服務的靈活性和可擴充性。

BlueXP ransomware protection工作流程進行了以下更改：

- Discovery 包含 FSx for ONTAP 9.15 工作環境中的工作負載。
- 「保護」標籤顯示 FSx for ONTAP環境中的工作負載。在這種環境中，您應該使用 FSx for ONTAP備份服務執行備份作業。您可以使用BlueXP ransomware protection快照恢復這些工作負載。



無法在BlueXP中設定在FSx for ONTAP上執行的工作負載的備份策略。Amazon FSx for NetApp ONTAP中設定的任何現有備份策略均保持不變。

- 警報事件展示了新的FSx for ONTAP工作環境。

有關詳細信息，請參閱 ["了解BlueXP ransomware protection與工作環境"](#)。

有關受支援選項的信息，請參閱 ["BlueXP ransomware protection的局限性"](#)。

需要BlueXP訪問角色

現在您需要以下存取角色之一來查看、發現或管理BlueXP ransomware protection：組織管理員、資料夾或專案管理員、勒索軟體保護管理員或勒索軟體保護檢視器。

["了解所有服務的BlueXP訪問角色"](#)。

2025年4月14日

準備演習報告

透過此版本，您可以查看勒索軟體攻擊準備演習報告。準備演練使您能夠模擬對新建立的範例工作負載的勒索軟體攻擊。然後，調查模擬攻擊並恢復樣本工作負載。此功能可協助您透過測試警報通知、回應和復原流程來了解在發生實際勒索軟體攻擊時是否已做好準備。

有關詳細信息，請參閱 ["進行勒索軟體攻擊準備演習"](#)。

新的基於角色的存取控制角色和權限

以前，您可以根據使用者的職責為其分配角色和權限，這有助於您管理使用者對BlueXP ransomware protection的存取。在這個版本中，有兩個特定於BlueXP ransomware protection的新角色具有更新的權限。新角色如下：

- 勒索軟體保護管理員
- 勒索軟體保護檢視器

有關權限的詳細信息，請參閱 ["BlueXP ransomware protection基於角色的功能訪問"](#)。

付款改進

此版本對支付流程進行了多項改進。

有關詳細信息，請參閱 ["設定許可證和付款選項"](#)。

2025年3月10日

模擬攻擊並做出回應

透過此版本，模擬勒索軟體攻擊來測試您對勒索軟體警報的回應。此功能可協助您透過測試警報通知、回應和復原流程來了解在發生實際勒索軟體攻擊時是否已做好準備。

有關詳細信息，請參閱 ["進行勒索軟體攻擊準備演習"](#)。

發現過程的增強

此版本包括對選擇性發現和重新發現過程的增強：

- 透過此版本，您可以發現新增到先前選擇的工作環境中的新建立的工作負載。
- 您也可以在此版本中選擇_新_工作環境。此功能可協助您保護新增至環境中的新工作負載。
- 您可以在最初的發現過程中或在設定選項中執行這些發現過程。

有關詳細信息，請參閱 ["發現先前選定的工作環境的新建立的工作負載"](#)和 ["使用"設定"選項配置功能"](#)。

偵測到高度加密時發出警報

在此版本中，即使沒有高檔案副檔名更改，您也可以在工作負載上偵測到高加密時查看警報。此功能使用ONTAP自主勒索軟體防護 (ARP) AI，可協助您識別面臨勒索軟體攻擊風險的工作負載。使用此功能並下載受影響文件的完整清單（無論擴展名是否更改）。

有關詳細信息，請參閱 ["響應檢測到的勒索軟體警報"](#)。

2024年12月16日

使用 **Data Infrastructure Insights** 儲存工作負載安全性偵測異常使用者行為

在此版本中，您可以使用 Data Infrastructure Insights 儲存工作負載安全性來偵測儲存工作負載中的異常使用者行為。此功能可協助您識別潛在的安全威脅並阻止潛在的惡意使用者以保護您的資料。

有關詳細信息，請參閱 ["響應檢測到的勒索軟體警報"](#)。

在使用 Data Infrastructure Insights 儲存工作負載安全性偵測異常使用者行為之前，您需要使用 BlueXP ransomware protection* 設定* 選項來設定此選項。

參考 ["配置 BlueXP ransomware protection 設置"](#)。

選擇要發現和保護的工作負載

在此版本中，您現在可以執行以下操作：

- 在每個連接器中，選擇您想要發現工作負載的工作環境。如果您想保護環境中的特定工作負載而不是其他工作負載，您可能會受益於此功能。
- 在工作負載發現期間，您可以啟用每個連接器的工作負載自動發現。此功能可讓您選擇要保護的工作負載。
- 發現先前選擇的工作環境的新建立的工作負載。

參考 ["發現工作負載"](#)。

2024年11月7日

啟用資料分類並掃描個人識別資訊 (PII)

在這個版本中，您可以啟用 BlueXP classification (BlueXP 系列的核心元件) 來掃描和分類檔案共用工作負載中的資料。將資料分類可以幫助您識別資料是否包含個人資訊或私人資訊，這可能會增加安全風險。此流程也會影響工作負載的重要性，並協助您確保使用適當的保護等級來保護工作負載。

部署了 BlueXP classification 的客戶通常可以在 BlueXP ransomware protection 中掃描 PII 資料。BlueXP classification 是作為 BlueXP 平台的一部分提供，無需額外付費，並且可以在本地或客戶雲端中部署。

若要啟動掃描，請在「保護」頁面上，選擇「保護」儀表板「隱私暴露」列中的 識別暴露。有關更多信息，請參閱 ["使用 BlueXP classification 掃描個人識別敏感資料"](#)。

SIEM 與 Microsoft Sentinel 集成

現在，您可以使用 Microsoft Sentinel 將資料傳送至安全性和事件管理系統 (SIEM) 以進行威脅分析和偵測。以前，您可以選擇 AWS Security Hub 或 Splunk Cloud 作為您的 SIEM。

["了解有關配置 BlueXP ransomware protection 設定的更多信息"](#)。

立即免費試用 **30** 天

隨著此版本的發布，BlueXP ransomware protection 的新部署現在有 30 天的免費試用期。在此之前，BlueXP ransomware protection 提供 90 天的免費試用。如果您已享有 90 天免費試用，則該優惠將持續 90 天。

在檔案層級恢復 **Podman** 的應用程式工作負載

在檔案層級恢復應用程式工作負載之前，您現在可以查看可能受到攻擊影響的檔案清單並確定要復原的檔案。以前，如果組織（以前是帳戶）中的BlueXP連接器正在使用 Podman，則此功能將被停用。現在它已為 Podman 啟用。您可以讓BlueXP ransomware protection 選擇要恢復的文件，您可以上傳列出受警報影響的所有文件的 CSV 文件，或者您可以手動識別要恢復的文件。

["了解有關從勒索軟體攻擊中恢復的更多信息"](#)。

2024年9月30日

檔案共享工作負載的自訂分組

在此版本中，您現在可以將文件共用分組，以便更輕鬆地保護您的資料資產。此服務可以同時保護群組中的所有磁碟區。以前，您需要單獨保護每個磁碟區。

["了解有關在勒索軟體保護策略中分組文件共享工作負載的更多信息"](#)。

2024年9月2日

來自**Digital Advisor**的安全風險評估

BlueXP ransomware protection 現在會從 NetApp Digital Advisor 收集與叢集相關的高風險和重大安全風險資訊。如果發現任何風險，BlueXP ransomware protection 會在控制面板的 建議操作 窗格中提供建議：「修正叢集上的已知安全漏洞 <name>」。從控制面板的建議中選擇 檢視並修復 後，系統會提示您查看 Digital Advisor 和一篇通用漏洞揭露（CVE）文章，以解決安全風險。如果存在多個安全風險，請查看 Digital Advisor 中的資訊。

參考 ["Digital Advisor 文檔"](#)。

備份到 **Google Cloud Platform**

在此版本中，您可以將備份目標設定為 Google Cloud Platform 儲存桶。以前，您只能將備份目標新增至 NetApp StorageGRID、Amazon Web Services 和 Microsoft Azure。

["了解有關配置BlueXP ransomware protection設定的更多信息"](#)。

支持 **Google Cloud Platform**

該服務現在支援適用於 Google Cloud Platform 的 Cloud Volumes ONTAP 進行儲存保護。先前，該服務僅支援適用於 Amazon Web Services 和 Microsoft Azure 的 Cloud Volumes ONTAP 以及本機 NAS。

["了解BlueXP ransomware protection以及支援的資料來源、備份目標和工作環境"](#)。

基於角色的存取控制

現在您可以使用基於角色的存取控制 (RBAC) 限制對特定活動的存取。BlueXP ransomware protection 使

用BlueXP的兩個角色：BlueXP帳號管理員和非帳號管理員（檢視者）。

有關每個角色可以執行的操作的詳細信息，請參閱 ["基於角色的存取控制權限"](#)。

2024年8月5日

使用 **Splunk Cloud** 進行威脅偵測

您可以自動將資料傳送到您的安全性和事件管理系統 (SIEM) 進行威脅分析和偵測。在先前的版本中，您只能選擇 AWS Security Hub 作為您的 SIEM。在此版本中，您可以選擇 AWS Security Hub 或 Splunk Cloud 作為您的 SIEM。

["了解有關配置BlueXP ransomware protection設定的更多信息"](#)。

2024年7月1日

自帶授權 (BYOL)

在此版本中，您可以使用 BYOL 許可證，它是您從NetApp銷售代表處獲得的NetApp許可證文件 (NLF)。

["了解有關設置許可的詳細信息"](#)。

在檔案層級恢復應用程式工作負載

在檔案層級恢復應用程式工作負載之前，您現在可以查看可能受到攻擊影響的檔案清單並確定要復原的檔案。您可以讓BlueXP ransomware protection選擇要恢復的文件，您可以上傳列出受警報影響的所有文件的 CSV 文件，或者您可以手動識別要恢復的文件。



在此版本中，如果帳戶中的所有BlueXP連接器均未使用 Podman，則啟用單一檔案復原功能。否則，該帳戶將被停用。

["了解有關從勒索軟體攻擊中恢復的更多信息"](#)。

下載受影響文件的列表

在檔案層級復原應用程式工作負載之前，您現在可以造訪「警報」頁面以 CSV 檔案形式下載受影響檔案的列表，然後使用「復原」頁面上傳該 CSV 檔案。

["了解有關在恢復應用程式之前下載受影響文件的更多信息"](#)。

刪除保護計劃

透過此版本，您現在可以刪除勒索軟體保護策略。

["了解有關保護工作負載和管理勒索軟體保護策略的更多信息"](#)。

2024年6月10日

主儲存體上的快照副本鎖定

啟用此功能可鎖定主儲存體上的快照副本，以便即使勒索軟體攻擊進入備份儲存目標，它們在一定時間內也無法被修改或刪除。

["了解有關在勒索軟體保護策略中保護工作負載和啟用備份鎖定的更多信息"](#)。

支援適用於 Microsoft Azure 的 Cloud Volumes ONTAP

此版本除了支援適用於 AWS 的 Cloud Volumes ONTAP 和本機 ONTAP NAS 之外，還支援適用於 Microsoft Azure 的 Cloud Volumes ONTAP 作為系統。

["Azure 中的 Cloud Volumes ONTAP 快速入門"](#)

["了解 BlueXP ransomware protection"](#)。

Microsoft Azure 新增為備份目標

現在您可以將 Microsoft Azure 與 AWS 和 NetApp StorageGRID 一起新增為備份目標。

["了解有關如何配置保護設定的更多信息"](#)。

2024年5月14日

許可更新

您可以註冊 90 天免費試用。很快您將能夠透過 Amazon Web Services Marketplace 購買即用即付訂閱或自備 NetApp 授權。

["了解有關設置許可的詳細信息"](#)。

CIFS 協定

該服務現在支援使用 NFS 和 CIFS 協定的 AWS 系統中的本機 ONTAP 和 Cloud Volumes ONTAP。先前的版本僅支援 NFS 協定。

工作負載詳情

此版本現在在保護和其他頁面的工作負載資訊中提供了更多詳細信息，以改善工作負載保護評估。從工作負載詳細資料中，您可以查看目前指派的策略並查看配置的備份目標。

["詳細了解如何在「保護」頁面中查看工作負載詳細信息"](#)。

應用程式一致性和虛擬機器一致性保護和恢復

現在，您可以使用 NetApp SnapCenter 軟體執行應用程式一致性保護，並使用 SnapCenter Plug-in for VMware vSphere 虛擬機器一致性保護，從而實現靜止且一致的狀態，以避免日後需要復原時可能的資料遺失。如果需要恢復，您可以將應用程式或虛擬機器恢復到任何先前可用的狀態。

["了解有關保護工作負載的更多信息"](#)。

勒索軟體防護策略

如果工作負載上不存在快照或備份策略，您可以建立勒索軟體防護策略，其中可以包含您在此服務中建立的以下策略：

- 快照策略
- 備份策略
- 檢測策略

["了解有關保護工作負載的更多信息"](#)。

威脅偵測

現在可以使用第三方安全性和事件管理 (SIEM) 系統啟用威脅偵測。儀表板現在顯示「啟用威脅偵測」的新建議，可以在「設定」頁面上進行設定。

["了解有關配置“設定”選項的詳細信息"](#)。

消除誤報

從「警報」標籤中，您現在可以消除誤報或決定立即恢復資料。

["詳細了解如何回應勒索軟體警報"](#)。

檢測狀態

新的偵測狀態出現在「保護」頁面上，顯示套用於工作負載的勒索軟體偵測的狀態。

["了解有關保護工作負載和查看保護狀態的更多信息"](#)。

下載 CSV 文件

您可以從保護、警報和復原頁面下載 CSV 檔案*。

["詳細了解如何從儀表板和其他頁面下載 CSV 文件"](#)。

文件連結

查看文件連結現在包含在 UI 中。您可以從儀表板垂直*操作*存取此文檔  選項。選擇“新增功能”以查看發行說明中的詳細信息，或選擇“文件”查看BlueXP ransomware protection文件主頁。

BlueXP backup and recovery

BlueXP 備份和復原服務不再需要在系統上預先啟用。請參閱["先決條件"](#)。BlueXP 勒索軟體防護服務可透過「設定」選項協助配置備份目標位置。請參閱["配置設定"](#)。

設定選項

現在您可以在BlueXP ransomware protection設定中設定備份目的地。

["了解有關配置“設定”選項的詳細信息"](#).

2024年3月5日

保護策略管理

除了使用預定義策略之外，您現在還可以建立策略。 ["了解有關管理策略的更多信息"](#)。

二級儲存的不變性 (DataLock)

現在，您可以使用物件儲存中的NetApp DataLock 技術使備份在二級儲存中不可變。 ["了解有關創建保護策略的更多信息"](#)。

自動備份到NetApp StorageGRID

除了使用 AWS 之外、您現在還可以選擇 StorageGRID 作為備份目的地 ["了解有關配置備份目標的更多信息"](#)。

調查潛在攻擊的附加功能

現在您可以查看更多取證詳細資訊來調查偵測到的潛在攻擊。 ["詳細了解如何回應偵測到的勒索軟體警報"](#)。

恢復過程

恢復過程得到了加強。現在，您可以按磁碟區或所有磁碟區恢復工作負載。 ["了解有關從勒索軟體攻擊中恢復的更多資訊 \(事件被消除後\)"](#)。

["了解BlueXP ransomware protection"](#)。

2023年10月6日

BlueXP ransomware protection服務是一種用於保護資料、偵測潛在攻擊以及從勒索軟體攻擊中恢復資料的 SaaS 解決方案。

預覽版服務可保護BlueXP組織內各個組織中 Oracle、VM 資料儲存和本機 NAS 儲存空間上的檔案共用以及 AWS 上的Cloud Volumes ONTAP (使用 NFS 協定) 上的應用程式工作負載，並將資料備份到 Amazon Web Services 雲端儲存。

BlueXP ransomware protection服務充分利用了多種NetApp技術，以便您的資料安全管理員或安全營運工程師能夠實現以下目標：

- 一目了然地查看所有工作負載的勒索軟體保護情況。
- 深入了解勒索軟體防護建議
- 根據BlueXP ransomware protection建議改進防護態勢。
- 指派勒索軟體保護策略，以保護您的主要工作負載和高風險資料免受勒索軟體攻擊。
- 監控您的工作負載的健康狀況，防範勒索軟體攻擊並尋找資料異常。
- 快速評估勒索軟體事件對您的工作量的影響。
- 透過恢復數據並確保不會再次感染儲存的數據，智慧地從勒索軟體事件中恢復。

NetApp Ransomware Resilience的已知限制

已知限制標識了該產品的此版本不支援或無法與其正確互通的平台、裝置或功能。仔細審查這些限制。

準備演習重置選項問題

如果您選擇ONTAP 9.11.1 磁碟區進行勒索軟體攻擊準備演習，勒索軟體復原能力會發送警報。如果您使用「複製到磁碟區」選項還原資料並重設鑽孔機，則重設操作將會失敗。

Amazon FSx for NetApp ONTAP限制

勒索軟體復原能力支援Amazon FSx for NetApp ONTAP系統。以下限制適用於Amazon FSx for ONTAP：

- Amazon FSx for ONTAP 不支援備份原則。在此環境中，您應該使用 Amazon FSx 執行備份作業。您可以使用 NetApp Ransomware Resilience 來恢復這些工作負載。
- 復原操作僅從快照執行。

Azure NetApp Files 限制

Azure NetApp Files 在 Ransomware Resilience 中受到支援。以下限制適用於 Azure NetApp Files：

- Azure NetApp Files 不支援使用備份原則的勒索軟體防護策略。但您可以使用 Azure NetApp Files 備份功能。
- Azure NetApp Files 不支援複製功能的勒索軟體防護策略。
- 選擇保護策略時，請確保其快照排程與 Azure NetApp Files 相容。Azure NetApp Files 中最常使用的快照排程是每小時一次。

開始

了解NetApp Ransomware Resilience

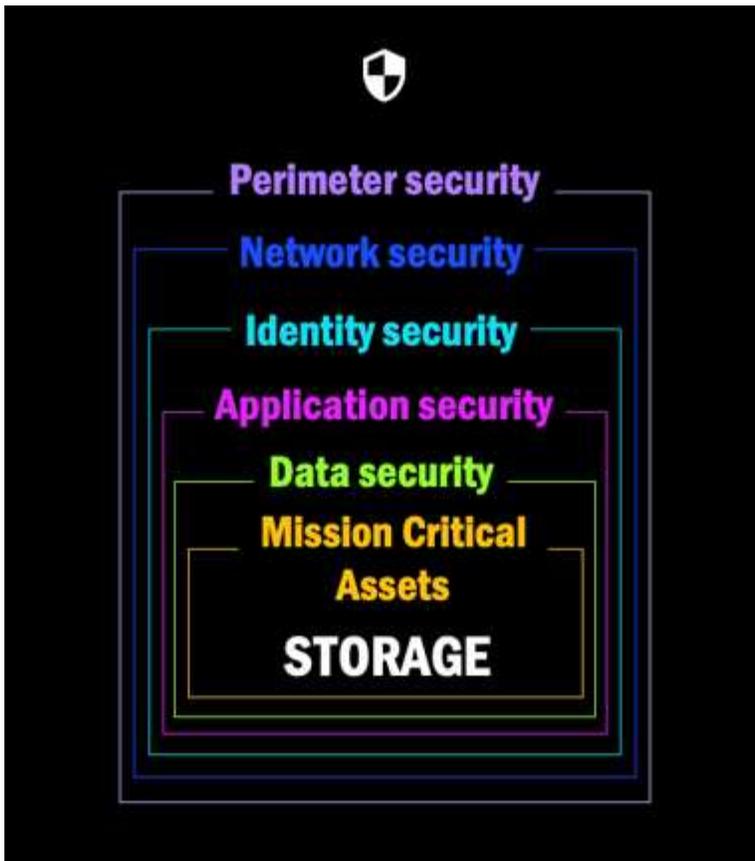
勒索軟體攻擊可以阻止對您資料的訪問，攻擊者可以要求贖金以換取資料發布或解密。據 IDC 稱，勒索軟體受害者遭受多次勒索軟體攻擊的情況並不少見。攻擊可能會中斷您對資料的訪問，時間從一天到幾週不等。

NetApp Ransomware Resilience 可保護您的資料免受勒索軟體攻擊。在 Ransomware Resilience 中，可為 Oracle 的應用程式型工作負載、VM 資料存放區，以及 NAS 儲存設備（NFS 和 CIFS 傳輸協定）和 SAN 儲存設備（FC、iSCSI 和 NVMe 傳輸協定）的檔案共用提供保護。Ransomware Resilience 支援內部部署儲存設備，以及適用於 Amazon Web Services 的 Cloud Volumes ONTAP、適用於 Google Cloud 的 Cloud Volumes ONTAP、適用於 Microsoft Azure 的 Cloud Volumes ONTAP、Azure NetApp Files 和 Amazon FSx for NetApp ONTAP，所有功能均可透過 NetApp Console 存取。您可以將資料備份到 Amazon Web Services、Google Cloud、Microsoft Azure 和 NetApp StorageGRID。

資料層的勒索軟體抵禦能力

您的安全態勢通常包含多層防禦，以防禦一系列網路威脅。

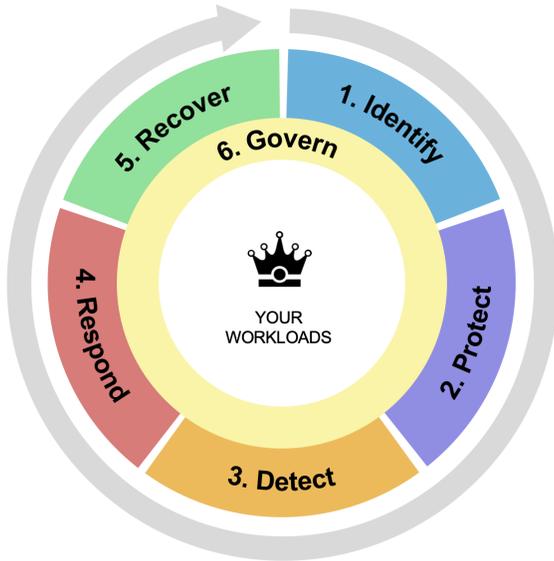
- 最外層：這是使用防火牆、入侵偵測系統和虛擬專用網路來保護網路邊界的第一道防線。
- 網路安全：這一層建立在網路分段、流量監控和加密的基礎上。
- 身分安全：使用身分驗證方法、存取控制和身管理來確保只有授權使用者才能存取敏感資源。
- 應用程式安全：使用安全編碼實踐、安全測試和運行時應用程式自我保護來保護軟體應用程式。
- 資料安全：透過資料保護、備份和復原策略保護您的資料。勒索軟體復原力在此層上運作。



勒索軟體復原能力可以做什麼

勒索軟體復原功能充分利用了多種NetApp技術，以便您的儲存管理員、資料安全管理員或安全營運工程師可以實現以下目標：

- 識別 在 NetApp 本地 NAS 和 SAN 系統中，基於應用程式、檔案共享或 VMware 管理的工作負載，並可於 NetApp Console、專案及 Console 代理程式中進行管理。在發現工作負載後，Ransomware Resilience 會識別提升勒索軟體韌性的機會。
- 透過對資料啟用備份、快照副本和勒索軟體保護策略來*保護*您的工作負載。
- *偵測*可能是勒索軟體攻擊的異常。註腳：[儘管攻擊可能未被發現，但我們的研究表明，NetApp技術已對某些基於文件加密的勒索軟體攻擊實現了高度檢測。]
- *應對*潛在的勒索軟體攻擊，自動啟動一個鎖定的時間點快照，以防止副本被意外或惡意刪除。您的備份資料將保持不可更改，並在來源端和目標端受到端到端的保護，免受勒索軟體攻擊。
- 透過協調多種NetApp技術來*恢復*您的工作負載，從而幫助加快工作負載的正常運作時間。您可以選擇恢復特定的磁碟區。勒索軟體彈性提供最佳選項的建議。
- 管理：實施勒索軟體保護策略並監控結果。



1. Automatically **discovers** and prioritizes data in NetApp storage **with a focus on top application-based workloads**

2. **One-click protection** of top workload data (backup, immutable/indelible snapshots, secure configuration, different security domain)

3. **Accurately detects** ransomware as **quickly** as possible using **next-generation AI-based anomaly detection**

4. Automated response to secure safe recovery point, attack alerting, and integration with top **SIEM and XDR solutions**

5. Rapidly restores data via simplified **orchestrated recovery** to accelerate application uptime

6. Implement your ransomware protection **strategy and policies**, and **monitor outcomes**

使用勒索軟體恢復能力的好處

勒索軟體復原能力有以下優勢：

- 發現工作負載及其現有的快照和備份計劃，並對其相對重要性進行排序。
- 評估您的勒索軟體防護狀況，並在易於理解的儀表中顯示，同時提供改進防護的建議。
- 一鍵存取即可套用 AI/ML 驅動的資料保護建議。
- 保護基於應用程式的工作負載（例如 Oracle、VMware 資料儲存和檔案共用）中的資料。
- 使用人工智慧技術即時偵測針對主儲存資料的勒索軟體攻擊。
- 透過建立快照副本和啟動有關異常活動的警報來啟動自動操作以回應偵測到的潛在攻擊。
- 應用精心策劃的恢復以滿足 RPO 政策。勒索軟體復原能力透過使用多種 NetApp 復原服務（包括 NetApp Backup and Recovery（以前稱為雲端備份）和 SnapCenter）來協調勒索軟體事件的復原。
- 使用基於角色的存取控制 (RBAC) 來管理對功能和操作的存取。

成本

您可以免費試用 Ransomware Resilience 30 天。NetApp 不會向您收取使用 Ransomware Resilience 試用版的費用。

如果您同時擁有備份和復原以及勒索軟體復原功能，則受這兩種產品保護的任何公開資料僅由勒索軟體復原功能計費。

當工作負載被歸類為受保護時，它會計入已購買的容量或 PayGo 訂閱。Ransomware Resilience 會在啟用了至少一項快照或備份原則的偵測原則時，將工作負載歸類為受保護。如果工作負載已啟用偵測原則，但沒有備份或快照原則，則會被歸類為有風險。存在風險的工作負載不會計入已購買的容量。

免費試用期結束後，受保護的工作負載將計入購買的容量或訂閱費用。NetApp Ransomware Resilience 會根據受保護工作負載相關資料在提高效率之前的每 GB 來收費。

授權

透過 Ransomware Resilience，您可以使用不同的授權計劃，包括免費試用、即用即付訂閱或自備授權。

勒索軟體復原需要NetApp ONTAP One 許可證。

勒索軟體恢復許可證不包括其他NetApp產品。即使您沒有許可證，Ransomware Resilience 也可以使用備份和還原。

為了偵測異常使用者行為，Ransomware Resilience 使用NetApp Autonomous Ransomware Protection，這是ONTAP內的一種機器學習 (ML) 模型，可偵測惡意檔案活動。該模型包含在勒索軟體恢復許可證中。

有關詳細信息，請參閱["設定許可"](#)。

NetApp Console

可透過NetApp Console存取勒索軟體復原功能。

NetApp Console提供企業級跨本機和雲端環境的NetApp儲存和資料服務的集中管理。需要控制台才能存取和使用NetApp資料服務。作為管理介面，它使您能夠從一個介面管理許多儲存資源。控制台管理員可以控制企業內所有系統的儲存和服務的存取。

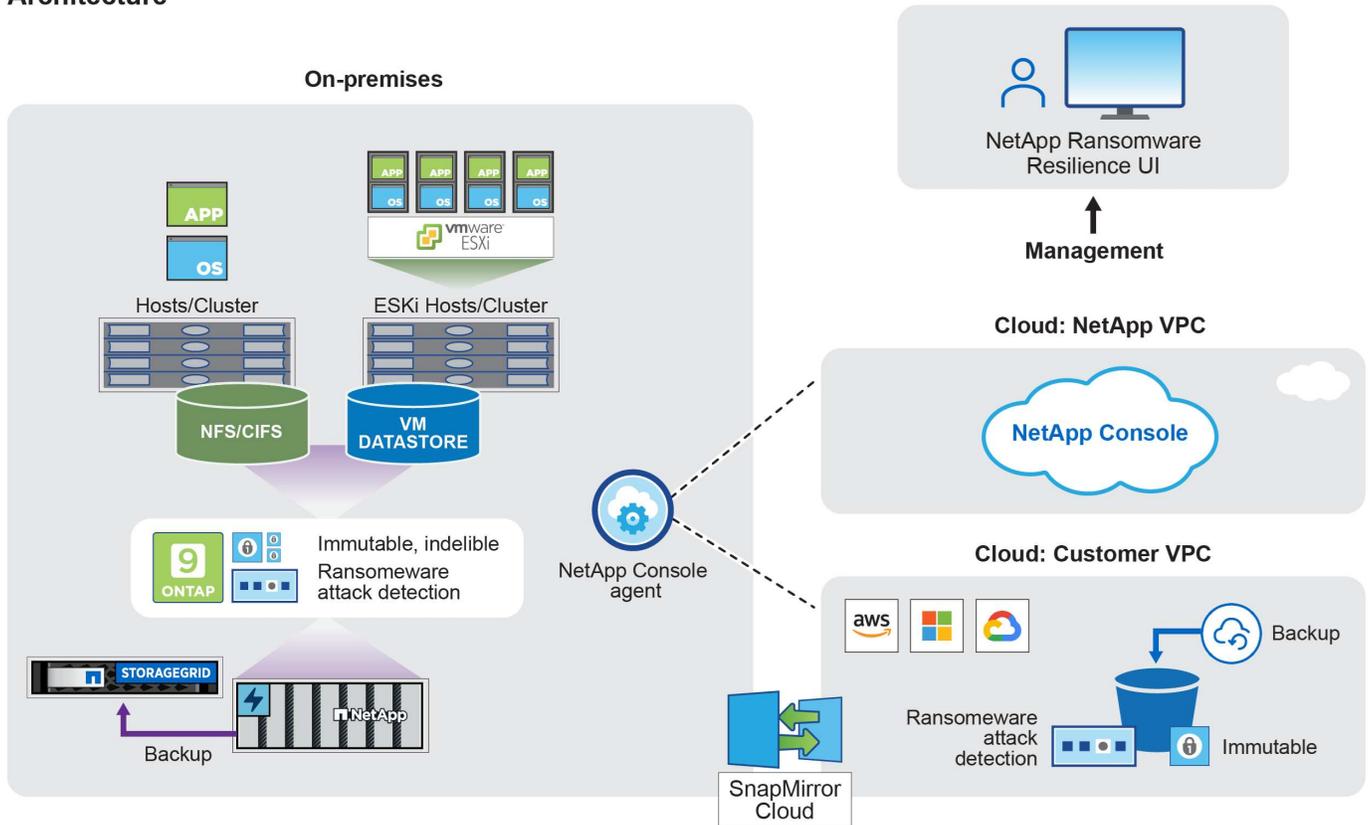
您無需許可證或訂閱即可開始使用 NetApp Console，只有在雲端部署 Console 代理程式以確保與儲存系統或 NetApp 資料服務的連線時才會產生費用。但是，某些可從 Console 存取的 NetApp 資料服務需要獲得許可或訂閱才能使用。

詳細了解["NetApp Console"](#)。

勒索軟體復原的工作原理

Ransomware Resilience 使用 NetApp Backup and Recovery 來探索並設定檔案共用工作負載的快照和備份原則。

Architecture



特徵	描述
確認	<ul style="list-style-type: none"> 尋找連接到控制台的所有客戶本地 NAS（NFS 和 CIFS 協定）、SAN（FC、iSCSI 和 NVMe）和 Cloud Volumes ONTAP 資料。 從 ONTAP 和 SnapCenter 服務 API 中識別客戶數據，並將其與工作負載關聯。深入瞭解 "ONTAP"。 發現每個磁碟區的目前 NetApp 快照副本和備份策略的保護等級以及任何機上偵測功能。然後，勒索軟體復原能力透過使用備份和復原、ONTAP 服務以及 NetApp 技術（例如自主勒索軟體保護（ARP 或 ARP/AI，取決於您的 ONTAP 版本）、FPolicy、備份策略和快照策略）將此保護狀態與工作負載關聯。了解更多 "自主勒索軟體防護"，"NetApp Backup and Recovery"，和 "ONTAP FPolicy"。 根據自動發現的保護等級為每個工作負載分配業務優先級，並根據工作負載的業務優先級建議保護策略。工作負載優先順序是基於已應用於與工作負載相關的每個磁碟區的快照頻率。
保護	<ul style="list-style-type: none"> 主動監控工作負載，並透過將原則套用至每個已識別的工作負載來協調 Backup and Recovery 和 ONTAP API 的使用。

特徵	描述
探測	<ul style="list-style-type: none"> • 使用整合式機器學習 (ML) 模型偵測潛在攻擊，該模型可偵測潛在的異常加密和活動。 • 提供雙層偵測，首先偵測主儲存中的潛在勒索軟體攻擊，然後透過取得額外的自動快照副本來建立最近的資料還原點，以回應異常活動。勒索軟體復原能力能夠更深入地挖掘以更精確地識別潛在攻擊，而不會影響主要工作負載的效能。 • 使用ONTAP、自主勒索軟體防護 (ARP 或 ARP/AI，取決於您的ONTAP版本) 和 FPolicy 技術確定攻擊相關工作負載的特定可疑檔案和對應。
回應	<ul style="list-style-type: none"> • 顯示相關數據，例如文件活動、使用者活動和熵，以幫助您完成有關攻擊的取證審查。 • 使用NetApp技術和產品 (例如ONTAP、自主勒索軟體防護 (ARP 或 ARP/AI，取決於您的ONTAP版本) 和 FPolicy) 啟動快速快照副本。
恢復	<ul style="list-style-type: none"> • 透過使用備份和復原、ONTAP、自主勒索軟體防護 (ARP 或 ARP/AI，取決於您的ONTAP版本) 以及 FPolicy 技術和服務，確定最佳快照或備份並推薦最佳復原點實際 (RPA)。 • 協調包括虛擬機器、文件共享、區塊儲存和資料庫在內的工作負載的恢復，並保持應用程式的一致性。
治理	<ul style="list-style-type: none"> • 分配勒索軟體保護策略 • 幫助您監控結果。

支援的備份目標、系統和工作負載資料來源

勒索軟體復原支援以下備份目標、系統和資料來源：

支援的備份目標

- 亞馬遜網路服務 (AWS) S3
- 谷歌雲端平台
- 微軟 Azure Blob
- NetAppStorageGRID

支援的系統

環境	協定	支援的版本
Amazon FSx for NetApp ONTAP*	CIFS、NFS 和 SAN	不適用
Azure NetApp Files	CIFS 和 NFS	不適用
適用於 AWS 的 Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN (iSCSI 和 NVMe)	9.17.1 及更高版本

環境	協定	支援的版本
適用於 Google Cloud Platform 的 Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN (iSCSI 和 NVMe)	9.17.1 及更高版本
適用於 Microsoft Azure 的 Cloud Volumes ONTAP	CIFS 和 NFS	9.12.1 及更高版本
	SAN (iSCSI 和 NVMe)	9.17.1 及更高版本
ONTAP (本地部署)	CIFS 和 NFS	9.11.1 及更高版本
	SAN (FC、iSCSI 和 NVMe)	9.17.1 及更高版本

* Amazon FSx for NetApp ONTAP 使用自主勒索軟體保護 (ARP) 而非 ARP/AI。有關兩者區別的更多信息，請參閱["ARP/AI"](#)。



在 ONTAP 中使用 ARP/AI 需要 ONTAP 9.16 或更高版本。+ ONTAP 不為 FabricPool FlexCache、FlexGroup 磁碟區、一致性群組掛載點磁碟區、掛載路徑磁碟區、離線磁碟區和資料保護 (DP) 磁碟區提供勒索軟體防護支援。請務必查看["ONTAP 中支援且不受支援的配置"](#)。

支援的工作負載資料來源

勒索軟體復原能力可保護主資料磁碟區上的以下基於應用程式的工作負載：

- 區塊儲存
- 資料庫:
 - 微軟 SQL 伺服器
 - 甲骨文
 - PostgreSQL
- NetApp 檔案分享
- VMware 資料儲存區

關鍵術語

了解一些與勒索軟體保護相關的術語可能會對您有所幫助。

- 保護：勒索軟體復原中的保護意味著確保使用保護策略定期在不同的安全域中進行快照和不可變備份。
- 工作負載：勒索軟體復原中的工作負載可以包括 Oracle 資料庫、VMware 資料儲存或檔案共用。

NetApp Ransomware Resilience 前提條件

為確保 NetApp Ransomware Resilience 的成功部署，請驗證您的操作環境、網路存取和網路瀏覽器是否已準備就緒。

請檢查並確保您符合以下要求。

支援的系統

請確保您使用的是受支援的系統：

環境	協定	支援的版本
Amazon FSx for NetApp ONTAP*	CIFS、NFS 和 SAN	不適用
Azure NetApp Files	CIFS 和 NFS	不適用
適用於 AWS 的 Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN (iSCSI 和 NVMe)	9.17.1 及更高版本
適用於 Google Cloud Platform 的 Cloud Volumes ONTAP	CIFS 和 NFS	9.11.1 及更高版本
	SAN (iSCSI 和 NVMe)	9.17.1 及更高版本
適用於 Microsoft Azure 的 Cloud Volumes ONTAP	CIFS 和 NFS	9.12.1 及更高版本
	SAN (iSCSI 和 NVMe)	9.17.1 及更高版本
ONTAP (本地部署)	CIFS 和 NFS	9.11.1 及更高版本
	SAN (FC、iSCSI 和 NVMe)	9.17.1 及更高版本

* Amazon FSx for NetApp ONTAP 使用自主勒索軟體保護 (ARP) 而非 ARP/AI。有關兩者區別的更多信息，請參閱 ["ARP/AI"](#)。

NetApp Console 需求

您的 NetApp Console 配置需要：

- 具有組織管理員權限的 NetApp Console 使用者帳戶，用於發現資源。
- 一個控制台組織和系統，其中至少有一個活動的控制台代理連接到 ["支援的系統"](#)。
 - 如果您的內部部署 ONTAP 叢集或 Cloud Volumes ONTAP 系統未在 Console 中設定，請參閱 ["了解如何配置控制台代理"](#) 和 ["標準控制台要求"](#)。



如果您在單一控制台組織中擁有多個控制台代理，則勒索軟體復原功能將掃描除控制台 UI 中目前選擇的代理之外的所有控制台代理中的 ONTAP 資源。

- 控制台代理必須具有 `cloudmanager-ransomware-protection` 容器處於活動狀態。
- 對於 ONTAP 或 Cloud Volumes ONTAP 叢集，Ransomware Resilience 要求 ONTAP 版本為 9.11.1 或更高版本。



若要在 SAN 工作負載上使用勒索軟體復原功能，您必須執行 ONTAP 9.17.1 或更高版本。

ONTAP 需求

- 您必須執行 ONTAP 9.11.1 或更高版本，並且在本機 ONTAP 實例上啟用 ONTAP One 授權。有關 ONTAP 支援的更多信息，請參閱 ["自主勒索軟體防護概述"](#)。
- 若要套用保護配置（例如啟用自主勒索軟體保護），勒索軟體復原能力需要 ONTAP 叢集上的管理員權限。ONTAP 叢集應該只使用 ONTAP 叢集管理員使用者憑證進行加入。



如果您已使用非管理員憑證將ONTAP叢集連接到控制台，則[您必須更新ONTAP叢集中的憑證](#update-non-admin-user-permissions-in-an-ontap-system)。

資料備份

- 在NetApp StorageGRID、AWS S3、Azure Blob 或 Google Cloud Platform 中擁有一個帳戶，用於備份目標，並配置了適當的存取權。

請參閱 ["AWS、Azure 或 S3 權限列表"](#) 了解詳情。

- 不需要在系統上啟用NetApp Backup and Recovery。

Ransomware Resilience 可透過「設定」選項配置備份目標位置。請參閱 ["新增備份目標"](#)。

可疑用戶行為要求

為了使 Ransomware Resilience 能夠發出有關可疑使用者行為的警報，您必須設定使用者活動代理程式。若要安裝使用者活動代理程式，請確保您的系統符合["要求"](#)。

更新ONTAP系統中的非管理員使用者權限

如果您需要更新特定系統中的非管理員使用者權限，請依照下列步驟操作。

1. 登入 Console。在儀表中，找到需要更新 ONTAP 使用者權限的系統。
2. 選擇系統以檢視其詳細資訊。
3. 選擇“查看其他資訊”以顯示使用者名稱。
4. 以管理員使用者身分登入ONTAP集群 CLI。
5. 顯示該使用者的現有角色：

```
security login show -user-or-group-name <username>
```

6. 更改使用者的角色。進入：

```
security login modify -user-or-group-name <username> -application  
console|http|ontapi|ssh|telnet -authentication-method password -role  
admin
```

7. 返回NetApp Console以使用勒索軟體復原功能。

NetApp Ransomware Resilience快速入門

了解設定勒索軟體保護功能和保護工作負載所需遵循的進階步驟。

請按照每個步驟中的連結獲取詳細資訊。

1

審查先決條件

這些任務需要 `_Console admin_` 角色。

- "確保已安裝控制台代理"
- "確保您的系統符合要求"
- "審查勒索軟體恢復使用者角色並為存取勒索軟體復原的使用者分配權限"
- "設定許可"

2

開始使用勒索軟體防禦

這些任務需要「勒索軟體復原管理員」角色。

- "在控制台中發現工作負載"
- "在儀表板上查看工作負載保護健康狀況"
- "（可選）進行勒索軟體攻擊準備演習"

3

在 **Ransomware Resilience** 中設定保護和偵測

這些任務需要「勒索軟體復原管理員」角色。配置可疑用戶行為活動需要額外的「勒索軟體恢復用戶行為管理員」角色。

- "保護工作負載"
 - 可選地，"透過配置可疑使用者活動偵測來增強保護"
- （可選）配置備份目標：
 - "準備NetApp StorageGRID、Amazon Web Services、Google Cloud Platform 或 Microsoft Azure 作為備份目標"。
 - "配置備份目標"
- "回應偵測到的潛在勒索軟體攻擊"
- "從攻擊中恢復（事件消除後）"

4

下一步是什麼？

在勒索軟體復原中配置保護後，您可以執行以下操作。

- "啟用資料分類來識別治理和安全風險"
- "向 SIEM 發送警報"
- "下載警報、保護、準備演習、恢復或摘要報告"

設定NetApp Ransomware Resilience

您可以輕鬆部署NetApp Ransomware Resilience。在開始之前，請查看["先決條件"](#)以確保您的環境已準備就緒。

準備備份目標

準備以下備份目標之一：

- NetAppStorageGRID
- 亞馬遜網路服務
- 谷歌雲端平台
- 微軟 Azure

在備份目的地本身設定選項後，稍後您需要將其設定為 Ransomware Resilience 中的備份目的地。有關如何在 Ransomware Resilience 中設定備份目的地的詳細資訊，請參閱 ["配置備份目標"](#)。

準備StorageGRID以成為備份目標

如果要使用StorageGRID作為備份目標，請參閱 ["StorageGRID文檔"](#)有關StorageGRID的詳細資訊。

準備 AWS 成為備份目標

- 在 AWS 中設定一個帳戶。
- 配置 ["AWS 權限"](#)在 AWS 中。

有關在控制台中管理 AWS 存儲的詳細信息，請參閱 ["管理您的 Amazon S3 儲存桶"](#)。

準備 Azure 以成為備份目標

- 在 Azure 中設定一個帳戶。
- 配置 ["Azure 權限"](#)在 Azure 中。

有關在控制台中管理 Azure 儲存體的詳細信息，請參閱 ["管理 Azure 儲存體帳戶"](#)。

設定NetApp Console

下一步是設定控制台和勒索軟體復原能力。

審查 ["標準模式的控制台要求"](#)。

建立控制台代理

聯絡您的NetApp銷售代表試用或使用此服務。然後，當您使用控制台代理時，它將包含適當的勒索軟體恢復功能。

若要使用勒索軟體復原功能建立控制台代理，請聯絡具有建立控制台代理權限的控制台組織管理員，並參考描述 ["如何建立控制台代理"](#)。



如果您有多個控制台代理，則勒索軟體復原功能會掃描除控制台中目前顯示的代理之外的所有控制台代理的資料。該服務發現與該組織相關的所有項目和所有控制台代理。

設定 NetApp Ransomware Resilience 的許可

NetApp Ransomware Resilience 提供不同的授權方案，讓您能夠在對貴組織有意義的地方訂閱服務。

要設定授權，您需要擁有 Organization admin、Folder 或 project admin 角色 "[了解控制台存取角色](#)"。

許可證類型

勒索軟體防護功能提供以下幾種許可類型：

- 30天免費試用
- 透過 Amazon Web Services (AWS) Marketplace、Google Cloud Marketplace 或 Azure Marketplace 購買即用即付 (PAYGO) 訂閱
- 自帶授權 (BYOL)：您從 NetApp 銷售代表取得的 NetApp 授權文件 (NLF)。您可以使用許可證序號在控制台中啟動 BYOL。

設定 BYOL 或購買 PAYGO 訂閱後，您可以在控制台的 Licenses and subscriptions 部分看到授權。

免費試用期結束或許可證或訂閱到期後，您仍然可以：

- 查看工作負載和工作負載健康狀況
- 刪除策略等資源
- 運行在試用期間或許可證下建立的所有計劃操作

其他許可證

勒索軟體恢復許可證不包括其他 NetApp 產品。但是，即使您沒有單獨的備份和復原許可證，勒索軟體復原能力也可以與 NetApp Backup and Recovery 整合。



如果您同時擁有備份和復原以及勒索軟體復原功能，則受這兩種產品保護的任何公開資料將僅由勒索軟體復原功能計費。

試試 Ransomware Resilience 30 天免費試用版

您可以免費試用 Ransomware Resilience 30 天。您必須是控制台組織管理員才能開始免費試用。

試用期間不強制執行儲存容量限制。

您可以隨時獲得許可證或訂閱，並且在 30 天試用期結束之前不會向您收費。要在 30 天試用期後繼續使用，您需要購買 BYOL 授權或 PAYGO 訂閱。

在試用期間，您可以使用全部功能。

步驟

1. 訪問 "安慰"。
2. 登入控制台。
3. 從NetApp Console中，選擇「保護」>「勒索軟體復原能力」。

如果這是您第一次登入此服務，則會出現登入頁面。

Ransomware Resilience
Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get full access to ransomware resilience with a 30-day free trial.

[Start 30-day free trial](#)

We won't read the contents of your data or change existing protection.

Identify and protect
Automatically identifies workloads at risk, recommends fixes, and protects with one-click

Detect and respond
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

Recover
Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

4. 如果您尚未為其他服務新增控制台代理，"添加一個"。
5. 在勒索軟體復原登陸頁面中，選擇*從發現工作負載開始*來發現您的工作負載。



僅當您成功安裝了控制台代理後，此選項才可用。

6. 要查看免費試用信息，請選擇右上角的下拉選項。

試用結束後，取得訂閱或授權

免費試用結束後，您可以透過其中一個市場進行訂閱，也可以從NetApp購買授權。

如果您已經擁有 PAYGO 訂閱，免費試用結束後許可證將自動切換到訂閱。

[透過 AWS Marketplace 訂閱](#) [透過 Microsoft Azure Marketplace 訂閱](#) [透過 Google Cloud Platform Marketplace 訂閱](#) [自帶授權 \(BYOL\)](#)

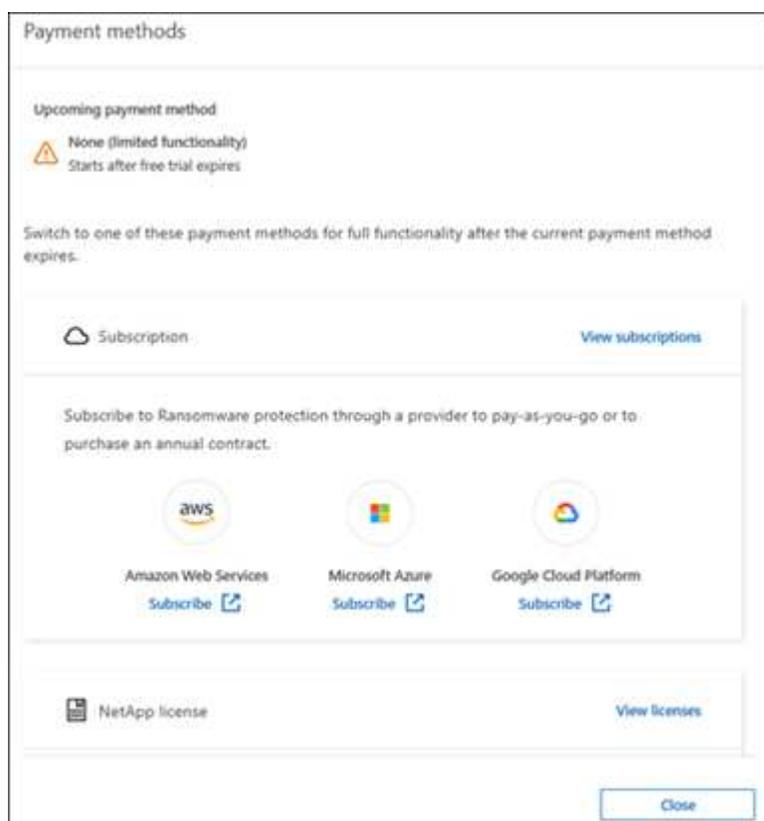
透過 AWS Marketplace 訂閱

此流程提供如何在 AWS Marketplace 中直接訂閱的高級概述。

步驟

1. 在「勒索軟體復原」中，執行以下操作之一：
 - 如果您收到一則訊息表示免費試用即將到期，請選擇*查看付款方式*。

- 如果您尚未開始試用，請選擇右上角的*免費試用*通知，然後選擇*查看付款方式*。



2. 在付款方式頁面中，選擇「訂閱」 **Amazon Web Services**。
3. 在 AWS Marketplace 中，選擇 查看購買選項。
4. 使用 AWS Marketplace 訂閱 * NetApp Intelligent Services* 和 * 勒索軟體復原能力 *。
5. 當您返回 Ransomware Resilience 時，會出現一則訊息表示您已訂閱。



系統會寄給您一封電子郵件，其中包含 Ransomware Resilience 序號，並表示您已在 AWS Marketplace 中訂閱 Ransomware Resilience。

6. 返回勒索軟體恢復付款方式頁面。
7. 透過選擇「新增許可證」將許可證新增至控制台。

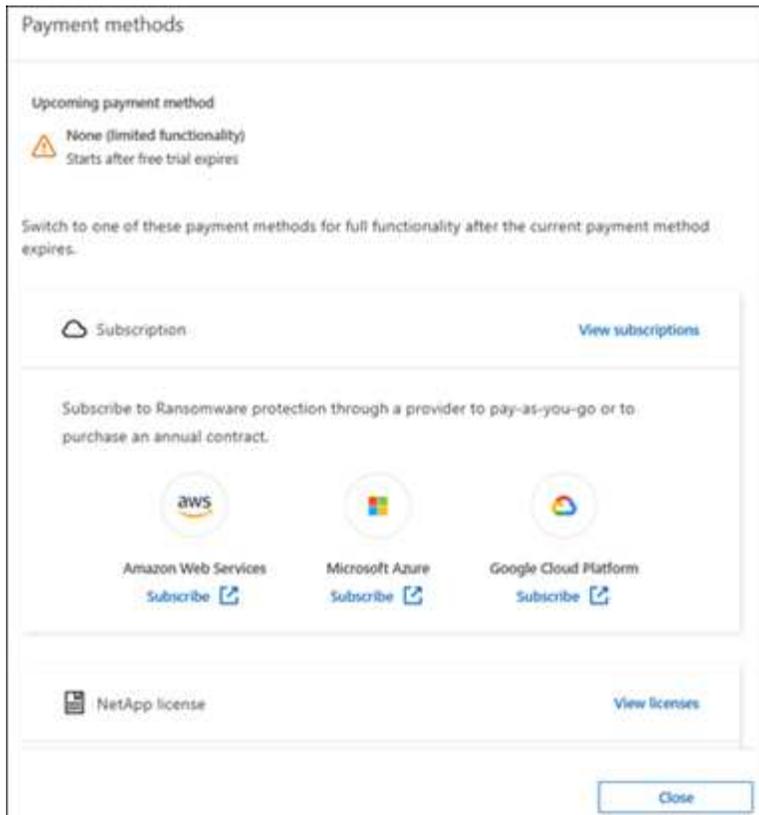
8. 在新增許可證頁面中，選擇*輸入序號*，輸入發送給您的電子郵件中包含的序號，然後選擇*新增許可證*。
9. 要查看許可證詳細信息，請從控制台左側導航中選擇“管理”>“**Licenses and subscriptions**”。
 - 若要查看訂閱訊息，請選擇*訂閱*。
 - 若要查看 BYOL 許可證，請選擇「資料服務許可證」。
10. 返回勒索軟體恢復能力。從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。
一則訊息確認許可證已新增。

透過 Microsoft Azure Marketplace 訂閱

此流程提供如何在 Azure 市場中直接訂閱的高級概述。

步驟

1. 在「勒索軟體復原」中，執行以下操作之一：
 - 如果您收到一則訊息表示免費試用即將到期，請選擇*查看付款方式*。
 - 如果您尚未開始試用，請選擇右上角的*免費試用*通知，然後選擇*查看付款方式*。



2. 在付款方式頁面中，選擇「訂閱」 **Microsoft Azure Marketplace**。
3. 在 Azure 市場中，選擇「查看購買選項」。
4. 使用 Azure Marketplace 訂閱 * NetApp Intelligent Services* 和 * 勒索軟體復原能力 *。
5. 當您返回 Ransomware Resilience 時，會出現一則訊息表示您已訂閱。



系統會寄給您一封電子郵件，其中包含 Ransomware Resilience 序號，並表示已在 Azure 市集訂閱 Ransomware Resilience。

6. 返回勒索軟體恢復付款方式頁面。
7. 若要新增許可證，請選擇*新增許可證*。

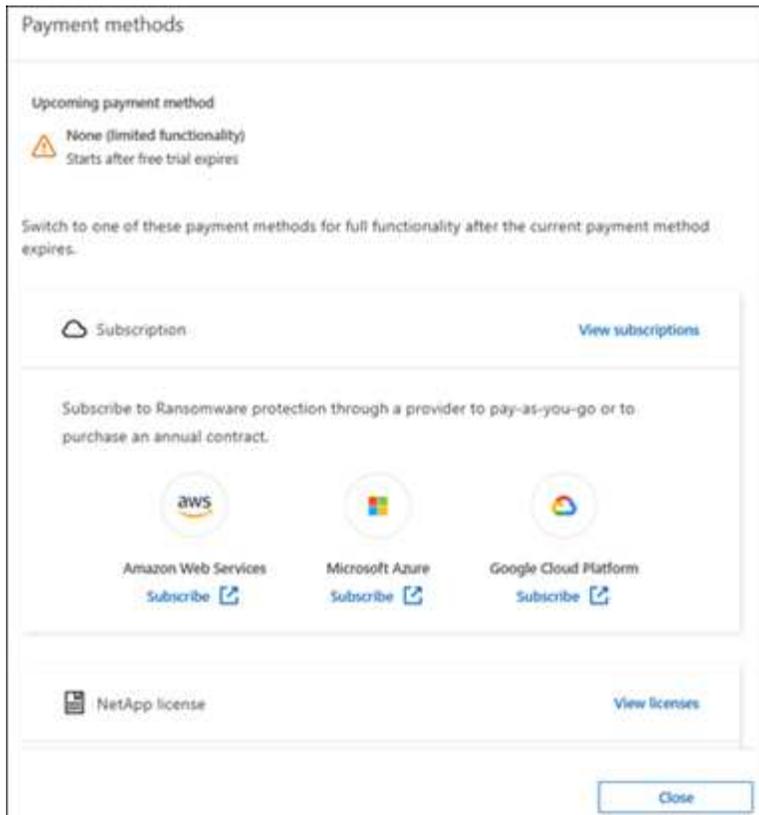
8. 在新增許可證頁面中，選擇*輸入序號*，然後輸入發送給您的電子郵件中的序號。選擇*新增許可證*。
9. 要查看Licenses and subscriptions中的許可證詳細信息，請從控制台左側導航中選擇“治理”>“Licenses and subscriptions”。
 - 若要查看訂閱訊息，請選擇*訂閱*。
 - 若要查看 BYOL 許可證，請選擇「資料服務許可證」。
10. 返回勒索軟體恢復能力。從控制台左側導航中，選擇*保護*>*勒索軟體恢復*。
出現一則訊息，表示已新增許可證。

透過 Google Cloud Platform Marketplace 訂閱

此流程概述如何在 Google Cloud Platform Marketplace 中直接訂閱。

步驟

1. 在勒索軟體復原中，執行以下操作之一：
 - 如果您收到一則訊息表示免費試用即將到期，請選擇*查看付款方式*。
 - 如果您尚未開始試用，請選擇右上角的*免費試用*通知，然後選擇*查看付款方式*。



2. 在付款方式頁面中，選擇「訂閱」 Google Cloud Platform Marketplace*。
3. 在 Google Cloud Platform Marketplace 中，選擇 訂閱。
4. 使用 Google Cloud Platform Marketplace 訂閱 * NetApp Intelligent Services* 和 * Ransomware Resilience*。
5. 當您返回 Ransomware Resilience 時，會出現一則訊息表示您已訂閱。



系統會寄給您一封電子郵件，其中包含 Ransomware Resilience 序號，並表示您已在 Google Cloud Platform Marketplace 中訂閱了 Ransomware Resilience。

6. 返回勒索軟體恢復付款方式頁面。
7. 若要將許可證新增至控制台，請選擇「新增許可證」。

8. 在新增許可證頁面中，選擇*輸入序號*。輸入發送給您的電子郵件中的序號。選擇*新增許可證*。
9. 要查看許可證詳細信息，請從控制台左側導航中選擇“治理”>“**Licenses and subscriptions**”。
 - 若要查看訂閱訊息，請選擇*訂閱*。
 - 若要查看 BYOL 許可證，請選擇「資料服務許可證」。
10. 返回勒索軟體恢復能力。從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。
 - 出現一則訊息，表示已新增許可證。

自帶授權 (BYOL)

如果您想自備許可證 (BYOL)，則需要購買許可證，取得NetApp許可證文件 (NLF)，然後將許可證新增至控制台。

將您的許可證文件新增至控制台

從NetApp銷售代表購買勒索軟體恢復許可證後，您可以透過輸入勒索軟體恢復序號和NetApp支援網站 (NSS) 帳戶資訊來啟動授權。

開始之前

您需要 Ransomware Resilience 序號。從您的銷售訂單中找到此號碼，或聯絡客戶團隊以取得此資訊。

步驟

1. 取得授權後，返回 Ransomware Resilience。選擇右上角的*查看付款方式*選項。或者，在免費試用即將到期的訊息中，選擇*訂閱或購買授權*。

2. 選擇「新增許可證」到控制台許可證和訂閱頁面。
3. 從「資料服務許可證」標籤中，選擇「新增許可證」。

Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

Enter Serial Number Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

Add License Cancel

4. 在「新增許可證」頁面中，輸入序號和NetApp支援網站帳戶資訊。
 - 如果您有控制台許可證序號並知道您的 NSS 帳戶，請選擇 輸入序號 選項並輸入該資訊。
如果您的NetApp支援網站帳號未從下拉清單中找到，["將 NSS 帳戶新增至控制台"](#)。
 - 如果您有 zvondlr 授權檔案（在暗站安裝時需要），請選擇 上傳授權檔案 選項並依照指示附加檔案。
5. 選擇*新增許可證*。

結果

Licenses and subscriptions頁面顯示 Ransomware Resilience 已取得授權。

控制台許可證到期後請更新

如果您的許可期限即將到期，或者您的許可容量已達到限制，您將在勒索軟體復原 UI 中收到通知。您可以在勒索軟體復原許可證到期之前進行更新，這樣您存取掃描資料的能力就不會受到干擾。



此訊息也出現在Licenses and subscriptions以及 ["通知設定"](#)。

步驟

1. 您可以發送電子郵件給支援人員以要求更新您的許可證。

在您支付許可證費用並在NetApp支援網站註冊後，控制台會自動更新許可證。數據服務許可證頁面將在 5 到 10 分鐘內反映變更。

2. 如果控制台無法自動更新許可證，則需要手動上傳許可證文件。
 - a. 您可以從NetApp支援網站取得許可證文件。
 - b. 在控制台中，選擇管理 > **Licenses and subscriptions**。
 - c. 選擇“資料服務許可證”選項卡，選擇要更新的序號的“操作...”圖標，然後選擇“更新許可證”。

結束 PAYGO 訂閱

如果您想終止 PAYGO 訂閱，您可以隨時終止。

步驟

1. 在 Ransomware Resilience 中，在右上角選擇授權選項。
2. 選擇*查看付款方式*。
3. 在下拉詳細資料中，取消勾選「目前付款方式過期後使用」方塊。
4. 選擇*儲存*。

更多資訊

- ["NetApp Console授權和訂閱文檔"](#)

在 NetApp Ransomware Resilience 中發現並管理工作負載

在使用NetApp Ransomware Resilience之前，它首先需要發現工作負載資料。在發現過程中，勒索軟體復原力會分析組織內所有控制台代理程式和專案系統中的所有捲和檔案。

在「發現」儀表中，「勒索軟體復原能力」顯示受支援且不受支援的系統配置。勒索軟體復原能力評估 Oracle 應用程式、VMware 資料儲存、檔案共用和區塊儲存。



勒索軟體復原能力無法發現使用FlexGroup 的磁碟區的工作負載。

勒索軟體復原能力會檢查您目前的備份保護、快照副本和NetApp自主勒索軟體保護選項。勒索軟體復原能力還可以偵測來自SnapCenter for VMware（用於 VM 資料儲存）、SnapCenter for Oracle 和NetApp Backup and Recovery（用於檔案共用和 VM 檔案共用）的保護資訊。然後它會推薦一些改善勒索軟體防護的方法。



雖然 Ransomware Resilience 可以識別來自 SnapCenter 的原則，但您無法透過 SnapCenter 使用 Ransomware Resilience 執行還原。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。["了解NetApp Console的勒索軟體復原角色"](#)。

選擇要發現和保護的工作負載

在每個控制台代理程式中，選擇您想要發現工作負載的系統。

步驟

1. 從NetApp Console中，選擇 保護 > 勒索軟體保護。

如果這是您的第一次登錄，則會出現登入頁面。

Ransomware Resilience
Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get full access to ransomware resilience with a 30-day free trial.

[Start 30-day free trial](#)

We won't read the contents of your data or change existing protection.

Identify and protect
Automatically identifies workloads at risk, recommends fixes, and protects with one-click

Detect and respond
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

Recover
Restores workloads in minutes through simplified, orchestrated workload-consistent recovery



如果您開始免費試用，開始 30 天免費試用*按鈕標籤將更改為*透過發現工作負載開始*。

2. 從初始登入頁面，選擇*從發現工作負載開始*。

勒索軟體復原力可發現受支援和不受支援的系統。此過程可能需要幾分鐘。

Discover workloads

Discover workloads

Find systems in your NetApp Console Agents. Then, select the systems in each Agent where you want to discover workloads.

Agents (3)

aws-connector-us-east-1	Provider: AWS Region: us-east-1	2/4	Select systems
gcp-connector-demo	Provider: GCP Region: us-east1	0/2	Select systems
onprem-connector	Provider: On-premises ONTAP Region: OnPrem	1/2	Select systems

Systems with no Agent (3)

Ransomware resilience won't discover systems with no Agent.

Systems (3)

Cancel Discover

3. 若要發現特定控制台代理程式的工作負載，請選擇要發現工作負載的控制台代理旁邊的「選擇系統」。
4. 選擇您想要發現工作負載的系統。

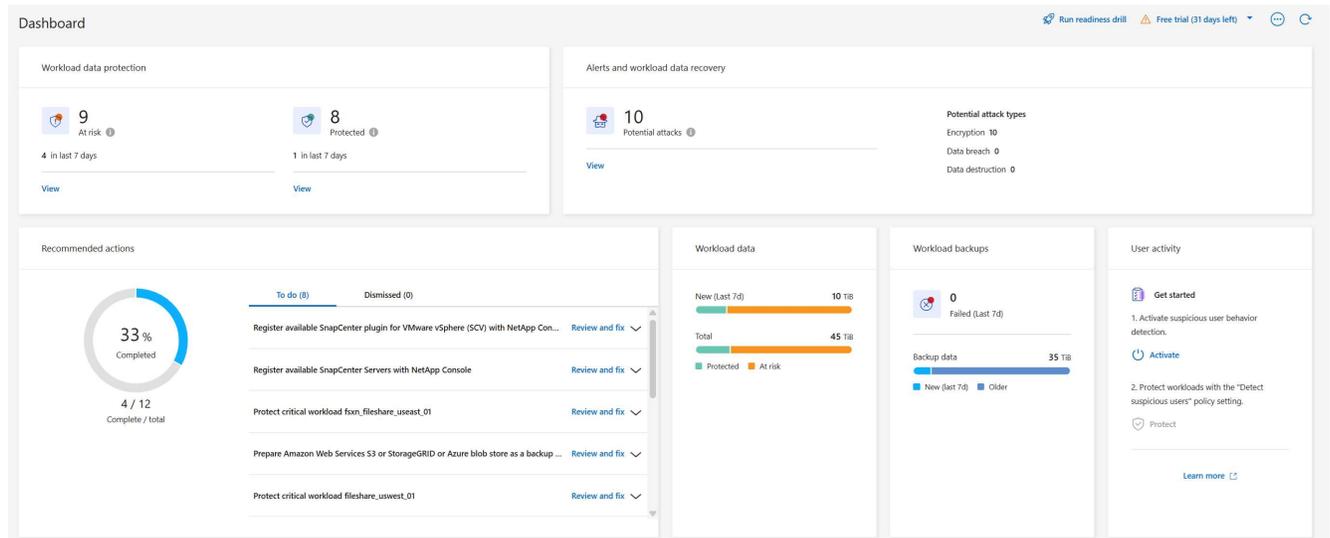
5. 選擇*發現*。

勒索軟體復原能力僅在選擇系統時才會發現工作負載資料。發現過程可能需要幾分鐘。

6. 若要下載已發現的工作負載列表，請選擇*下載結果*。

7. 若要顯示勒索軟體恢復儀表板，請選擇「前往儀表板」。

儀表板顯示資料保護健全狀況。存在風險或受到保護的工作負載數量會隨著新工作負載的發現而更新。



"了解儀表板顯示的內容。"

發現先前選定的系統新建立的工作負載

如果您已向先前發現的系統新增了工作負載，則需要重新啟動發現以保護新的工作負載。

步驟

1. 要確定上次發現的時間，請查看勒索軟體恢復儀表板右上角「刷新」圖示旁的日期和時間戳記。
2. 從控制台中、選取 **Refresh** 圖示以尋找新的工作負載。



如果您發現已發現的系統中存在未顯示的捲，則這些卷可能不受支援。若要尋找不支援的磁碟區列表，請前往「設定」選單，然後選擇「工作負載發現」卡中的操作選單，下載支援和不支援的磁碟區的 JSON 報表。

發現新系統

如果您已經探索工作負載，可以尋找新的或先前未選取的工作負載。

步驟

1. 從 Ransomware Resilience 中、選取 **Settings**。
2. 在工作負載發現卡中，選擇*發現工作負載*。發現過程可能需要幾分鐘。載入圖示顯示進度。
3. 勒索軟體復原力可以發現受支援和不受支援的系統。如果系統的ONTAP版本低於所需版本，則不支援該系統。當您將滑鼠停留在某個不支援的系統上時，工具提示會顯示原因。選擇您想要發現工作負載的系統。

4. 選擇*發現*。

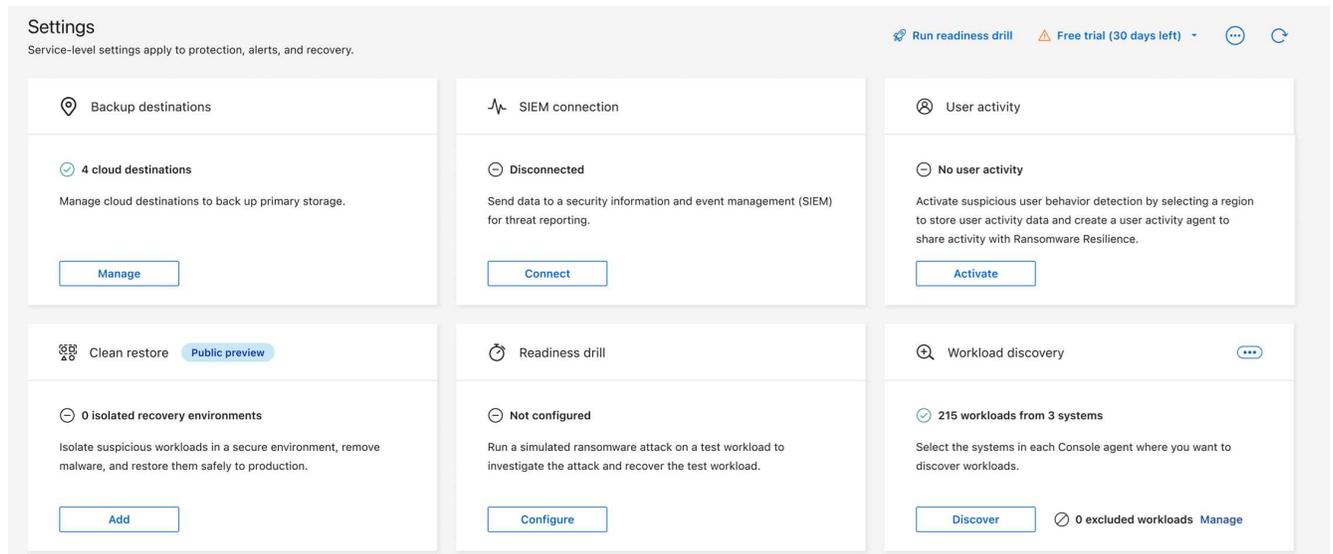
排除工作負載

勒索軟體復原功能可讓您將系統中的特定工作負載排除在勒索軟體保護和偵測之外。

您只能排除受支援且已成功發現的工作負載。您可以隨時修改已排除的工作負載清單。對於未納入勒索軟體復原功能的工作負載，您無需付費。

將工作負載新增至排除的工作負載清單中

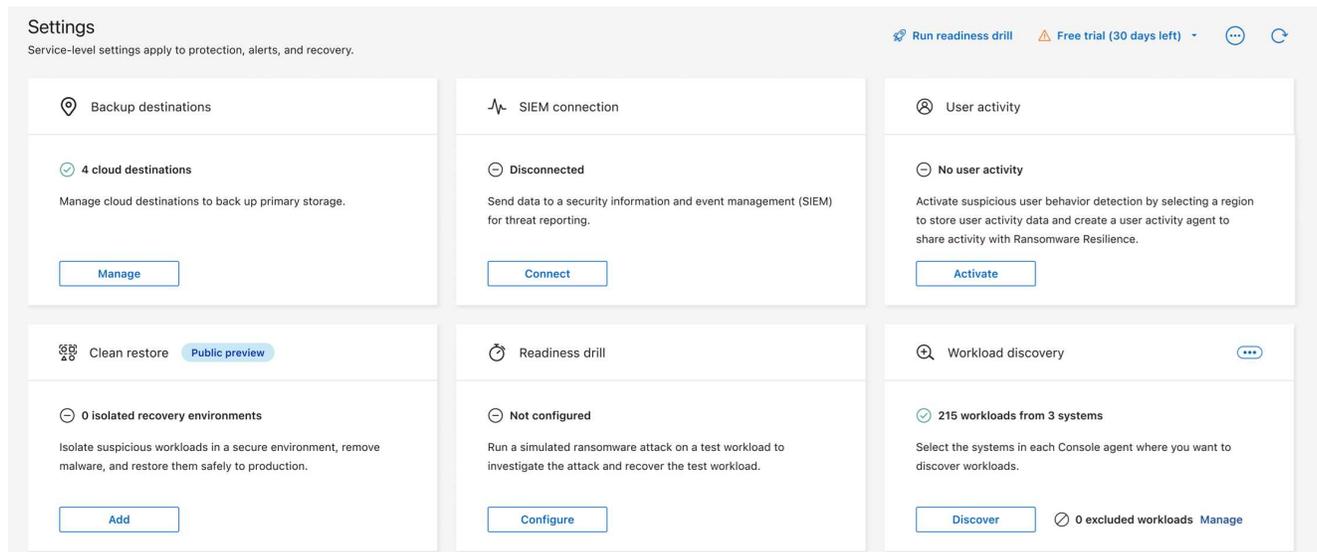
1. 在勒索軟體恢復功能中，選擇設定。
2. 在「設定」儀表板中，找到「工作負載發現」儀表板。該卡片標明了已排除的工作負載數量。若要新增工作負載，請在排除的工作負載旁邊選擇管理。



3. 在「排除的工作負載」頁面中，選擇新增。
4. 選擇要排除的工作負載，然後按一下新增。
5. 請查看「已排除的工作負載」頁面，以了解已排除的工作負載。新增工作負載時，其名稱旁會顯示進度指示器。如果工作負載未成功排除，則不會顯示在頁面上。

從排除的工作負載清單中移除工作負載

1. 在勒索軟體恢復功能中，選擇設定。
2. 在「設定」儀表板中，找到「工作負載發現」儀表板。該卡片標明了已排除的工作負載數量。在排除的工作負載旁邊，選擇管理。

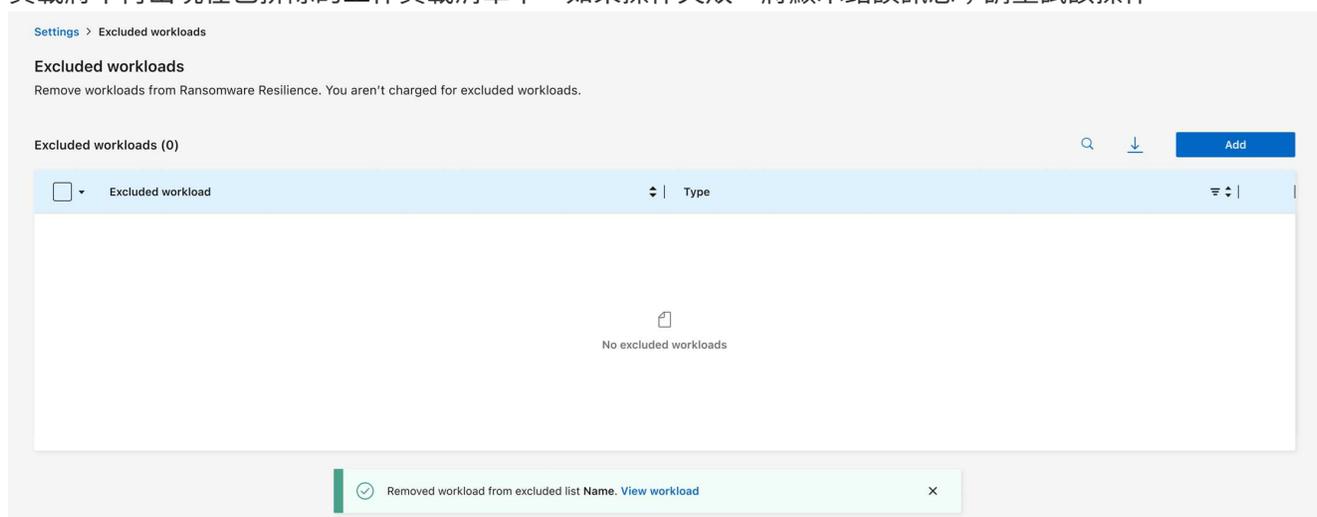


3. 若要從排除清單中刪除單一工作負載，請選擇要刪除的工作負載的操作功能表。

若要刪除多個工作負載，請選取要刪除的工作負載旁的複選框，然後選擇從排除清單中刪除。

4. 在對話方塊中，選擇「刪除」以確認要從排除清單中刪除工作負載。

5. 如果成功從排除的工作負載清單中刪除工作負載，則「排除的工作負載」頁面上將顯示成功訊息，且該工作負載將不再出現在已排除的工作負載清單中。如果操作失敗，將顯示錯誤訊息；請重試該操作。



使用勒索軟體彈性

存取NetApp Ransomware Resilience

若要存取 NetApp Ransomware Resilience，您必須透過 NetApp Console 登入。

若要登入控制台，您可以使用您的NetApp支援網站憑證，也可以使用您的電子郵件和密碼註冊NetApp雲端登入。["了解有關登入的更多信息"](#)。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。["了解NetApp Console的勒索軟體復原角色"](#)。

步驟

1. 打開網頁瀏覽器並前往["主機"](#)。

出現控制台登入頁面。

2. 登入控制台。
3. 從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。

如果這是您第一次登入此服務，則會出現登入頁面。



如果您沒有控制台代理或它不是此服務的代理，則需要部署一個。["了解如何設定控制台代理"](#)。

Ransomware Resilience
Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get full access to ransomware resilience with a 30-day free trial.

[Start 30-day free trial](#)

We won't read the contents of your data or change existing protection.



Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click



Detect and respond

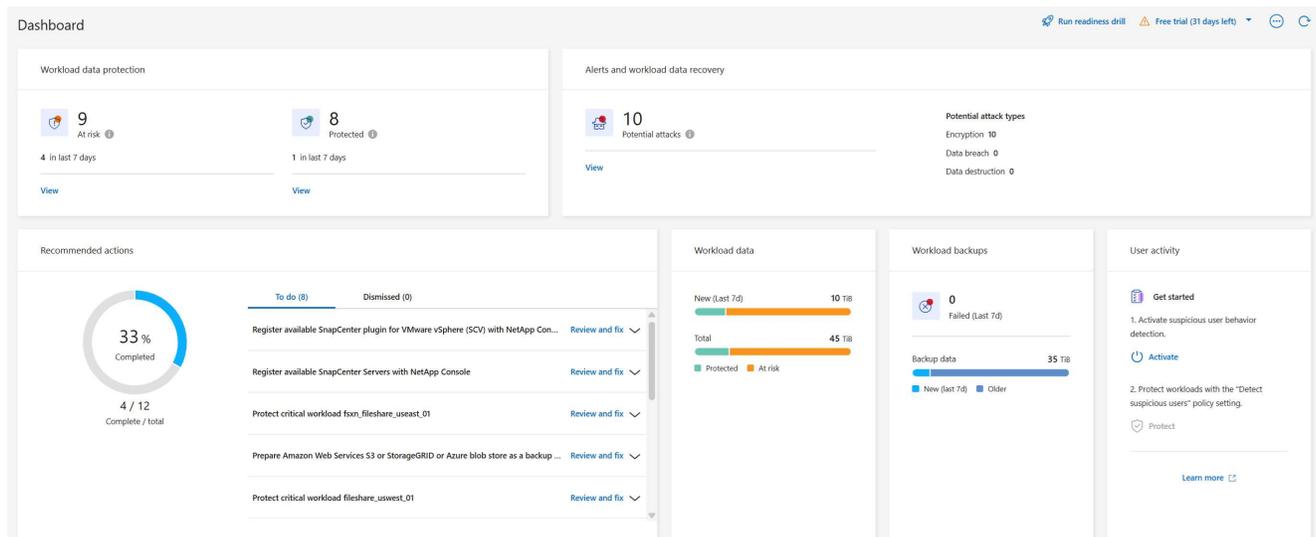
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point



Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

否則，將出現勒索軟體復原力儀表板。



4. 如果您還沒有這樣做，請選擇「發現工作負載」選項。

請參閱["發現工作負載"](#)。

在 NetApp Ransomware Resilience 中監控工作負載健全狀況

NetApp Ransomware Resilience 儀表板可讓您一目了然地了解工作負載的保護狀況。您可以快速確定哪些工作負載有風險或已受到保護、識別受事件影響或正在復原的工作負載，並透過查看受保護或有風險的儲存量來評估保護程度。

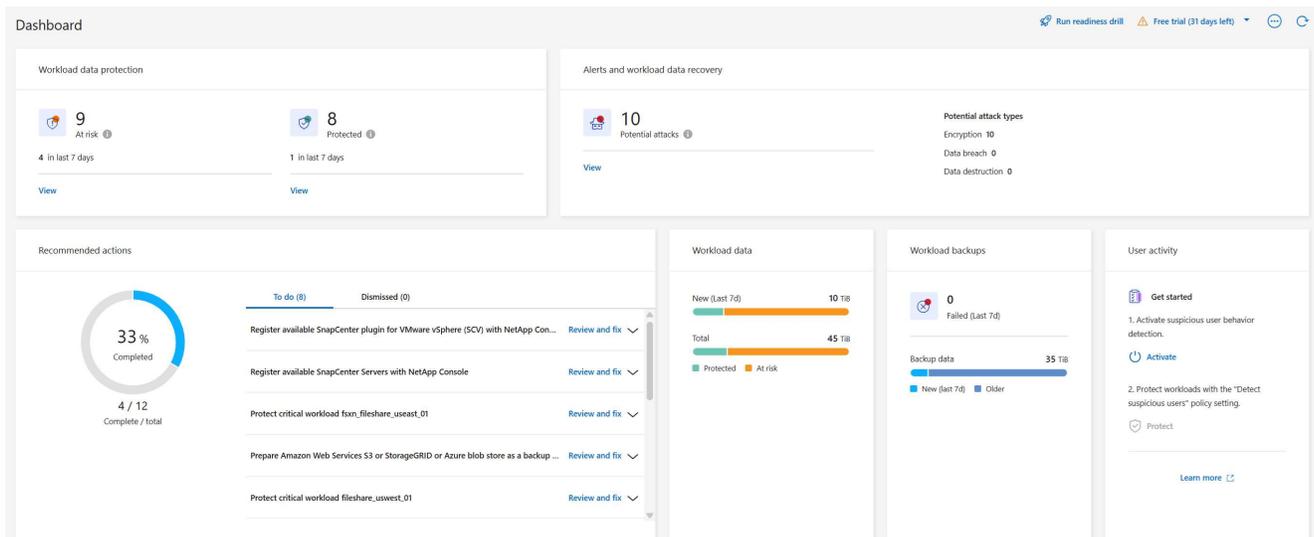
使用儀表板檢視保護建議、變更設定及下載報告。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。["了解NetApp Console的勒索軟體復原角色"](#)。

使用儀表板檢視工作負載健全狀況

步驟

1. 控制台發現您的工作負載後，勒索軟體恢復儀表板將顯示工作負載資料保護健康狀況。



2. 從儀表板中，您可以在每個窗格中執行下列動作：

- 工作負載資料保護：選擇*查看全部*可在保護頁面上查看所有處於危險中或受保護的工作負載。當保護等級與保護策略不符時，工作負載就會面臨風險。請參閱["保護工作負載"](#)。



選擇“i”工具提示即可查看有關此數據的提示。若要增加工作量限制，請選擇此 i 註解內的增加工作量限制。選擇此選項將帶您進入控制台支援頁面，您可以在其中建立案例單。

- 警報和工作負載資料復原：選擇*查看全部*可查看已影響您的工作負載的活動事件、在事件消除後準備恢復的事件或正在復原的事件。請參閱["響應偵測到的警報"](#)。
 - 事件分為以下狀態之一：
 - 新的
 - 已解散
 - 解散
 - 已解決
 - 警報可以具有以下狀態之一：
 - 新的
 - 不活躍
 - 工作負載可以具有以下還原狀態之一：
 - 需要恢復
 - 進行中
 - 已恢復
 - 失敗的
- 建議的措施：為了增強保護，請查看每項建議，然後選擇*查看並修復*。

請參閱 ["在控制面板上檢視保護建議"](#) 或 ["保護工作負載"](#)。

Ransomware Resilience 會顯示您上次造訪儀表板後的新建議，並附有「New」標籤，持續 24 小時。

動作會按優先順序顯示，最重要的顯示在頂部。檢閱、執行或忽略每個建議。

總操作數不包括您已忽略的操作。

- 工作負載資料：監控過去 7 天內保護覆蓋範圍的變化。
- 工作負載備份：監控過去 7 天內由勒索軟體復原所建立的失敗或成功完成的工作負載備份的變更。

在儀表板上檢視保護建議

勒索軟體復原能力會評估您工作負載的保護情況，並建議採取措施來改善保護。

您可以查看建議並採取行動，這會將建議狀態變更為「完成」。或者，如果您想稍後採取行動，您可以忽略它。忽略某項操作會將建議移至已忽略操作清單中，以便您稍後查看。

以下是 Ransomware Resilience 提供的一些建議。

推薦	描述	如何解決
增加勒索軟體保護策略。	工作負載目前不受保護。	為工作負載分配策略。請參閱 "保護工作負載免受勒索軟體攻擊" 。
連接到 SIEM 進行威脅報告。	將資料傳送到安全性和事件管理系統 (SIEM) 進行威脅分析和偵測。	輸入 SIEM/XDR 伺服器詳細資訊以啟用威脅偵測。請參閱 "連線至 SIEM" 。
改善系統的安全態勢	NetApp Digital Advisor 已發現至少一個高或嚴重的安全風險。	審查 NetApp Digital Advisor 中的所有安全風險。參考 "Digital Advisor 文檔" 。
使政策更加有力。	某些工作負載可能沒有足夠的保護。透過策略加強對工作負載的保護。	增加保留、新增備份、強制執行不可變備份、阻止可疑檔案副檔名、啟用二級儲存偵測等。請參閱 "保護工作負載免受勒索軟體攻擊" 。
準備 <備份提供者> 作為備份目標來備份您的工作負載資料。	工作負載目前沒有任何備份目標。	為該工作負載新增備份目標以保護它。請參閱 "新增備份目標" 。
保護關鍵或高度重要的應用程式工作負載免受勒索軟體的攻擊。	保護頁面顯示未受保護的關鍵或高度重要（基於分配的優先順序）應用程式工作負載。	為這些工作負載分配策略。請參閱 "保護工作負載免受勒索軟體攻擊" 。
保護關鍵或高度重要的文件共享工作負載免受勒索軟體的侵害。	保護頁面顯示未受保護的檔案共用或資料儲存類型的關鍵或高度重要的工作負載。	為每個工作負載分配策略。請參閱 "保護工作負載免受勒索軟體攻擊" 。請參閱 "保護工作負載免受勒索軟體攻擊" 。
查看新警報。	存在新的警報。	查看新警報。請參閱 "響應檢測到的勒索軟體警報" 。

步驟

1. 從勒索軟體復原中的「建議動作」窗格中，選擇一個建議，然後選擇「檢視並修復」。
2. 若要稍後再取消該操作，請選擇「取消」。

該建議將從「待辦事項」清單中清除並出現在「已忽略」清單中。



您稍後可以將已消除的項目變更為待辦事項。當您將某項標記為已完成或將已解除的項目變更為待辦事項時，總運算元會增加 1。

3. 要查看有關如何根據建議採取行動的信息，請選擇*訊息*圖示。

將保護資料匯出到 CSV 文件

您可以匯出資料並下載顯示保護、警報和復原詳細資訊的 CSV 檔案。

您可以從任何主選單選項下載 CSV 檔案：

- 保護：包含所有工作負載的狀態和詳細信息，包括勒索軟體彈性標記為受保護或處於危險中的工作負載總數。
- 警報：包括所有警報的狀態和詳細信息，包括警報總數和自動快照。
- 恢復：包括需要恢復的所有工作負載的狀態和詳細信息，包括勒索軟體恢復標記為「需要恢復」、「進行中」、「恢復失敗」和「成功恢復」的工作負載總數。

從網頁下載的 CSV 檔案僅包含該網頁中的資料。

CSV 檔案包含所有控制台系統上所有工作負載的資料。

步驟

1. 在勒索軟體復原能力控制面板中，選擇「刷新」。  右上角有刷新檔案中顯示的資料的選項。
2. 執行下列操作之一：
 - 從頁面上選擇“下載”按鈕。  選項。
 - 從勒索軟體恢復選單中，選擇*報告*。
3. 如果您選擇了「報告」選項，請選擇預先配置的命名文件，然後選擇「下載 (CSV)」或「下載 (JSON)」。

存取技術文檔

您可以從以下位置存取勒索軟體復原技術文檔"docs.netapp.com"或從勒索軟體恢復力內部。

步驟

1. 從勒索軟體復原力儀表板中，選擇垂直*操作*  選項。
2. 選擇以下選項之一：
 - 新功能 查看發行說明中目前或先前版本的功能資訊。
 - 文件 檢視勒索軟體復原文件首頁和此文件。

保護和偵測

在 NetApp Ransomware Resilience 中檢視保護狀態

NetApp Ransomware Resilience 的保護儀表板提供工作負載保護狀態和就緒情況的概覽。使用保護儀表板，您可以深入了解哪些內容已受到保護、哪些內容需要保護以及保護範圍。

一旦您了解目前保護的範圍，"[您可以為您的工作負載建立和套用勒索軟體防護策略](#)"

檢視工作負載的保護

保護工作負載的第一步是查看目前工作負載及其保護狀態。您可以看到以下類型的工作負載：

- 應用程式工作負載
- 阻止工作負載
- 檔案共享工作負載
- 虛擬機器工作負載

步驟

1. 從控制台左側導覽列中選擇“保護”>“勒索軟體恢復”。
2. 執行下列操作之一：
 - 在儀表板的「資料保護」窗格中、選取 **View all** 。
 - 從選單中選擇*保護*。

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

3. 在此頁面中，您可以查看和變更工作負載的保護詳細資料。



請參閱"[增加勒索軟體防護策略](#)"以瞭解在已有 NetApp Backup and Recovery 保護原則的情況下使用 NetApp Ransomware Resilience 。

了解保護儀表板

Ransomware Resilience 中的防護儀表板除了顯示防護狀態的相關資訊外，還提供有關工作負載的詳細資訊（例如，工作負載名稱和類型、Console 代理、系統和儲存虛擬機器）。使用防護儀表板可以查看和管理工作負載的勒索軟體防護準備。以下欄位對於了解您的防護狀況特別重要：

保護狀態：工作負載可以顯示下列保護狀態之一，以指示是否套用了政策：

- 受保護：已套用原則。與工作負載相關的所有磁碟區上均啟用了 ARP（或 ARP/AI，取決於 ONTAP 版本）。
- 存在風險：未應用任何保單。如果工作負載沒有啟用主要偵測策略，那麼即使啟用了快照和備份策略，它仍然「處於危險之中」。
- 進行中：政策正在應用但尚未完成。
- 失敗：策略已套用但不起作用。

偵測狀態：

+ Ransomware Resilience 可協助您了解已在工作負載上配置的勒索軟體偵測原則的範圍。請使用以下欄位檢視偵測範圍。

- 加密偵測狀態
- 可疑使用者行為偵測狀態
- 封鎖可疑的檔案副檔名

Snapshot、replication 和 backup 策略：此欄顯示管理該策略的產品或服務。如果沒有策略，則該欄位顯示 N/A。

重要性

勒索軟體復原能力根據對每個工作負載的分析，在發現過程中為每個工作負載分配重要性或優先順序。工作負載重要性由下列快照頻率決定：

- 關鍵：每小時會建立多個快照副本（高度激進的保護計畫）
- 重要提示：快照副本的建立頻率低於每小時一次，但高於每天一次。
- 標準：每天拍攝多次快照副本

隱私洩漏：選擇此選項以["使用 NetApp Data Classification 掃描個人可識別資訊"](#)。

Replication destination：如果您已設定 snapshot 複寫，則會列出目標儲存 VM 和系統的名稱。如果沒有複寫，此欄位將顯示「N/A」。

備份目標：如果您已設定了具有備份的 ransomware protection 策略，則備份目標系統的名稱將在此處列出。

後續步驟

- ["使用勒索軟體保護策略保護工作負載"](#)
- ["管理保護群組"](#)
- ["掃描個人識別資訊"](#)

在 NetApp Ransomware Resilience 中新增備份目的地

當 NetApp Ransomware Resilience 發現工作負載時、如果已設定備份、Ransomware Resilience 會辨識備份目的地。如果您打算使用備份做為 "勒索軟體防護策略" 的一部分、但尚未在工作負載上設定備份目的地、則必須在 NetApp Ransomware Resilience 中新增備份目的地、以提高網路恢復能力。

您可以選擇以下備份目標位置之一：

- NetAppStorageGRID
- 亞馬遜網路服務 (AWS)
- 谷歌雲端平台
- 微軟 Azure



Amazon FSx for NetApp ONTAP 和 Azure NetApp Files 中的工作負載無法使用備份目標。請使用原生備份解決方案執行備份作業：FSx for ONTAP 備份服務或 Azure NetApp Files 備份。

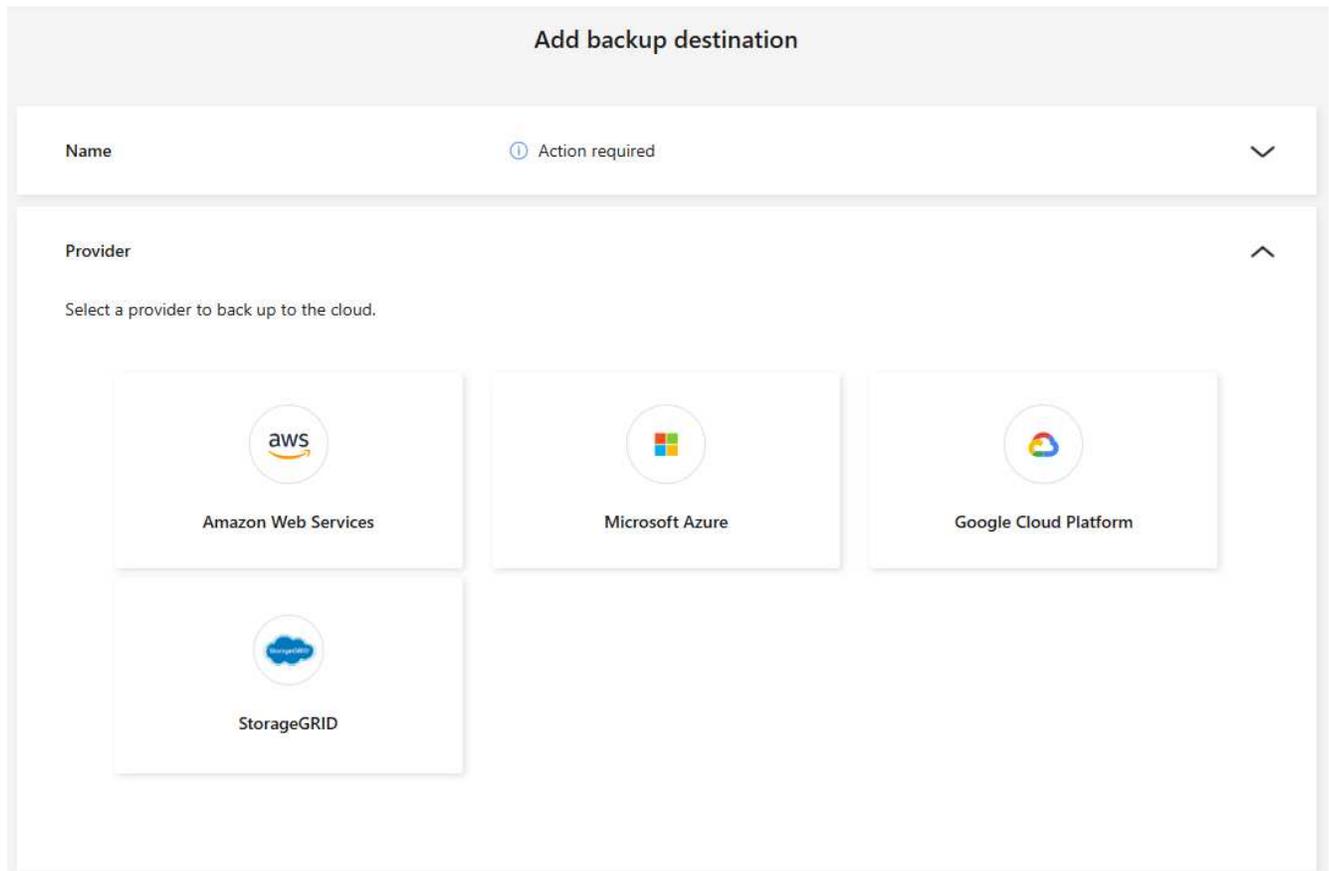
所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

新增StorageGRID作為備份目標

若要將NetApp StorageGRID設定為備份目標，請輸入下列資訊。

步驟

1. 在勒索軟體恢復功能中，選擇設定。
2. 在 **Backup Destinations** 磁貼中、選取 **View**。
3. 選擇新增。
4. 輸入備份目標的名稱。



5. 選擇* StorageGRID*。

6. 選取每個設定旁的向下箭頭以檢視必填欄位：

- 提供者設定：
 - 選擇 **Create a new bucket** 或 **Bring your own bucket**。
 - 請提供 **Gateway** 節點完全限定網域名稱（FQDN）和 **Port**。
 - 提供 StorageGRID 憑證：存取金鑰和秘密金鑰。
- 網路：選擇 IP 空間。
 - IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
- 備份鎖定

選擇是否要設定備份鎖定。使用備份鎖定时、複本會受到保護、避免遭到修改或刪除、並掃描勒索軟體威脅。設定備份目的地之後、您無法修改此設定。如果您不想要備份鎖定、請選取 **None**。選取 **Governance mode**、允許具有特定權限的使用者在保留期間覆寫或刪除受保護的備份檔案。選取 **Compliance mode****、防止使用者在保留期間覆寫或刪除受保護的備份檔案。

7. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。

Settings > Backup destinations

Backup destinations

Backup destinations (5) 🔍 ⬇️ Add

Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
aws	netapp-backup-vsavhk7dpp	us-east-1	n/a	Default	None	ViaWorkingEnvironment-VHk7DFp	Backup and Recovery
aws	netapp-backup-vsac2gmsuu	us-east-1	n/a	Default	None	ViaWorkingEnvironment-C2Gmsuu	Backup and Recovery
aws	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
aws	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
aws	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience

新增 Amazon Web Services 作為備份目標

若要將 AWS 設定為備份目標，請輸入以下資訊。

有關在 Console 中管理 AWS 儲存的詳細資訊，請參閱 ["管理您的 Amazon S3 儲存桶"](#)。

步驟

1. 在勒索軟體恢復功能中，選擇設定。
2. 在 **Backup Destinations** 磁貼中、選取 **View**。
3. 選擇新增。
4. 選擇*Amazon Web Services*。
5. 選擇每個設定旁邊的向下箭頭並輸入或選擇值：

- 提供者設定：

- 建立一個新的儲存桶，如果控制台中已經存在儲存桶，請選擇一個現有儲存桶，或使用您自己的儲存桶來儲存備份。
- AWS 帳戶、區域、AWS 憑證的存取金鑰和金鑰

["如果您想要自備儲存桶，請參閱新增 S3 儲存桶"](#)。

- 加密：如果您正在建立新的 S3 儲存桶，請輸入提供者提供給您的加密金鑰資訊。如果您選擇現有儲存桶，加密資訊已經可用。

預設情況下，儲存桶中的資料使用 AWS 管理的金鑰加密。您可以繼續使用 AWS 管理的金鑰，也可以使用您自己的金鑰管理資料的加密。

- 網路：選擇 IP 空間以及是否使用私有端點。

- IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
- 或者，選擇是否使用您先前配置的 AWS 私人終端節點 (PrivateLink)。

如果您想使用 AWS PrivateLink，請參閱 ["適用於 Amazon S3 的 AWS PrivateLink"](#)。

- 備份鎖定：選擇是否希望勒索軟體復原功能保護備份不被修改或刪除。此選項使用 NetApp DataLock 技術。每個備份將在保留期內鎖定，或至少 30 天，再加上最多 14 天的緩衝期。



如果現在配置備份鎖定設定，則在配置備份目的地後將無法變更該設定。

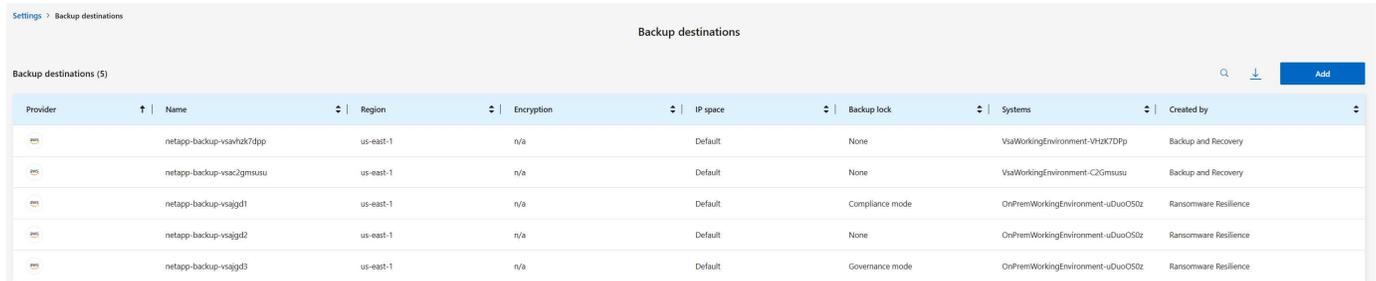
- 治理模式：特定使用者（具有 s3:BypassGovernanceRetention 權限）可以在保留期間內覆寫或刪除受保護的檔案。

- 合規模式：使用者在保留期間內無法覆寫或刪除受保護的備份檔案。

6. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。



Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
NetApp	netapp-backup-vsavhzk7dpp	us-east-1	n/a	Default	None	VisaWorkingEnvironment-VHk7DTP	Backup and Recovery
NetApp	netapp-backup-vsac2gmsusu	us-east-1	n/a	Default	None	VisaWorkingEnvironment-C2Gmsusu	Backup and Recovery
NetApp	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
NetApp	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
NetApp	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience

新增 Google Cloud Platform 作為備份目標

若要將 Google Cloud Platform (GCP) 設定為備份目標，請輸入以下資訊。

有關在 Console 中管理 GCP 儲存的詳細資訊，請參閱 ["Google Cloud 中的控制台代理安裝選項"](#)。

步驟

1. 在勒索軟體恢復功能中，選擇設定。
2. 在 **Backup Destinations** 磁貼中、選取 **View**。
3. 選擇新增。
4. 輸入備份目標的名稱。
5. 選擇*Google Cloud Platform*。
6. 選擇每個設定旁邊的向下箭頭並輸入或選擇值：
 - 提供者設定：
 - 選擇 **Create a new bucket** 或 **Bring your own bucket**。
 - 提供 Google Cloud Platform 憑證：存取金鑰和秘密金鑰。
 - 選取您的 **Project** 及其所在的 **Region**。

Add backup destination

Name	✔ gcp-backup	▼
Provider	✔ Google Cloud Platform	▼
Provider settings ▲		
<input checked="" type="radio"/> Create new bucket <input type="radio"/> Bring your own bucket		
<small>Netapp ransomware resilience will create the bucket in your provider environment.</small>		
Google Cloud Platform credentials		
Access key	Secret key 👁	
<input type="text"/>	<input type="text"/>	
Google Cloud Platform details		
Project	Region	
<input type="text" value="Select project"/> ▼	<input type="text" value="Select region"/> ▼	
Encryption ▼		
<input checked="" type="radio"/> Google-managed key		
Backup lock ▼		
⚠ Not supported		

- 加密：如果您正在建立新的儲存桶，請輸入提供者提供給您的加密金鑰資訊。如果您選擇現有儲存桶，加密資訊已經可用。

儲存桶中的資料預設使用 Google 管理的金鑰進行加密。您可以選取 **Google** 管理的金鑰 繼續使用預設設定，或使用 **客戶**管理的金鑰。

7. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。

新增 **Microsoft Azure** 作為備份目標

若要將 Azure 設定為備份目標，請輸入以下資訊。

有關在控制台中管理 Azure 憑證和市場訂閱的詳細信息，請參閱 ["管理 Azure 憑證和市集訂閱"](#)。

步驟

1. 在勒索軟體恢復功能中，選擇設定。
2. 在 **Backup Destinations** 磁貼中、選取 **View** 。

3. 選擇新增。

4. 選擇“Azure”。

5. 選擇每個設定旁邊的向下箭頭並輸入或選擇值：

◦ 提供者設定：

- 建立一個新的儲存帳戶，如果控制台中已經存在，請選擇一個現有的儲存帳戶，或使用您自己的儲存帳戶來儲存備份。
- 請提供應用程式（client）ID、Client secret 和目錄（tenant）ID。選擇 **Authenticate**。
- 選擇 Azure 訂閱的 Azure 訂閱、區域和資源群組。

["如果您想自備儲存帳戶，請參閱新增 Azure Blob 儲存體帳戶"](#)。

◦ 加密：預設情況下，資料使用 Microsoft 管理的金鑰進行加密。選擇 **Microsoft** 管理的金鑰可保留此選項；或者，選擇客戶管理的金鑰可使用您自己的金鑰進行加密。

◦ 網路：選擇 IP 空間以及是否使用私有端點。

- IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
- 或者，選擇是否使用先前設定的 Azure 專用終端點。

如果您想使用 Azure PrivateLink，請參閱 ["Azure PrivateLink"](#)。

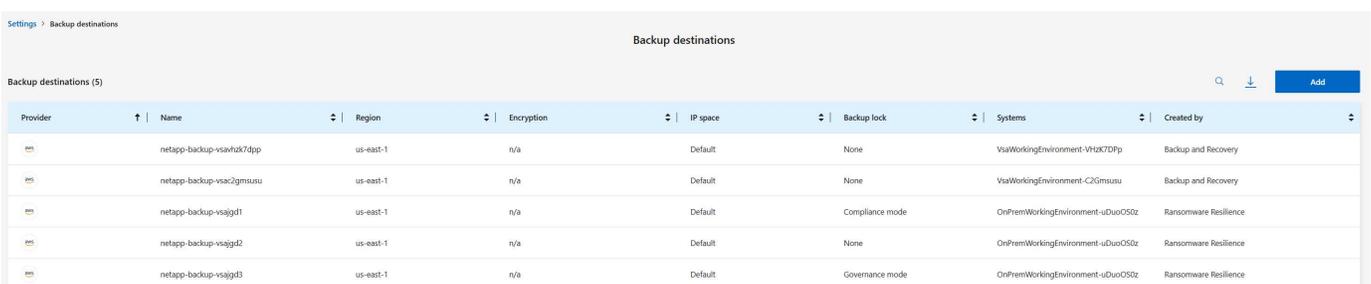
◦ 備份鎖定

選擇是否要設定備份鎖定。使用備份鎖定时、複本會受到保護、避免遭到修改或刪除、並掃描勒索軟體威脅。設定備份目的地之後、您無法修改此設定。如果您不想要備份鎖定、請選取 **None**。選取 **Governance mode**、允許具有特定權限的使用者在保留期間覆寫或刪除受保護的備份檔案。選取 **Compliance mode****、防止使用者在保留期間覆寫或刪除受保護的備份檔案。

6. 選擇“新增”。

結果

新的備份目標將會加入備份目標清單。



Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
	netapp-backup-vsahk7dpp	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHk7DfP	Backup and Recovery
	netapp-backup-vsac2gmsusu	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	Backup and Recovery
	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience

使用NetApp Ransomware Resilience保護策略保護工作負載

勒索軟體防護策略是 NetApp Ransomware Resilience 的關鍵功能：它們支援偵測、防護和複寫。防護策略是網路安全態勢的重要組成部分。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。["了解NetApp Console的勒索軟體復原角色"](#)。

了解勒索軟體防護策略

勒索軟體防護策略包括_偵測_、_保護_和_複製_策略。

- 偵測策略 辨識勒索軟體威脅
- 保護策略包含快照和備份策略。保護策略中需要偵測和快照策略。備份策略是可選的。

如果您使用其他NetApp產品來保護您的工作負載，勒索軟體復原能力會發現這些產品並提供以下選項：

- 使用勒索軟體偵測策略並繼續使用其他NetApp工具建立的快照和備份策略，或者
- 使用勒索軟體彈性來管理偵測、快照和備份。
- 複製策略 使您能夠將勒索軟體復原功能的快照複製到輔助網站。複製計劃可以設定為每小時、每天、每週或每月一次的頻率。

目前，您只能將快照複製到本機ONTAP儲存。



如果您正在為 Amazon FSx for ONTAP 和 Azure NetApp Files 配置保護策略，請參閱"[每項服務的限制](#)"。



為了更好地管理和保護您的資料資產，您可以建立"[群組工作負載](#)"，以便在一個策略下統一保護多個磁碟區。

與其他NetApp託管服務結合的保護策略

除了 Ransomware Resilience 之外，您還可以使用 NetApp Backup and Recovery 來管理檔案共用、VM 檔案共用的保護。

來自 Backup & Recovery 服務的保護資訊會顯示在 Ransomware Resilience 中。您可以使用 Ransomware Resilience 為這些服務新增偵測原則。使用 Ransomware Resilience 新增保護原則會取代現有的保護原則。

Ransomware Resilience 也會發現 SnapCenter for VMware 虛擬機器資料儲存區和 SnapCenter for Oracle 的保護原則。您無法使用這些服務透過 Ransomware Resilience 進行還原。

如果勒索軟體偵測策略由ONTAP中的自主勒索軟體防護（ARP 或 ARP/AI，取決於ONTAP版本）和 FPolicy 管理，則這些工作負載將受到保護並將繼續由 ARP 和 FPolicy 管理。



Amazon FSx for NetApp ONTAP 或 Azure NetApp Files 中的工作負載無法使用備份目的地。請使用 FSx for ONTAP 備份服務執行備份作業。您需要在 AWS 中為 FSx for ONTAP 工作負載設定備份原則，而不是在 Ransomware Resilience 中設定。備份原則會顯示在 Ransomware Resilience 中，並且與 AWS 中的設定保持一致。

針對不受NetApp應用程式保護的工作負載的保護策略

如果您的工作負載未由 Backup and Recovery 或 Ransomware Resilience 管理，則可能已建立快照，這些快照是 ONTAP 或其他產品的一部分。如果已啟用 ONTAP FPolicy 保護，您可以使用 ONTAP 變更 FPolicy 保護。

預定義的檢測策略

您可以選擇以下勒索軟體復原預定義策略之一，這些策略與工作負載重要性相符。



加密使用者擴充策略是唯一支援可疑使用者行為偵測的預先定義策略。

+ 關鍵複製策略 是唯一支援將快照複製到ONTAP 的預先定義策略。

政策層面	快照	頻率	保留時間 (天)	快照副本數量	快照副本的最大數量
關鍵工作 量政策	每刻鐘	每15分鐘	3	288	309
	日常的	每 1 天	14	14	309
	每週	每 1 週	35	5	309
	每月	每 30 天	60	2	309
重要的工 作量政策	每刻鐘	每30分鐘一班	3	144	165
	日常的	每 1 天	14	14	165
	每週	每 1 週	35	5	165
	每月	每 30 天	60	2	165
標準工作 量保單	每刻鐘	每30分鐘	3	72	93
	日常的	每 1 天	14	14	93
	每週	每 1 週	35	5	93
	每月	每 30 天	60	2	93
加密用戶 擴充	每刻鐘	每30分鐘	3	72	93
	日常的	每 1 天	14	14	93
	每週	每 1 週	35	5	93
	每月	每 30 天	60	2	93

政策層面	快照	頻率	保留時間 (天)	快照副本數量	快照副本的最大數量
關鍵複製策略	每刻鐘	每15分鐘	3	288	309
	日常的	每 1 天	14	14	309
	每週	每 1 週	35	5	309
	每月	每 30 天	60	2	309

增加勒索軟體防護策略

有三種增加勒索軟體保護策略：

- 如果您沒有快照或備份策略，請建立勒索軟體保護策略。

勒索軟體防護策略包括：

- 快照策略
- 勒索軟體檢測政策
- 備份策略
- 將 **Backup and Recovery** 保護中現有的快照或備份原則替換為由 **Ransomware Resilience** 管理的保護策略。

勒索軟體防護策略包括：

- 快照策略
- 勒索軟體檢測政策
- 備份策略
- *使用其他NetApp產品或服務中管理的現有快照和備份策略為工作負載建立偵測策略。*

檢測策略不會改變其他產品中管理的策略。

如果自主勒索軟體保護和 FPolicy 保護已在其他服務中激活，則偵測策略將啟用它們。詳細了解["自主勒索軟體防護"](#)，["備份和復原"](#)，和["ONTAP FPolicy"](#)。

建立勒索軟體保護策略（如果您沒有快照或備份策略）

如果工作負載上不存在快照或備份策略，您可以建立勒索軟體保護策略，其中可以包含您在勒索軟體復原中建立的以下策略：

- 快照策略
- 備份策略
- 勒索軟體檢測政策

- 二次複製到ONTAP

創建勒索軟體保護策略的步驟

1. 從勒索軟體恢復選單中，選擇*保護*。

Protection status

9 At risk (35 TiB data at risk) | 9 Protected (10 TiB data at risk)

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. 在「保護」頁面中，選擇一個工作負載，然後選擇「保護」。
3. 在勒索軟體防護策略頁面中，選擇*新增*。

Add Ransomware Resilience strategy

Ransomware Resilience strategy name:

Copy from existing Ransomware Resilience strategy: Select

Detection	1 / 3 enabled	▼
Snapshot policy	Action required	▼
Backup policy	None	▼

4. 輸入新的策略名稱，或輸入現有名稱進行複製。如果您輸入的是現有名稱，請選擇要複製的名稱並選擇*複製*。



如果您選擇複製並修改現有策略，Ransomware Resilience 會在原始名稱後面附加「_copy」。您應該更改名稱和至少一個設定以使其唯一。

5. 對於每個項目，選擇*向下箭頭*。

◦ 檢測政策：

- 策略：選擇預先設計的偵測策略之一。
- 主要偵測：啟用勒索軟體復原功能，以偵測潛在的勒索軟體攻擊。
- 可疑使用者行為偵測：啟用使用者行為偵測，將使用者活動事件傳輸到勒索軟體復原能力並偵測可疑事件，例如資料外洩。
- 封鎖檔案副檔名：啟用勒索軟體復原功能，以封鎖已知的可疑檔案副檔名。啟用主偵測功能後，勒索軟體復原功能會自動建立快照副本。

如果您想更改被封鎖的檔案副檔名，請在系統管理員中編輯它們。

◦ 快照策略：

- 快照策略基礎名稱：選擇一個政策或選擇*建立*並輸入快照策略的名稱。
- 快照鎖定：啟用此功能可鎖定主儲存體上的快照副本，以便即使勒索軟體攻擊進入備份儲存目標，它們在一定時間內也無法被修改或刪除。這也稱為_不可變儲存_。這使得恢復時間更快。

當快照被鎖定时，磁碟區的過期時間設定為快照副本的過期時間。

Snapshot 副本鎖定適用於ONTAP 9.12.1 及更高版本。要了解有關SnapLock 的更多信息，請參閱 "[ONTAP 中的SnapLock](#)"。

◦ 快照計畫：選擇計畫選項、要保留的快照副本數量，然後選擇啟用計畫。

▪ 複製策略：

- 複製策略基本名稱：輸入新名稱或選擇現有名稱。基本名稱是附加到所有快照的前綴。
- 複製計畫：切換要啟用的頻率（每小時、每天、每週或每月），並為每個啟用的計畫設定保留值（要保留的複製快照的數量）。

▪ 備份策略：

- 備份策略基本名稱：輸入新名稱或選擇現有名稱。
- 備份計畫：選擇二級儲存的計畫選項並啟用該計畫。



若要在輔助儲存裝置上啟用備份鎖定，請使用 **Settings** 選項來設定備份目標位置。如需詳細資訊，請參閱 "[配置設定](#)"。

6. 選擇“新增”。

在 **Backup and Recovery** 管理的、具有現有快照和備份原則的工作負載中新增偵測原則

Ransomware Resilience 可讓您為已在其他 NetApp 產品或服務中管理現有快照和備份保護的工作負載指派偵測原則或保護原則。Backup and Recovery 使用原則來管理快照、複寫到次要儲存設備或備份到物件儲存設備。

在具有現有備份或快照策略的工作負載中新增偵測策略

如果您已在 NetApp Backup and Recovery 中設定了快照或備份策略，則可以新增策略來偵測勒索軟體攻擊。若要使用 NetApp Ransomware Resilience 管理保護和偵測，請參閱[利用勒索軟體抵禦能力進行保護](#)。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。

The screenshot displays the 'Protection status' section at the top, which is divided into two columns. The left column shows '9 At risk' with a warning icon and '35 TiB data at risk'. The right column shows '9 Protected' with a shield icon and '10 TiB data at risk'. Below this, there are tabs for 'Workloads' and 'Protection groups', with 'Workloads' selected. A search bar and a 'Manage protection strategies' button are visible. The main area contains a table with 19 workloads. The table has columns for Workload, Protection status, Snapshot and back..., Type, Protec..., Encryption detecti..., Suspected u, and Actions.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. 在「保護」頁面中，選擇一個工作負載，然後選擇「保護」。
3. NetApp Ransomware Resilience 會偵測是否有現有的有效 NetApp Backup and Recovery 原則。
4. 若要保留現有的 Backup and Recovery 策略，僅套用_偵測_策略，請取消選取取代現有策略方塊。
5. 選擇所需的偵測設定：
 - 加密偵測
 - 可疑使用者行為偵測
 - 封鎖可疑的檔案副檔名
6. 選擇下一步。
7. 如果您選擇了 **Suspicious user behavior detection** 作為偵測設置，請選擇 **User activity agent** 或"**或創建一個**"。

用戶活動代理託管新的資料收集器。Ransomware Resilience 會自動建立資料收集器，將使用者活動事件傳送到 Ransomware Resilience 以偵測異常使用者行為。

8. 選擇下一步。
9. 審查您的選擇。選擇創建來啟動檢測。
10. 在「保護」頁面上，查看檢測狀態以確認檢測處於活動狀態。

用勒索軟體保護策略取代現有的備份或快照策略

您可以用勒索軟體保護策略取代現有的備份或快照策略。這種方法會刪除外部管理的保護，並在勒索軟體復原中配置偵測和保護。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。

The screenshot shows a dashboard with a 'Protection status' header. It displays two summary cards: '9 At risk' with '35 TiB data at risk' and '9 Protected' with '10 TiB data at risk'. Below this is a table of workloads with columns for Workload, Protection status, Snapshot and back..., Type, Protec..., Encryption detecti..., Suspected u, and Actions. The table lists several workloads like FSxN_fileshare_useast_01, LUN_storage_01, MySQL_4781, MySQL_8009, MySQL_9294, and Oracle_2115 with their respective protection statuses and actions.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. 在「保護」頁面中，選擇一個工作負載，然後選擇「保護」。
3. Ransomware Resilience 會偵測是否有現有的作用中 Backup and Recovery 原則。若要取代現有原則、請選取 取代現有原則 方塊。當您選取此方塊時、Ransomware Resilience 會將偵測原則清單取代為偵測原則。
4. 選擇保護策略。如果不存在保護策略，請選擇新增來建立新策略。有關建立策略的信息，請參閱[建立保護策略](#)。選擇下一步。
5. 如果您的策略包含複製，請選擇目標系統和目標儲存虛擬機器。選擇下一步。
6. 選擇備份目標或建立新的備份目標。選擇下一步。
 - a. 如果您的保護策略包含使用者行為偵測，請在您的環境中選擇一個使用者活動代理程式來託管新的資料收集器。Ransomware Resilience 會自動建立資料收集器，將使用者活動事件傳送到 Ransomware Resilience 以偵測異常使用者行為。
7. 查看新的保護策略，然後選擇保護來套用它。
8. 在「保護」頁面上，查看檢測狀態以確認檢測處於活動狀態。

分配不同的策略

您可以用其他策略取代現有策略。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。
2. 在「保護」頁面的工作負載行上，選擇「編輯保護」。
3. 如果工作負載已有 NetApp Backup and Recovery 策略且您希望保留該策略，請取消勾選 **Replace existing policies**。若要取代現有策略，請勾選 **Replace existing policies**。
4. 在「策略」頁面中，選擇要指派的策略的向下箭頭以查看詳細資訊。

5. 選擇您想要指派的策略。

6. 選擇*保護*以完成變更。

管理勒索軟體防護策略

您可以刪除勒索軟體策略。

查看受勒索軟體保護策略保護的工作負載

在刪除勒索軟體保護策略之前，您可能需要查看哪些工作負載受該策略保護。

您可以從策略清單中或在編輯特定策略時查看工作負載。

查看策略的步驟

1. 從勒索軟體恢復選單中，選擇*保護*。
2. 在「保護」頁面中，選擇「管理保護策略」。

勒索軟體防護策略頁面顯示策略清單。

Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads
<input type="radio"/> rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3
<input type="radio"/> rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1
<input checked="" type="radio"/> rps-standard-plan Recommended	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0
<input type="radio"/> rr-strategy-enc-user-ext	3 / 3 enabled	standard-ss-policy	standard-bu-policy	0

3. 在「勒索軟體保護策略」頁面的「受保護的工作負載」欄位中，選擇行末的向下箭頭。

移除勒索軟體防護策略

您可以刪除目前未與任何工作負載關聯的保護策略。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。
2. 在「保護」頁面中，選擇「管理保護策略」。
3. 在“管理策略”頁面中，選擇“操作”...您想要刪除的策略的選項。
4. 從操作選單中，選擇*刪除策略*。

設定使用者活動偵測

瞭解 **NetApp Ransomware Resilience** 中的使用者活動偵測

透過使用者活動偵測，NetApp Ransomware Resilience 讓您能夠在使用者層級處理勒索軟體事件，阻止資料外洩和大規模刪除等事件。

NetApp Ransomware Resilience 透過監控可疑的使用者活動，提供 AI 驅動的資料外洩偵測。讀取活動的急劇增加以及讀取活動的存取模式被用來判斷惡意意圖。一旦偵測到，Ransomware Resilience 會自動在 NetApp Console、電子郵件以及任何已設定的安全生態系統（例如 SIEM）中產生警示。

透過可疑使用者行為偵測和警示，NetApp Ransomware Resilience 會在發現可疑的資料外洩和破壞企圖及模式時發出警示。在每次警示中，NetApp Ransomware Resilience 都會識別出您可以封鎖的使用者。

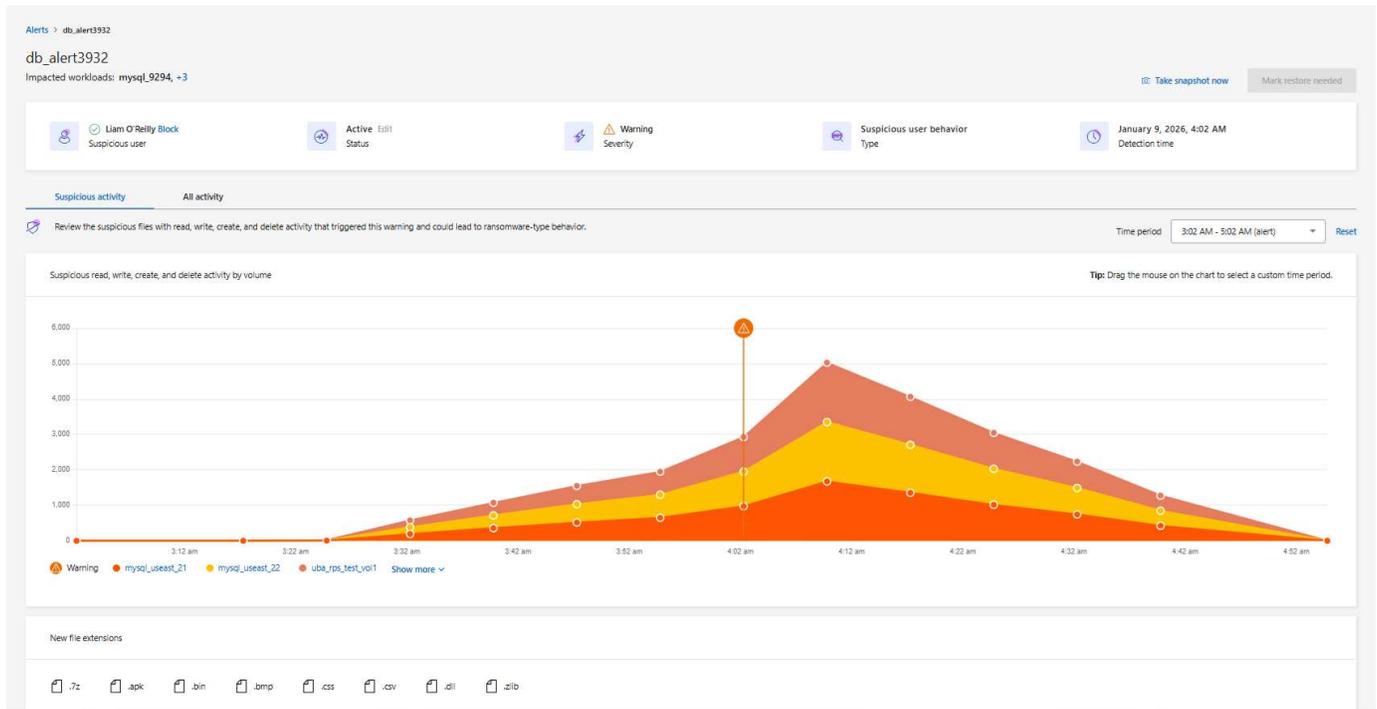
勒索軟體彈性透過分析 ONTAP 中 FPolicy 產生的使用者活動事件來偵測可疑的使用者活動。要收集用戶活動數據，您需要部署一個或多個用戶活動代理程式。該代理程式是可連接到租用戶上的裝置的 Linux 伺服器或 VM。



目前 SAN 工作負載不支援使用者活動偵測。您可以在 Amazon FSxN for ONTAP、Cloud Volumes ONTAP 和 ONTAP 中使用 NAS 工作負載的使用者活動偵測。

可疑使用者活動取證

Ransomware Resilience 提供使用者行為取證：透過清單和圖表顯示可疑活動發生的時間以及通知發送的時間。這些圖表詳細記錄了一段時間內檔案、目錄、磁碟區和工作負載上可疑活動的頻率，幫助您繪製事件圖。您也可以觀察新檔案副檔名的出現。



您可以將可疑活動與所有活動視圖進行比較。在所有活動視圖中，除了存取權限變更和存取被拒絕事件外，您還可以查看讀取、寫入、重新命名、移動、建立和刪除事件。



o

元件

Ransomware Resilience 可疑使用者行為活動偵測包含三個關鍵組成部分。

- 使用者活動代理程式是資料收集器的可執行環境。您必須設定使用者活動代理程式。
- 資料收集器會將使用者活動事件與 Ransomware Resilience 共用。當您"啟用勒索軟體防護策略，並偵測可疑的使用者活動"時，資料收集器會自動建立。
- 使用者目錄連接器能夠建立使用者名稱和使用者 ID 之間的映射關係，從而在應對可疑使用者行為時提供更清晰的線索。您必須配置使用者目錄連接器。

Ransomware Resilience 與 Data Infrastructure Insights

Ransomware Resilience 的可疑使用者行為偵測功能與 Data Infrastructure Insights (DII) Workload Security 整合，並使用"Data Infrastructure Insights 端點"。您無需任何 DII 組態即可在 Ransomware Resilience 中啟用使用者行為偵測。若要啟用使用者行為偵測，"建立所需的代理程式和收集器，並啟用適當的勒索軟體防護策略"。

如果您已在使用 NetApp Data Infrastructure Insights (DII) Workload Security、建議您將相同的 Workload Security 代理程式用於 Ransomware Resilience。您無需為 Ransomware Resilience 單獨部署 Workload Security 代理程式、但使用相同的 Workload Security 代理程式需要 Ransomware Resilience Console 組織與 DII Storage Workload Security 租戶建立配對關係。請聯絡您的客戶代表以啟用此配對。

後續步驟

- "使用者行為活動偵測的要求"
- "設定使用者行為活動代理程式和偵測器"

NetApp Ransomware Resilience 中的使用者行為偵測需求

NetApp Ransomware Resilience 使用者行為偵測使您能夠應對使用者層級的勒索軟體事件。您必須建立一組代理程式才能啟用使用者行為偵測。在啟用偵測之前，您必須確保您符合規定的作業系統、伺服器 and 網路要求，以便 Ransomware Resilience 能夠正確偵測和

報告事件。

雲端供應商支援

可疑用戶活動資料可以儲存在 AWS 和 Azure 的以下區域：

雲端提供者	地區
AWS	<ul style="list-style-type: none">• 亞太地區（雪梨）（ap-southeast-2）• 歐洲（法蘭克福）（eu-central-1）• 美國東部（維吉尼亞北部）（us-east-1）
Azure	美國東部

作業系統要求

以下作業系統支援可疑使用者行為偵測：

作業系統	支援的版本
AlmaLinux	9.4（64 位元）至 9.5（64 位元）和 10（64 位元），包括 SELinux
CentOS	CentOS Stream 9（64 位元）
Debian	11（64 位元）、12（64 位元），包括 SELinux
OpenSUSE 飛躍	15.3（64 位）至 15.6（64 位）
Oracle Linux	8.10（64 位元）、9.1（64 位元）至 9.6（64 位元），包括 SELinux
紅帽	8.10（64 位元）、9.1（64 位元）至 9.6（64 位元）和 10（64 位元），包括 SELinux
洛基	Rocky 9.4（64 位）至 9.6（64 位），包括 SELinux
SUSE 企業 Linux	15 SP4（64 位元）至 15 SP6（64 位元），包括 SELinux
Ubuntu	20.04 LTS（64 位元）、22.04 LTS（64 位元）和 24.04 LTS（64 位元）



用于用户活动代理的计算机不应运行其他应用程序级别的软件。建議使用專用伺服器。

這 unzip 安裝需要該指令。這 `sudo su -` 該命令用於安裝、運行腳本和卸載。

伺服器要求

伺服器必須滿足以下最低要求：

- CPU：4 核
- 內存：16GB 內存

- 磁碟空間：36 GB 可用磁碟空間

伺服器建議

- 分配額外的磁碟空間以用於建立檔案系統。請確保檔案系統中至少有 35 GB 的可用空間。+ 如果 /opt 這是從 NAS 儲存裝置掛載的資料夾，本機使用者必須有權限存取此資料夾。如果本機使用者沒有必要的權限，則使用者活動代理程式建立可能會失敗。
- 建議您將使用者活動代理安裝在與 Ransomware Resilience 環境不同的系統上。如果確實要安裝在同一台機器上，則應預留 50 至 55 GB 的磁碟空間。對於 Linux 系統，請分配 25-30 GB 的空間至 /opt/netapp，並分配 25 GB 至 var/log/netapp。
- 建議您使用網路時間協定 (NTP) 或簡單網路時間協定 (SNTP) 同步 ONTAP 系統和使用者活動代理程式電腦上的時間。

雲端網路存取規則

查看您所在地區（亞太地區、歐洲或美國）的雲端網路存取規則。



在初始安裝期間，請將 <site_name> 替換為萬用字元 (* 權限。代理程式啟動並完全運作後，您可以將權限替換為網站名稱。請聯絡您的 NetApp 代表以取得網站名稱。



使用者活動代理程式使用 NetApp Data Infrastructure Insights 技術，因此需要使用 `cloudinsights` 端點。如需詳細資訊，請參閱

基於亞太地區的使用者活動代理程式部署

協定	港口	來源	目的地	描述
HTTPS (TCP)	443	使用者活動代理	<ul style="list-style-type: none"> • <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com 	取得勒索軟體復原能力

歐洲使用者活動代理程式部署

協定	港口	來源	目的地	描述
HTTPS (TCP)	443	使用者活動代理	<ul style="list-style-type: none"> • <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com 	取得勒索軟體復原能力

美國使用者活動代理程式部署

協定	港口	來源	目的地	描述
HTTPS (TCP)	443	使用者活動代理	<ul style="list-style-type: none"> • <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com 	取得勒索軟體復原能力

網路內規則

協定	港口	來源	目的地	描述
TCP	389 (LDAP) 636 (LDAP/啟動-tls)	使用者活動代理	LDAP 伺服器 URL	連線到 LDAP
HTTPS (TCP)	443	使用者活動代理	叢集或SVM管理IP位址 (取決於SVM收集器配置)	API 與ONTAP進行通信

協定	港口	來源	目的地	描述
TCP	35000 - 55000	SVM 資料 LIF IP 位址	使用者活動代理	ONTAP與使用者活動代理程式之間關於 Fpolicy 事件的通訊。為了讓ONTAP能夠向用戶活動代理發送事件，必須向其開放這些端口，包括用戶活動代理本身上的任何防火牆（如果存在）。+ 注意：您不需要預留*所有*這些端口，但您為此預留的端口必須在此範圍內。建議您先預留 100 個端口，如有必要再增加。
TCP	35000-55000	叢集管理IP	使用者活動代理	ONTAP叢集管理 IP 與使用者活動代理程式之間關於 EMS 事件的通訊。為了讓ONTAP向用戶活動代理發送 EMS 事件，必須向用戶活動代理開放這些端口，包括用戶活動代理本身上的任何防火牆。+ 注意：您不需要預留*所有*這些端口，但您為此預留的端口必須在此範圍內。建議您先預留 100 個端口，如有必要再增加。
SSH	22	使用者活動代理	叢集管理	需要 CIFS/SMB 使用者阻止。

下一步

- ["設定使用者活動代理程式和收集器"](#)

在 **NetApp Ransomware Resilience** 中設定代理程式與收集器以偵測使用者活動

NetApp Ransomware Resilience 的使用者活動偵測功能可協助您預防使用者等級的勒索軟體攻擊事件。若要啟用 Ransomware Resilience 中的可疑使用者行為偵測功能，您必須安裝至少一個使用者活動代理程式。該代理程式會建立一個資料收集環境，用於監控使用者行為中是否存在類似勒索軟體攻擊的異常模式。

使用者活動代理程式包含資料收集器和使用者目錄連接器，它們都會將資料傳送到 SaaS 位置進行分析。

- 資料收集器會從 ONTAP 收集使用者活動資料。當您建立包含使用者行為偵測的保護策略時，系統會自動建立資料收集器。
- 使用者目錄連接器用於連接到您的目錄，並將使用者 ID 對應到使用者名稱。您必須配置使用者目錄連接器。

使用者活動代理程式、資料收集器和使用者目錄連接器都可以從 Ransomware Resilience 設定儀表板進行管理。



如果您已在使用 NetApp Data Infrastructure Insights (DII) Workload Security、建議您將相同的 Workload Security 代理程式用於 Ransomware Resilience。您無需為 Ransomware Resilience 單獨部署 Workload Security 代理程式、但使用相同的 Workload Security 代理程式需要 Ransomware Resilience Console 組織與 DII Storage Workload Security 租戶建立配對關係。請聯絡您的客戶代表以啟用此配對。

+ 如果您_未_使用 DII，請按照此處的設定說明進行操作。

開始之前

- 確保您符合"[作業系統、伺服器 and 網路要求](#)"。

需要 **Console** 角色 若要啟用可疑使用者活動偵測，您需要 **Organization admin role**。針對後續的可疑使用者活動設定，您需要 **Ransomware Resilience user behavior admin role**。"[了解NetApp Console的勒索軟體復原角色](#)"。

確保每個角色都在組織層級套用。

建立使用者活動代理程式

使用者活動代理程式是 "[資料收集器](#)" 的可執行環境；資料收集器與 Ransomware Resilience 共用使用者活動事件。您必須建立至少一個使用者活動代理程式才能啟用可疑使用者活動偵測功能。

步驟

1. 如果這是您第一次建立使用者活動代理，請前往儀表板。在使用者活動圖塊中，選擇啟動。

如果您要新增其他使用者活動代理，請前往*設定*，找到使用者活動圖塊，然後選擇管理。在使用者活動畫面上，選擇使用者活動代理選項卡，然後選擇新增。

2. 選擇雲端提供者，然後選擇區域。選擇下一步。
3. 提供用戶活動代理詳細資訊：
 - 使用者活動代理名稱
 - 控制台代理 - 控制台代理程式應與使用者活動代理程式位於同一網路中，並可透過 SSH 連線至使用者活動代理程式的 IP 位址。
 - **VM DNS** 名稱或 IP 位址
 - **VM SSH Key** - 請使用以下格式輸入 SSH 金鑰：

```
-----BEGIN OPENSSH PRIVATE KEY-----  
private-key-contents  
-----END OPENSSH PRIVATE KEY-----
```

User activity agent name

Select a Console agent located near the user activity agent to minimize latency when transmitting activity to Ransomware Resilience.

Console agent i

Provide the VM executable environment with "root" access for collectors in this user activity agent.

VM DNS name or IP address

VM SSH key i

4. 選擇下一步。
5. 檢查您的設定。選擇*啟動*以完成新增使用者活動代理程式。
6. 確認使用者活動代理程式已成功建立。在「使用者活動」磁貼中，成功部署後會顯示為 **Running**。

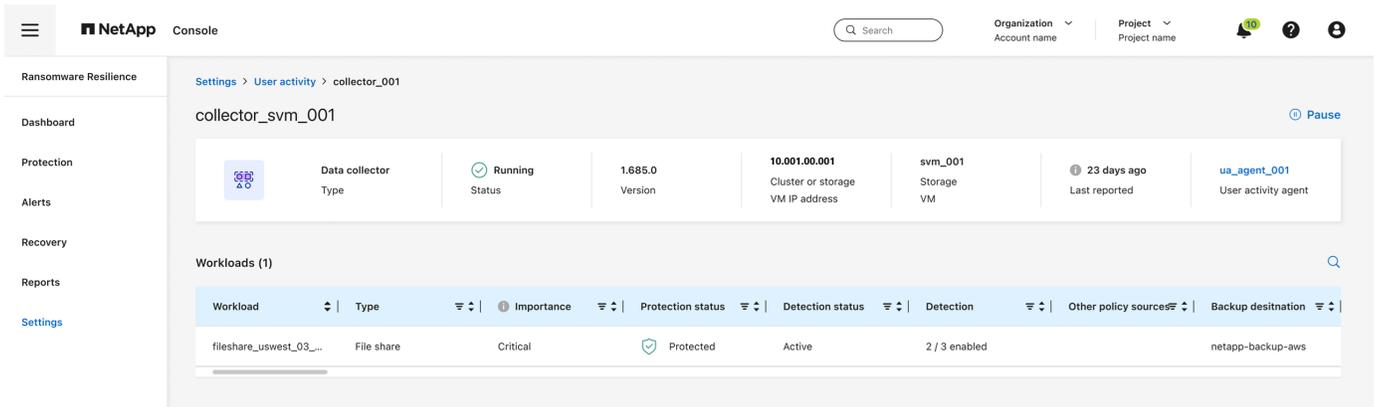
結果

使用者活動代理程式成功建立後、返回 **Settings** 功能表、然後在 User activity 磚中選取 **Manage**。選取 **User activity agents** 索引標籤、然後選取使用者活動代理程式以檢視其詳細資料、包括資料收集器和使用者目錄連接器。

新增資料收集器

啟用包含可疑使用者活動偵測功能的勒索軟體防護策略時，系統會自動建立資料收集器。如需詳細資訊，請參閱 ["新增檢測策略"](#)。

您可以查看資料收集器的詳細資訊。從「設定」中，選擇「使用者活動」圖塊中的「管理」。選擇資料收集器選項卡，然後選擇資料收集器以查看其詳細資訊或暫停它。



建立使用者目錄連接器

若要將使用者 ID 對應到使用者名，您必須建立使用者目錄連接器。

步驟

1. 在勒索軟體復原中，前往*設定*。
2. 在使用者活動圖塊中，選擇管理。
3. 選擇使用者目錄連接器選項卡，然後選擇新增。
4. 配置連接。請在每個欄位中填寫所需資訊。

場地	描述
姓名	請為使用者目錄連接器輸入一個唯一的名稱
使用者目錄類型	目錄類型
伺服器IP位址或網域名稱	連接所在伺服器的 IP 位址或完全限定網域名稱 (FQDN)
森林名稱或搜尋名稱	您可以將目錄結構的林級別指定為直接網域名稱（例如： <code>unit.company.com</code> ）或一組相對專有名詞（例如： <code>DC=unit,DC=company,DC=com</code> ）。你也可以輸入一個 OU 按組織單元或 CN 僅限特定使用者（例如： <code>CN=user,OU=engineering,DC=unit,DC=company,DC=com</code> ）。
綁定DN	BIND DN 是被允許搜尋目錄的使用者帳戶，例如 <code>user@domain.com</code> 。使用者需要網域唯讀權限。
綁定密碼	BIND DN 中提供的使用者密碼
協定	協定字段為可選字段。您可以使用 LDAP、LDAPS 或基於 StartTLS 的 LDAP。
港口	請輸入您選擇的連接埠號

User directory

Connect to your user directories to identify specific users performing potentially suspicious behavior. [Get help](#)

Connection ^

<p>Name</p> <input type="text" value="Unique name required"/>	<p>User directory type</p> <input type="text" value="Active Directory"/>
<p>User activity agent</p> <input type="text" value="Select..."/>	<p>Server IP or DNS name</p> <input type="text"/>
<p>Forest name or search name i</p> <input type="text"/>	<p>Bind DN</p> <input type="text"/>
<p>Bind password</p> <input type="password" value=""/>	<p>Protocol Optional</p> <input type="text" value="LDAP"/>
<p>Port</p> <input type="text" value="389"/>	

Attribute mapping v

Not set

提供屬性映射詳細資訊：

- 顯示名稱
- **SID** (如果您使用 LDAP)
- 使用者名稱
- **Unix ID** (如果您使用 NFS)
- 如果您選擇“包含可選屬性”，您還可以新增電子郵件地址、電話號碼、角色、州/省、國家/地區、部門、照片、經理 DN 或群組。選擇“進階”以新增可選的搜尋查詢。

5. 選擇新增。
6. 傳回使用者目錄連接器標籤以檢查使用者目錄連接器的狀態。如果建立成功，使用者目錄連接器的狀態顯示為*正在執行*。

刪除使用者目錄連接器

步驟

1. 在勒索軟體復原中，前往*設定*。
2. 找到使用者活動圖塊，選擇管理。
3. 選擇使用者目錄連接器選項卡。
4. 確定要刪除的使用者目錄連接器。在行尾的操作選單中，選擇三個點`...`然後刪除。
5. 在彈出的對話方塊中、選取 **Delete** 進行確認。

將使用者排除在警示範圍之外

如果某些受信任使用者的行為可能會觸發使用者行為警示，您可以將他們從警示中排除。

步驟

1. 在勒索軟體恢復功能中，選擇設定。
2. 在「設定」儀表中，找到「使用者活動」卡片，然後選取 **Manage**。
3. 選擇 **Excluded users** 標籤。
4. 若要在使用者介面中檢閱個別使用者，請選擇 手動選取。若要上傳排除的使用者清單，請選取 上傳。
 - a. 如果您選擇了 **Select manually**，請選取要排除的特定使用者名稱旁的核取方塊。
 - b. 如果您選擇 **Upload**，則必須先下載包含所有使用者清單的 CSV 檔案。選擇 **Download** 即可存取該清單。

檢閱 CSV 檔案。移除所有您想要維持偵測的使用者名稱。當清單僅包含您想要從偵測中排除的使用者名稱時，請儲存該清單。選取 **Upload** 以找到檔案，然後選擇該檔案。

5. 選擇 **Add** 以完成將使用者新增至排除清單的操作。
6. 在「已排除使用者」標籤中，現在會在儀表中顯示已從使用者行為偵測警示中移除的使用者名稱。



您也可以直接將使用者從警示中排除。如需詳細資訊，請參閱 "[回應勒索軟體警示](#)"。

從排除使用者清單中移除使用者

之後您可以將使用者重新加入偵測。

步驟

1. 在「設定」儀表中，找到「使用者活動」卡片，然後選取 **Manage**。
2. 選擇 **Excluded users** 標籤。
3. 從排除使用者清單中找到要移除的使用者名稱。在該使用者名稱所在的行選擇操作選單 (...)，然後選擇移除。
4. 在對話方塊中、選取 **Remove** 以確認您要移除所選使用者。

回應可疑用戶活動警報

配置可疑使用者活動偵測後，您可以在警報頁面監控事件。如需詳細資訊，請參閱 "[偵測惡意活動和可疑使用者行為](#)"。

在 NetApp Ransomware Resilience 中管理保護群組

NetApp Ransomware Resilience 提供保護群組，以便更輕鬆地管理您的資料資產。保護群組是工作負載的邏輯分組。Ransomware Resilience 可以使用單一保護策略，同時保護保護群組中的所有磁碟區，讓您無需為每個工作負載分別套用策略。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

建立保護組

您可以建立群組，無論其保護狀態如何（即未受保護的群組和受保護的群組）。在保護群組新增保護策略時，新的保護策略將取代任何現有策略，包括由 NetApp Backup and Recovery 管理的策略。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。

Protection status

9 At risk 9 in last 7 days 35 TiB data at risk

9 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption dete...	Suspected u...	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. 在「保護」儀表中，選擇 **Protection groups** 標籤。

Workloads Protection groups

Protection group (1)

Protection group	Protection status	Ransomware Resilience strategy	Protected count
pg_important	Protected	rps-important-plan	2 / 2

3. 選擇“新增”。

Workloads

Select workloads to add to the protection group.

Protection group name: NoRansomwareOnThisFileShare

Workloads (17) | Selected rows (2)

Select workloads with no other policy source or with Backup and Recovery as a policy source.

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
azure_vol1_4872	File share	azure-connector-demo	Critical	n/a	At risk	N/A	N/A	N/A
fileshare_uswest_02_7453	File share	aws-connector-us-west-1-account...	Critical	n/a	Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsajgd1
fsxn_fileshare_usast_01	File share	aws-connector-us-east-1	Critical	High	At risk	N/A	N/A	N/A
gcp_ha_vol1_7496-ws	File share	gcp-connector-demo	Critical	n/a	At risk	N/A	N/A	N/A
lun_storage_01	Block	aws-connector-us-east-1	Critical	n/a	Protected	1 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd3
mysql_8009	MySQL	aws-connector-us-east-1	Critical	n/a	At risk	N/A	Backup and Recovery	netapp-backup-vsajgd1
mysql_9294	MySQL	aws-connector-us-east-1	Critical	n/a	Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsajgd3
oracle_2115	Oracle	aws-connector-us-east-1	Critical	n/a	At risk	N/A	SnapCenter	netapp-backup-vsajgd1

Next

4. 輸入保護組的名稱。

5. 選擇要新增到群組中的工作負載。



要查看有關工作負載的更多詳細信息，請滾動到右側。

6. 選擇“下一步”。

Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads
<input type="radio"/> rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3
<input type="radio"/> rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1
<input type="radio"/> rps-standard-plan	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0

7. 為該群組選擇保護策略。

8. 如果保護策略包含複製功能，請檢查複製設定。

- 若要將所有快照複製到相同目標位置，請勾選「每個工作負載使用相同目標位置」。在控制台代理部分，為工作負載選擇*目標系統*和*目標儲存虛擬機器*。+ 若要使用不同的目的地，請取消選取該方塊。檢查每個控制台代理程式下的每個工作負載，並為每個工作負載分配一個*目標系統*和*目標儲存虛擬機器*。選擇下一步。

9. 若要設定備份策略，請選擇一個，然後選擇下一步。

10. 如果您的偵測策略包含使用者行為偵測，請選擇您想要使用的資料收集器，然後按一下下一步。

11. 檢查保護組的選擇。

12. 若要完成保護群組、請選取 **Add**。



在查看 Ransomware Resilience 中的保護儀表板時、您可以按保護群組對工作負載進行排序。

編輯組保護

您可以變更現有群組的偵測策略。

步驟

- 從勒索軟體恢復選單中，選擇*保護*。
- 在「保護」頁面中，選擇「保護群組」選項卡，然後選擇要修改其政策的群組。
- 從保護群組的概覽頁面中，選擇「編輯保護」。
- 選擇要套用的現有保護原則，或選擇 **Add** 以建立新的保護原則。如需新增保護原則的詳細資訊，請參閱 "[建立保護策略](#)"。然後選擇 **Save**。
- 在備份目標概覽中，選擇現有的備份目標或新增新的備份目標。

6. 選擇下一步來查看您的變更。

從保護群組移除工作負載

之後您可能需要從現有保護群組中移除工作負載。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。
2. 在「保護」頁面中，選擇「保護群組」標籤。
3. 選擇要從中刪除一個或多個工作負載的群組。

The screenshot shows the AWS IAM console interface for a protection group named 'pg_important'. At the top, there are three summary cards: '3 File shares', '2 Applications', and '0 VM datastores'. Below these is a table of workloads. The table has columns for Workload, Type, Console agent, Importance, Privacy exposure, Protection status, Detection, Snapshot and backup policies, and Backup destination. There are 5 rows of workloads listed.

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_us-east_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_us-west_01	File share	aws-connector-us-west-1-account...	Critical	High	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_us-west_02_3223	File share	aws-connector-us-west-1-account...	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
mysql_4781	MySQL	aws-connector-us-west-1-account...	Standard	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1

4. 在保護群組頁面中、選擇要從群組中移除的工作負載、然後選擇 **Actions ...** 選項。
5. 從「操作」功能表中，選擇「刪除工作負載」。
6. 確認您要刪除工作負載並選擇*刪除*。

刪除保護群組

刪除保護群組時、Ransomware Resilience 會移除該群組及工作負載上的保護策略。它不會刪除個別工作負載。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。
2. 在「保護」頁面中，選擇「保護群組」標籤。
3. 選擇要從中刪除一個或多個工作負載的群組。

pg_important
Protection group

Workloads

3 File shares 2 Applications 0 VM datstores

Protection

rpis-important-plan
Ransomware Resilience strategy
View

Workloads (5)

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_us-east_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_us-west_01	File share	aws-connector-us-west-1-account...	Critical	High	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_us-west_02_3223	File share	aws-connector-us-west-1-account...	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
mysql_4781	MySQL	aws-connector-us-west-1-account...	Standard	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1

4. 在選定的保護群組頁面的右上角，選擇「刪除保護群組」。
5. 確認您要刪除該群組並選擇*刪除*。

使用勒索軟體復原中的NetApp Data Classification掃描個人識別資訊

在NetApp Ransomware Resilience中，您可以使用NetApp Data Classification來掃描和分類檔案共用工作負載中的資料。對資料進行分類可以幫助您確定資料集是否包含個人識別資訊 (PII)，這可能會增加安全風險。資料分類是NetApp Console的核心元件，無需額外付費即可使用。

"資料分類"利用人工智慧驅動的自然語言處理進行情境資料分析和分類，為您的資料提供可操作的見解，以滿足合規性要求、偵測安全漏洞、優化成本並加速遷移。



此過程可以影響工作負載的重要性，以幫助確保您獲得適當的保護。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

透過資料分類識別隱私暴露

在使用勒索軟體復原功能中的資料分類之前，您需要"[啟用資料分類來掃描您的數據](#)"。

您可以在勒索軟體復原的保護頁面內部署資料分類。依照程式識別隱私洩漏。當您選擇識別暴露時，如果您尚未部署資料分類，則會顯示對話框，讓您啟用資料分類。

有關數據分類的更多信息，請參閱：

- "[了解資料分類](#)"
- "[私人資料類別](#)"
- "[調查組織中儲存的數據](#)"

開始之前

如果您已"[部署資料分類](#)"。資料分類作為控制台的一部分提供，無需額外付費，並且可以在本地或客戶雲端中部署。

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。
2. 在「保護」頁面的「工作負載」欄位中找到檔案共享工作負載。

Protection

Protection status

7 At risk 7 in last 7 days 35 TiB data at risk 11 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (23)

Workload	Type	Protection status	Protect...	Encryption detectio...	Suspected user beh...	Block suspicious fil...	Snapshot and back...	Console agent	Importance	Privacy ex...	Backup destination	Actions
azure_voll_4872	File share	At risk	N/A	N/A	N/A	N/A	N/A	azure-connector-demo	Critical	Identify exposure	N/A	Protect
fileshare_uswest_02	File share	Protected	pg.important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-east-1	Standard	Medium	netapp-backup-vsajgd1	Edit protection
fileshare_uswest_01	File share	Protected	pg.important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	High	netapp-backup-vsajgd1	Edit protection
fileshare_uswest_02_3223	File share	Protected	pg.important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fileshare_uswest_02_7453	File share	Protected	N/A	Enabled	N/A	N/A	Backup and Recovery	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fsxn_fileshare_useast_01	File share	At risk	N/A	N/A	N/A	N/A	N/A	aws-connector-us-east-1	Critical	High	N/A	Protect
gcp_h_voll_7496-ws	File share	At risk	N/A	N/A	N/A	N/A	N/A	gcp-connector-demo	Critical	Identify exposure	N/A	Protect
lun_storage_01	Block	Protected	N/A	Enabled	N/A	N/A	Ransomware Resilience	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd3	Edit protection
mysql_4781	MySQL	Protected	pg.important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Standard	N/A	netapp-backup-vsajgd1	Edit protection
mysql_8009	MySQL	At risk	N/A	N/A	N/A	N/A	Backup and Recovery	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd1	Protect

3. 若要啟用資料分類來掃描您的資料中的 PII，請在「隱私暴露」欄位中選擇「識別暴露」。



如果您尚未部署資料分類，選擇「識別暴露」將開啟一個對話方塊來部署資料分類。選擇*部署*。部署資料分類後，您可以返回「保護」頁面，然後選擇「識別暴露」。

結果

掃描可能需要幾分鐘，具體取決於文件的大小和數量。在掃描過程中，保護頁面指示它正在識別文件並提供文件數量。掃描完成後，「隱私暴露」欄位將暴露等級評定為「低」、「中」或「高」。

審查隱私暴露情況

在對 PII 進行資料分類掃描後，評估風險。

PII 資料分為以下三類：

- 高：超過 70% 的檔案包含 PII
- 中：超過 30% 且少於 70% 的檔案包含 PII
- 低：大於 0% 且小於 30% 的檔案包含 PII

步驟

1. 從勒索軟體恢復選單中，選擇*保護*。
2. 在「保護」頁面中，在「工作負載」欄位中找到顯示「隱私權暴露」列中狀態的檔案共用工作負載。

Protection

Protection status

7 At risk 7 in last 7 days 35 TiB data at risk

11 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (23)

Workload	Type	Protection status	Protect...	Encryption detecto...	Suspected user beh...	Block suspicious fil...	Snapshot and back...	Console agent	Importance	Privacy ex...	Backup destination	Actions
azure_vo1_4872	File share	At risk	N/A	N/A	N/A	N/A	N/A	azure-connector-demo	Critical	Identify exposure	N/A	Protect
fileshare_useast_02	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-east-1	Standard	Medium	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_01	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	High	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_3223	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_7453	File share	Protected	N/A	Enabled	N/A	N/A	Backup and Recovery	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fsxn_fileshare_useast_01	File share	At risk	N/A	N/A	N/A	N/A	N/A	aws-connector-us-east-1	Critical	High	N/A	Protect
gcpa_vo1_7496-ws	File share	At risk	N/A	N/A	N/A	N/A	N/A	gcp-connector-demo	Critical	Identify exposure	N/A	Protect
lun_storage_01	Block	Protected	N/A	Enabled	N/A	N/A	Ransomware Resilience	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd3	Edit protection
mysql_4781	MySQL	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Standard	N/A	netapp-backup-vsajgd1	Edit protection
mysql_8009	MySQL	At risk	N/A	N/A	N/A	N/A	Backup and Recovery	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd1	Protect

3. 選擇「工作負載」列中的工作負載連結即可查看工作負載詳情。

Protection > FSxN_fileshare_useast_01

FSxN_fileshare_useast_01

Critical Importance

Protected Protection health Edit protection

0 Alerts

Not marked for recovery Recovery

High Privacy exposure

Files with PII 181 hits in 150 files

Types of PII

- Credit cards 20 hits in 150 files
- Contacts 95 hits in 150 files
- Passwords 28 hits in 150 files
- Data subjects 38 hits in 150 files

Protection

2 / 3 enabled Detection

rps-critical-plan Policy View policy

n/a Backup destination View backup destination

File share

Location svm-fsxEnvironment

Console agent console-agent-us-east

FSx Amazon FSx for NetApp ONTAP

Volume: FSxN_fileshare_useas...

Cluster id aaa111a1a-1a11-11aa-1...

System name fsxEnvironment...

Storage VM name svm-fsxEnvironment...

4. 在「工作負載詳細資料」頁面中，查看「隱私暴露」圖塊中的詳細資訊。

隱私暴露對工作負載重要性的影響

隱私暴露的變化可能會影響工作負載的重要性。

當隱私暴露時：	從這次隱私曝光來看：	對於此隱私暴露：	那麼，工作量重要性會這樣做：
減少	高、中或低	中、低或無	保持不變

當隱私暴露時：	從這次隱私曝光來看：	對於此隱私暴露：	那麼，工作量重要性會這樣做：
增加	沒有任何	低的	保持標準
	低的	中等的	從標準到重要的變化
	低或中	高的	從標準或重要變成關鍵

更多資訊

有關資料分類的詳細信息，請參閱資料分類文件：

- ["了解資料分類"](#)
- ["私人資料類別"](#)
- ["調查組織中儲存的數據"](#)

回應並恢復

在NetApp Ransomware Resilience中管理警報

當 NetApp Ransomware Resilience 偵測到可能的攻擊時，會在儀表板和通知選單中顯示警示。Ransomware Resilience 會立即建立快照。當你收到警示時，請在 Ransomware Resilience 警示 分頁中檢視潛在風險，以評估對資料的影響並防止潛在的勒索軟體攻擊。

如果 Ransomware Resilience 偵測到可能的攻擊，NetApp Console 通知設定中會顯示通知，並且會傳送電子郵件至設定的位址。該電子郵件包含有關嚴重性、受影響工作負載的資訊，以及指向 Ransomware Resilience Alerts 標籤中警示的連結。

您可以忽略誤報或決定立即恢復資料。



如果您關閉警報，勒索軟體復原功能會了解此行為，將其與正常操作關聯，並且不會再次對其發出警報。

要開始恢復數據，請將警報標記為準備好恢復，以便儲存管理員可以開始恢復程序。

每個警報可能包含不同數量和狀態的多個事件。審查所有事件。

警示的產生方式

Ransomware Resilience 依靠資料熵模式、檔案副檔名類型和加密方式等方面的證據來產生警報。警報基於以下事件：

- 資料外洩
- 資料銷毀
- 文件擴展名已建立或更改

- 建立文件並比較檢測率與預期率
- 文件刪除，並比較檢測率與預期率
- 可疑的使用者行為
- 當加密程度較高時，無需更改檔案副檔名



對於資料外洩、資料銷毀和可疑使用者行為警示，您必須設定 "使用者活動偵測"。

警示類型和狀態

警示有兩種狀態：**New** 或 **Inactive**。

警示分為以下幾種類型之一：

- 潛在攻擊：當出現以下情況時、警報將被歸類為潛在攻擊：
 - 自主勒索軟體防護偵測到新的副檔名，並且在過去 24 小時內重複出現超過 20 次（預設行為）。
 - 偵測到資料外洩。
 - 偵測到資料銷毀。
- 警告：基於以下行為會出現警告：
 - 之前沒有發現過新的擴展，並且相同行為沒有重複足夠多次以將其聲明為攻擊。
 - 觀察到高熵。
 - 文件讀取、寫入、重新命名或刪除活動比正常水平增加了一倍。



對於 SAN 環境，警告僅基於高熵值。

證據基於 ONTAP 中的自主勒索軟體防護資訊。有關詳細信息，請參閱 "[自主勒索軟體防護概述](#)"。

警示狀態

警報事件可以具有以下幾種狀態：

狀態	描述
新的	所有事件在首次發現時都會被標記為「新」。
* 正在審核中 *	您可以在評估警示事件時，手動將其標記為「審核中」。
已解除	如果您懷疑該活動並非勒索軟體攻擊，您可以將狀態變更為「已駁回」。+ 注意：駁回攻擊後，您將無法恢復其狀態。如果您駁回工作負載，則所有為應對潛在勒索軟體攻擊而自動建立的快照副本都將永久刪除。
已解決	此事件已修復。
* 自動解決 *	對於低優先級警報，如果在五天內沒有對其採取任何行動，則該事件將自動解決。

查看警報

您可以從 Ransomware Resilience 儀表板或 **Alerts** 標籤存取警報。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

步驟

1. 在 Ransomware Resilience 儀表板中、檢視「警示」窗格。
2. 選擇其中一個狀態下的「查看全部」。
3. 選擇一個警報來查看每個警報的每個磁碟區上的所有事件。
4. 若要查看其他警報，請選擇左上角麵包屑中的「警報」。
5. 查看警報頁面上的警報。

Alert ID	Alert type	Severity	Suspicious user	Workload	Console agent	Status	Incidents	Impacted data	Detected
ub_alert3223	Suspicious user behavior	Potential attack	Aiden Smith	fileshare_uswest_02_3223, +3	aws-connector-us-east-1	Active	1	2 GiB	8 days ago
ee_alert8727	Encryption	Potential attack	Unable to detect	oracle_8821	aws-connector-us-east-1	Active	2	2 GiB	14 days ago
ee_alert9823	Encryption	Potential attack	Unable to detect	oracle_9819	aws-connector-us-east-1	Active	1	2 GiB	17 days ago
db_alert3932	Suspicious user behavior	Warning	Liam O'Reilly	mysql_9294, +3	aws-connector-us-east-1	Active	4	2 GiB	26 days ago
dd_alert7918	Data destruction	Potential attack	Amina Khan	vm_datastore_4719, +3	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_other_alert5319	Encryption	Potential attack	Raj Patel	vm_fileshare_6699	aws-connector-us-west-1...	Active	1	2 GiB	1 month ago
lun_alert_6285	Encryption	Potential attack	Unable to detect	lun_storage_01	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_alert_v01	Data breach	Potential attack	Raj Patel	uba_rpx_test_v01, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_v02	Data breach	Potential attack	Raj Patel	uba_rpx_test_v02, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_v03	Data breach	Potential attack	Raj Patel	uba_rpx_test_v03, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago

6. 繼續執行下列操作之一：

- [\[偵測惡意活動和異常使用者行為\]](#)。
- [\[將勒索軟體事件標記為可恢復（事件被消除後）\]](#)。
- [\[忽略不屬於潛在攻擊的事件\]](#)。

回覆警報電子郵件

當 Ransomware Resilience 偵測到潛在攻擊時，它會根據使用者在 NetApp Console 設定中配置的訂閱通知偏好，向已訂閱使用者發送電子郵件通知。該電子郵件包含有關警示的資訊，包括嚴重程度和受影響的資源。



若要在 Console 中設定電子郵件通知，請參閱 "[設定電子郵件通知設定](#)"。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

步驟

1. 查看電子郵件。
2. 在電子郵件中、選取 **View alert** 並登入 NetApp Ransomware Resilience 。
出現「警報」頁面。
3. 檢視每個磁碟區上每個警報的所有事件。
4. 若要查看其他警報，請選擇左上角麵包屑中的「警報」。
5. 繼續執行下列操作之一：
 - [\[偵測惡意活動和異常使用者行為\]](#) 。
 - [\[將勒索軟體事件標記為可恢復（事件被消除後）\]](#) 。
 - [\[忽略不屬於潛在攻擊的事件\]](#) 。

偵測惡意活動和異常使用者行為

查看「警報」標籤，您可以識別是否有惡意活動或異常使用者行為。

您必須設定使用者活動代理並啟用包含使用者行為偵測的保護策略才能查看使用者層級警報。***可疑使用者***欄位僅在啟用使用者行為偵測後才會顯示在警報儀表中。若要啟用可疑使用者偵測，請參閱 ["可疑的用戶活動"](#)。

查看惡意活動

當 Autonomous Ransomware Protection 在 NetApp Ransomware Resilience 中觸發警示時、您可以檢視下列詳細資料：

- 警示觸發時
- 當存取權限被更改或拒絕時
- 輸入資料的熵
- 預期的新文件創建率與檢測到的速率的比較
- 預期檔案刪除率與偵測率的比較
- 檔案的預期重命名率與偵測到的重命名率的比較
- 受影響的工作負載、磁碟區、檔案和目錄



這些詳細資訊對於 NAS 工作負載是可見的。對於 SAN 環境，只有熵資料可用。

步驟

1. 從勒索軟體恢復選單中，選擇***警報***。
2. 選擇一個警報。
3. 查看警報中的事件。

Alerts > ee_alert8727

ee_alert8727
Impacted workloads: oracle_8821 Mark restore needed

⚡ 2 Potential attacks
📁 286 Impacted files
💾 2 GiB Impacted data
🕒 September 25, 2025, 6:51 AM
First detected

Incidents (2) 🔍 ⬇️ Edit status

<input type="checkbox"/>	Incident ID	Volume	Storage VM	System	Severity	Status	First detec...	Most rece...	Evidence	Automated res...
<input type="checkbox"/>	inc4922	oracle_useast_data2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	4 new extensions...	1 snapshot
<input type="checkbox"/>	inc3163	oracle_useast_log2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	6 new extensions...	1 snapshot

4. 選擇一個事件來查看該事件的詳細資訊。

查看異常用戶行為

如果您已設定可疑使用者偵測以查看異常使用者行為，則可以查看使用者級資料並封鎖特定使用者。若要啟用可疑使用者設定，請參閱 ["設定代理程式和收集器以偵測使用者活動"](#)。

步驟

1. 從勒索軟體恢復選單中，選擇*警報*。
2. 選擇一個警報。
3. 查看警報中的事件。
 - a. 若要封鎖環境中的可疑使用者，請在使用者名稱旁邊選取 **Block**。
 - b. 若要停用針對特定使用者的警報（該使用者收到的警報為誤報），請選擇三個點 (...，然後選擇將此使用者從監控中排除。查看對話框，然後選擇排除進行確認。



若要重新啟用某個使用者的警報，請返回該警報。選擇三個點，然後選擇 **Include this user in monitoring**。您也可以["排除使用者"](#)從監控。

將勒索軟體事件標記為可恢復（事件被消除後）

停止攻擊後，通知您的儲存管理員資料已準備就緒，以便他們可以啟動復原程序。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。["了解NetApp Console的勒索軟體復原角色"](#)。

步驟

1. 從勒索軟體恢復選單中，選擇*警報*。

Alerts

Overview

10 Alerts 20 GiB Impacted data

Automated responses

9 Snapshots

Alerts (10)

Alert ID	Alert type	Severity	Suspicious user	Workload	Console agent	Status	Incidents	Impacted data	Detected
ub_alert3223	Suspicious user behavior	Potential attack	Aiden Smith	fileshare_uswest_02_3223, +3	aws-connector-us-east-1	Active	1	2 GiB	8 days ago
ee_alert8727	Encryption	Potential attack	Unable to detect	oracle_8821	aws-connector-us-east-1	Active	2	2 GiB	14 days ago
ee_alert9823	Encryption	Potential attack	Unable to detect	oracle_9819	aws-connector-us-east-1	Active	1	2 GiB	17 days ago
db_alert3932	Suspicious user behavior	Warning	Liam O'Reilly	mysql_9294, +3	aws-connector-us-east-1	Active	4	2 GiB	26 days ago
dd_alert7918	Data destruction	Potential attack	Amina Khan	vm_dbtestore_4719, +3	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_other_alert5319	Encryption	Potential attack	Raj Patel	vm_fileshare_6699	aws-connector-us-west-1...	Active	1	2 GiB	1 month ago
lun_alert_6286	Encryption	Potential attack	Unable to detect	lun_storage_01	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_alert_vo1	Data breach	Potential attack	Raj Patel	uba_rps_test_vo1, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_vo2	Data breach	Potential attack	Raj Patel	uba_rps_test_vo2, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_vo3	Data breach	Potential attack	Raj Patel	uba_rps_test_vo3, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago

2. 在警報頁面中，選擇警報。
3. 查看警報中的事件。

Alerts > ee_alert8727

ee_alert8727

Impacted workloads: oracle_8821

Mark restore needed

2 Potential attacks 286 Impacted files 2 GiB Impacted data September 25, 2025, 6:51 AM First detected

Incidents (2)

Incident ID	Volume	Storage VM	System	Severity	Status	First detec...	Most rece...	Evidence	Automated res...
inc4922	oracle_useast_data2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	4 new extensions...	1 snapshot
inc3163	oracle_useast_log2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	6 new extensions...	1 snapshot

4. 如果您確定事件已準備好恢復，請選擇*標記需要恢復*。
5. 確認操作並選擇*標記需要恢復*。
6. 若要啟動工作負載恢復，請在訊息中選擇“恢復*工作負載”或選擇“*恢復”標籤。

結果

將警報標記為恢復後，警報將從「警報」標籤移至「恢復」標籤。

忽略不屬於潛在攻擊的事件

審查事件後，您需要確定該事件是否為潛在的攻擊。如果它們不構成實際威脅，就可以忽略不計。

您可以忽略誤報或決定立即恢復資料。如果您忽略警報，勒索軟體復原能力會學習此行為並將其與正常操作關聯起來，並且不會再次針對此類行為發出警報。

如果您解除工作負載，則為應對潛在勒索軟體攻擊而自動取得的所有快照副本都將永久刪除。



如果您關閉警報，則無法變更其狀態或撤銷此變更。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色"。

步驟

1. 從勒索軟體恢復選單中，選擇*警報*。

Alert ID	Alert type	Severity	Suspicious user	Workload	Console agent	Status	Incidents	Impacted data	Detected
ub_alert3223	Suspicious user behavior	Potential attack	Aiden Smith	fileshare_uswest_02_3223, +3	aws-connector-us-east-1	Active	1	2 GiB	8 days ago
ee_alert8727	Encryption	Potential attack	Unable to detect	oracle_8821	aws-connector-us-east-1	Active	2	2 GiB	14 days ago
ee_alert9823	Encryption	Potential attack	Unable to detect	oracle_9819	aws-connector-us-east-1	Active	1	2 GiB	17 days ago
db_alert3932	Suspicious user behavior	Warning	Liam O'Reilly	mysql_9294, +3	aws-connector-us-east-1	Active	4	2 GiB	26 days ago
dd_alert7918	Data destruction	Potential attack	Amina Khan	vm_datastore_4719, +3	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_other_alert5319	Encryption	Potential attack	Raj Patel	vm_fileshare_6699	aws-connector-us-west-1-...	Active	1	2 GiB	1 month ago
lun_alert6285	Encryption	Potential attack	Unable to detect	lun_storage_01	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_alert_vo1	Data breach	Potential attack	Raj Patel	uba_rps_test_vo1, +2	aws-connector-us-east-1-...	Active	3	2 GiB	1 month ago
uba_alert_vo2	Data breach	Potential attack	Raj Patel	uba_rps_test_vo2, +2	aws-connector-us-east-1-...	Active	3	2 GiB	1 month ago
uba_alert_vo3	Data breach	Potential attack	Raj Patel	uba_rps_test_vo3, +2	aws-connector-us-east-1-...	Active	3	2 GiB	1 month ago

2. 在警報頁面中，選擇警報。

Incident ID	Volume	Storage VM	System	Severity	Status	First detected	Most recent	Evidence	Automated res...
inc4922	oracle_useast_data2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	4 new extensions...	1 snapshot
inc3163	oracle_useast_log2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	6 new extensions...	1 snapshot

3. 選擇一個或多個事件。或者，選擇表格左上角的「事件 ID」框，選擇所有事件。
4. 如果您確定該事件不構成威脅，請將其視為誤報：
 - 選擇事件。
 - 選擇表格上方的*編輯狀態*按鈕。

Edit status

Change the status to keep track of incidents that are not a threat.

Status

Select status ▲

Resolved

Dismissed

Save

Cancel

5. 在「編輯狀態」方塊中，選擇「已解僱」狀態。

顯示了有關工作負載和快照副本被刪除的更多資訊。

6. 選擇*儲存*。

事件狀態變更為「已駁回」。

查看受影響文件的列表

在檔案層級復原應用程式工作負載之前，您可以查看受影響檔案的清單。您可以造訪警報頁面下載受影響文件的清單。然後使用恢復頁面上傳列表並選擇要恢復的檔案。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

步驟

使用「警報」頁面檢索受影響文件的清單。

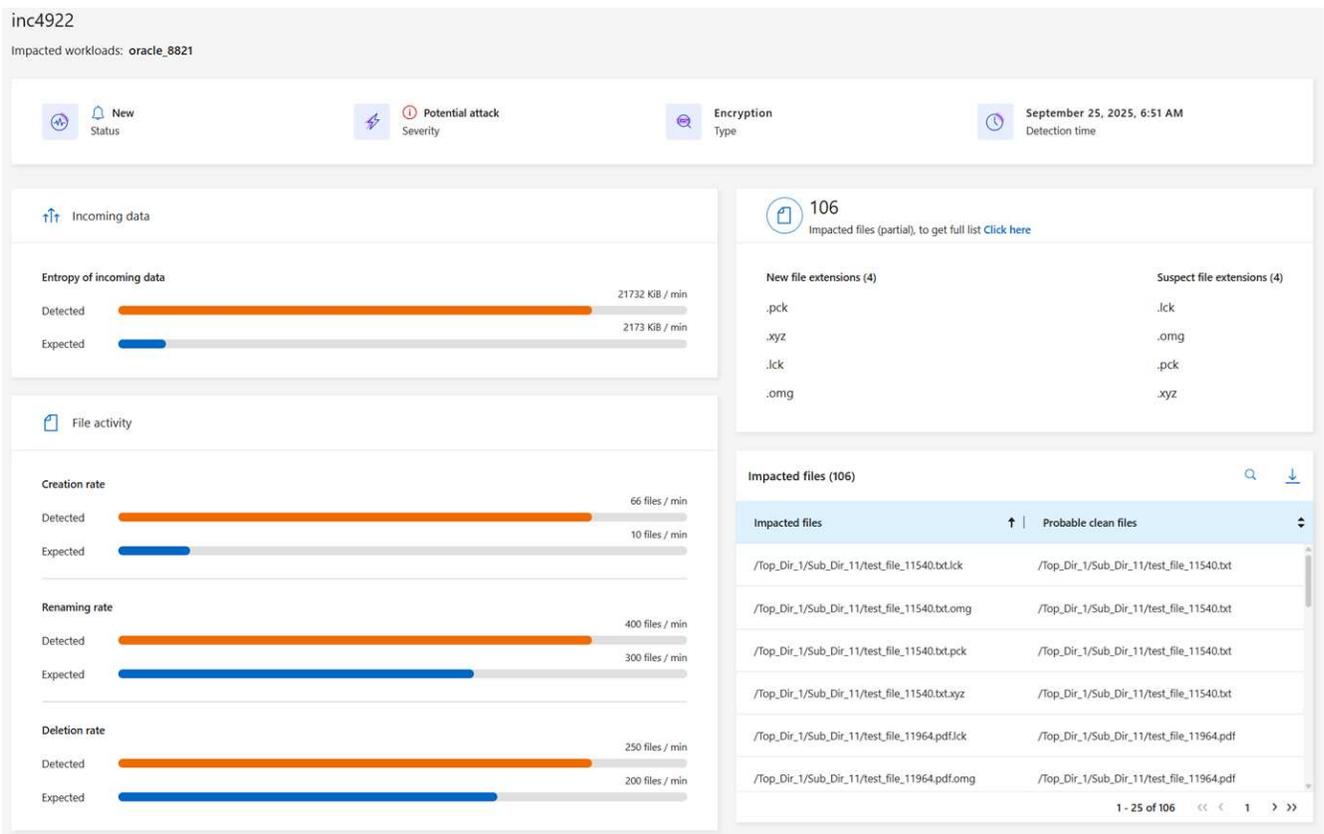


如果某個磁碟區有多個警報，您可能需要下載每個警報的受影響檔案的 CSV 清單。

1. 從勒索軟體恢復選單中，選擇*警報*。
2. 在「警報」頁面上，按工作負載對結果進行排序，以顯示要恢復的應用程式工作負載的警報。

3. 從該工作負載的警報清單中選擇一個警報。

4. 對於該警報，選擇一個事件。



5. 對於該事件，選擇下載圖示以 CSV 格式下載受影響文件的清單。

透過 NetApp Ransomware Resilience，在勒索軟體攻擊發生後恢復

在工作負載被標記為「需要復原」後，NetApp Ransomware Resilience 會建議實際復原點 (RPA) 並協調工作流程以實現抗崩潰復原。

- 如果應用程式或 VM 由 NetApp Backup and Recovery 或 Ransomware Resilience 管理，Ransomware Resilience 會執行當機一致性還原，其中磁碟區中同一時間點的所有資料都會還原，例如系統當機時。

您可以透過選擇所有磁碟區、特定磁碟區或特定檔案來還原工作負載。



工作負載恢復可能會影響正在運行的工作負載。您應該與適當的利害關係人協調恢復過程。

工作負載可以具有以下還原狀態之一：

- 需要恢復：需要恢復工作負載。
- 進行中：復原作業目前正在進行中。
- 已恢復：工作量已恢復。
- 失敗：工作負載復原過程無法完成。

查看已準備好恢復的工作負載

查看處於「需要恢復」恢復狀態的工作負載。

步驟

1. 執行下列操作之一：
 - 從儀表板檢閱「警示」窗格中的「需要還原」總計，然後選取 **View all**。
 - 從選單中選擇*恢復*。
2. 查看“恢復”頁面中的工作負載資訊。

Workload	Type	Location	Console agent	Snapshot and backup poli.	Recovery status	Progress	Importance	Total data	Action
lun_storage_01	Block	10.0.1.10	aws-connector-us-east-1	Ransomware Resilience	Restore needed	N/A	Critical	2 GiB	Restore
mysql_9284	MySQL	10.0.1.10	aws-connector-us-east-1	Backup and Recovery	Restore needed	N/A	Critical	2 GiB	Restore
oracle_9819	Oracle	10.0.1.10	aws-connector-us-east-1	SnapCenter	Restore needed	N/A	Critical	2 GiB	Restore
uba_rps_test_vo1	File share	svm_cvoawsesd01rpsdemosand...	aws-connector-us-east-1-account-14092025	Ransomware Resilience	Restore needed	N/A	Critical	2 GiB	Restore
uba_rps_test_vo2	File share	svm_cvoawsesd01rpsdemosand...	aws-connector-us-east-1-account-14092025	Ransomware Resilience	Restore needed	N/A	Critical	2 GiB	Restore
uba_rps_test_vo3	File share	svm_cvoawsesd01rpsdemosand...	aws-connector-us-east-1-account-14092025	Ransomware Resilience	Restore needed	N/A	Critical	2 GiB	Restore
vm_datastore_4719	VM datastore	10.0.1.17	aws-connector-us-east-1	SnapCenter for VMware	Restore needed	N/A	Standard	2 GiB	Restore
vm_fileshare_6699	VM file share	10.0.1.215	aws-connector-us-west-1-account-LX2N400...	Ransomware Resilience	Restore needed	N/A	Critical	2 GiB	Restore

還原工作負載

使用勒索軟體復原能力，儲存管理員可以決定如何從建議的還原點或首選的還原點最佳地復原工作負載。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

安全儲存管理員可以恢復不同等級的資料：

- 恢復所有捲
- 在磁碟區層級或檔案和資料夾層級復原應用程式。
- 在磁碟區層級、目錄或資料/資料夾層級還原檔案共用。
- 從虛擬機器層級的資料儲存中復原。

過程根據工作負載類型而有所不同。

步驟

1. 從勒索軟體恢復選單中，選擇*恢復*。
2. 查看“恢復”頁面中的工作負載資訊。
3. 選擇處於「需要恢復」狀態的工作負載。
4. 若要恢復，請選擇*恢復*。
5. 復原範圍：選擇您想要完成的復原類型：

- 所有捲
- 依體積
- 按下檔案：您可以指定要還原的資料夾或單一檔案。



對於 SAN 工作負載，您只能按工作負載進行復原。

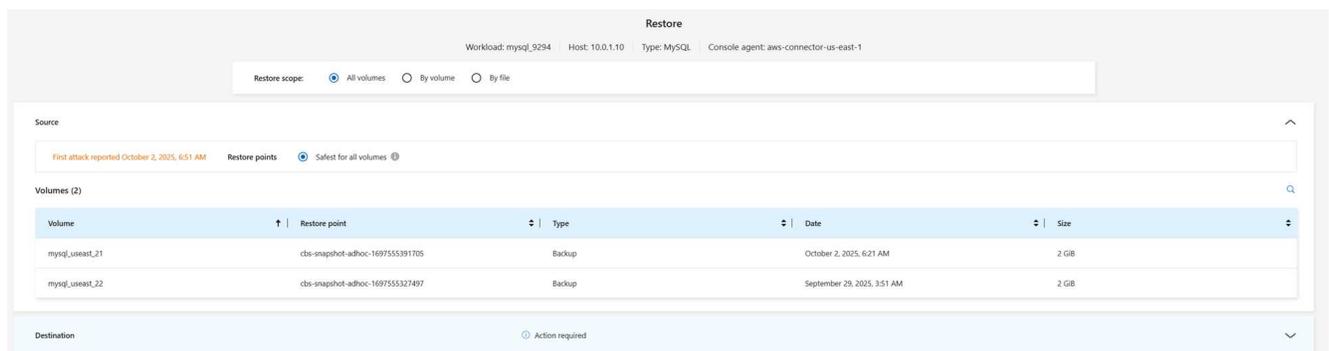


您最多可以選擇 100 個檔案或一個資料夾。

6. 根據您選擇的是應用程式、磁碟區還是文件，繼續執行以下步驟之一。

恢復所有捲

1. 從勒索軟體恢復選單中，選擇*恢復*。
2. 選擇處於「需要恢復」狀態的工作負載。
3. 若要恢復，請選擇*恢復*。
4. 在「還原」頁面的「還原範圍」中，選擇「所有磁碟區」。



5. 來源：選擇來源旁的向下箭頭查看詳細資訊。
 - a. 選擇要用於還原資料的還原點。



勒索軟體復原能力將最佳還原點識別為事件發生前的最新備份，並顯示「對所有磁碟區最安全」的指示。這意味著所有磁碟區都將恢復到偵測到的第一個磁碟區受到第一次攻擊之前的副本。

6. 目的地：選擇目的地旁的向下箭頭查看詳細資訊。
 - a. 選擇系統。
 - b. 選擇儲存虛擬機器。
 - c. 選擇聚合。
 - d. 變更將會新增到所有新磁碟區的捲前綴。



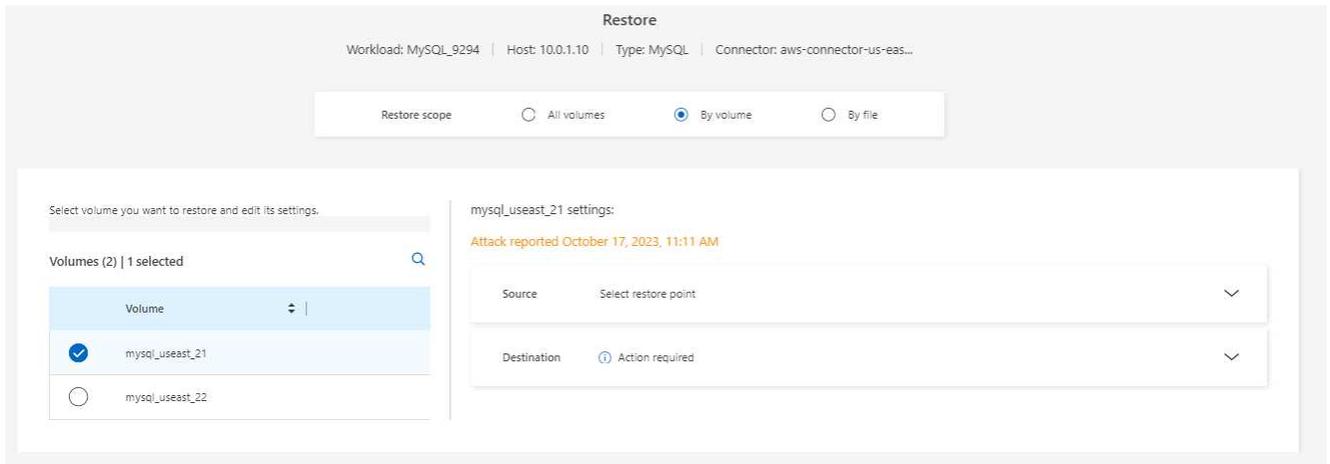
新磁碟區名稱顯示為前綴+原始磁碟區名稱+備份名稱+備份日期。

7. 選擇*儲存*。

- 選擇“下一步”。
- 檢查您的選擇。
- 選擇*恢復*。
- 從頂部選單中，選擇“恢復”以查看“恢復”頁面上的工作負載，其中操作的狀態會在各個狀態之間移動。

在磁碟區層級恢復應用程式工作負載

- 從勒索軟體恢復選單中，選擇*恢復*。
- 選擇處於「需要恢復」狀態的應用程式工作負載。
- 若要恢復，請選擇*恢復*。
- 在「還原」頁面的「還原範圍」中，選擇「按磁碟區」。



- 在磁碟區清單中，選擇要還原的磁碟區。
- 來源：選擇來源旁的向下箭頭查看詳細資訊。
 - 選擇要用於還原資料的還原點。



勒索軟體復原能力將最佳還原點識別為事件發生前的最新備份，並顯示「建議」指示。

- 目的地：選擇目的地旁的向下箭頭查看詳細資訊。
 - 選擇系統。
 - 選擇儲存虛擬機器。
 - 選擇聚合。
 - 查看新的磁碟區名稱。



新的磁碟區名稱顯示為原始磁碟區名稱+備份名稱+備份日期。

- 選擇*儲存*。
- 選擇“下一步”。
- 檢查您的選擇。

11. 選擇*恢復*。

12. 從頂部選單中，選擇“恢復”以查看“恢復”頁面上的工作負載，其中操作的狀態會在各個狀態之間移動。

在檔案層級恢復應用程式工作負載

在檔案層級復原應用程式工作負載之前，您可以查看受影響檔案的清單。您可以造訪警報頁面下載受影響文件的清單。然後使用恢復頁面上傳列表並選擇要恢復的檔案。

您可以將檔案層級的應用程式工作負載還原到相同或不同的系統。

取得受影響文件清單的步驟

使用「警報」頁面檢索受影響文件的清單。



如果某個磁碟區有多個警報，您將需要下載每個警報的受影響檔案的 CSV 清單。

1. 從勒索軟體恢復選單中，選擇*警報*。
2. 在「警報」頁面上，按工作負載對結果進行排序，以顯示要恢復的應用程式工作負載的警報。
3. 從該工作負載的警報清單中選擇一個警報。
4. 對於該警報，選擇一個事件。

The screenshot displays the Oracle Security Cloud interface for workload 'inc4922'. It features several key sections:

- Header:** 'Inc4922', 'Impacted workloads: oracle_8821', and navigation options for 'New Status', 'Potential attack Severity', 'Encryption Type', and 'September 25, 2025, 6:51 AM Detection time'.
- Incoming data:** A bar chart comparing 'Entropy of incoming data' with 'Detected' (21732 KB/min) and 'Expected' (2173 KB/min) values.
- File activity:** Three bar charts showing 'Creation rate' (66 files/min detected vs 10 expected), 'Renaming rate' (400 files/min detected vs 300 expected), and 'Deletion rate' (250 files/min detected vs 200 expected).
- Impacted files (106):** A table listing file paths and extensions. It includes a search bar and a download icon. The table shows columns for 'Impacted files' and 'Probable clean files'.

Impacted files	Probable clean files
/Top_Dir_1/Sub_Dir_11/test_file_11540.txt.lck	/Top_Dir_1/Sub_Dir_11/test_file_11540.txt
/Top_Dir_1/Sub_Dir_11/test_file_11540.txt.omg	/Top_Dir_1/Sub_Dir_11/test_file_11540.txt
/Top_Dir_1/Sub_Dir_11/test_file_11540.txt.pck	/Top_Dir_1/Sub_Dir_11/test_file_11540.txt
/Top_Dir_1/Sub_Dir_11/test_file_11540.txt.xyz	/Top_Dir_1/Sub_Dir_11/test_file_11540.txt
/Top_Dir_1/Sub_Dir_11/test_file_11964.pdf.lck	/Top_Dir_1/Sub_Dir_11/test_file_11964.pdf
/Top_Dir_1/Sub_Dir_11/test_file_11964.pdf.omg	/Top_Dir_1/Sub_Dir_11/test_file_11964.pdf

5. 若要查看完整的檔案列表，請選擇「受影響的檔案」窗格頂部的「按一下此處」。

6. 對於該事件，選擇下載圖示並以 CSV 格式下載受影響文件的清單。

恢復這些文件的步驟

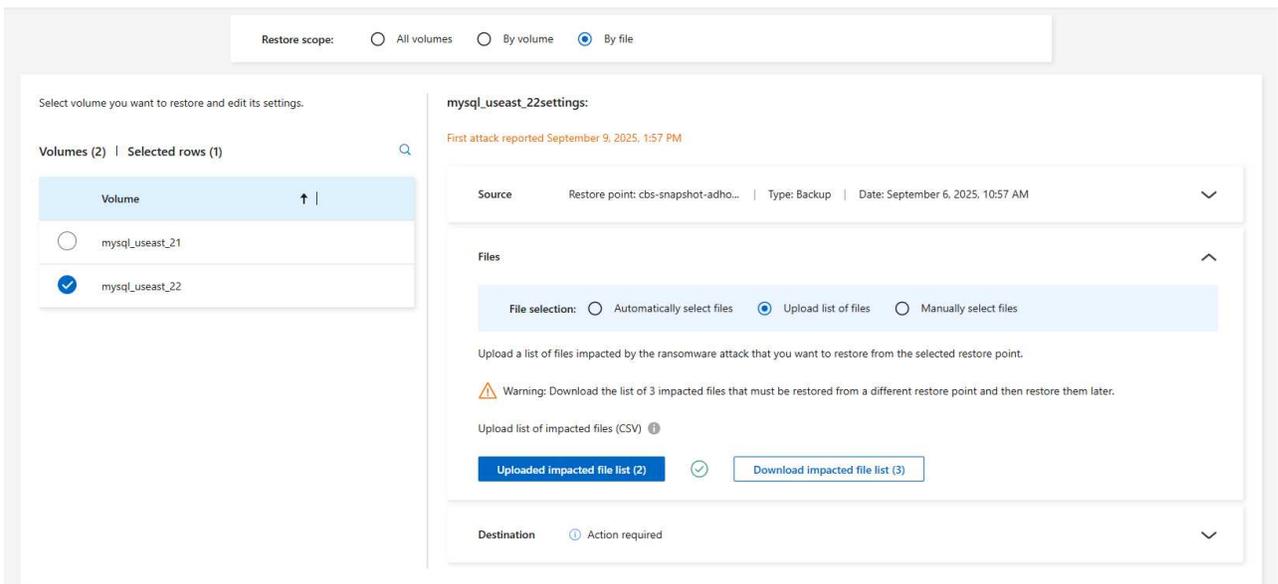
1. 從勒索軟體恢復選單中，選擇*恢復*。
2. 選擇處於「需要恢復」狀態的應用程式工作負載。
3. 若要恢復，請選擇*恢復*。
4. 在「還原」頁面的「還原範圍」中，選擇「按檔案」。
5. 在磁碟區清單中，選擇包含要還原的檔案的磁碟區。
6. 還原點：選擇*還原點*旁的向下箭頭查看詳細資料。選擇要用於還原資料的還原點。



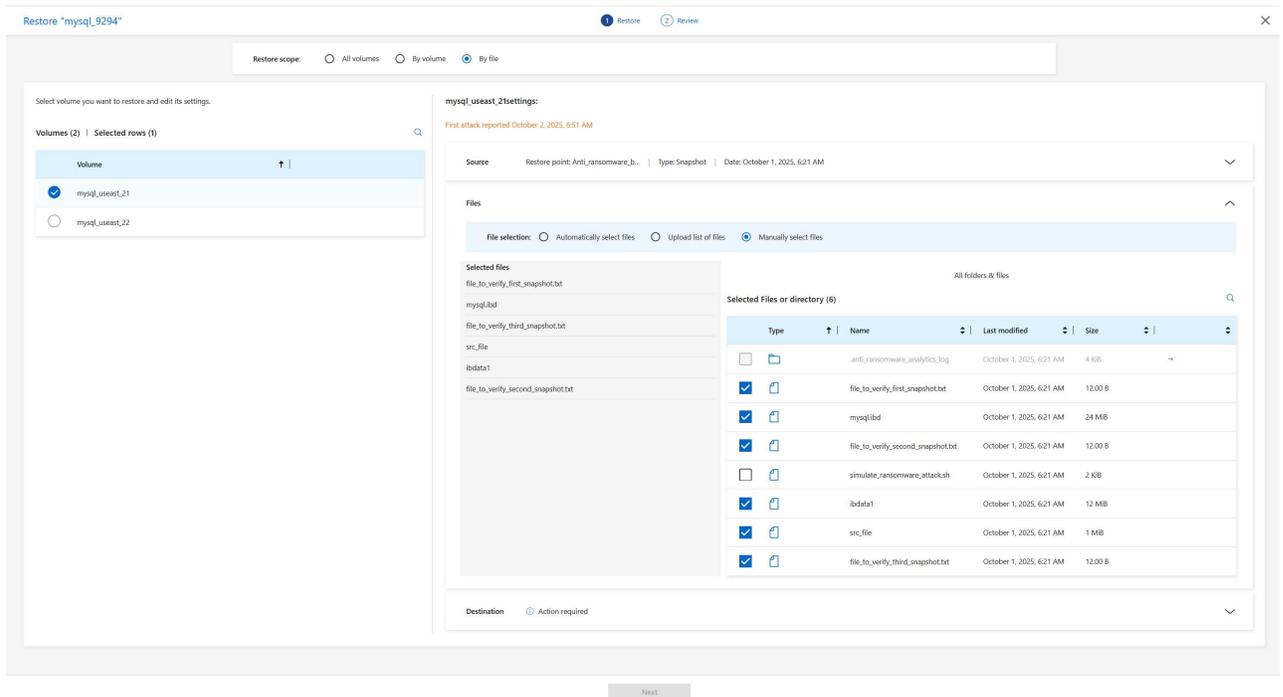
還原點窗格中的「原因」欄位顯示快照或備份的原因為「排程」或「對勒索軟體事件的自動回應」。

7. 文件：

- 自動選擇檔案：讓勒索軟體復原功能選擇要復原的檔案。
- 上傳文件清單：上傳一個 CSV 文件，其中包含您從警報頁面取得的或您擁有的受影響文件的清單。您一次最多可以恢復 10,000 個檔案。



- 手動選擇檔案：選擇最多 10,000 個檔案或單一資料夾進行復原。



如果無法使用所選還原點還原任何文件，則會出現一條訊息，指示無法還原的文件數量，並允許您透過選擇「下載受影響文件的清單」來下載這些文件的清單。

8. 目的地：選擇目的地旁的向下箭頭查看詳細資訊。
 - a. 選擇復原資料的位置：原始來源位置或您可以指定的備用位置。



雖然原始檔案或目錄將被復原的資料覆蓋，但原始檔案和資料夾名稱將保持不變，除非您指定新名稱。

- b. 選擇系統。
- c. 選擇儲存虛擬機器。
- d. (可選) 輸入路徑。



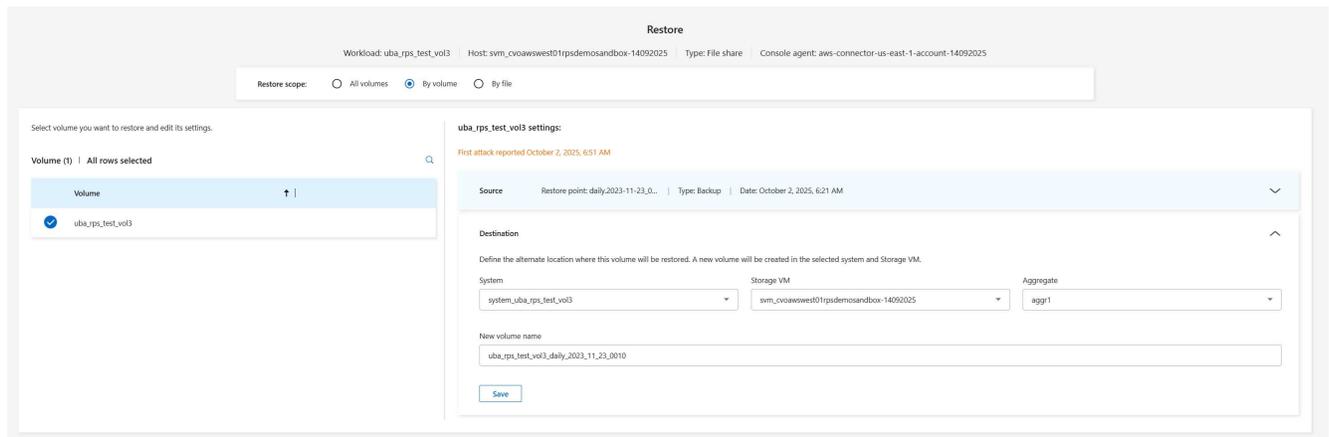
如果您沒有指定還原路徑，檔案將會還原到頂層目錄的新磁碟區。

- e. 選擇是否希望復原的檔案或目錄的名稱與目前位置的名稱相同或不同。

9. 選擇“下一步”。
10. 檢查您的選擇。
11. 選擇*恢復*。
12. 從頂部選單中，選擇“恢復”以查看“恢復”頁面上的工作負載，其中操作的狀態會在各個狀態之間移動。

恢復文件共享或資料存儲

1. 選擇要還原的檔案共用或資料儲存後，在「還原」頁面的「還原範圍」中，選擇「按卷」。



2. 在磁碟區清單中，選擇要還原的磁碟區。
3. 來源：選擇來源旁的向下箭頭查看詳細資訊。
 - a. 選擇要用於還原資料的還原點。



勒索軟體復原能力將最佳還原點識別為事件發生前的最新備份，並顯示「建議」指示。

4. 目的地：選擇目的地旁的向下箭頭查看詳細資訊。
 - a. 選擇復原資料的位置：原始來源位置或您可以指定的備用位置。



雖然原始檔案或目錄將被復原的資料覆蓋，但原始檔案和資料夾名稱將保持不變，除非您指定新名稱。

- b. 選擇系統。
- c. 選擇儲存虛擬機器。
- d. (可選) 輸入路徑。



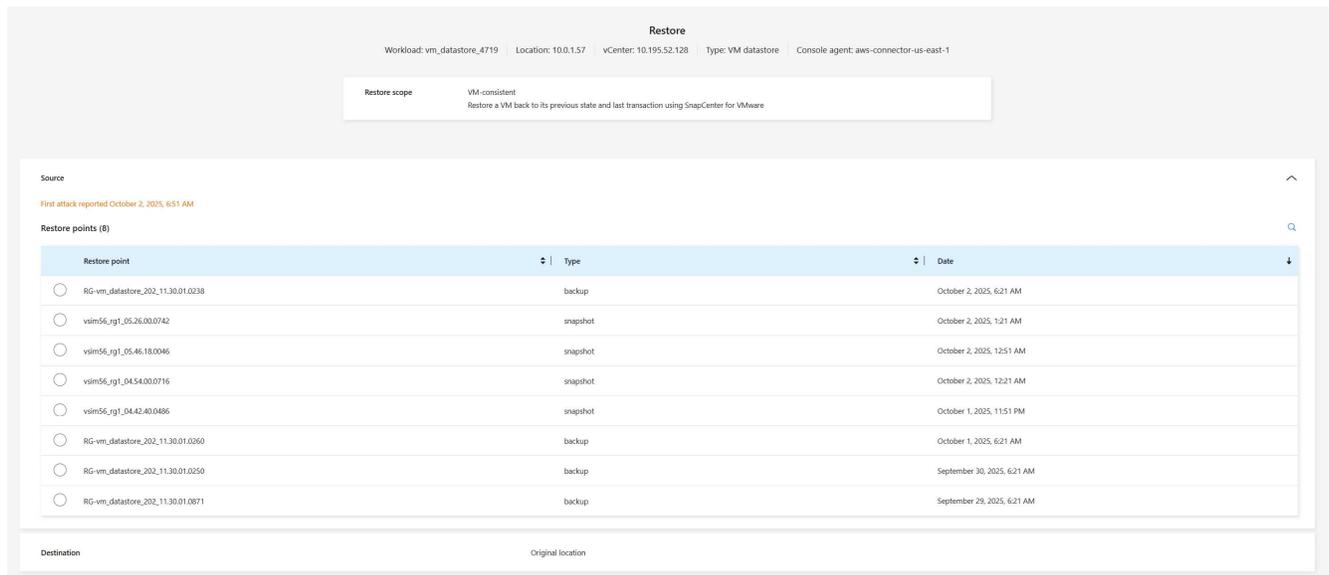
如果您沒有指定還原路徑，檔案將會還原到頂層目錄的新磁碟區。

5. 選擇*儲存*。
6. 檢查您的選擇。
7. 選擇*恢復*。
8. 從選單中，選擇「恢復」以查看「恢復」頁面上的工作負載，其中操作的狀態在各個狀態之間移動。

在 VM 層級還原 VM 檔案共享

選擇要還原的虛擬機器後，在復原頁面上繼續執行下列步驟。

1. 來源：選擇來源旁的向下箭頭查看詳細資訊。



2. 選擇要用於還原資料的還原點。
3. 目的地：返回原始位置。
4. 選擇“下一步”。
5. 檢查您的選擇。
6. 選擇*恢復*。
7. 從選單中，選擇「恢復」以查看「恢復」頁面上的工作負載，其中操作的狀態在各個狀態之間移動。

在NetApp Ransomware Resilience中進行勒索軟體攻擊準備演練

透過模擬對新樣本工作負載的攻擊來運行勒索軟體攻擊準備演習。調查模擬攻擊並恢復工作負載。使用此功能來測試警報通知、回應和恢復。根據需要經常進行演練。



您的實際工作量資料不會受到影響。

您可以對 NFS 和 CIFS (SMB) 工作負載進行準備情況演練。

配置勒索軟體攻擊準備演習

在執行模擬之前，請在「設定」頁面上設定演練。從頂部選單中的操作選項存取設定頁面。

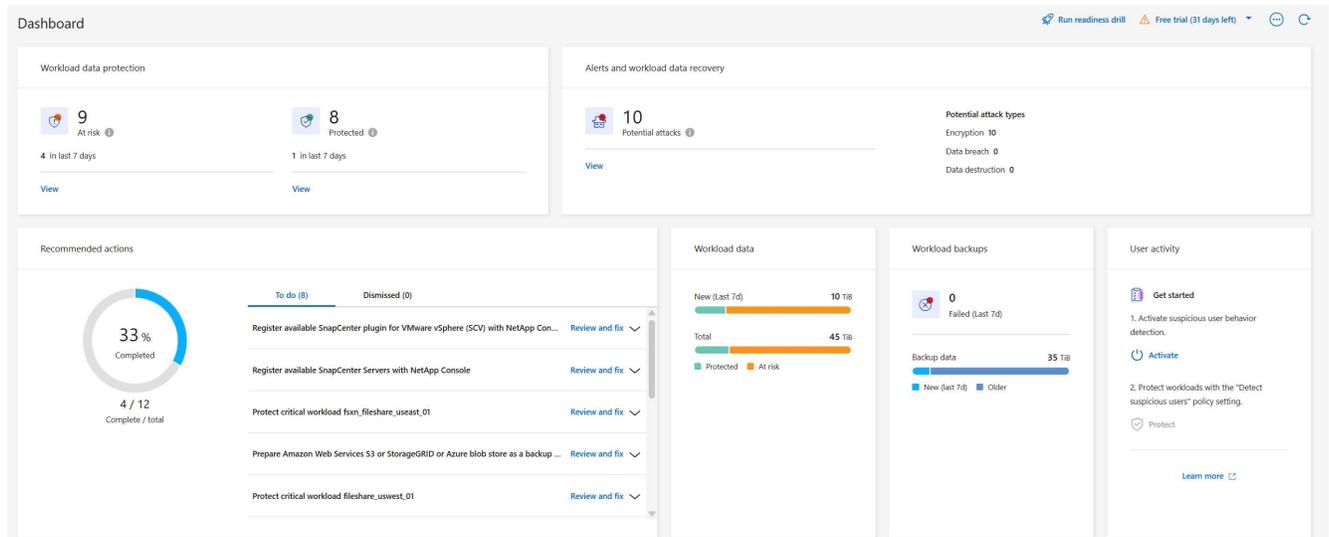
以下情況需要輸入使用者名稱和密碼：

- 如果先前選擇的儲存虛擬機器的使用者名稱或密碼發生更改
- 如果您選擇不同的 CIFS (SMB) 儲存體 VM
- 如果您輸入不同的測試工作負載名稱

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。[了解NetApp Console的勒索軟體復原角色](#)。

步驟

1. 從NetApp Ransomware Resilience選單中，選擇右上角的 執行準備演練 按鈕。



2. 在設定頁面的準備練習卡中，選擇*配置*。

控制台顯示配置準備度演練頁面。

Readiness drill

Run a simulated ransomware attack on a new test workload that will be saved in the selected system. Then, investigate the simulated attack and recover the test workload. You can run a readiness drill multiple times.

 Your real workload data will not be impacted.

Select a readiness drill test environment where the new test workload will be created.

Console agent

System

Storage VM

New test workload

 Requires 10 GiB of storage

Readiness drill type

Save

Cancel

3. 執行以下操作：

- 選擇您想要用於準備情境演練的控制台代理程式。
- 選擇一個測試系統。
- 選擇測試儲存 SVM。
- 如果您選擇了 CIFS (SMB) 儲存虛擬機，則會出現使用者名稱和密碼欄位。輸入儲存虛擬機器的使用者名稱和密碼。
- 選擇準備演習類型。若要從加密資料外洩手動恢復，請選擇自訂恢復。若要從可疑用戶活動中恢復，請選擇資料外洩。
- 輸入要建立的新測試工作負載的名稱。名稱中不要包含破折號。

4. 選擇*儲存*。



您可以稍後使用「設定」頁面編輯準備演練配置。

開始準備演習

配置準備狀況演練後，即可開始演練。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

當您開始準備演習時，勒索軟體復原力會跳過學習模式並以主動模式開始演習。工作負載的偵測狀態為「活動」。

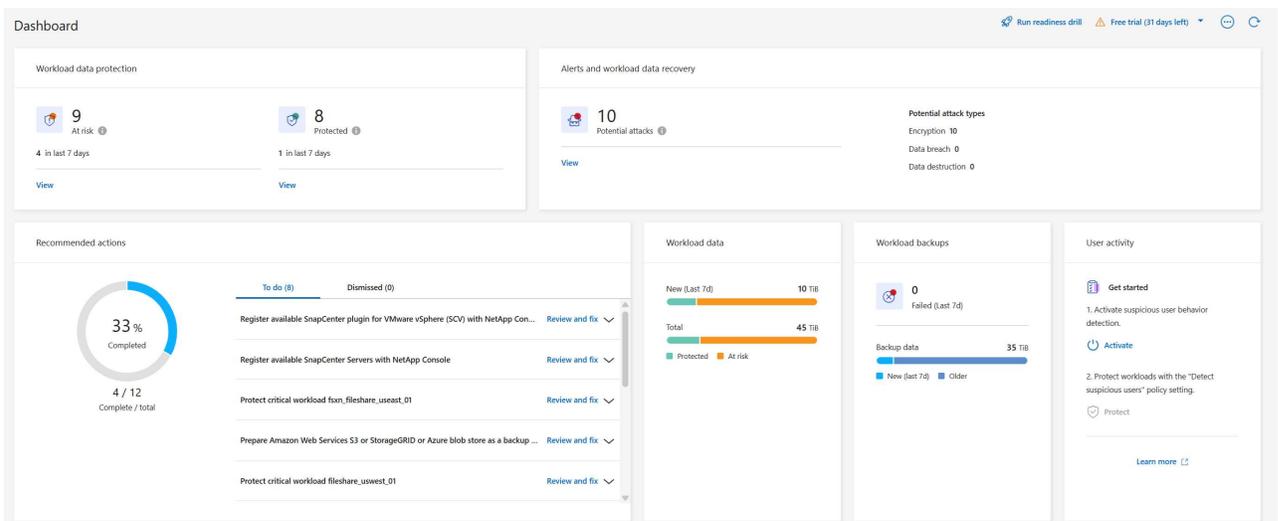


當最近分配了檢測策略並且勒索軟體恢復掃描工作負載時，工作負載可以具有勒索軟體檢測*學習模式*狀態。

步驟

1. 執行下列操作之一：

- 從勒索軟體復原選單中，選擇右上角的「運行準備演練」按鈕。



- 或者，從「設定」頁面的「準備好練習卡」中選擇「開始」。



演練運行時，您無法編輯準備演練配置。您可以重置鑽孔機以停止它並修改配置。

響應戰備演習警報

透過回應準備演習警報來測試您的準備。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

步驟

1. 從勒索軟體恢復選單中，選擇*警報*。

控制台顯示警報頁面。在警報 ID 欄位中，您會在 ID 旁看到「準備好演練」。

Alerts (6)

Alert ID	Workload	Location	Type	Status	Connector	Incidents	Impacted data	First detected
alert8727	Oracle_8821	10.0.1.193	Oracle	New	aws-connector-us-east-1	2	2 GiB	23 days ago
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	New	aws-connector-us-east-1	1	2 GiB	23 days ago
alert3932	MySQL_9294	10.0.1.10	MySQL	New	aws-connector-us-east-1	2	2 GiB	23 days ago
alert7918	vm_datastore_202_735...	10.195.52.126	VM datastore	New	onprem-connector	1	2 GiB	23 days ago
alert5319	vm_datastore_uswest_...	10.0.1.215	VM file share	New	aws-connector-us-west-1-account-LXtf4X...	1	2 GiB	23 days ago
alert1407	rps_test_gri	rps_test_readiness_drill_svm	File share	New	aws-connector-us-east-1	1	2 GiB	1 minute ago

Workload rps_test_readiness-drill-workload-test, marked restore needed. Restore workload

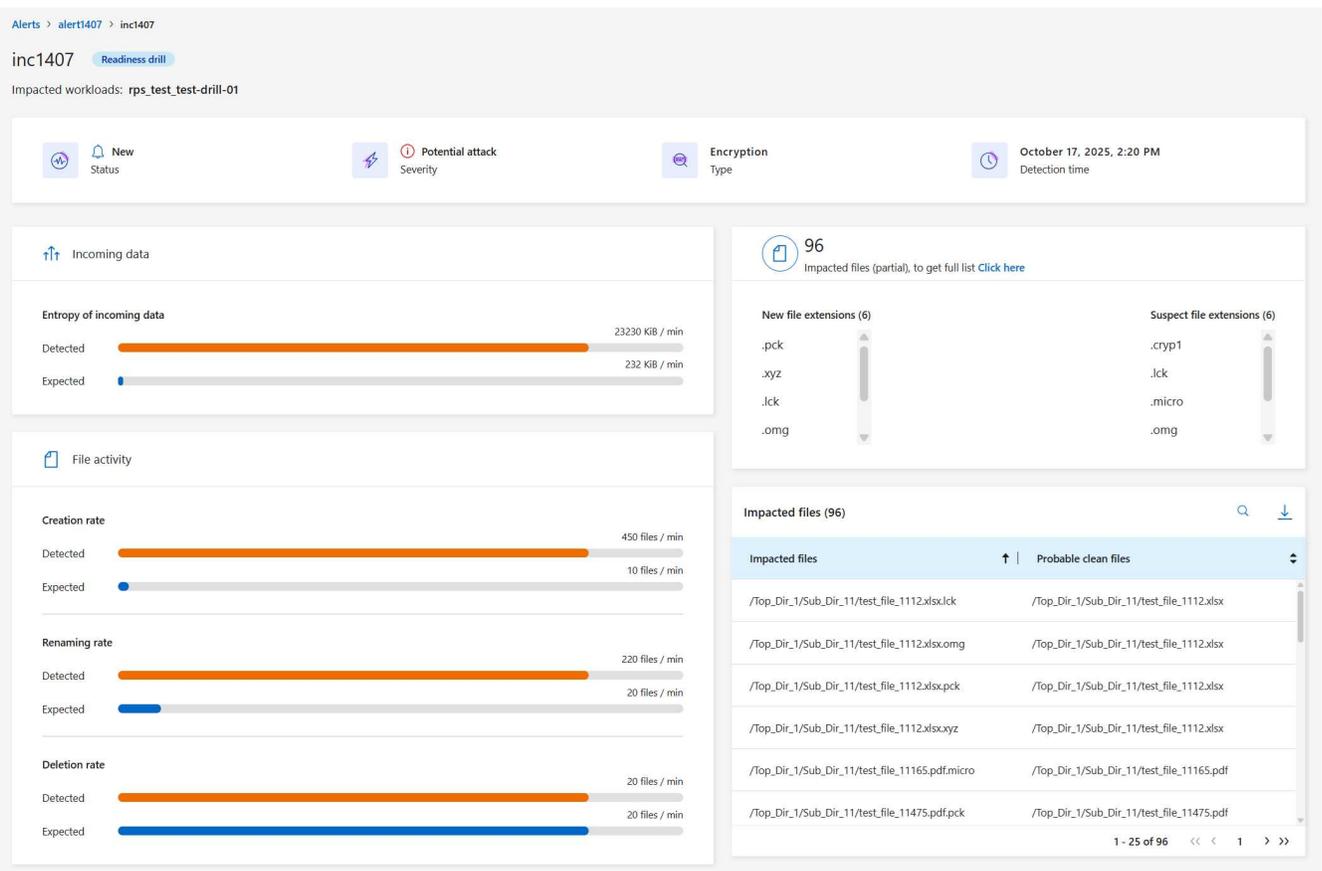
2. 選擇帶有「準備演習」指示的警報。事件警報清單出現在警報詳細資訊頁面。

Alerts (7)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data	First detected	Most rec
alert1407	rps_test_awsSystemTest	svm_rps_test_readi...	File share	Active	aws-connector-us-east-1	1	2 GiB	Just now	Just now

3. 查看警報事件。

4. 選擇一個警報事件。



以下是需要注意的一些事項：

- 查看潛在攻擊的嚴重性。
如果嚴重性表明使用者涉嫌惡意活動，請檢查使用者名稱。您還可以"封鎖該用戶。"
- 查看文件活動和可疑進程：
 - 查看傳入的檢測數據與預期數據的比較。
 - 查看偵測到的文件的建立率與預期率的比較。
 - 查看偵測到的檔案重新命名率與預期率的比較。
 - 查看刪除率與預期刪除率的比較。
- 查看受影響文件的清單。查看可能導致攻擊的擴展。
- 透過查看受影響的檔案和目錄的數量來確定攻擊的影響和廣度。

恢復測試工作負載

審查準備情況演習警報後，如有必要，恢復測試工作量。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色"。

步驟

1. 返回警報詳細資訊頁面。

2. 如果需要恢復測試工作負載，請執行下列操作：
 - 選擇*標記需要恢復*。
 - 查看確認訊息，然後在確認框中選擇*標記需要恢復*。
 - 從勒索軟體恢復選單中，選擇*恢復*。
 - 選擇要復原的標示為「準備演練」的測試工作負載。
 - 選擇*恢復*。
 - 在「還原」頁面中，提供還原的資訊：
 - 選擇來源快照副本。
 - 選擇目標磁碟區。
3. 在恢復審核頁面中，選擇*恢復*。

控制台在恢復頁面上顯示準備演練恢復的狀態為「進行中」。

恢復完成後，控制台將工作負載的狀態變更為*已復原*。

4. 查看恢復的工作負載。



有關恢復過程的詳細信息，請參閱"[從勒索軟體攻擊中恢復（事件被消除後）](#)"。

準備演練後更改警報狀態

審查準備情況演習警報並恢復工作量後，根據需要變更警報狀態。

需要控制台角色 組織管理員、資料夾或專案管理員或勒索軟體復原管理員。"[了解所有服務的控制台存取角色](#)"。

步驟

1. 返回警報詳細資訊頁面。
2. 再次選擇警報。
3. 透過選擇*編輯狀態*來指示狀態，並將狀態變更為以下之一：
 - 已解除：如果您懷疑該活動不是勒索軟體攻擊，請將狀態變更為已解除。



解除攻擊後，您將無法將其改回。如果您解除工作負載，則為應對潛在勒索軟體攻擊而自動取得的所有快照副本都將永久刪除。如果您解除警報，則準備演習即視為完成。

- 已解決：事件已得到緩解。

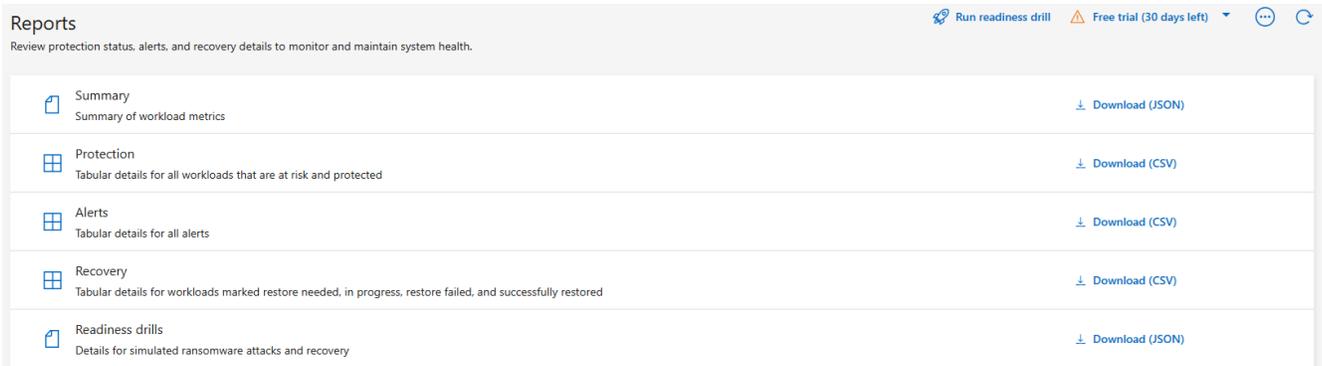
審查準備演習報告

準備演習完成後，您可能需要查看並儲存演習報告。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

步驟

1. 從勒索軟體恢復選單中，選擇*報告*。



2. 選擇*準備演習*和*下載*以下載準備演習報告。

將 NetApp Ransomware Resilience 連接到安全性與事件管理系統 (SIEM)，以進行威脅分析與偵測

安全資訊和事件管理系統 (SIEM) 集中管理日誌和事件數據，以便深入了解安全事件和合規性。NetApp Ransomware Resilience 支援自動將資料傳送到您的 SIEM，從而簡化威脅分析和偵測流程。

Ransomware Resilience 支援下列 SIEM：

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

在 Ransomware Resilience 中啟用 SIEM 之前，您需要設定您的 SIEM 系統。

傳送至 **SIEM** 的事件資料

Ransomware Resilience 可以將以下事件資料傳送到您的 SIEM 系統：

- 情境:
 - **os**：這是一個具有 ONTAP 值的常數。
 - **os_version**：系統上執行的 ONTAP 版本。
 - **connector_id**：管理系統的控制台代理的 ID。
 - **cluster_id**：ONTAP 為系統報告的叢集 ID。
 - **svm_name**：發現警報的 SVM 的名稱。
 - **volume_name**：發現警報的磁碟區的名稱。
 - **volume_id**：ONTAP 為系統報告的磁碟區的 ID。
- 事件：

- **incident_id**：勒索軟體復原力針對勒索軟體復原力中受到攻擊的捲所產生的事件 ID。
- **alert_id**：勒索軟體復原能力為工作負載產生的 ID。
- 嚴重性：以下警報等級之一：「嚴重」、「高」、「中」、「低」。
- 描述：有關檢測到的警報的詳細信息，例如“在工作負載 arp_learning_mode_test_2630 上檢測到潛在的勒索軟體攻擊”

設定 AWS Security Hub 進行威脅偵測

在 Ransomware Resilience 中啟用 AWS Security Hub 之前，您需要在 AWS Security Hub 中執行以下幾個主要步驟：

- 在 AWS Security Hub 中設定權限。
- 在 AWS Security Hub 中設定身份驗證存取金鑰和金鑰。（此處未提供這些步驟。）

在 **AWS Security Hub** 中設定權限的步驟

1. 前往 **AWS IAM** 控制台。
2. 選擇*政策*。
3. 使用以下 JSON 格式的程式碼建立策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

設定 Microsoft Sentinel 進行威脅偵測

在 Ransomware Resilience 中啟用 Microsoft Sentinel 之前，您需要在 Microsoft Sentinel 中執行下列高階步驟：

- 先決條件

- 啟用 Microsoft Sentinel。
- 在 Microsoft Sentinel 中建立自訂角色。
- 登記
 - 註冊 Ransomware Resilience 以接收來自 Microsoft Sentinel 的事件。
 - 為註冊創建一個秘密。
- 權限：為應用程式指派權限。
- 身份驗證：輸入應用程式的身份驗證憑證。

啟用 **Microsoft Sentinel** 的步驟

1. 前往 Microsoft Sentinel。
2. 建立*Log Analytics 工作區*。
3. 啟用 Microsoft Sentinel 以使用您剛剛建立的 Log Analytics 工作區。

在 **Microsoft Sentinel** 中建立自訂角色的步驟

1. 前往 Microsoft Sentinel。
2. 選擇*訂閱* > 存取控制 (**IAM**)。
3. 輸入自訂角色名稱。使用名稱 **Ransomware Resilience Sentinel Configurator**。
4. 複製以下 JSON 並將其貼上到 **JSON** 標籤中。

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes": ["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. 檢查並儲存您的設定。

註冊勒索軟體復原能力以接收來自 **Microsoft Sentinel** 的事件的步驟

1. 前往 Microsoft Sentinel。
2. 選擇 **Entra ID** > 應用程式 > 應用程式註冊。
3. 對於應用程式的*顯示名稱*，輸入「**Ransomware Resilience**」。
4. 在 支援的帳戶類型 欄位中，選擇 僅限此組織目錄中的帳戶。
5. 選擇將推送事件的*預設索引*。
6. 選擇*審核*。
7. 選擇*註冊*來儲存您的設定。

註冊後，Microsoft Entra 管理中心將顯示應用程式概述窗格。

建立註冊密鑰的步驟

1. 前往 Microsoft Sentinel。
2. 選擇*憑證和機密* > 客戶端機密 > 新客戶端機密。
3. 為您的應用程式機密新增描述。
4. 為秘密選擇一個*到期日*或指定自訂有效期限。



客戶端金鑰的有效期限限制為兩年（24 個月）或更短。Microsoft 建議您設定小於 12 個月的到期值。

5. 選擇“新增”來建立您的秘密。
6. 記錄身份驗證步驟中使用的秘密。離開此頁面後，該秘密將不再顯示。

為應用程式指派權限的步驟

1. 前往 Microsoft Sentinel。
2. 選擇*訂閱* > 存取控制 (IAM)。
3. 選擇*新增* > 新增角色分配。
4. 對於*特權管理員角色*字段，選擇*勒索軟體彈性哨兵配置器*。



這是您之前創建的自訂角色。

5. 選擇“下一步”。
6. 在*指派存取權限*欄位中，選擇*使用者、群組或服務主體*。
7. 選擇“選擇成員”。然後，選擇*Ransomware Resilience Sentinel Configurator*。
8. 選擇“下一步”。
9. 在*使用者可以做什麼*欄位中，選擇*允許使用者指派除特權管理員角色擁有者、UAA、RBAC（建議）之外的所有角色*。
10. 選擇“下一步”。
11. 選擇*審核並分配*來分配權限。

輸入應用程式驗證憑證的步驟

1. 前往 Microsoft Sentinel。
2. 輸入憑證：
 - a. 輸入租用用戶 ID、客戶端應用程式 ID 和客戶端應用程式金鑰。
 - b. 選擇 **Authenticate**。



認證成功後，會出現「已認證」的資訊。

3. 輸入應用程式的 Log Analytics 工作區詳細資訊。
 - a. 選擇訂閱 ID、資源群組和 Log Analytics 工作區。

設定 Splunk Cloud 進行威脅偵測

在 Ransomware Resilience 中啟用 Splunk Cloud 之前，您需要在 Splunk Cloud 中執行下列進階步驟：

- 在 Splunk Cloud 中啟用 HTTP 事件收集器以透過 HTTP 或 HTTPS 從控制台接收事件資料。
- 在 Splunk Cloud 中建立事件收集器令牌。

在 **Splunk** 中啟用 **HTTP** 事件收集器的步驟

1. 轉到 Splunk Cloud。
2. 選擇*設定* > 資料輸入。
3. 選擇 **HTTP** 事件收集器 > 全域設定。
4. 在所有令牌切換上，選擇*已啟用*。
5. 若要讓事件收集器透過 HTTPS 而不是 HTTP 進行監聽和通信，請選擇「啟用 SSL」。
6. 在「HTTP 連接埠號碼」中輸入 HTTP 事件收集器的連接埠。

在 **Splunk** 中建立事件收集器令牌的步驟

1. 轉到 Splunk Cloud。
2. 選擇*設定* > 新增資料。
3. 選擇*監控* > **HTTP** 事件收集器。
4. 輸入令牌的名稱並選擇*下一步*。
5. 選擇將推播事件的*預設索引*，然後選擇*審核*。
6. 確認端點的所有設定正確，然後選擇*提交*。
7. 複製令牌並將其貼上到另一個文件中，以準備進行身份驗證步驟。

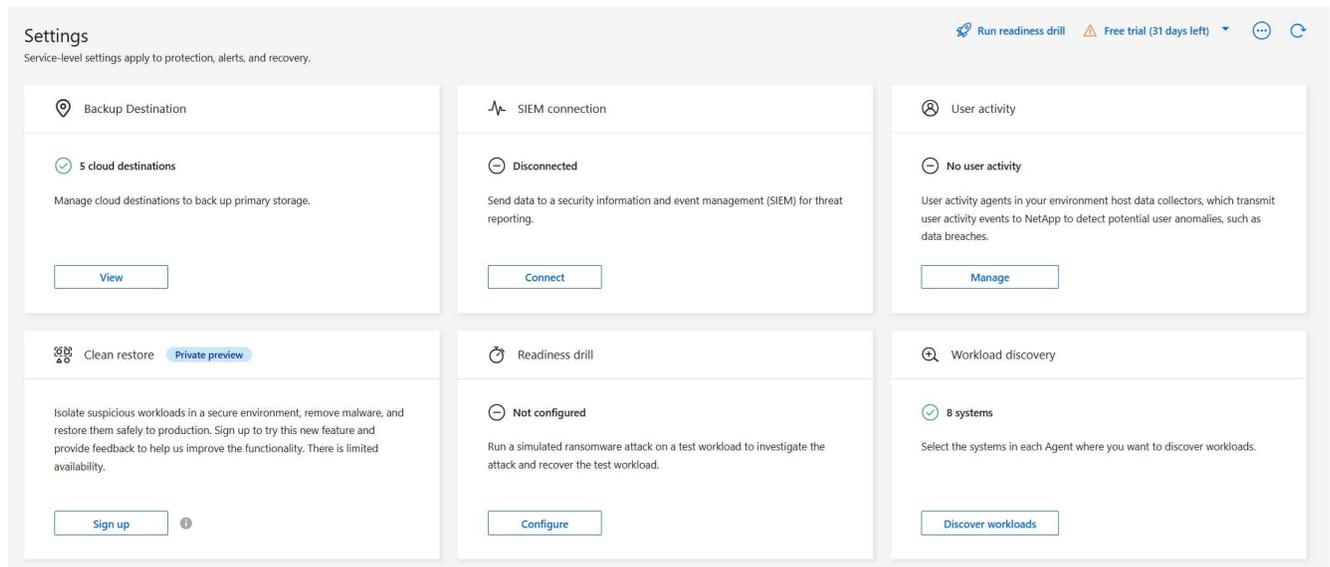
在勒索軟體防禦中連接 SIEM

啟用 SIEM 會將勒索軟體復原資料傳送到您的 SIEM 伺服器以進行威脅分析和報告。

步驟

1. 從控制台選單中，選擇*保護*>*勒索軟體恢復*。
2. 從勒索軟體恢復選單中，選擇垂直  ... 右上角的選項。
3. 選擇“設定”。

出現「設定」頁面。



4. 在「設定」頁面中，選擇 SIEM 連線圖塊中的「連線」。



5. 選擇其中一個 SIEM 系統。
6. 輸入您在 AWS Security Hub 或 Splunk Cloud 中配置的令牌和驗證詳細資訊。

 您輸入的資訊取決於您選擇的 SIEM。

7. 選擇*啟用*。

設定頁面顯示「已連線」。

在NetApp Ransomware Resilience中下載報告

NetApp Ransomware Resilience 提供 CSV 和 JSON 格式的報告，詳細展示受支援和不受支援的磁碟區、攻擊準備演練、防護、警示和還原情況。使用這些報告，您可以儲存並離線查看有關演練、防護狀態、警示和還原事件的報告。



下載檔案之前，請先刷新儀表板以取得報告中的最新資料。

所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員、勒索軟體復原管理員或勒索軟體復原檢視器角色。"[了解NetApp Console的勒索軟體復原角色](#)"。

*您可以下載哪些資料？ *您可以從任何主選單選項下載檔案：

- 摘要：包括支援和不受支援的工作負載清單、改善網路彈性態勢的建議措施，以及勒索軟體彈性儀表板中捕獲的資訊。
- 保護：包括所有工作負載的狀態和詳細信息，包括受保護和處於風險中的工作負載總數。
- 警報：包括所有警報的狀態和詳細信息，包括警報總數和自動快照。
- 恢復：包括所有需要恢復的工作負載的狀態和詳細信息，包括標記為“需要恢復”、“進行中”、“恢復失敗”和“恢復成功”的工作負載總數。
- 報告：您可以從任何頁面匯出資料並下載檔案。



您只能從*報告*頁面下載準備情況演習報告。

如果您從保護、警報或復原頁面下載 CSV 或 JSON 文件，則資料僅顯示該頁面上的資料。

CSV 或 JSON 檔案包含所有控制台系統上所有工作負載的資料。

步驟

1. 從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。

The screenshot shows the NetApp console dashboard with the following sections:

- Workload data protection:** 9 At risk (4 in last 7 days), 8 Protected (1 in last 7 days).
- Alerts and workload data recovery:** 10 Potential attacks. Potential attack types: Encryption 10, Data breach 0, Data destruction 0.
- Recommended actions:** 33% Completed (4 / 12). Actions include: Register available SnapCenter plugin for VMware vSphere (SCV) with NetApp Con..., Register available SnapCenter Servers with NetApp Console, Protect critical workload fsm, fileshare_uswest_01, Prepare Amazon Web Services S3 or StorageGRID or Azure blob store as a backup..., Protect critical workload fileshare_uswest_01.
- Workload data:** New (Last 7d) 10 TiB, Total 45 TiB. Legend: Protected (green), At risk (orange).
- Workload backups:** 0 Failed (Last 7d). Backup data 35 TiB. Legend: New (last 7d) (blue), Older (grey).
- User activity:** Get started steps: 1. Activate suspicious user behavior detection. 2. Protect workloads with the "Detect suspicious users" policy setting. Status: Protect.

2. 在儀表板或其他頁面中，選擇右上角的 **Refresh**  選項，即可重新整理報告中顯示的資料。
3. 執行下列操作之一：

- 從頁面選擇*下載*  選項。
- 從NetApp Ransomware Resilience選單中，選擇 報告。

4. 如果您選擇了“報告”選項，請選擇預先配置的檔案名稱並選擇“下載”。

Reports Run readiness drill Free trial (30 days left) ⋮ ↻

Review protection status, alerts, and recovery details to monitor and maintain system health.

 Summary Summary of workload metrics	Download (JSON)
 Protection Tabular details for all workloads that are at risk and protected	Download (CSV)
 Alerts Tabular details for all alerts	Download (CSV)
 Recovery Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored	Download (CSV)
 Readiness drills Details for simulated ransomware attacks and recovery	Download (JSON)

知識和支持

註冊以獲得支持

需要進行支援註冊才能獲得針對NetApp Console及其儲存解決方案和資料服務的技術支援。還需要支援註冊才能啟用Cloud Volumes ONTAP系統的關鍵工作流程。

註冊支援並不能使NetApp獲得雲端提供者文件服務的支援。有關雲端提供者文件服務、其基礎設施或使用該服務的任何解決方案的技術支持，請參閱該產品文件中的「取得協助」。

- ["適用於ONTAP 的Amazon FSx"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

支援註冊概述

啟動支持權利的註冊方式有兩種：

- 註冊您的NetApp Console帳戶序號（您的 20 位元 960xxxxxxxx 序號位於控制台中的「支援資源」頁面上）。

這可作為控制台內任何服務的單一支援訂閱 ID。每個控制台帳戶都必須註冊。

- 在您的雲端供應商市場中註冊與訂閱相關的Cloud Volumes ONTAP序號（這些是 20 位元 909201xxxxxxxx 序號）。

這些序號通常稱為_PAYGO 序號_，由NetApp Console在Cloud Volumes ONTAP部署時產生。

註冊兩種類型的序號可以實現開立支援票和自動產生案例等功能。透過將NetApp支援網站 (NSS) 帳戶新增至控制台即可完成註冊，如下所述。

註冊NetApp Console以取得NetApp支持

要註冊支援並啟動支援權利，您的NetApp Console帳戶中的一名使用者必須將NetApp支援網站帳戶與其控制台登入名稱關聯。如何註冊NetApp支援取決於您是否已經擁有NetApp支援網站 (NSS) 帳號。

擁有 NSS 帳戶的現有客戶

如果您是擁有 NSS 帳戶的NetApp客戶，只需透過控制台註冊即可獲得支援。

步驟

1. 選擇“管理”>“憑證”。
2. 選擇*使用者憑證*。
3. 選擇*新增 NSS 憑證*並依照NetApp支援網站 (NSS) 驗證提示進行操作。
4. 若要確認註冊過程是否成功，請選擇「幫助」圖標，然後選擇「支援」。

*資源*頁面應顯示您的控制台帳戶已註冊以獲得支援。

請注意，如果其他控制台使用者尚未將NetApp支援網站帳戶與其登入名稱關聯，他們將看不到相同的支援註冊狀態。但是，這並不意味著您的帳戶沒有註冊支援。只要組織中的一名使用者遵循了這些步驟，您的帳戶就已註冊。

現有客戶但沒有 NSS 帳戶

如果您是現有的NetApp客戶，擁有現有授權和序號但沒有 NSS 帳戶，則需要建立 NSS 帳戶並將其與您的控制台登入關聯。

步驟

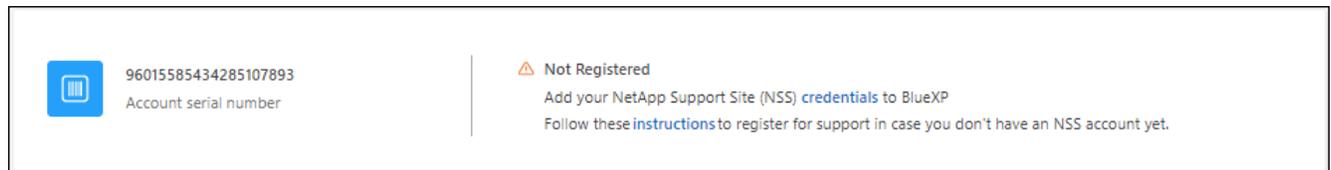
1. 透過完成以下操作建立NetApp支援網站帳戶 "[NetApp支援網站使用者註冊表](#)"
 - a. 請務必選擇適當的使用者級別，通常為* NetApp客戶/最終使用者*。
 - b. 請務必複製上面用於序號欄位的控制台帳戶序號（960xxxx）。這將加快帳戶處理速度。
2. 完成以下步驟，將您的新 NSS 帳戶與您的控制台登入名稱關聯。[擁有 NSS 帳戶的現有客戶](#)。

NetApp全新產品

如果您是NetApp新使用者且沒有 NSS 帳戶，請依照下列步驟操作。

步驟

1. 在控制台的右上角，選擇「幫助」圖標，然後選擇「支援」。
2. 從支援註冊頁面找到您的帳戶 ID 序號。



3. 導航至 "[NetApp 的支援註冊網站](#)"並選擇*我不是註冊的NetApp客戶*。
4. 填寫必填欄位（帶有紅色星號的欄位）。
5. 在*產品線*欄位中，選擇*雲端管理員*，然後選擇適用的計費提供者。
6. 從上面的步驟 2 複製您的帳戶序號，完成安全性檢查，然後確認您已閱讀 NetApp 的全球資料隱私政策。

一封電子郵件會立即發送到提供的郵箱以完成此安全交易。如果幾分鐘內沒有收到驗證電子郵件，請務必檢查您的垃圾郵件資料夾。

7. 從電子郵件中確認操作。

確認向NetApp提交您的請求並建議您建立NetApp支援網站帳戶。

8. 透過完成以下操作建立NetApp支援網站帳戶 "[NetApp支援網站使用者註冊表](#)"
 - a. 請務必選擇適當的使用者級別，通常為* NetApp客戶/最終使用者*。
 - b. 請務必複製上面用於序號欄位的帳戶序號（960xxxx）。這將加快處理速度。

完成後

NetApp應該在過程中與您聯繫。這是針對新用戶的一次性入職培訓。

擁有NetApp支援網站帳號後，請依照下列步驟將該帳號與您的控制台登入關聯擁有 [NSS 帳戶的現有客戶](#)。

關聯 NSS 憑證以獲得Cloud Volumes ONTAP支持

需要將NetApp支援網站憑證與您的控制台帳戶關聯，才能為Cloud Volumes ONTAP啟用以下關鍵工作流程：

- 註冊即用即付Cloud Volumes ONTAP系統以獲得支持
需要您的 NSS 帳戶才能啟動對您的系統的支援並獲得NetApp技術支援資源的存取權限。
- 自帶授權 (BYOL) 時部署Cloud Volumes ONTAP
需要您的 NSS 帳戶，以便控制台可以上傳您的許可證金鑰並啟用您購買的期限的訂閱。這包括期限續訂的自動更新。
- 將Cloud Volumes ONTAP軟體升級至最新版本

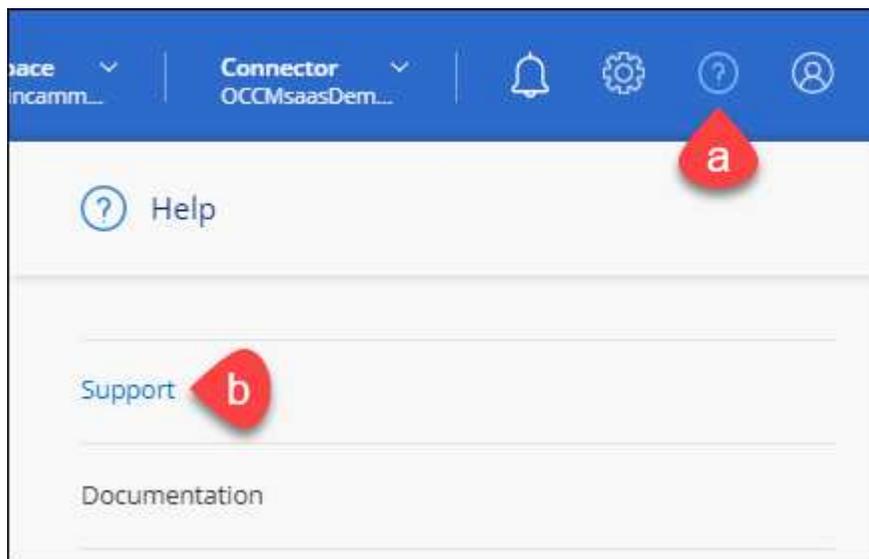
將 NSS 憑證與您的NetApp Console帳戶關聯與將 NSS 帳戶與控制台使用者登入相關聯。

這些 NSS 憑證與您的特定控制台帳戶 ID 相關聯。屬於控制台組織的使用者可以從*支援 > NSS 管理*存取這些憑證。

- 如果您有客戶級帳戶，則可以新增一個或多個 NSS 帳戶。
- 如果您有合作夥伴或經銷商帳戶，則可以新增一個或多個 NSS 帳戶，但不能與客戶級帳戶一起新增。

步驟

1. 在控制台的右上角，選擇「幫助」圖標，然後選擇「支援」。



2. 選擇*NSS 管理 > 新增 NSS 帳號*。
3. 當出現提示時，選擇「繼續」以重新導向至 Microsoft 登入頁面。

NetApp使用 Microsoft Entra ID 作為特定於支援和授權的身份驗證服務的身份提供者。

4. 在登入頁面，提供您的NetApp支援網站註冊的電子郵件地址和密碼以執行驗證程序。

這些操作使控制台能夠使用您的 NSS 帳戶進行許可證下載、軟體升級驗證和未來支援註冊等操作。

請注意以下事項：

- NSS 帳戶必須是客戶級帳戶（不是訪客或臨時帳戶）。您可以擁有多個客戶級 NSS 帳戶。
- 如果該帳戶是合作夥伴等級帳戶，則只能有一個 NSS 帳戶。如果您嘗試新增客戶級 NSS 帳戶且合作夥伴級帳戶已存在，您將收到以下錯誤訊息：

“此帳戶不允許使用 NSS 客戶類型，因為已經存在不同類型的 NSS 用戶。”

如果您已有客戶級 NSS 帳戶並嘗試新增合作夥伴級帳戶，情況也是如此。

- 成功登入後，NetApp將儲存 NSS 使用者名稱。

這是系統產生的映射到您的電子郵件的 ID。在*NSS 管理*頁面上，您可以顯示來自 **...** 菜單。

- 如果您需要刷新登入憑證令牌，還有一個*更新憑證*選項 **...** 菜單。

使用此選項會提示您再次登入。請注意，這些帳戶的令牌將在 90 天後過期。我們將發布通知來提醒您此事。

獲取協助

NetApp以多種方式為NetApp Console及其雲端服務提供支援。全天候提供廣泛的免費自助支援選項，例如知識庫 (KB) 文章和社群論壇。您的支援註冊包含透過網路工單取得的遠端技術支援。

獲取雲端提供者文件服務的支持

有關雲端提供者文件服務、其基礎設施或使用該服務的任何解決方案的技術支持，請參閱該產品的文檔。

- ["適用於ONTAP 的Amazon FSx"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

要獲得特定於NetApp及其儲存解決方案和資料服務的技術支持，請使用下面所述的支援選項。

使用自助選項

這些選項每週 7 天、每天 24 小時免費提供：

- 文件
您目前正在檢視的NetApp Console文件。
- ["知識庫"](#)

搜尋NetApp知識庫以尋找有助於解決問題的文章。

- ["社群"](#)

加入NetApp Console社區，關注正在進行的討論或創建新的討論。

向NetApp支援建立案例

除了上述自助支援選項之外，您還可以在啟動支援後與NetApp支援專家合作解決任何問題。

開始之前

- 若要使用「建立案例」功能，您必須先將您的NetApp支援網站憑證與您的控制台登入關聯。["了解如何管理與控制台登入相關的憑證"](#)。
- 如果您要為具有序號的ONTAP系統開啟案例，那麼您的NSS帳戶必須與該系統的序號相關聯。

步驟

1. 在NetApp Console中，選擇「說明」>「支援」。
2. 在「資源」頁面上，選擇「技術支援」下的可用選項之一：
 - a. 如果您想透過電話與某人交談，請選擇「致電我們」。您將被引導至 netapp.com 上的一個頁面，其中列出了您可以撥打的電話號碼。
 - b. 選擇「建立案例」向NetApp支援專家開立票據：
 - 服務：選擇與問題相關的服務。例如，* NetApp Console* 特定於控制台內的工作流程或功能的技術支援問題。
 - 系統：如果適用於存儲，請選擇* Cloud Volumes ONTAP* 或 **On-Prem**，然後選擇相關的工作環境。

系統清單位於控制台組織範圍內，並且您在頂部橫幅中選擇了控制台代理。
 - 個案優先級：選擇個案的優先級，可以是低、中、高或嚴重。

要了解有關這些優先事項的更多詳細信息，請將滑鼠懸停在欄位名稱旁邊的資訊圖示上。
 - 問題描述：提供問題的詳細描述，包括任何適用的錯誤訊息或您執行的故障排除步驟。
 - 其他電子郵件地址：如果您想讓其他人知道此問題，請輸入其他電子郵件地址。
 - 附件（選購）：一次最多上傳五個附件。

每個附件檔案大小限制為 25 MB。支援以下檔案副檔名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

ntapitdemo 
NetApp Support Site Account

Service Working Environment

Select Select

Case Priority 

Low - General guidance ▼

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional) 

Type here

Attachment (Optional) Upload 

No files selected  

完成後

將會出現一個彈出窗口，其中顯示您的支援案例編號。NetApp支援專家將審查您的案例並儘快回覆您。

若要查看支援案例的歷史記錄，您可以選擇*設定>時間軸*並尋找名為「建立支援案例」的操作。最右邊的按鈕可讓您展開操作以查看詳細資訊。

嘗試建立案例時，您可能會遇到以下錯誤訊息：

“您無權針對所選服務建立案例”

此錯誤可能表示 NSS 帳戶及其關聯的記錄公司與NetApp Console帳戶序號的記錄公司不同（即。960xxxx）或工作環境序號。您可以使用以下選項之一尋求協助：

- 提交非技術案例 <https://mysupport.netapp.com/site/help>

管理您的支援案例

您可以直接從控制台檢視和管理活動和已解決的支援案例。您可以管理與您的 NSS 帳戶和公司相關的案例。

請注意以下事項：

- 頁面頂部的案例管理儀表板提供兩種視圖：
 - 左側視圖顯示了您提供的使用者 NSS 帳戶在過去 3 個月內開啟的案件總數。
 - 右側的視圖根據您的使用者 NSS 帳戶顯示了過去 3 個月內貴公司層級開設的案件總數。表中的結果反映了與您選擇的視圖相關的案例。
- 您可以新增或刪除感興趣的列，並且可以過濾優先順序和狀態等列的內容。其他欄位僅提供排序功能。請查看以下步驟以了解更多詳細資訊。
- 在每個案件級別，我們提供更新案件記錄或關閉尚未關閉或待關閉狀態的案件的案件的功能。

步驟

1. 在 NetApp Console 中，選擇「說明」>「支援」。
2. 選擇*案例管理*，如果出現提示，請將您的 NSS 帳戶新增至控制台。

案例管理*頁面顯示與您的控制台使用者帳戶關聯的 **NSS** 帳戶相關的未結案例。這與出現在 ***NSS** 管理 頁面頂部的 NSS 帳戶相同。

3. (可選) 修改表中顯示的資訊：
 - 在「組織的案例」下，選擇「查看」以查看與您的公司相關的所有案例。
 - 透過選擇精確的日期範圍或選擇不同的時間範圍來修改日期範圍。
 - 過濾列的內容。
 - 透過選擇  然後選擇您想要顯示的列。
4. 透過選擇管理現有案例  並選擇其中一個可用選項：
 - 查看案例：查看有關特定案例的完整詳細資訊。
 - 更新案例說明：提供有關您的問題的更多詳細信息，或選擇*上傳文件*以附加最多五個文件。

每個附件檔案大小限制為 25 MB。支援以下檔案副檔名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

- 結案：提供有關結案原因的詳細信息，然後選擇*結案*。

關於NetApp Ransomware Resilience的常見問題解答

如果您只是想快速找到有關NetApp Ransomware Resilience的問題的答案，那麼這個常見問題解答可以提供協助。

部署

使用勒索軟體恢復功能需要許可證嗎？

您可以使用以下許可證類型：

- 註冊 30 天免費試用。
- 透過 Amazon Web Services (AWS) Marketplace、Google Cloud Marketplace 和 Microsoft Azure Marketplace 購買NetApp Intelligent Services和勒索軟體復原的即用即付 (PAYGO) 訂閱。
- 自帶授權 (BYOL)，即您從NetApp銷售代表取得的NetApp授權文件 (NLF)。您可以使用許可證序號在控制台的「Licenses and subscriptions」部分啟動 BYOL。

如何啟用勒索軟體防禦能力？

您可以從NetApp Console存取勒索軟體復原功能。請確保您已 ["訪問角色"](#) 和 ["先決條件"](#)。如果您已成功設定控制台代理，則可以執行下列操作：["發現工作負載"](#)。

有關詳細信息，請參閱["存取勒索軟體彈性"](#)和["勒索軟體抵禦能力快速入門指南"](#)。

勒索軟體防護是否提供標準模式、限制模式和私有模式？

勒索軟體恢復功能目前僅在標準模式下可用。

有關所有NetApp資料服務中這些模式的說明，請參閱 ["NetApp Console部署模式"](#)。

使用權

勒索軟體復原能力網址是什麼？

在瀏覽器中輸入 ["https://console.netapp.com/ransomware-resilience"](https://console.netapp.com/ransomware-resilience) 訪問控制台。

存取權限是如何管理的？

["了解所有服務的控制台存取角色"](#)。勒索軟體復原能力也具備 ["專用存取角色"](#)。

哪種設備解析度最佳？

勒索軟體恢復的建議設備解析度為 1920x1080 或更高。

我該使用哪個瀏覽器？

您可以使用任何現代網頁瀏覽器存取NetApp Console。

互通性

Ransomware Resilience 是否了解ONTAP中的保護設定？

是的，Ransomware Resilience 發現了在ONTAP中設定的快照計劃。

勒索軟體復原功能如何與**NetApp Backup and Recovery**和**SnapCenter**互動？

勒索軟體復原功能與備份和復原功能協同工作，以發現並設定檔案共享工作負載的快照和備份策略。

Ransomware Resilience 可與 SnapCenter 或 SnapCenter for VMware 搭配使用，以發現並設定應用程式和虛擬機器工作負載的快照和備份策略。目前，您無法將 Ransomware Resilience 與 SnapCenter 搭配使用進行復原。

NetApp Ransomware Resilience 也可與 NetApp Backup and Recovery 搭配使用，以執行檔案和工作負載一致的還原。

對於許可和計費，即使您沒有單獨的備份和復原許可證，勒索軟體復原功能也可以與備份和復原功能整合。如果您同時擁有備份和復原以及勒索軟體復原功能，則受這兩種產品保護的任何公開資料僅由勒索軟體復原功能計費。

工作負載

在勒索軟體防禦的脈絡下，什麼是工作負載？

工作負載是一個應用程式、一個虛擬機器或一個檔案共用。工作負載包括單一應用程式執行個體所使用的所有磁碟區。

例如，考慮部署在 ora3.host.com 上的 Oracle 資料庫。vol11 包含數據和 vol12 包含日誌。這兩個磁碟區構成了該 Oracle 資料庫執行個體的工作負載。

勒索軟體復原能力如何決定工作負載資料的優先順序？

工作負載優先順序（關鍵、標準、重要）由已應用於與工作負載關聯的每個磁碟區的快照頻率和排程備份決定。

["了解工作負載優先順序或重要性"](#)。

勒索軟體復原能力支援哪些工作負載？

勒索軟體復原能力可以識別以下工作負載：Oracle、檔案共享、區塊儲存、虛擬機器和虛擬機器資料儲存。

如果您正在使用 SnapCenter 或 SnapCenter for VMware，則這些產品支援的所有工作負載也會在 Ransomware Resilience 中被識別。

如何將資料與工作負載關聯？

勒索軟體復原能力會發現捲和檔案副檔名，並將它們與相應的工作負載關聯起來。

如果您擁有 SnapCenter 或 SnapCenter for VMware，並且在備份和復原中配置了工作負載，那麼勒索軟體復原功能將發現由 SnapCenter 和 SnapCenter for VMware 管理的工作負載及其關聯的磁碟區。

什麼是受保護的工作負載？

在勒索軟體復原能力中，當工作負載啟用了主要偵測策略時，其狀態將顯示為“受保護”，這意味著 **"自主勒索軟體防護 (ARP)"** 已在與工作負載相關的所有磁碟區上啟用。

什麼是「高風險」工作量？

如果工作負載未啟用主偵測策略，即使啟用了備份和快照策略，也會被標記為「有風險」。為了防止勒索軟體攻擊，您應該啟用... **"檢測策略"**。

我新增了一個新卷，但它還沒有顯示出來。我該怎麼辦？

如果您在環境中新增加了新磁碟區，請重新啟動工作負載發現。在發現體積後，"[採取保護策略以保護新增容量](#)"。

保護策略

勒索軟體復原策略是否可以與其他類型的工作負載策略共存？

目前，備份和復原（雲端備份）支援每個磁碟區一個備份策略。如果您使用備份和復原功能來設定備份保護，它將與勒索軟體復原功能共用備份策略。

快照副本不受限制，可以從每個服務單獨新增。

勒索軟體防護策略需要哪些策略？

一個 "[勒索軟體防護策略](#)" 需要：

- 勒索軟體偵測策略，以及
- 快照策略

勒索軟體抵禦策略中不需要備份策略。

Ransomware Resilience 是否了解ONTAP中的保護設定？

是的，Ransomware Resilience 可以發現 ONTAP 中設定的快照排程。它還可以發現已發現工作負載中的所有磁碟區是否都啟用了 ARP 和 FPolicy。您在 Ransomware Resilience 儀表中看到的資訊是從其他 NetApp 解決方案和產品彙總而來。

勒索軟體復原功能是否了解備份和復原以及SnapCenter中已製定的策略？

是的，如果您在備份和復原或SnapCenter中管理工作負載，則這些產品管理的策略將納入勒索軟體復原能力。

能否修改從NetApp Backup and Recovery和/或SnapCenter繼承的策略？

不可以，您無法從 Ransomware Resilience 修改由備份和還原或SnapCenter管理的政策。您可以在「備份和復原」或SnapCenter中管理對這些政策的任何變更。

如果ONTAP中存在政策（例如 ARP、FPolicy 和快照），這些策略是否會在勒索軟體復原功能中變更？

不會。勒索軟體復原不會修改ONTAP中的任何現有偵測策略（ARP、FPolicy 設定）。

註冊勒索軟體復原功能後，如果在備份和復原或SnapCenter中新增政策會發生什麼情況？

勒索軟體復原能力可以識別備份和復原或SnapCenter中新建立的策略和原則變更。

能否透過ONTAP更改策略？

是的，您可以在 Ransomware Resilience 中從ONTAP更改策略。您也可以在建勒索軟體復原中建立新策略並將其應用於工作負載。此操作將以在勒索軟體復原中建立的策略取代現有的ONTAP策略。

可以在ONTAP中停用策略嗎？

您可以使用ONTAP中的系統管理員 UI、API 或 CLI 在偵測策略中停用 ARP。

您可以透過套用不包含 FPolicy 和備份策略的其他策略來停用它們。

法律聲明

法律聲明提供對版權聲明、商標、專利等的存取。

版權

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NETAPP、NETAPP 標誌和NetApp商標頁面上列出的標誌是NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

專利

NetApp擁有的專利的最新清單可在以下位置找到：

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

隱私權政策

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

開源

通知文件提供有關NetApp軟體中使用的第三方版權和許可的資訊。

- ["NetApp Console通知"](#)

版權資訊

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

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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