使用勒索軟體彈性

NetApp Ransomware Resilience

NetApp
February 27, 2026

目錄

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

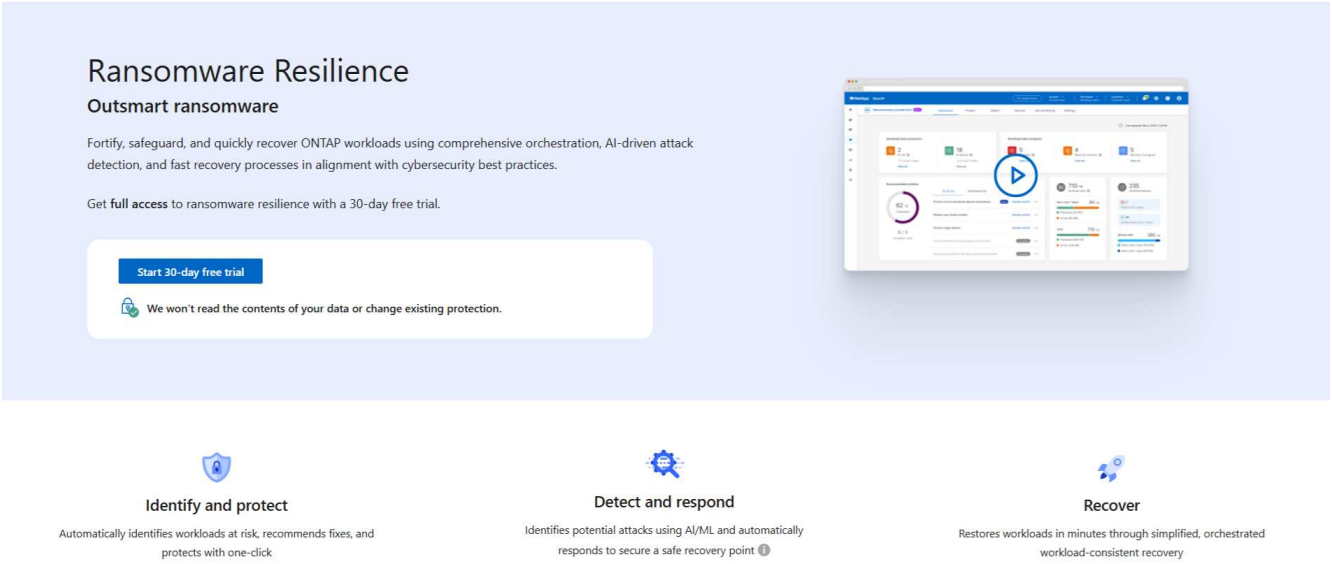
1. 打開網頁瀏覽器並前往"主機"。

   出現控制台登入頁面。

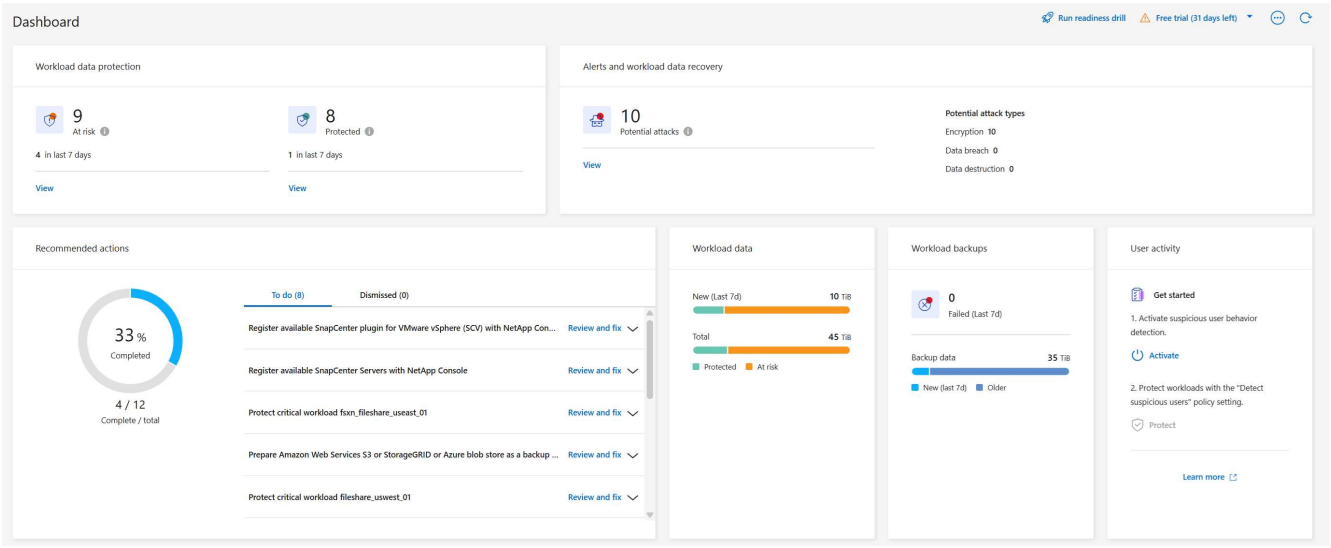
2. 登入控制台。
3. 從控制台左側導覽中，選擇*保護*>*勒索軟體恢復*。

   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" 。



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。

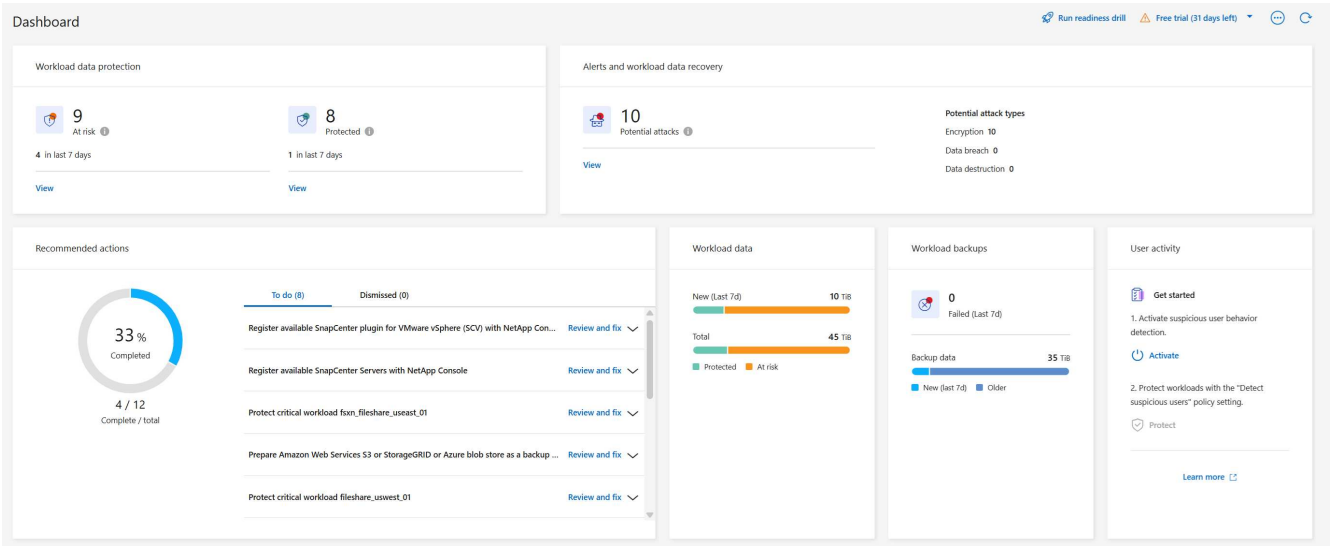
使用儀表板檢視保護建議、變更設定及下載報告。

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"。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"

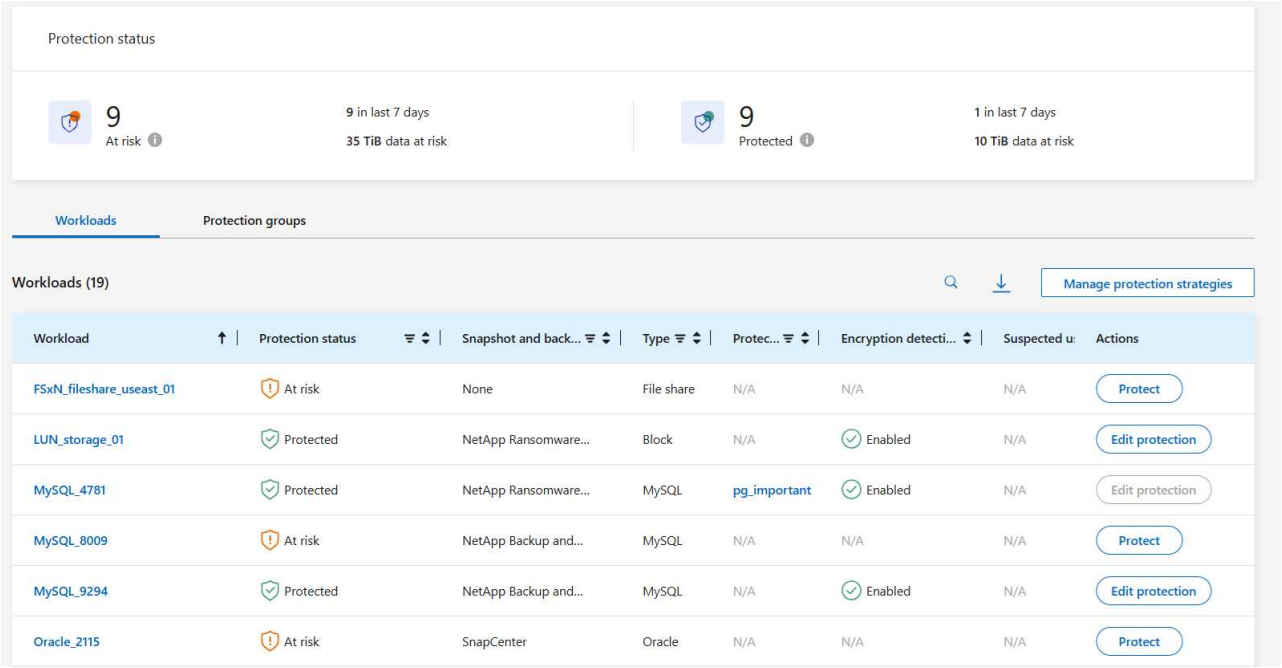
檢視工作負載的保護

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*。



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。

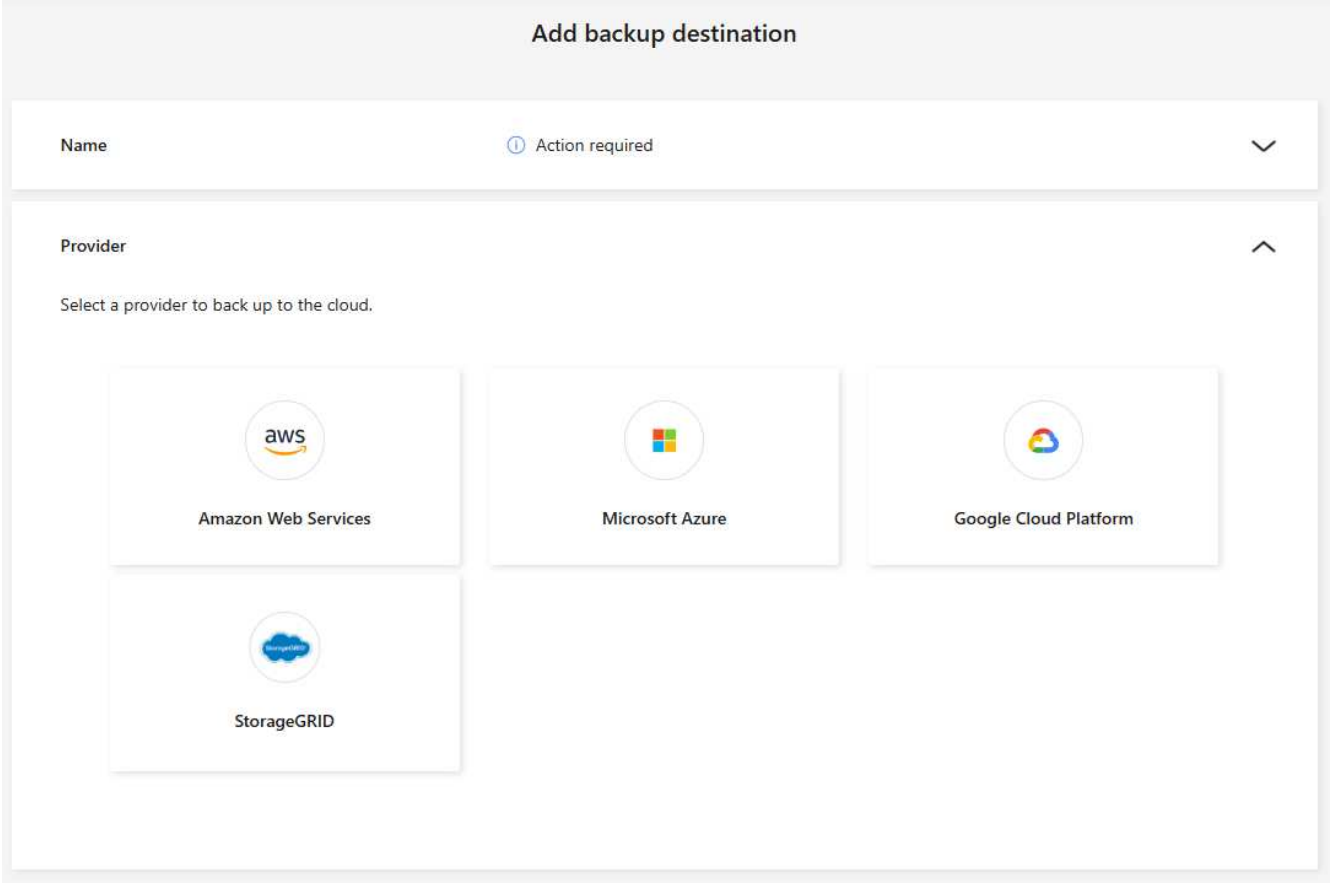
所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

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。

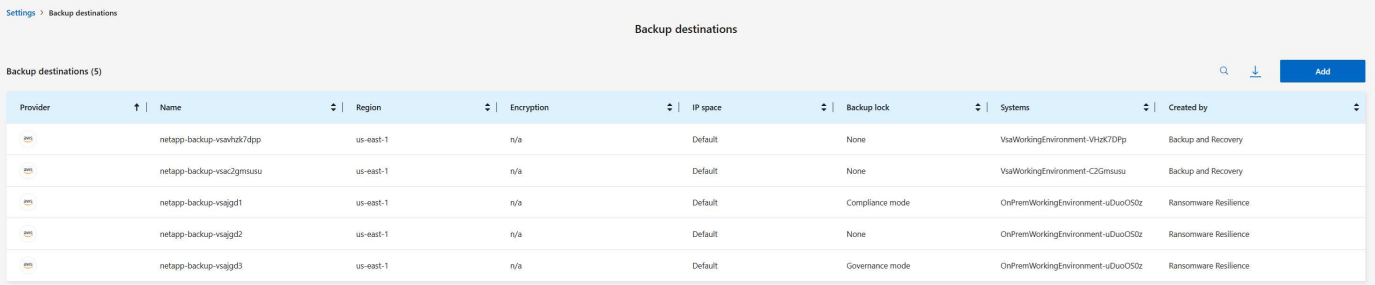


5. 選擇* StorageGRID*。
6. 選取每個設定旁的向下箭頭以檢視必填欄位：
   - 提供者設定：
     - 選擇 **Create a new bucket** 或 **Bring your own bucket** 。
     - 請提供 **Gateway** 節點完全限定網域名稱（**FQDN**） 和 **Port**。
     - 提供 StorageGRID 憑證：存取金鑰和秘密金鑰。
   - 網路：選擇 IP 空間。
     - IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
   - 備份鎖定

     選擇是否要設定備份鎖定。使用備份鎖定時、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。



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。

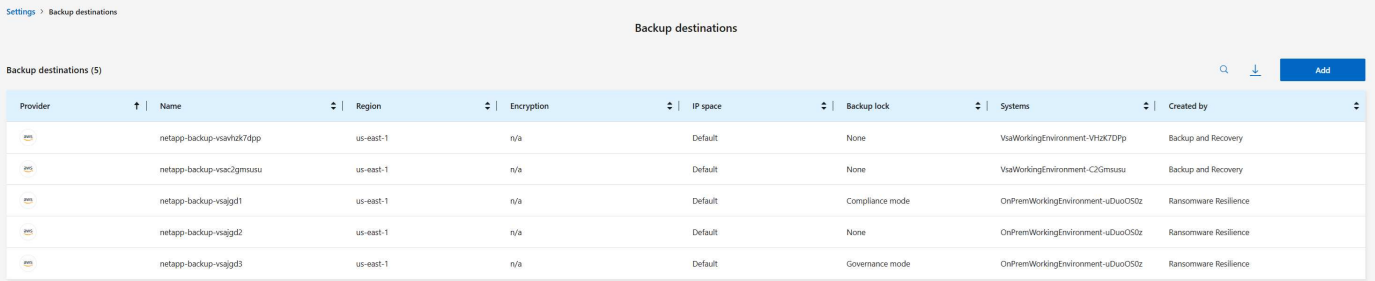
     如果現在配置備份鎖定設定，則在配置備份目的地後將無法變更該設定。
     - 治理模式：特定使用者（具有 s3:BypassGovernanceRetention 權限）可以在保留期間內覆寫或刪除受保護的檔案。

- 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。



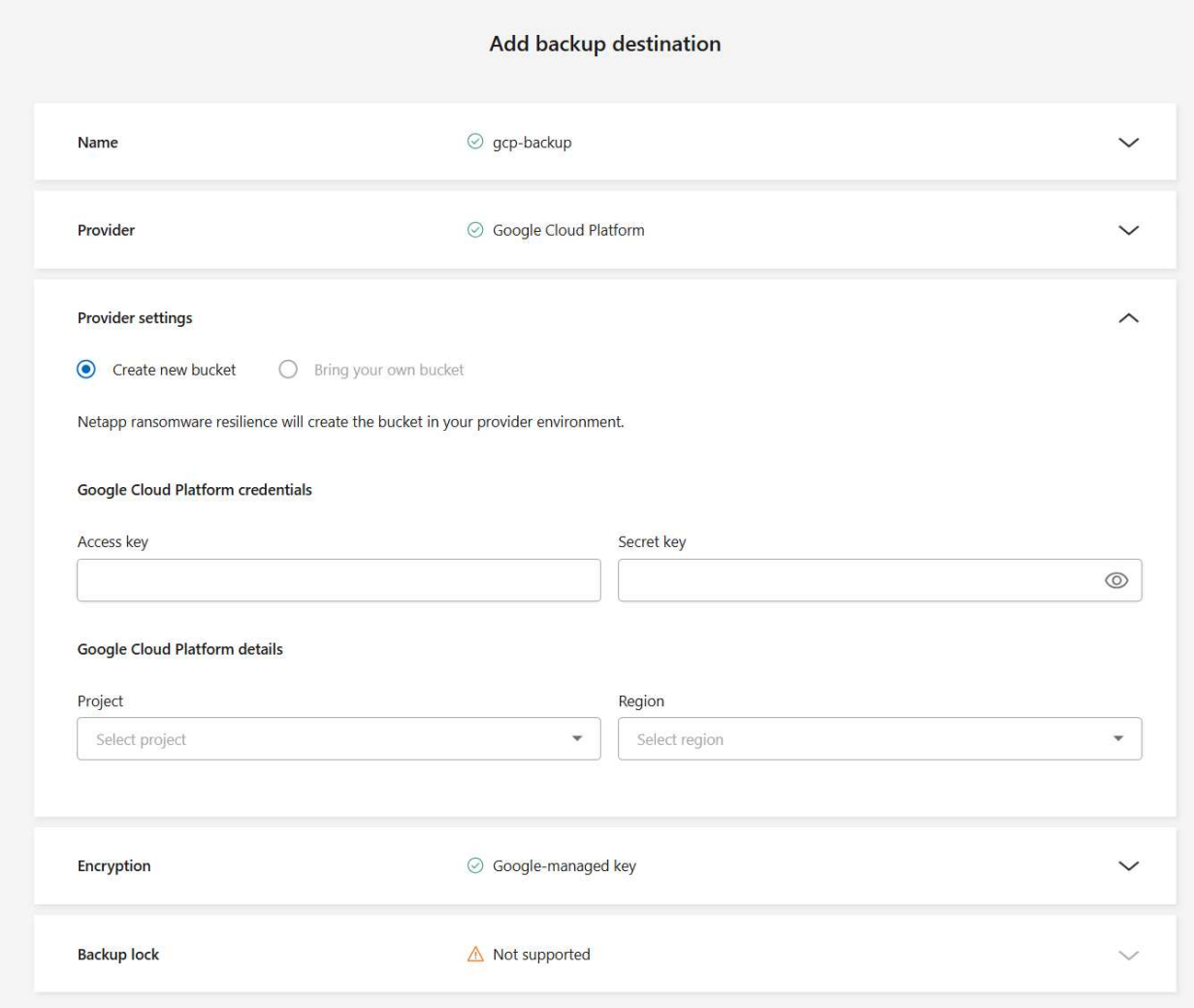
新增 **Google Cloud Platform** 作為備份目標

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** 。



- 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。

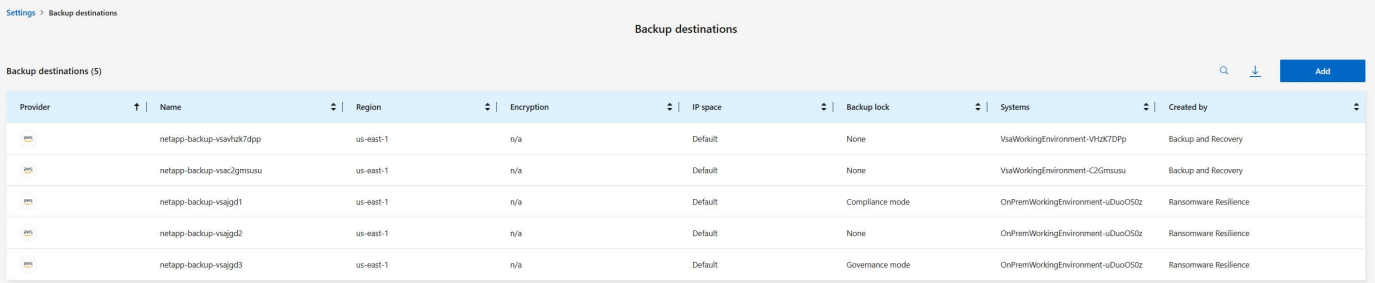
       "如果您想自備儲存帳戶，請參閱新增 Azure Blob 儲存體帳戶" 。
   - 加密：預設情況下，資料使用 Microsoft 管理的金鑰進行加密。選擇 **Microsoft** 管理的金鑰可保留此選項；或者，選擇客戶管理的金鑰可使用您自己的金鑰進行加密。
   - 網路：選擇 IP 空間以及是否使用私有端點。
     - IP 空間是您要備份的磁碟區所在的叢集。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
     - 或者，選擇是否使用先前設定的 Azure 專用終端點。

       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。使用備份鎖定時、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。



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 FSxN 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）

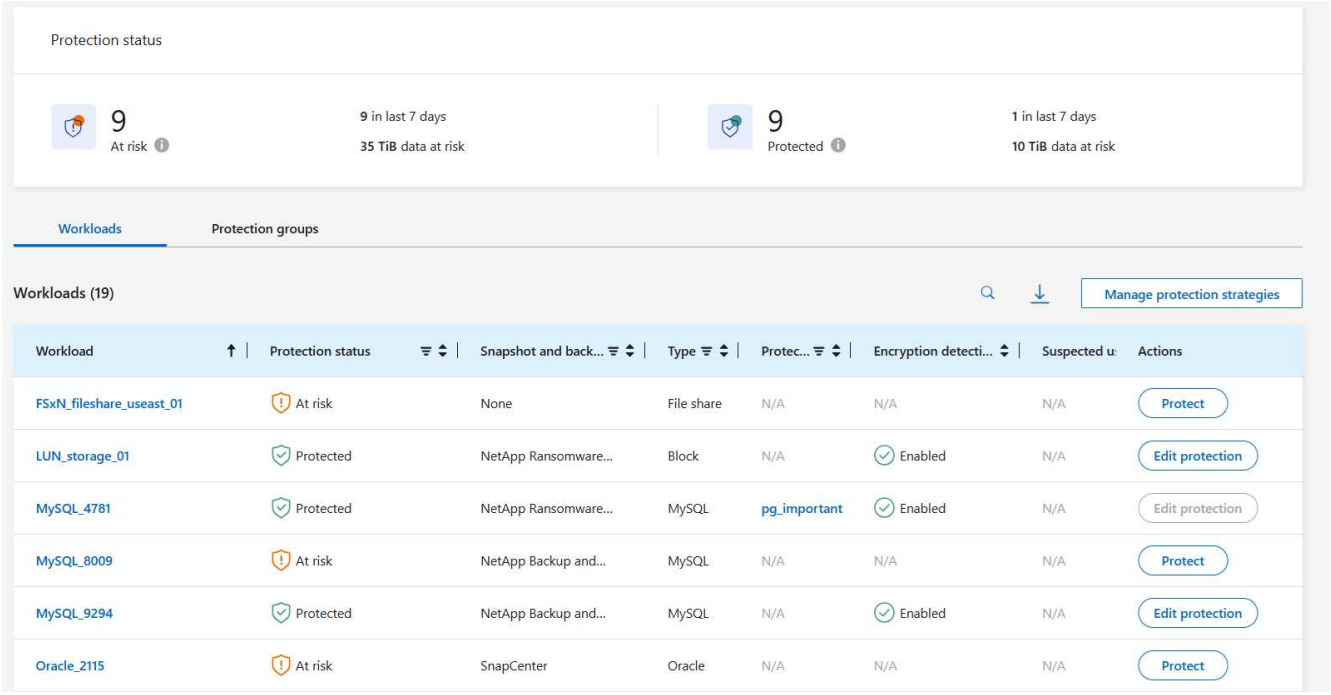
如果工作負載上不存在快照或備份策略，您可以建立勒索軟體保護策略，其中可以包含您在勒索軟體復原中建立的以下策略：

- 快照策略
- 備份策略
- 勒索軟體檢測政策

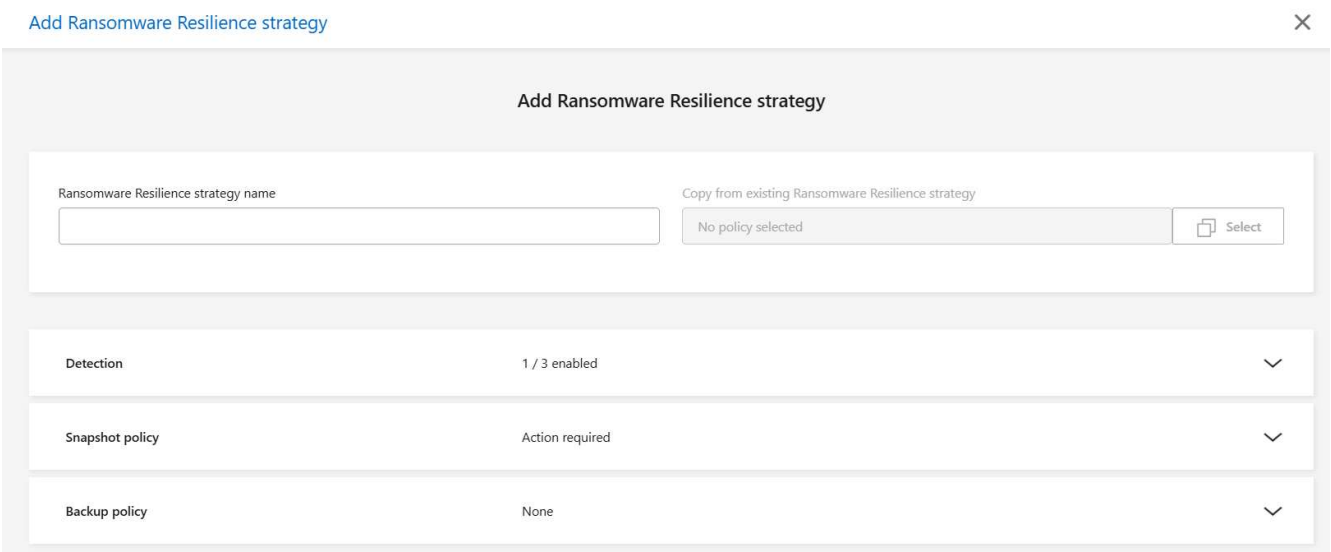
- 二次複製到ONTAP

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*。



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*。



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。

       當快照被鎖定時，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"。

   - 快照計劃：選擇計劃選項、要保留的快照副本數量，然後選擇啟用計劃。
     - 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

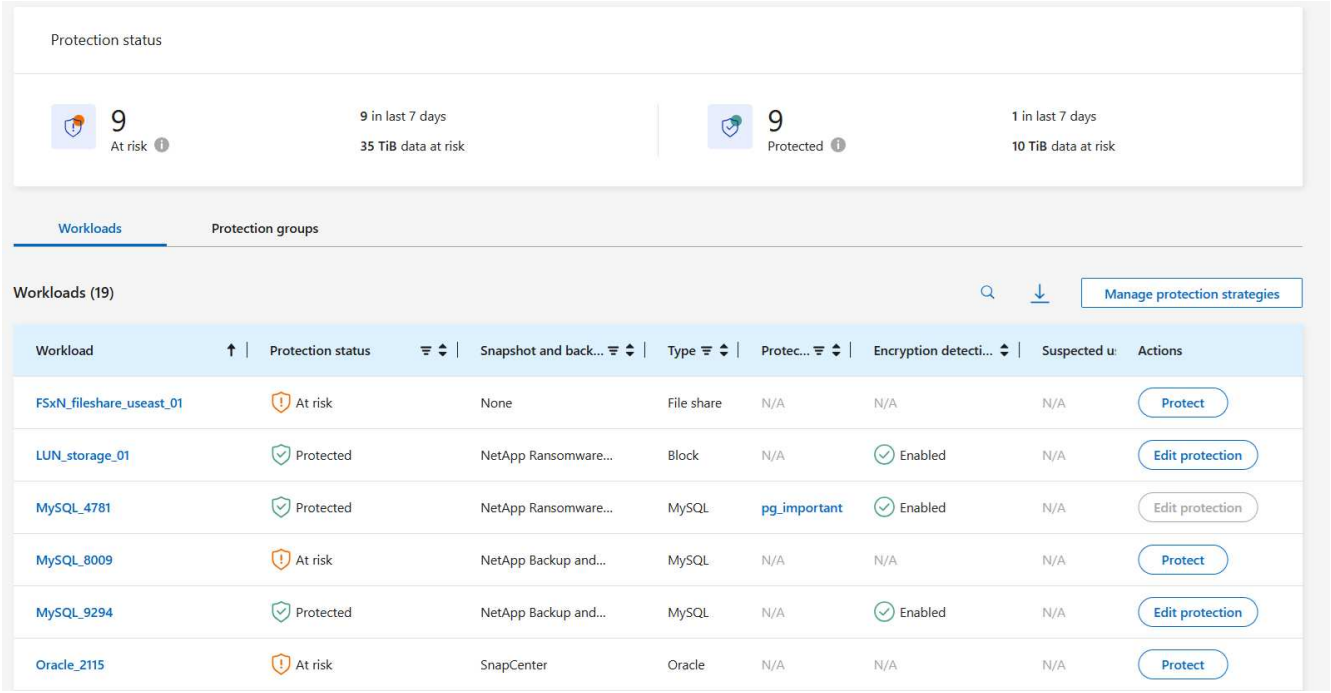
Ransomware Resilience 可讓您為已在其他 NetApp 產品或服務中管理現有快照和備份保護的工作負載指派偵測原則或保護原則。Backup and Recovery 使用原則來管理快照、複寫到次要儲存設備或備份到物件儲存設備。

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*。



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。

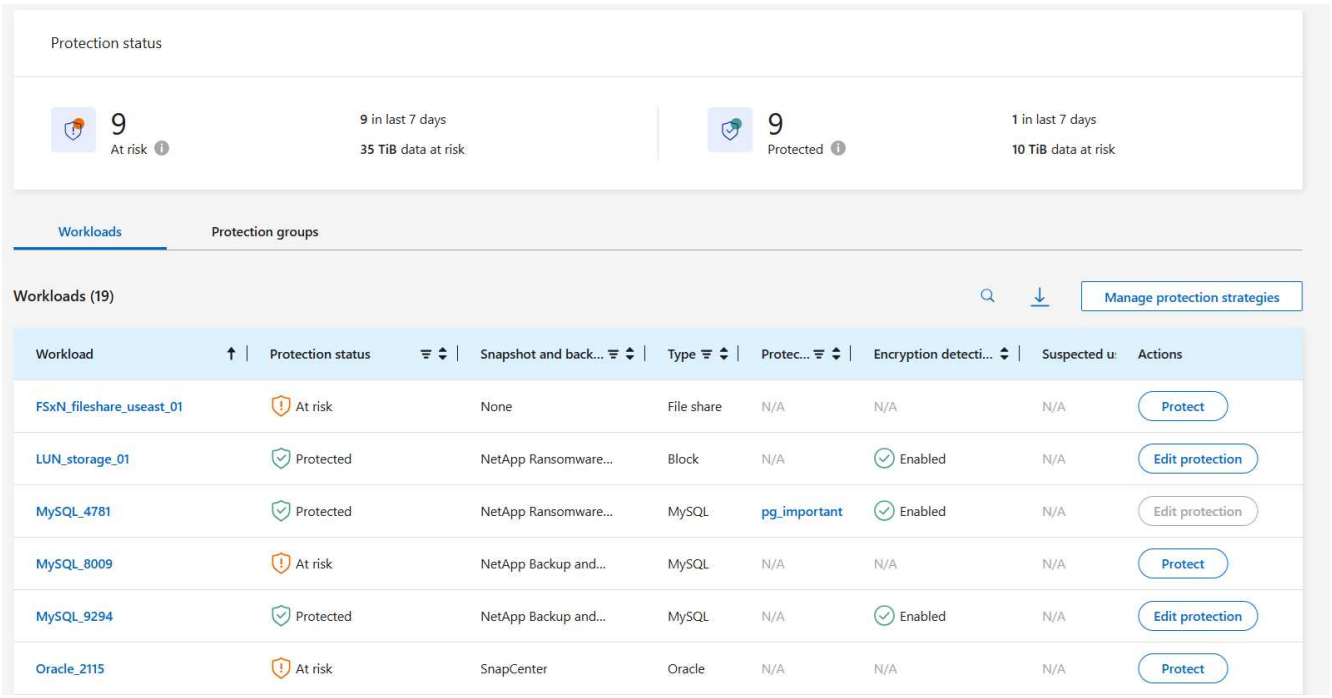
8. 選擇下一步。
9. 審查您的選擇。選擇創建來啟動檢測。
10. 在「保護」頁面上，查看檢測狀態以確認檢測處於活動狀態。

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*。



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

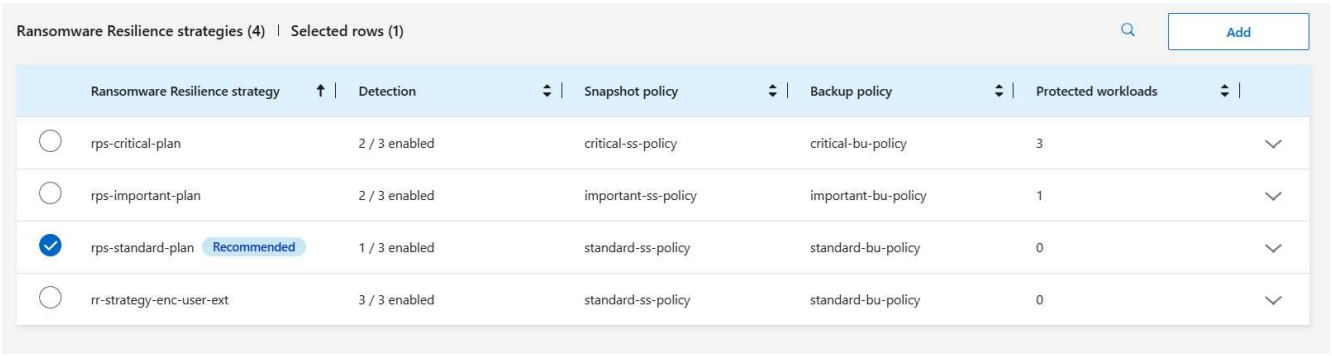
在刪除勒索軟體保護策略之前，您可能需要查看哪些工作負載受該策略保護。

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。



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。

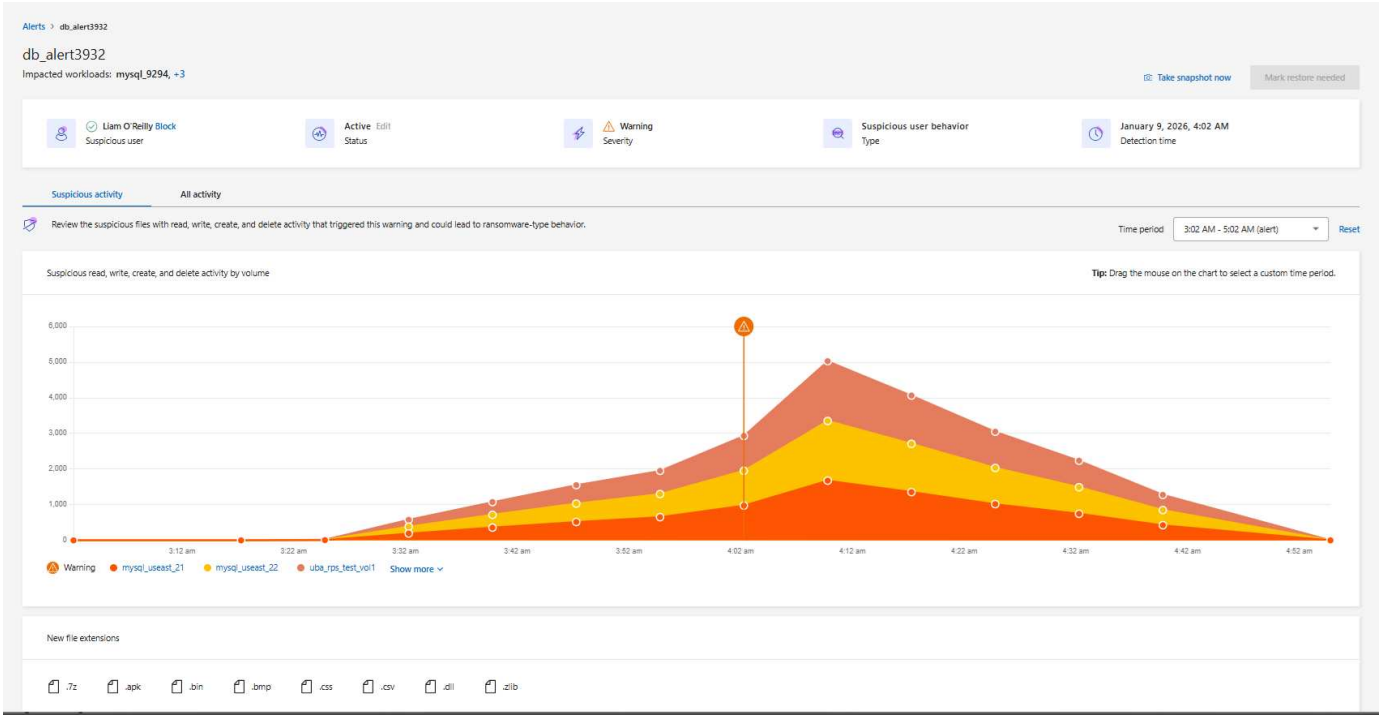
透過可疑使用者行為偵測和警示，NetApp Ransomware Resilience 會在發現可疑的資料外洩和破壞企圖及模式時發出警示。在每次警示中，NetApp Ransomware Resilience 都會識別出您可以封鎖的使用者。

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。

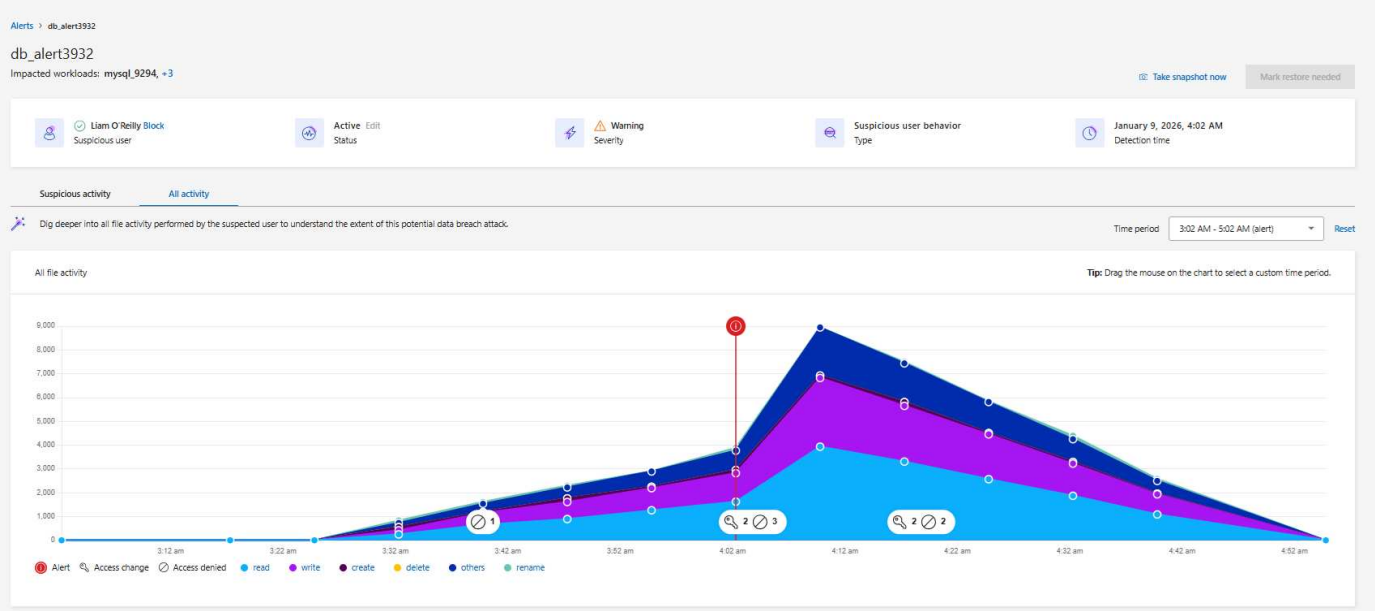
目前 SAN 工作負載不支援使用者活動偵測。您可以在 Amazon FSxN for ONTAP、Cloud Volumes ONTAP 和 ONTAP 中使用 NAS 工作負載的使用者活動偵測。

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。



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、伺服器和網路要求，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	• 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	• <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	• <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	• <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、伺服器和網路要求"。

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。

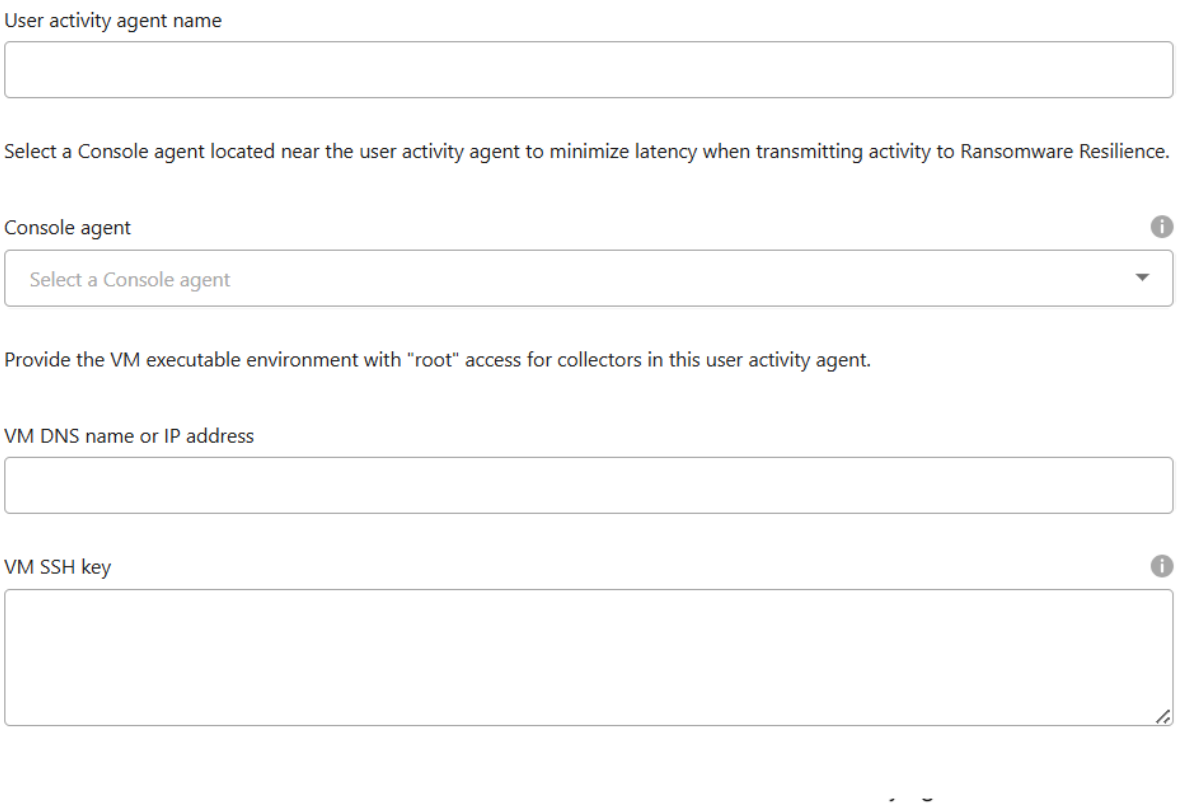
步驟

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-----
```



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**。

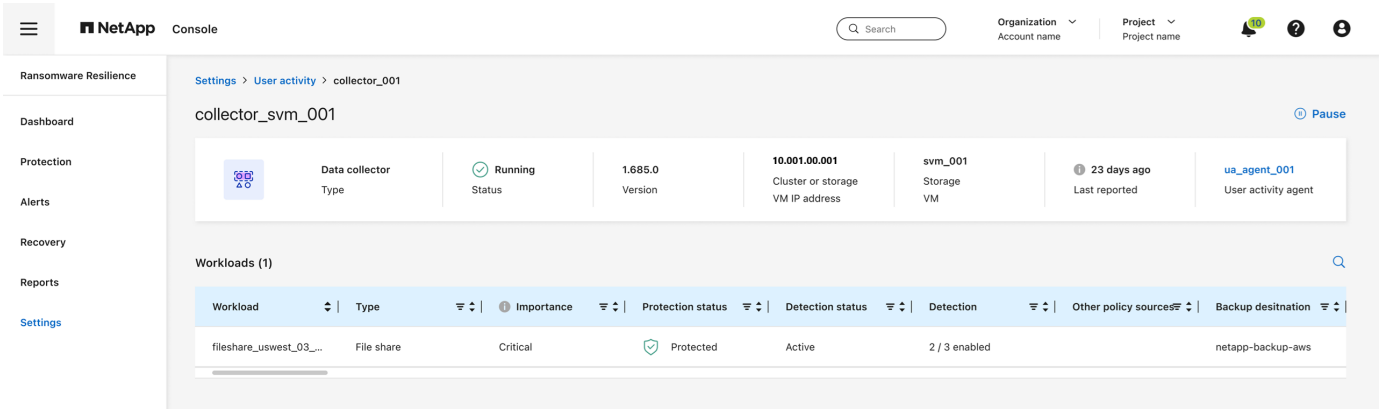
結果

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。



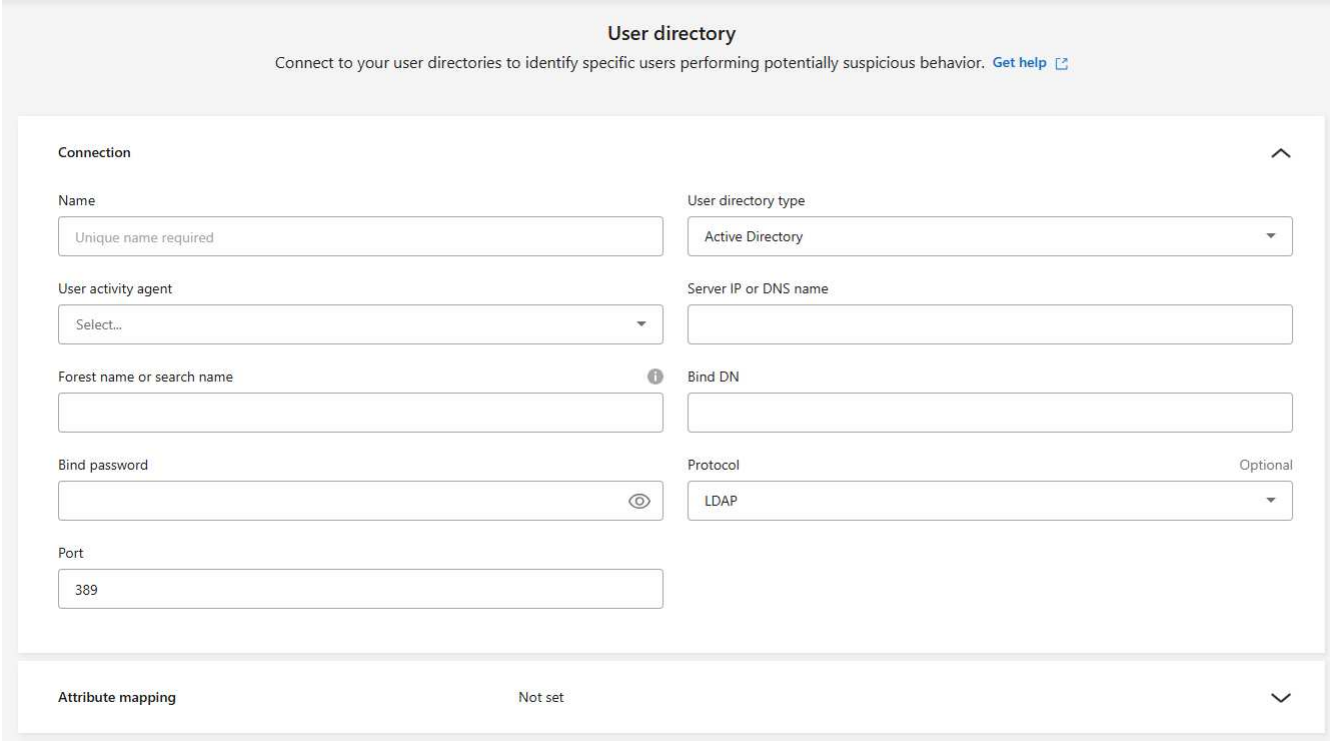
建立使用者目錄連接器

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）。`unit.company.com`）或一組相對專有名詞（例如：`DC=unit,DC=company,DC=com`）。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：`CN=user,OU=engineering,DC=unit,DC=company,DC=com`）。
綁定DN	BIND DN 是被允許搜尋目錄的使用者帳戶，例如 user@domain.com。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



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」儀表板中，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，現在會在儀表板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」儀表板中，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。

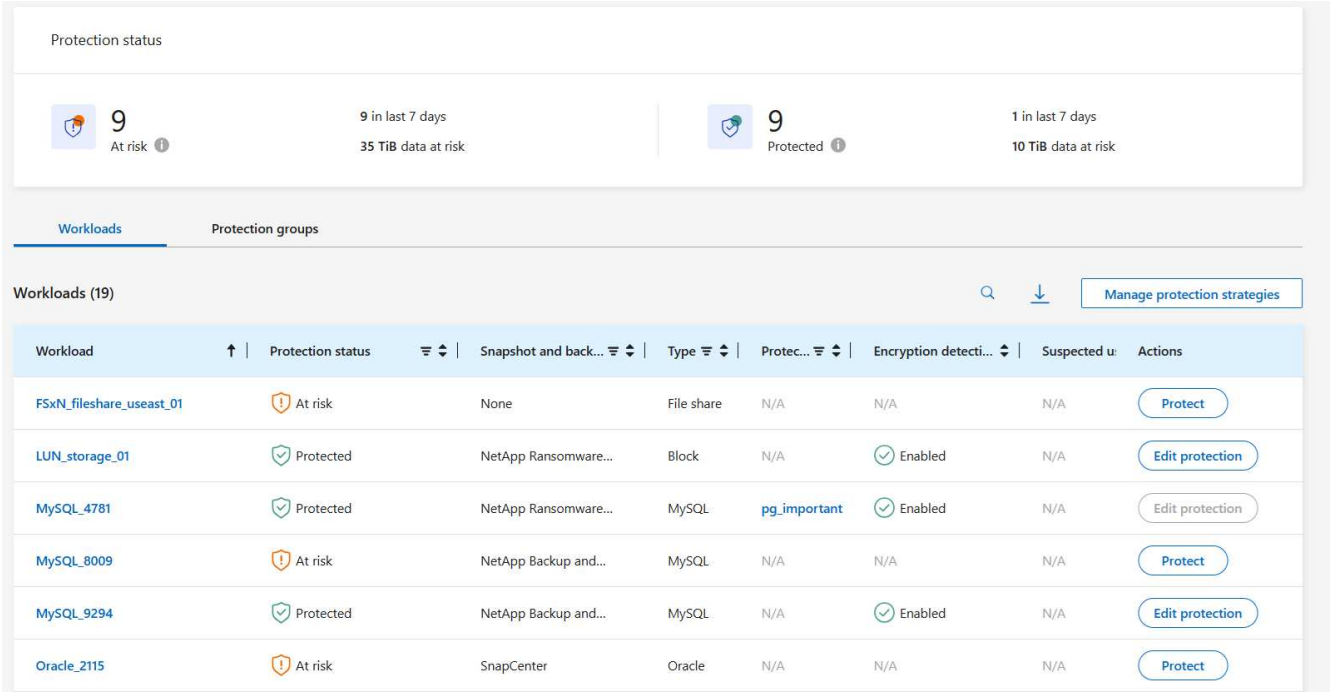
所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

建立保護組

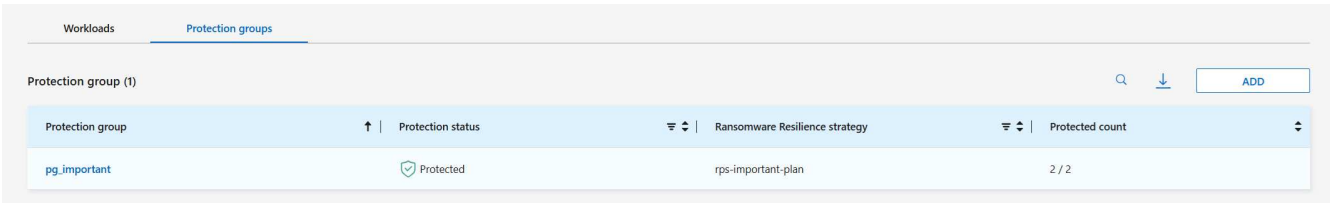
您可以建立群組，無論其保護狀態如何（即未受保護的群組和受保護的群組）。在保護群組新增保護策略時，新的保護策略將取代任何現有策略，包括由 NetApp Backup and Recovery 管理的策略。

步驟

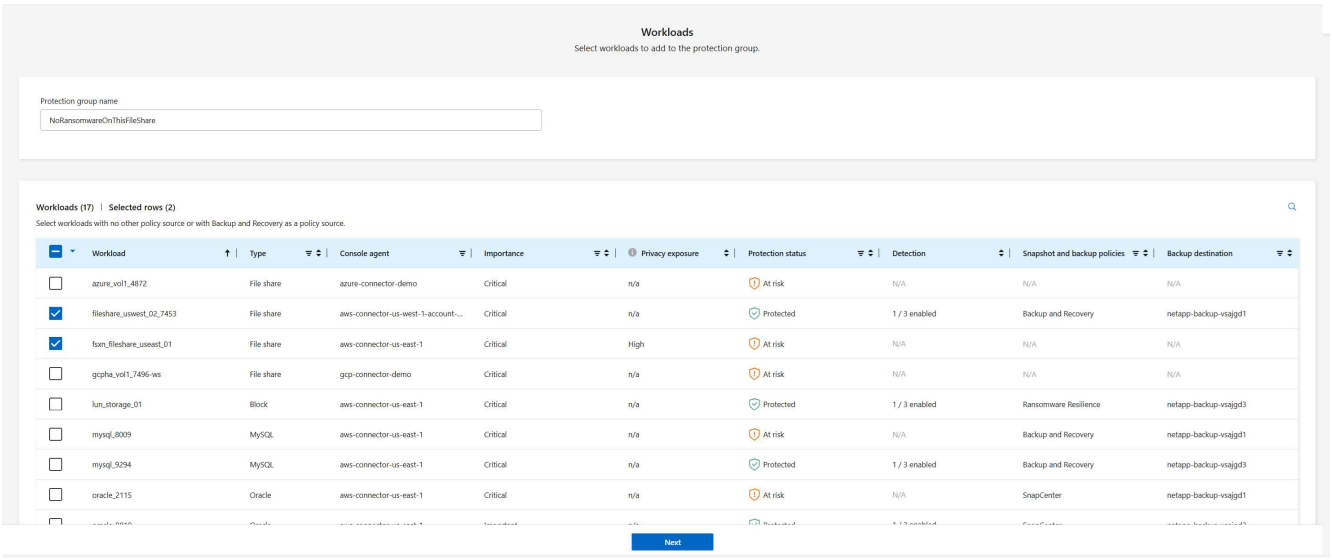
1. 從勒索軟體恢復選單中，選擇*保護*。



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



3. 選擇“新增”。

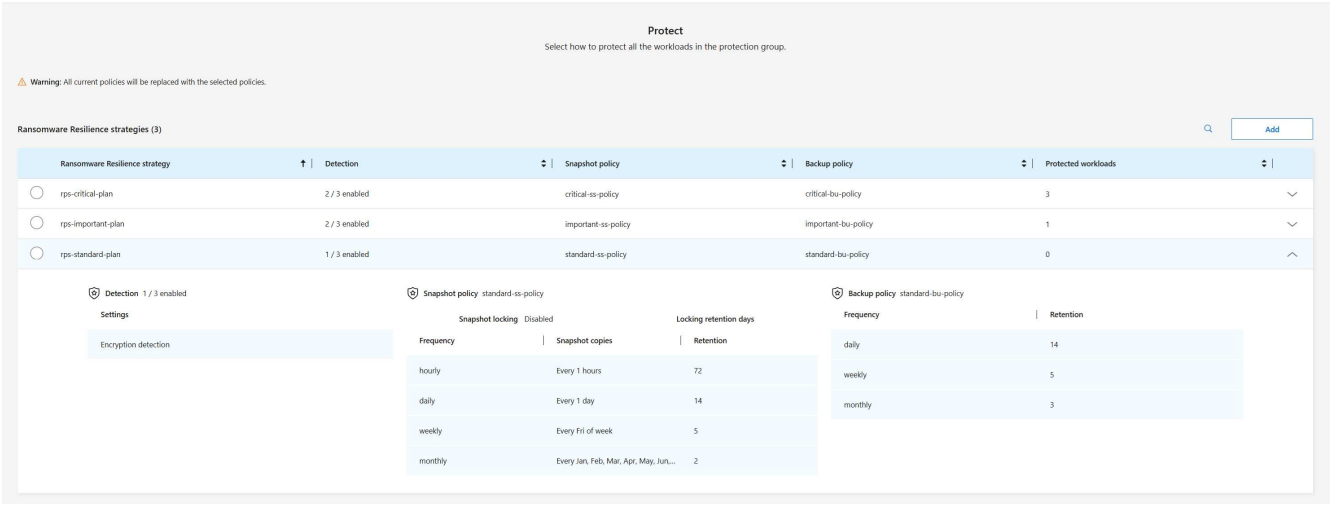


4. 輸入保護組的名稱。

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”。



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。
   a. 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

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」選項卡，然後選擇要修改其政策的群組。
3. 從保護群組的概覽頁面中，選擇「編輯保護」。
4. 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**。
5. 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。

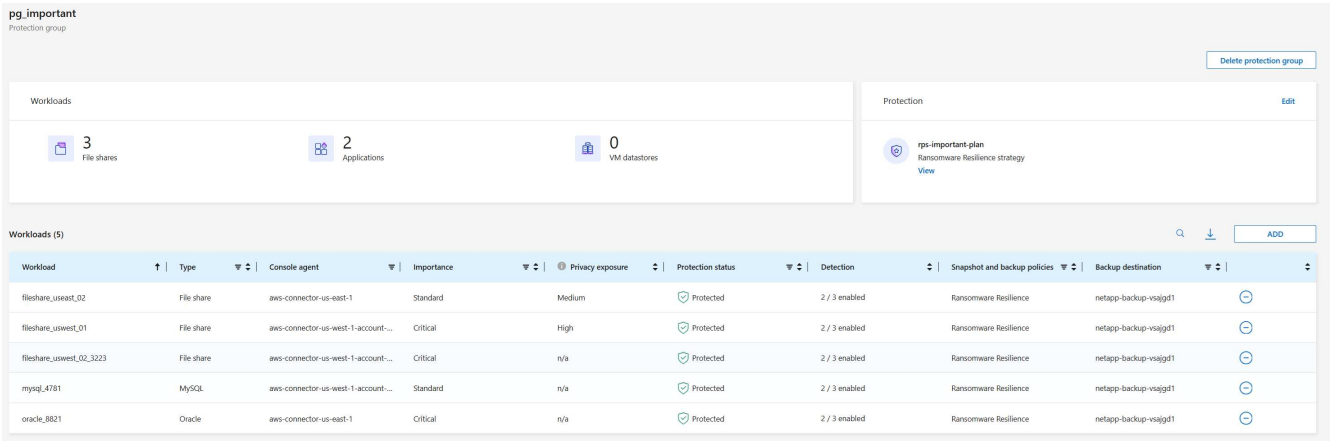
6. 選擇下一步來查看您的變更。

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。



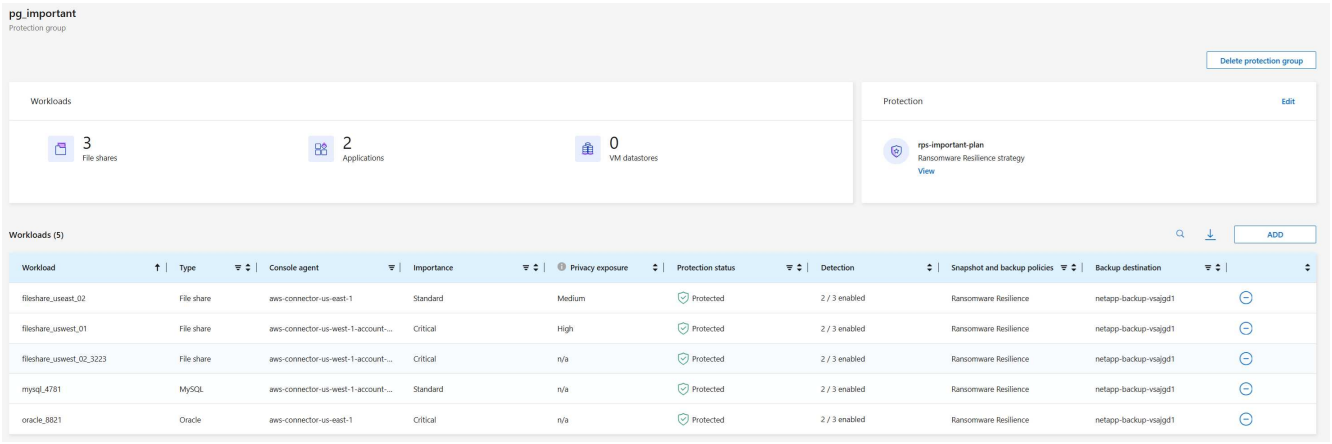
4. 在保護群組頁面中、選擇要從群組中移除的工作負載、然後選擇 **Actions** ••• 選項。
5. 從「操作」功能表中，選擇「刪除工作負載」。
6. 確認您要刪除工作負載並選擇*刪除*。

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。



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：

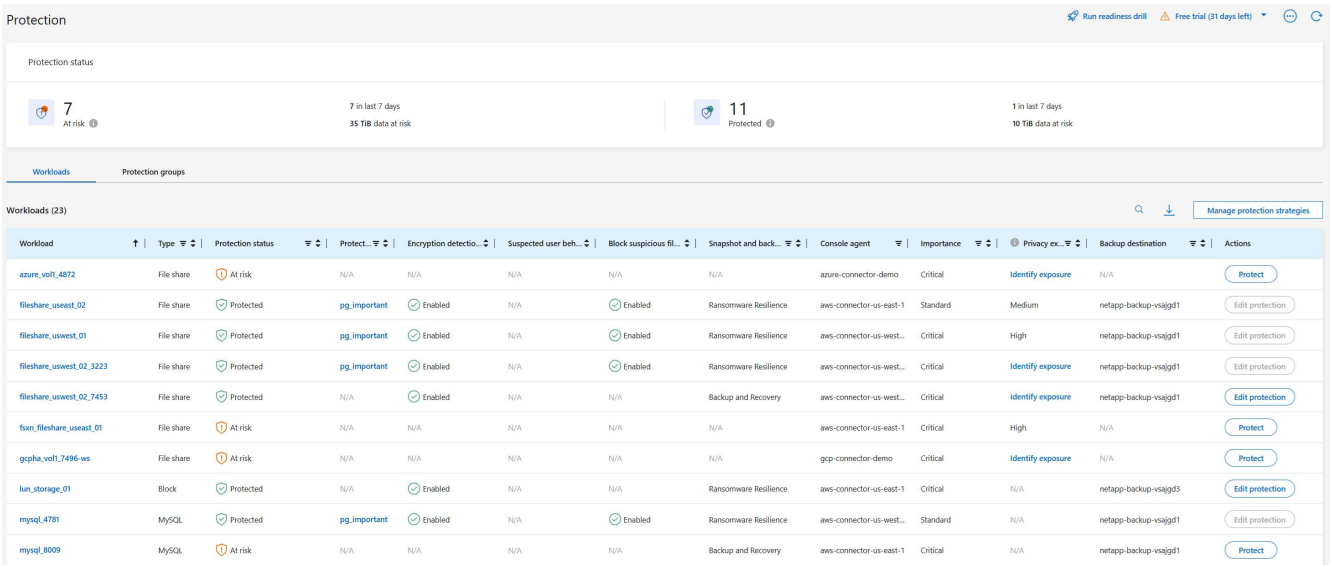
- "了解資料分類"
- "私人資料類別"
- "調查組織中儲存的數據"

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。



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

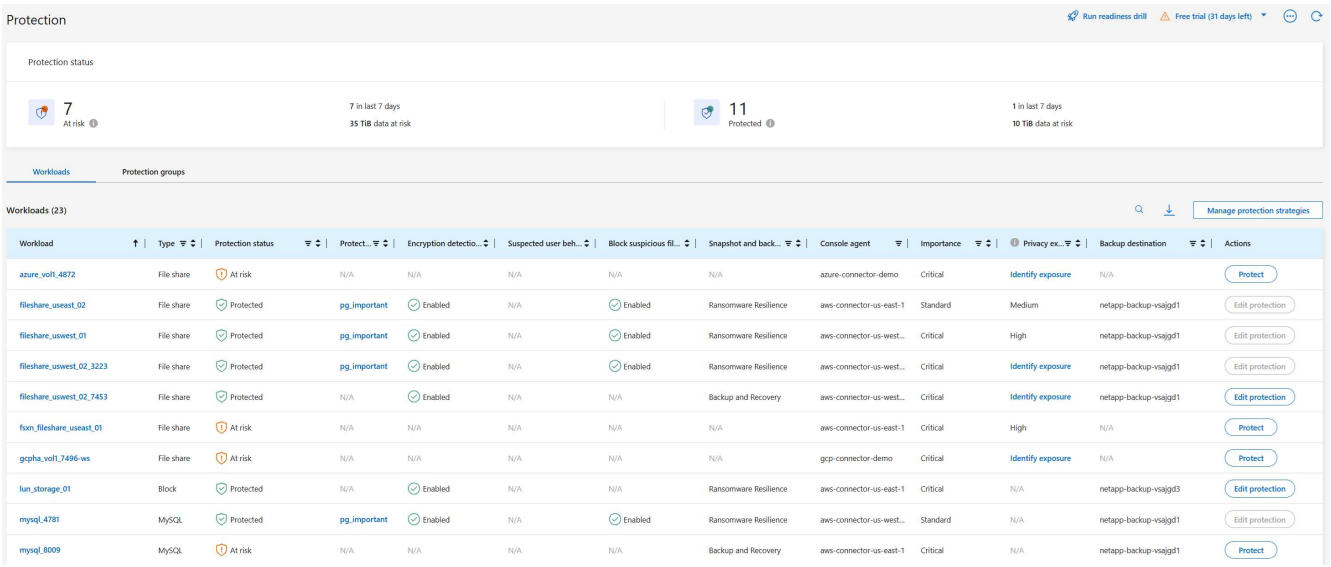
在對 PII 進行資料分類掃描後，評估風險。

PII 資料分為以下三類：

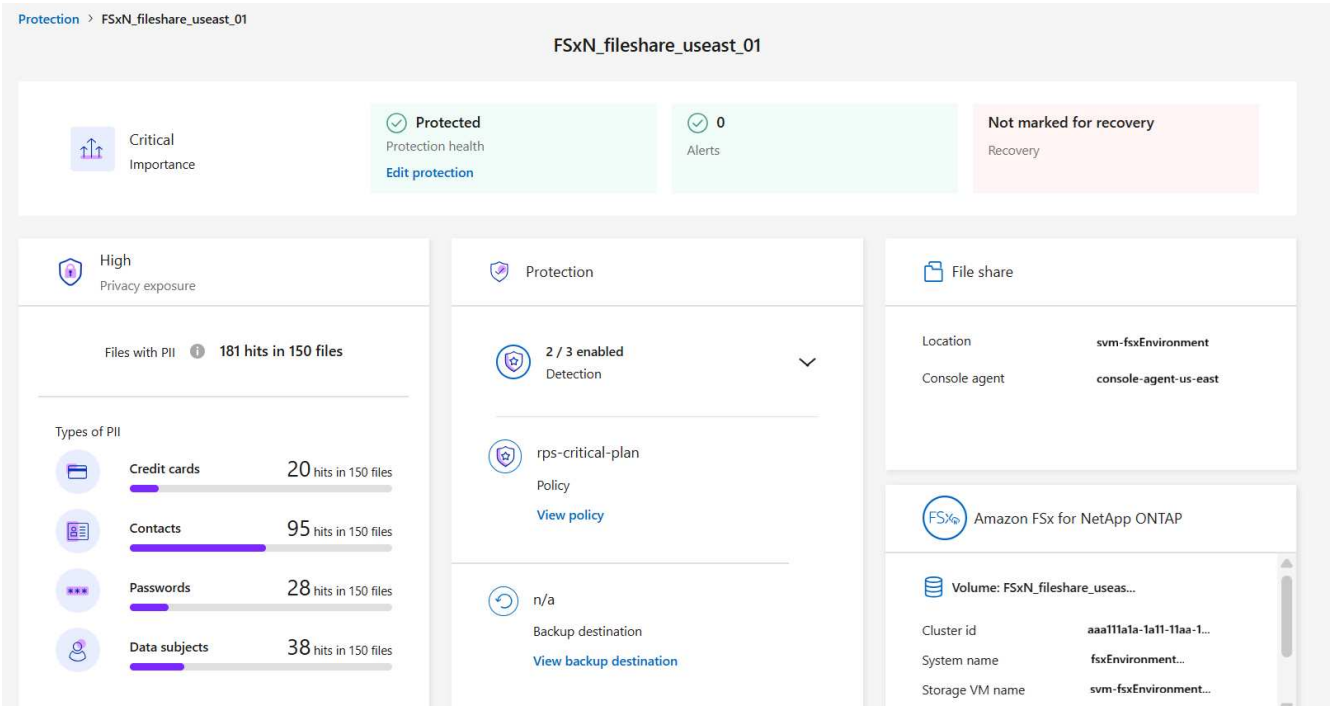
- 高：超過 70% 的檔案包含 PII
- 中：超過 30% 且少於 70% 的檔案包含 PII
- 低：大於 0% 且小於 30% 的檔案包含 PII

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。



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。



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。

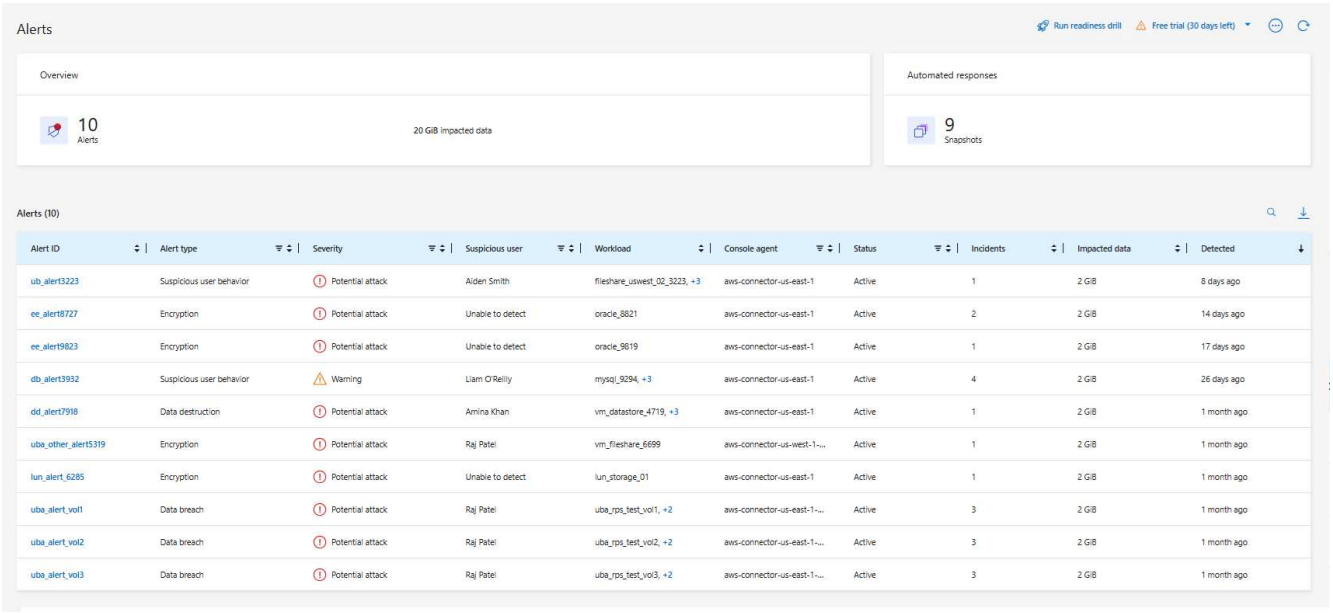
查看警報

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。



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板中。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

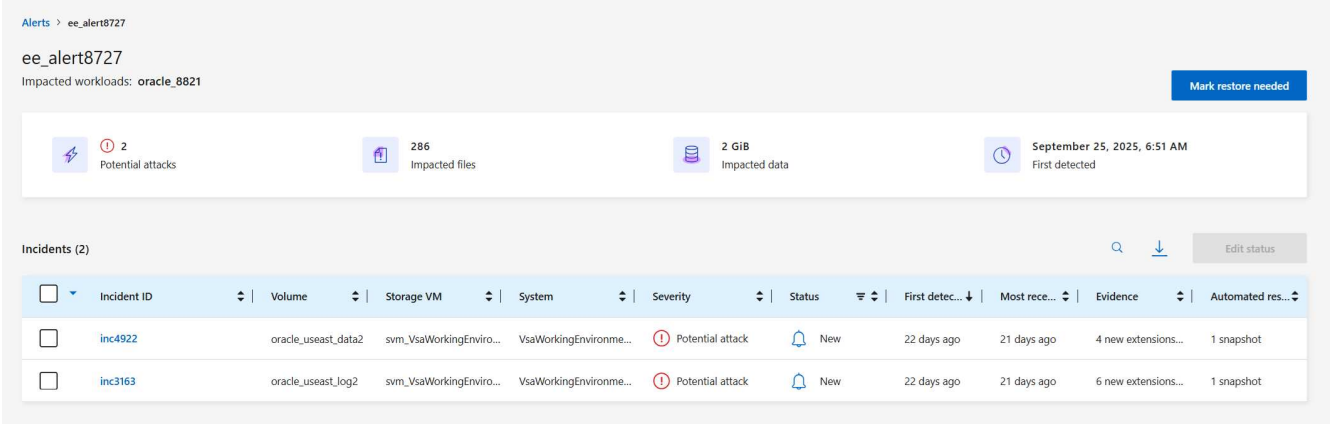
當 Autonomous Ransomware Protection 在 NetApp Ransomware Resilience 中觸發警示時、您可以檢視下列詳細資料：

- 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。



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。

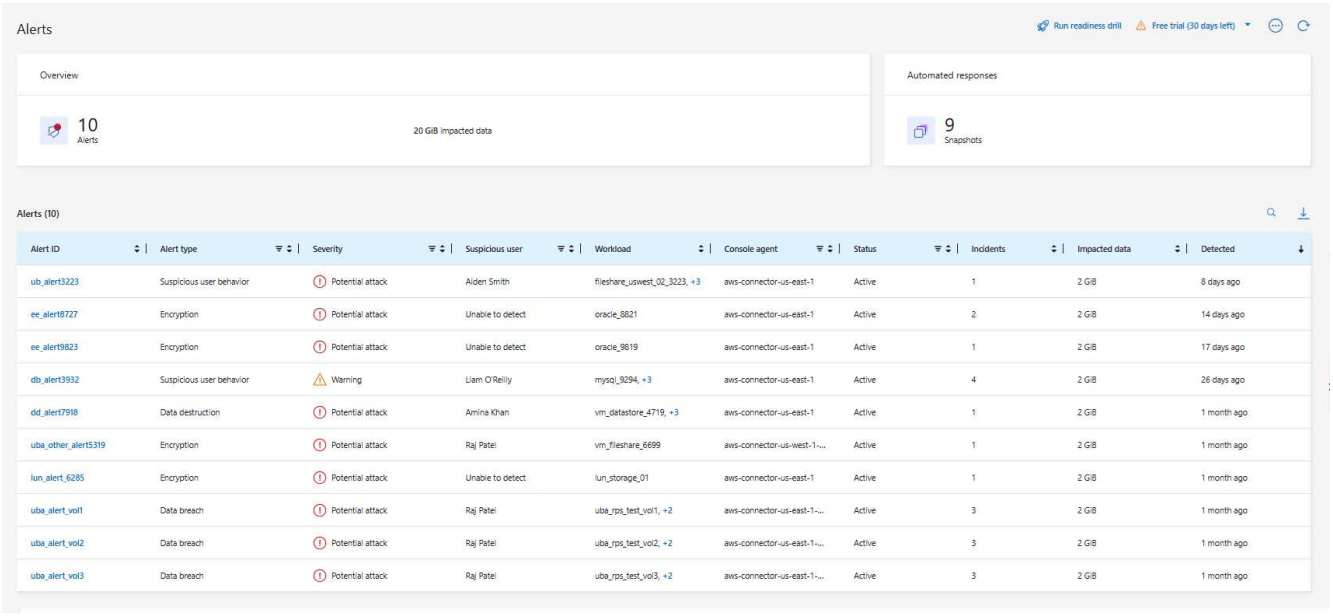
將勒索軟體事件標記為可恢復（事件被消除後）

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。

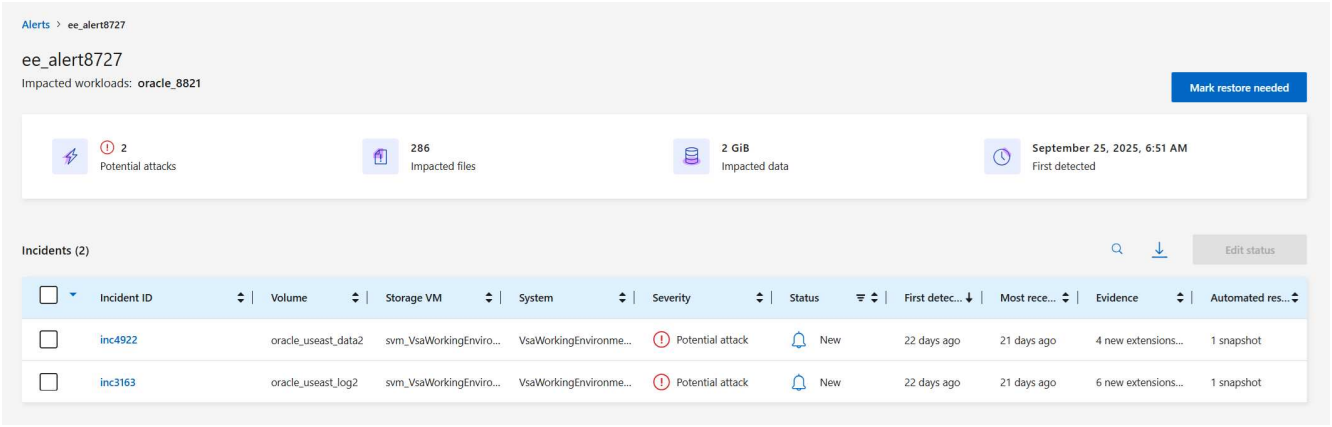
所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

步驟

1. 從勒索軟體恢復選單中，選擇*警報*。



2. 在警報頁面中，選擇警報。
3. 查看警報中的事件。



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。

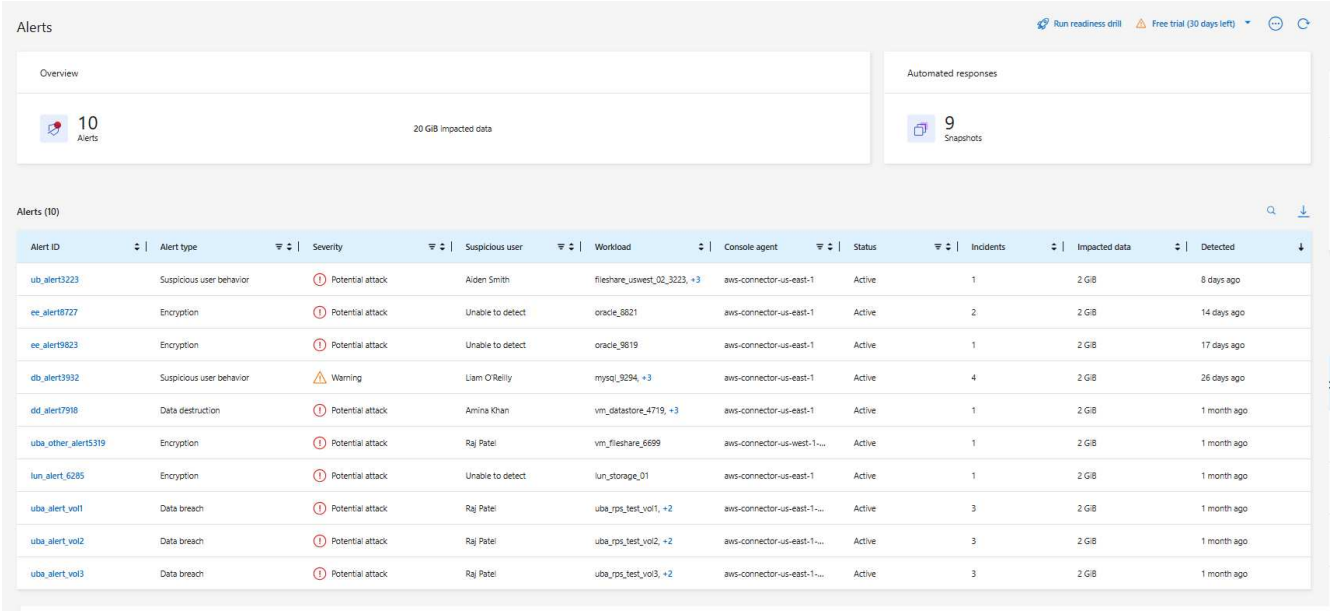
如果您解除工作負載，則為應對潛在勒索軟體攻擊而自動取得的所有快照副本都將永久刪除。

如果您關閉警報，則無法變更其狀態或撤銷此變更。

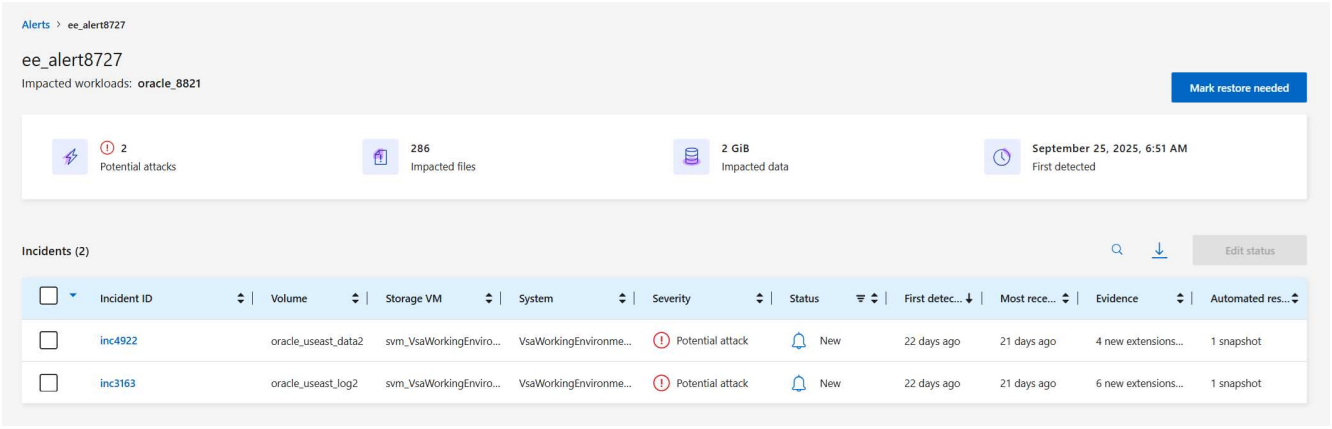
所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

步驟

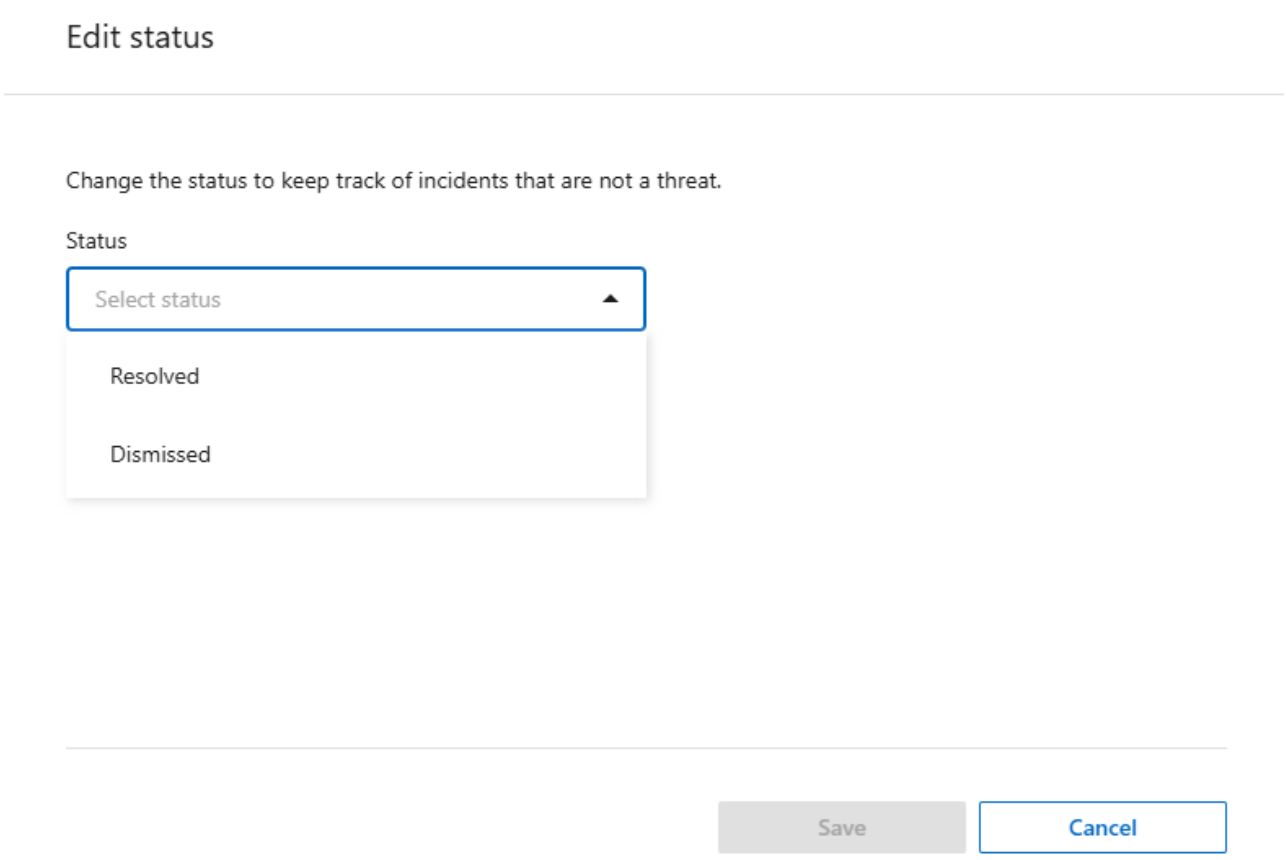
1. 從勒索軟體恢復選單中，選擇*警報*。



2. 在警報頁面中，選擇警報。



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。



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" 。

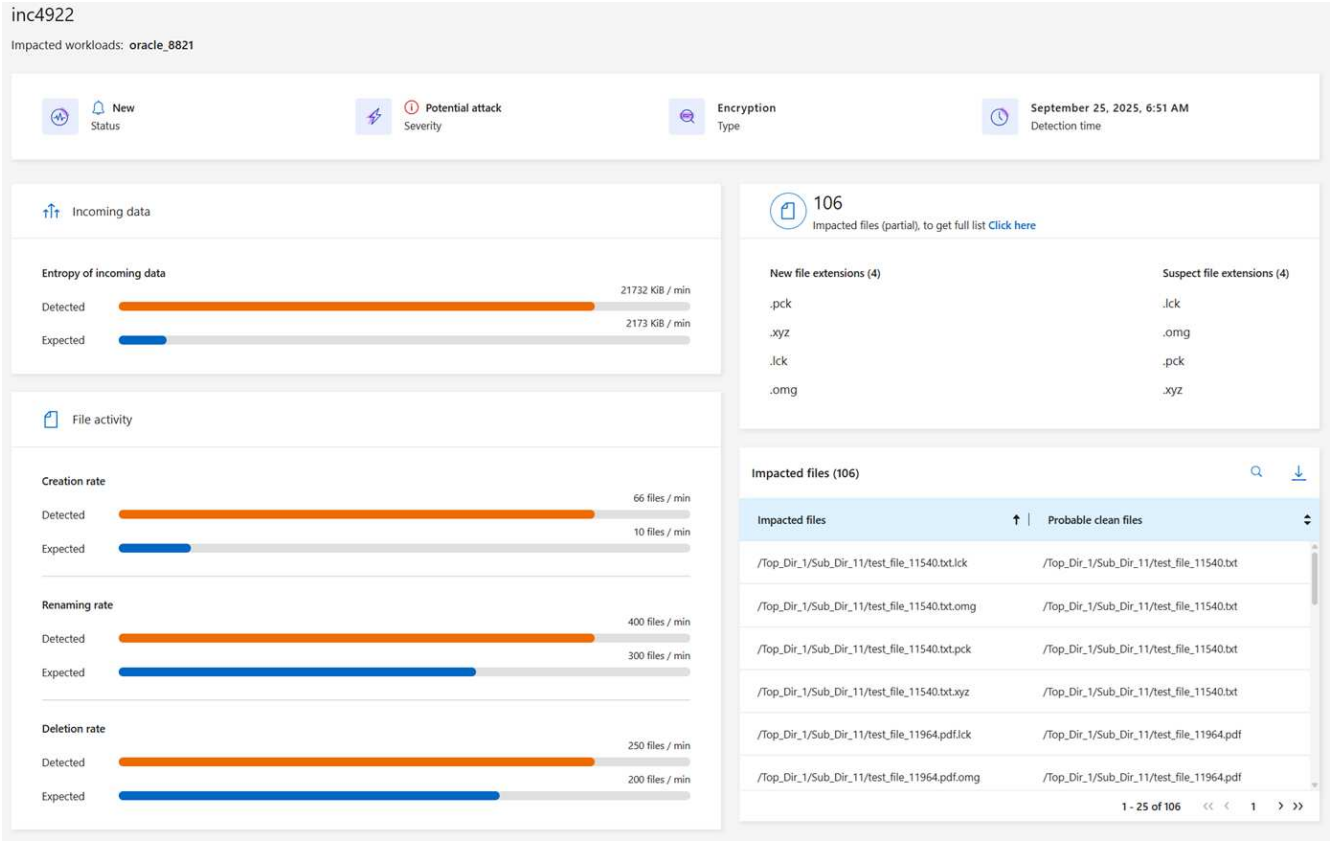
步驟

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：

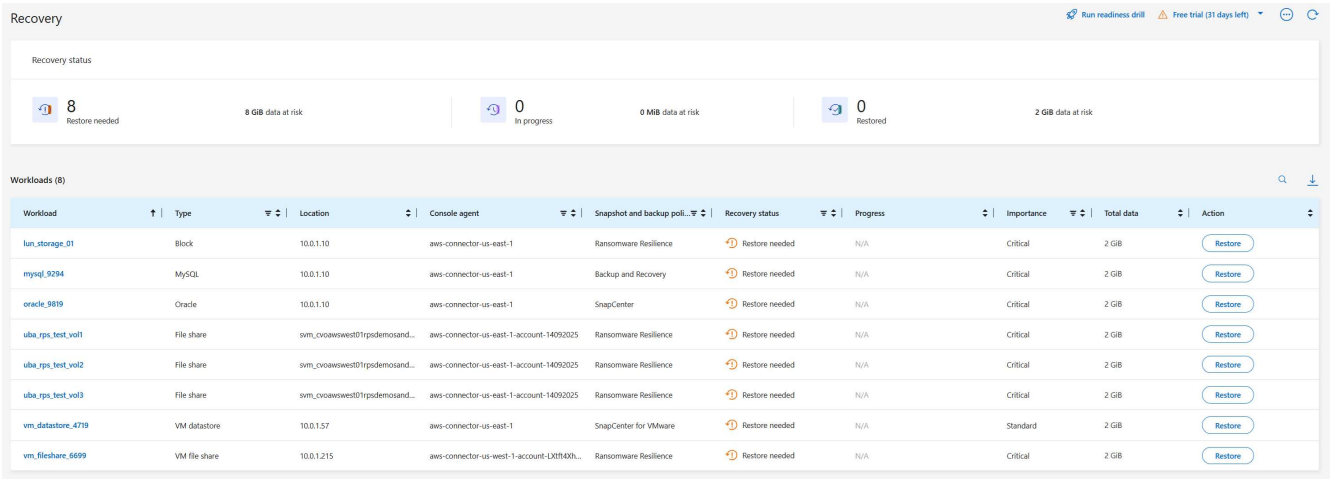
- 需要恢復：需要恢復工作負載。
- 進行中：復原作業目前正在進行中。
- 已恢復：工作量已恢復。
- 失敗：工作負載復原過程無法完成。

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。



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。

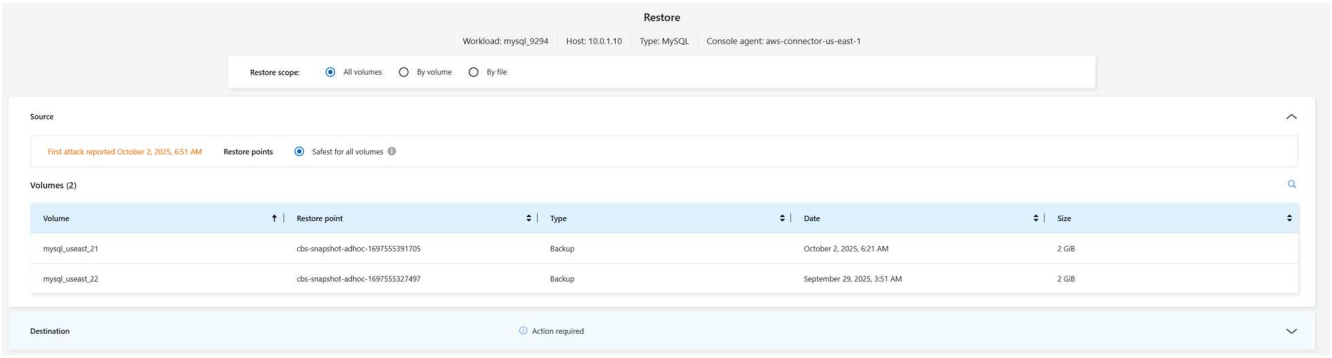
對於 SAN 工作負載，您只能按工作負載進行復原。

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。

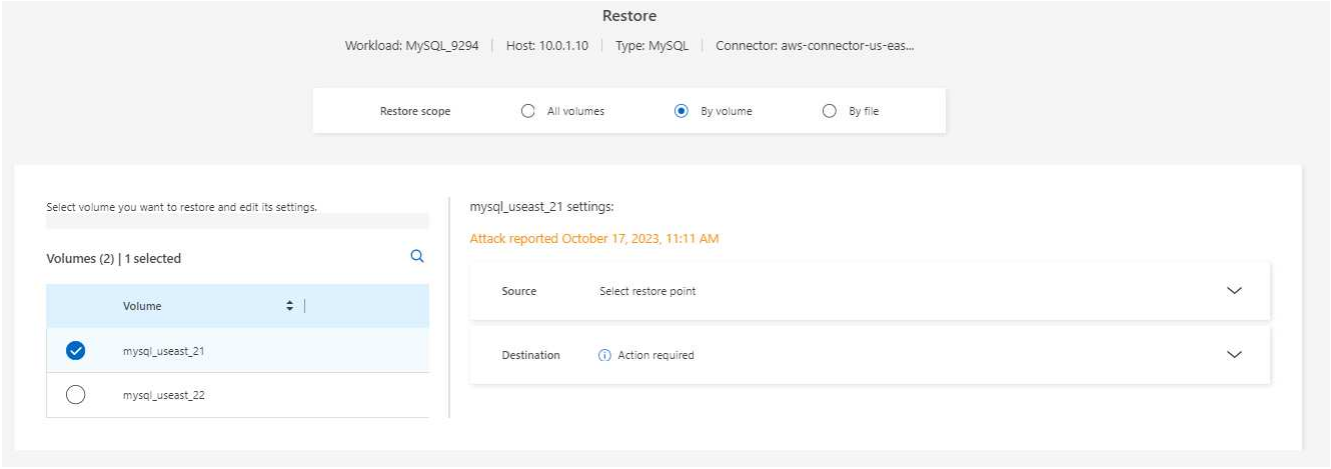
新磁碟區名稱顯示為前綴+原始磁碟區名稱+備份名稱+備份日期。

7. 選擇*儲存*。

8. 選擇“下一步”。
9. 檢查您的選擇。
10. 選擇*恢復*。
11. 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

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「按磁碟區」。



5. 在磁碟區清單中，選擇要還原的磁碟區。
6. 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。

7. 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. 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。

8. 選擇*儲存*。
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。

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。

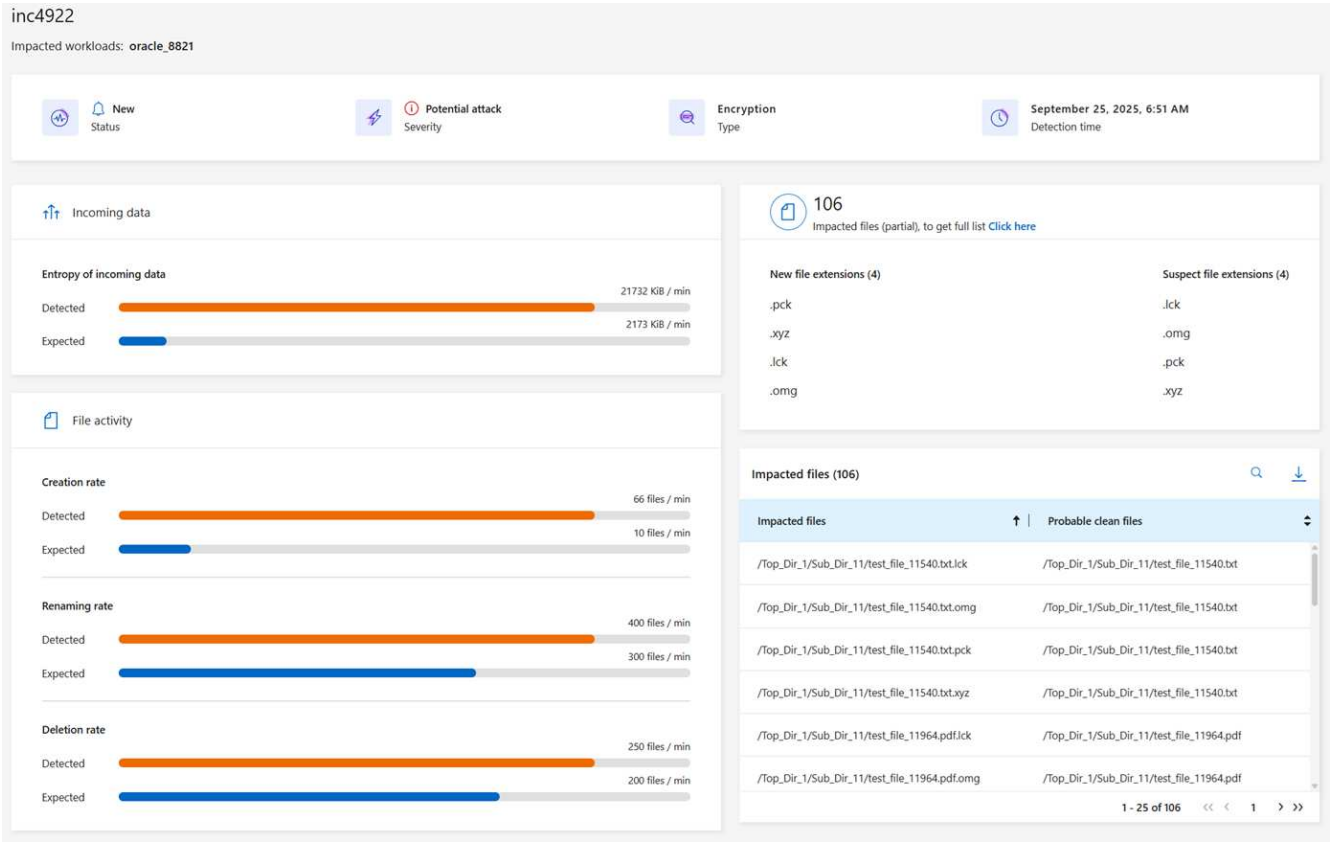
您可以將檔案層級的應用程式工作負載還原到相同或不同的系統。

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。



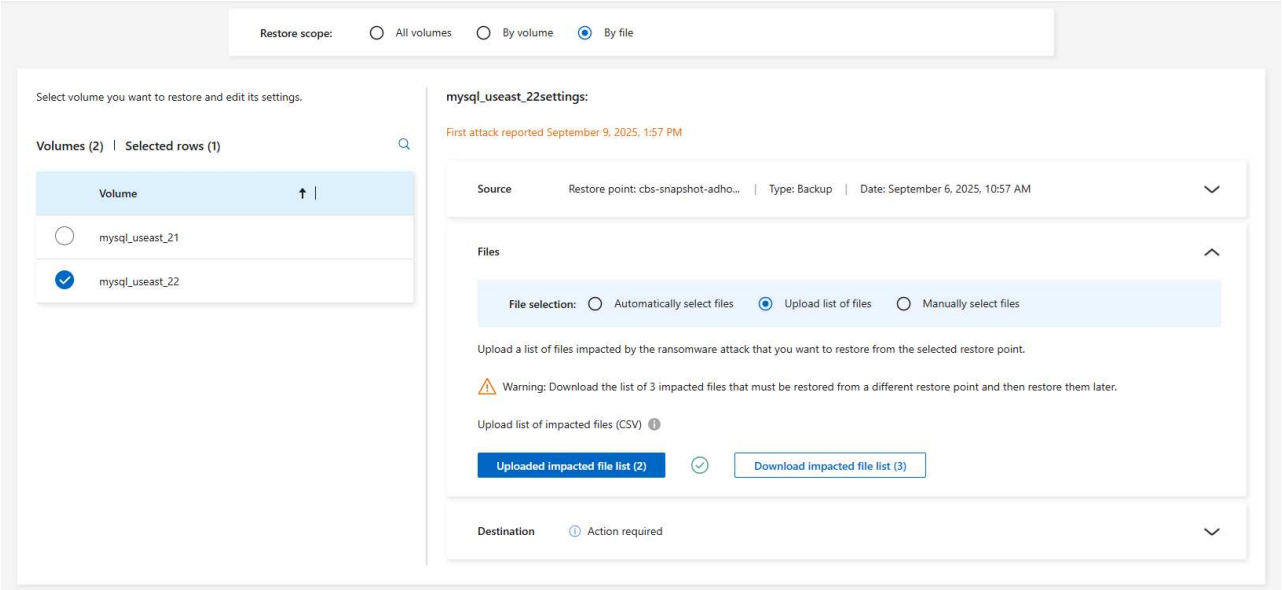
5. 若要查看完整的檔案列表，請選擇「受影響的檔案」窗格頂部的「按一下此處」。
6. 對於該事件，選擇下載圖示並以 CSV 格式下載受影響文件的清單。

恢復這些文件的步驟

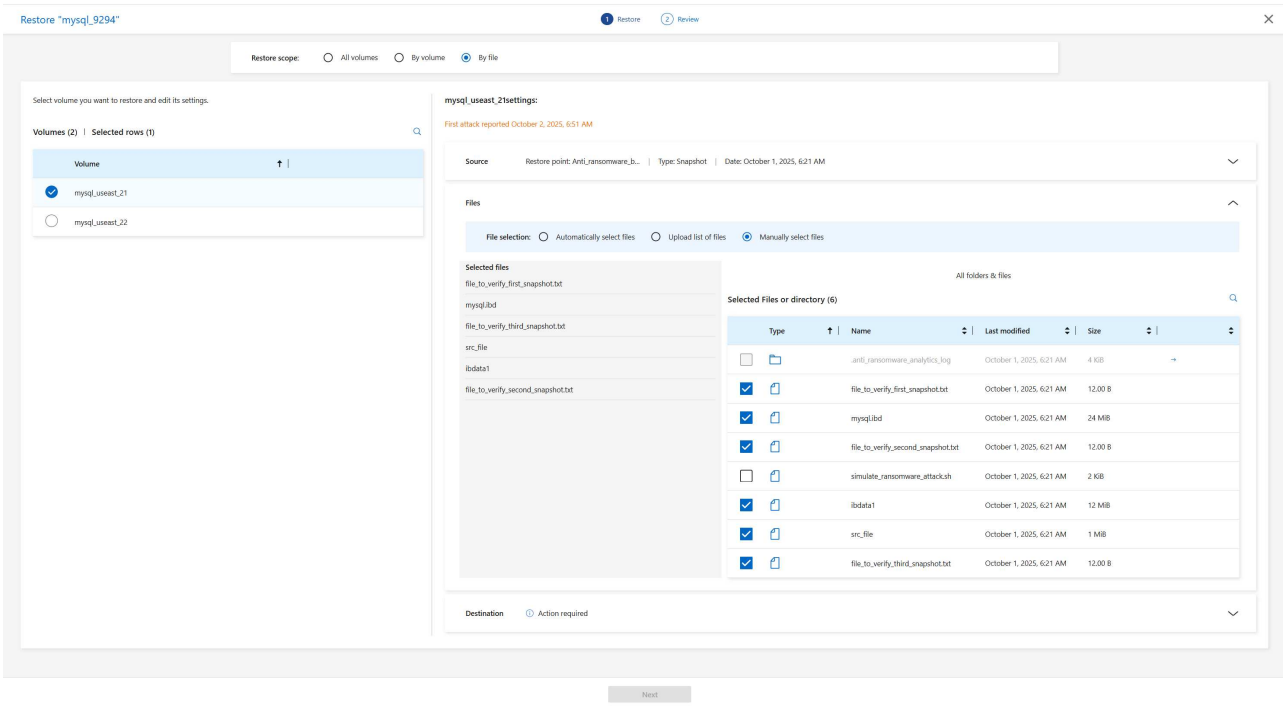
1. 從勒索軟體恢復選單中，選擇*恢復*。
2. 選擇處於「需要恢復」狀態的應用程式工作負載。
3. 若要恢復，請選擇*恢復*。
4. 在「還原」頁面的「還原範圍」中，選擇「按檔案」。
5. 在磁碟區清單中，選擇包含要還原的檔案的磁碟區。
6. 還原點：選擇*還原點*旁的向下箭頭查看詳細資料。選擇要用於還原資料的還原點。

> 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。

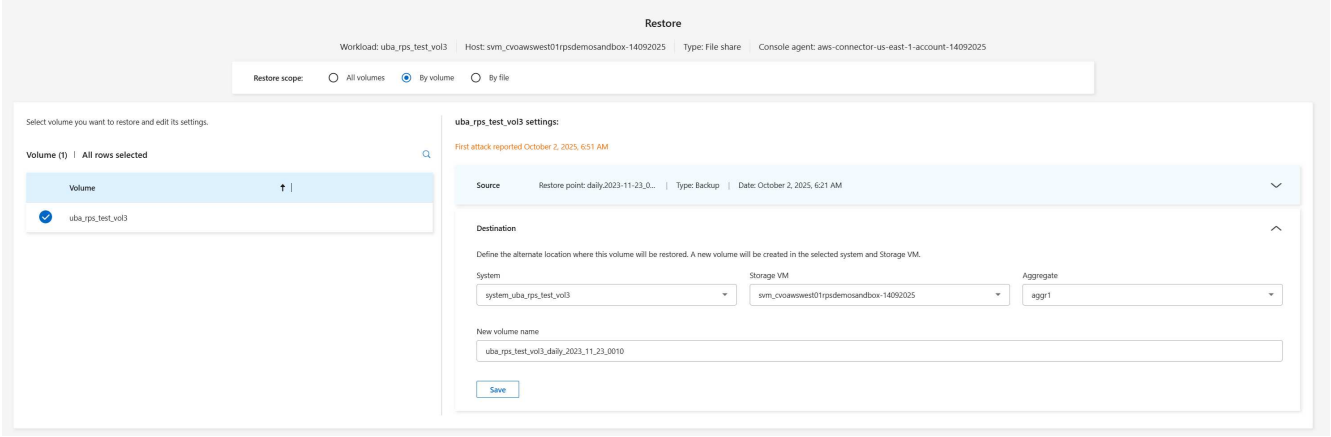
   b. 選擇系統。
   c. 選擇儲存虛擬機器。
   d. （可選）輸入路徑。

      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。

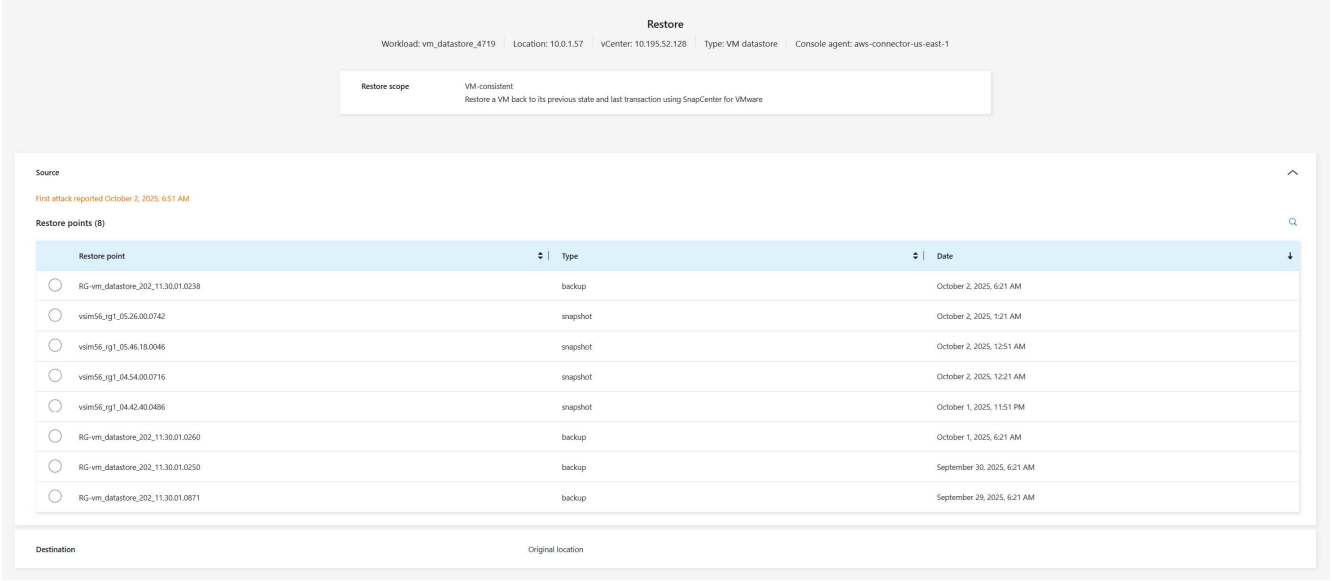
   如果您沒有指定還原路徑，檔案將會還原到頂層目錄的新磁碟區。

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。

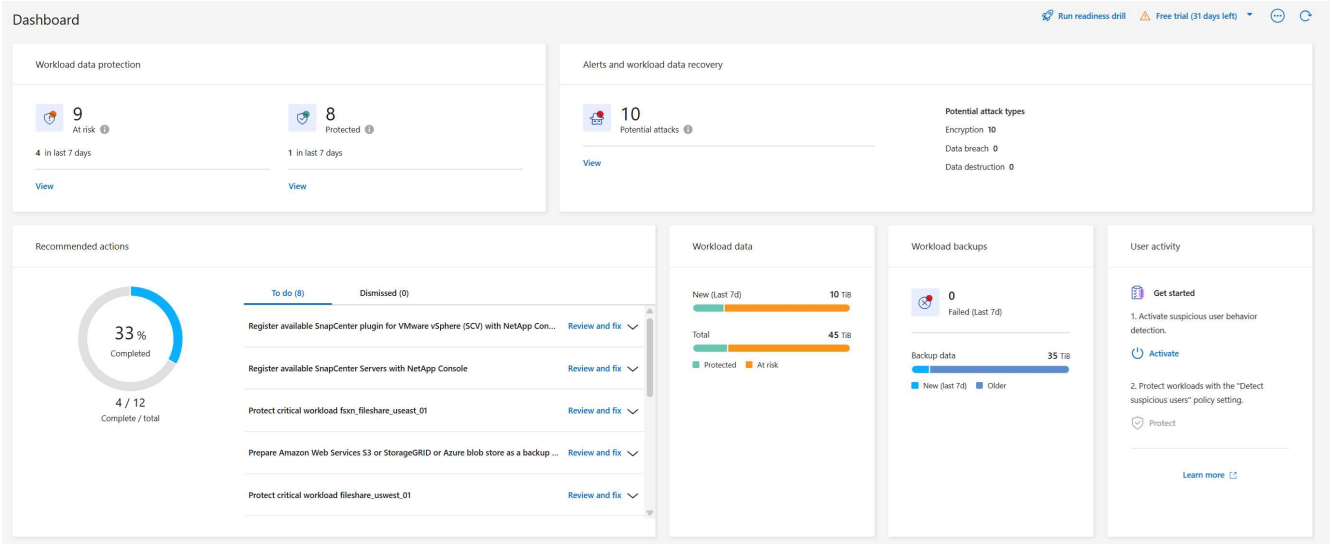
以下情況需要輸入使用者名稱和密碼：

- 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" 。

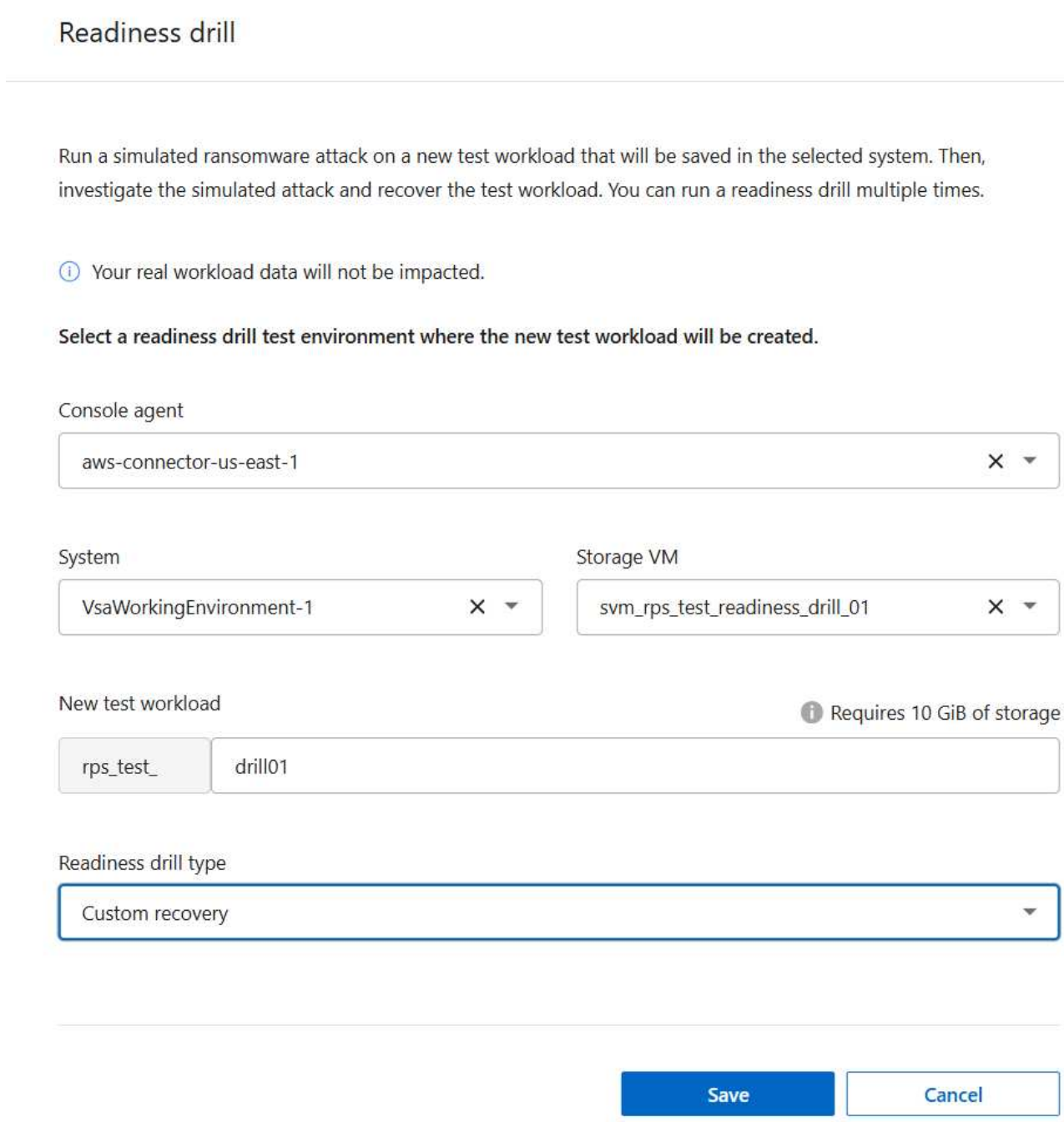
步驟

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。



3. 執行以下操作：
   a. 選擇您想要用於準備情境演練的控制台代理程式。
   b. 選擇一個測試系統。
   c. 選擇測試儲存 SVM。
   d. 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。
   e. 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。
   f. 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。

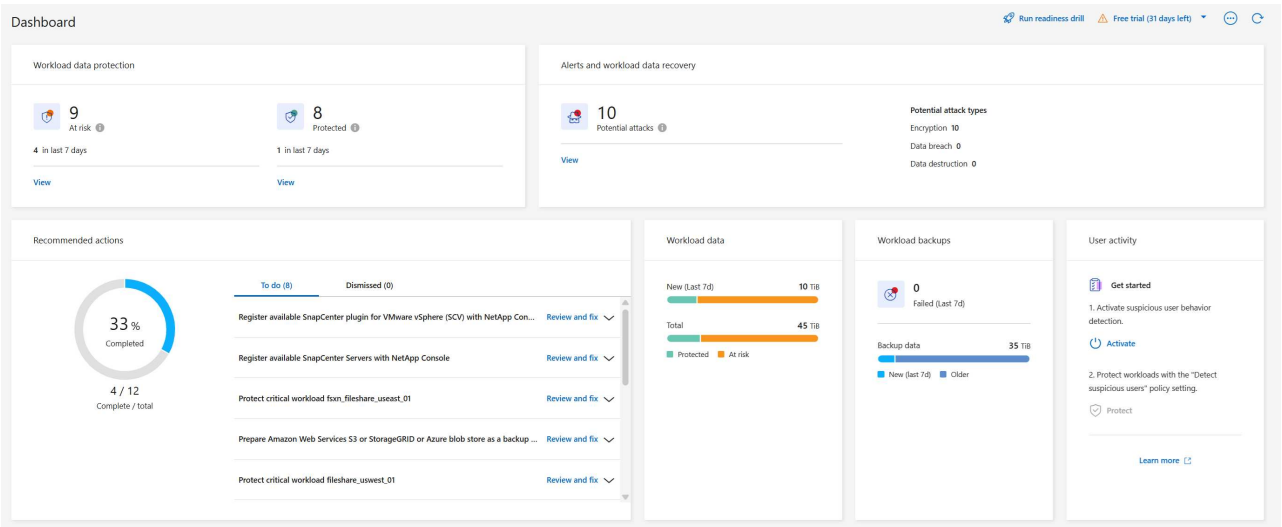
所需的控制台角色 要執行此任務，您需要組織管理員、資料夾或專案管理員或勒索軟體復原管理員角色。"了解NetApp Console的勒索軟體復原角色" 。

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

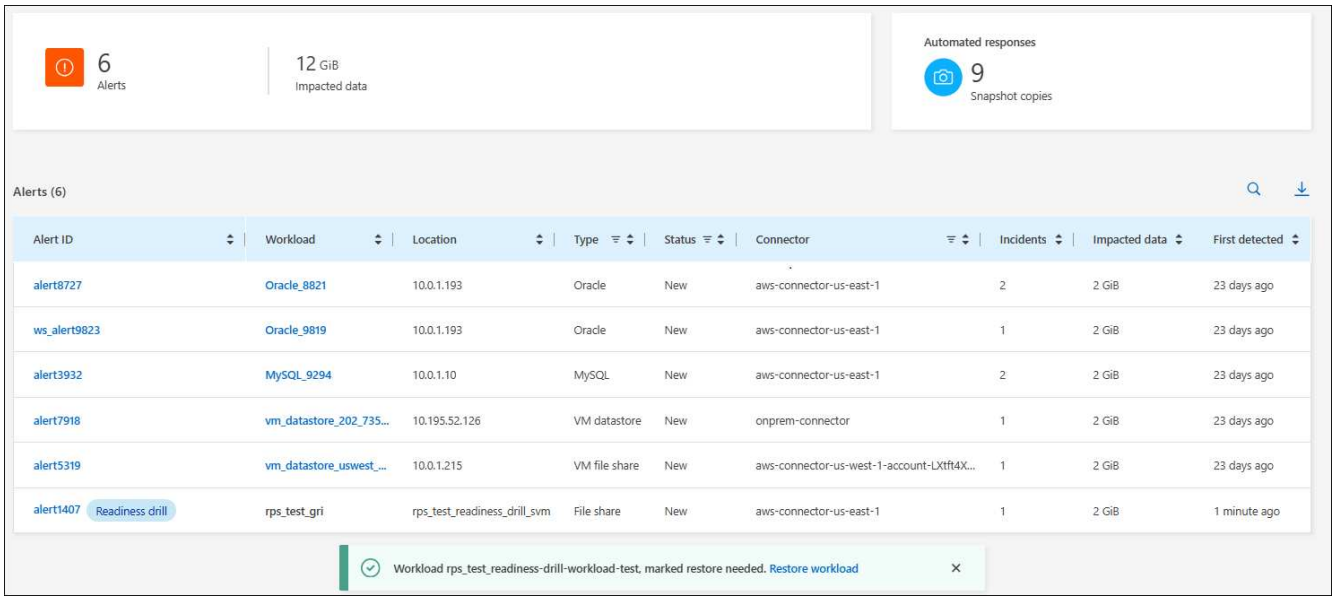
透過回應準備演習警報來測試您的準備。

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" 。

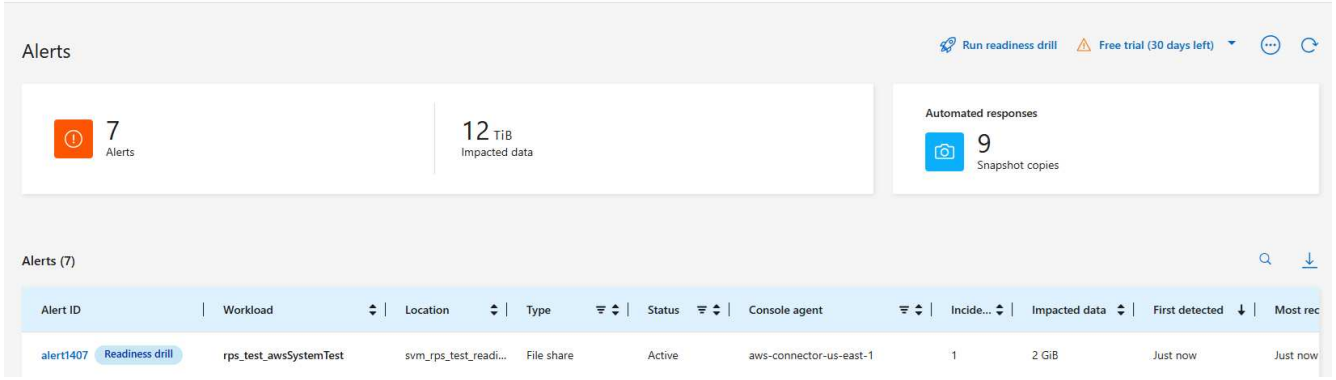
步驟

1. 從勒索軟體恢復選單中，選擇*警報*。

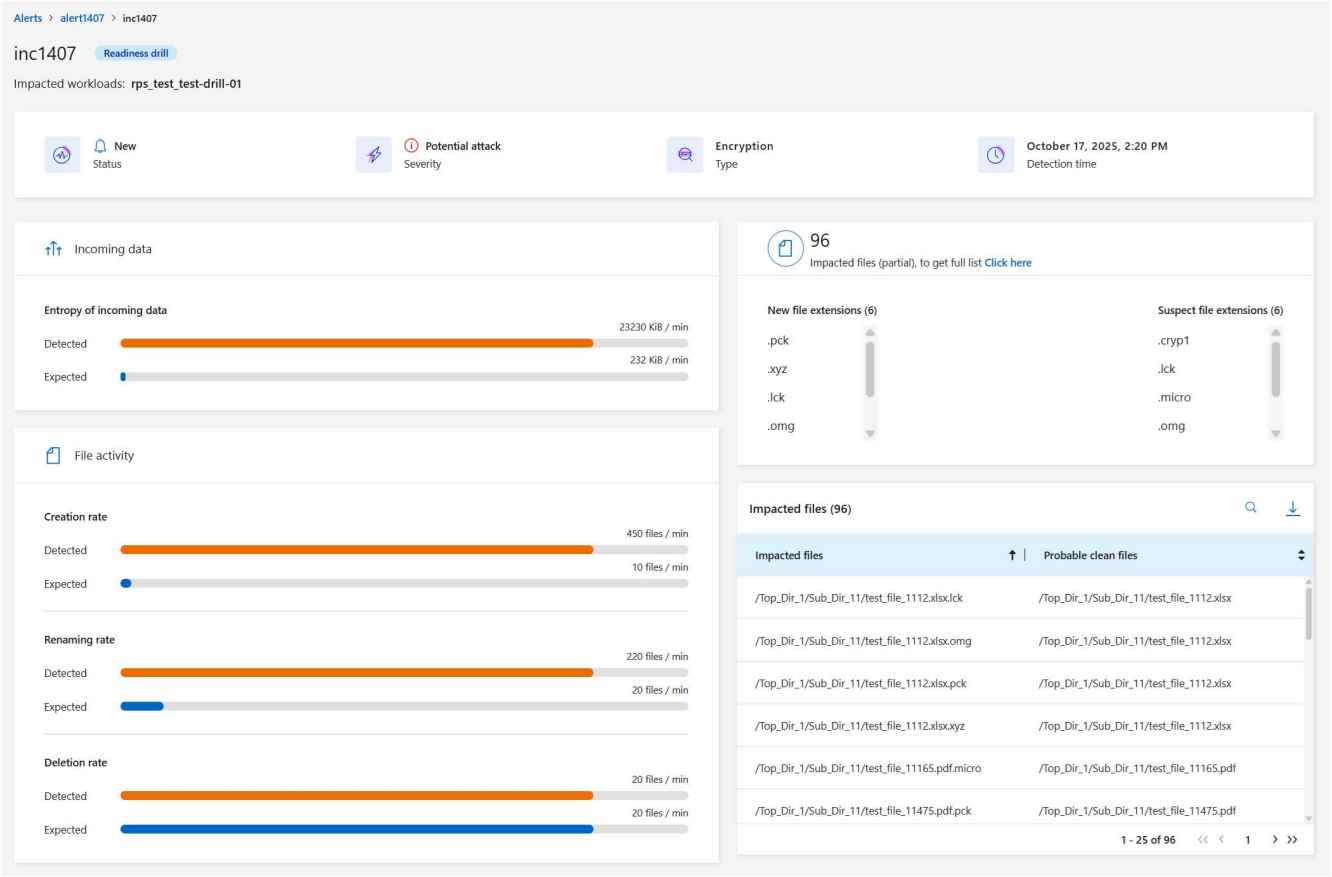
   控制台顯示警報頁面。在警報 ID 欄位中，您會在 ID 旁看到「準備好演練」。



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。



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。

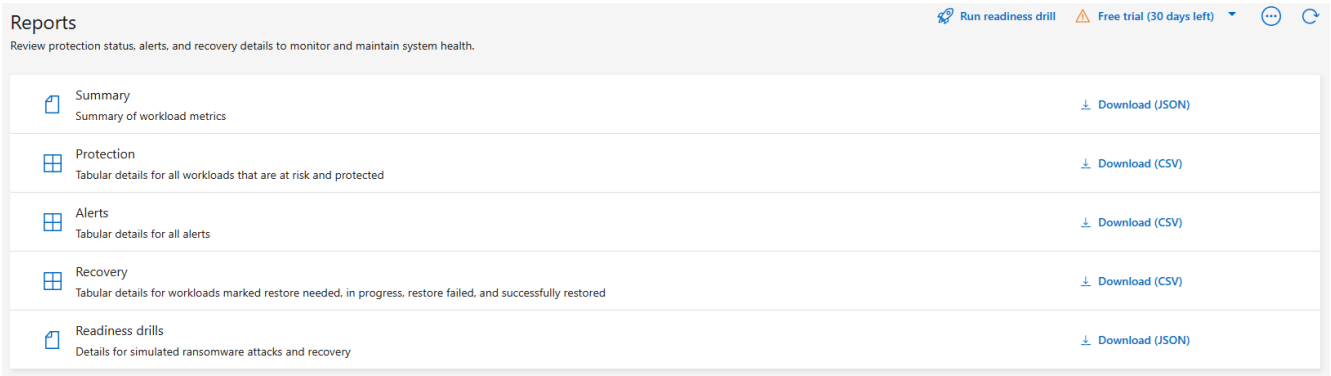
審查準備演習報告

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。

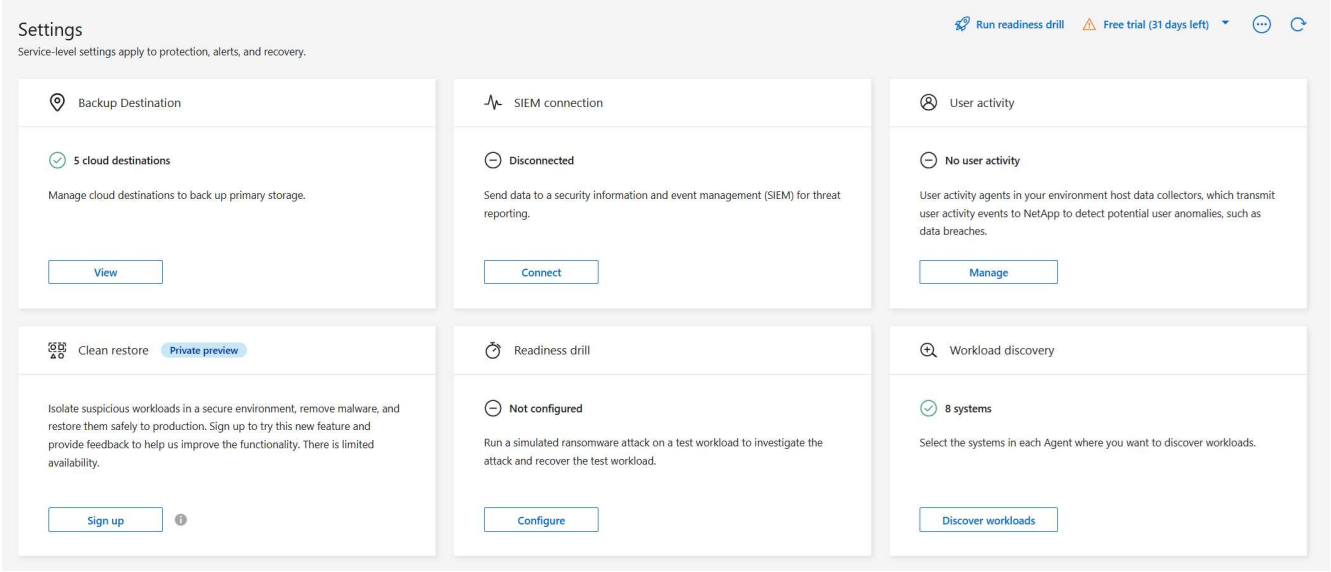
在勒索軟體防禦中連接 **SIEM**

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。

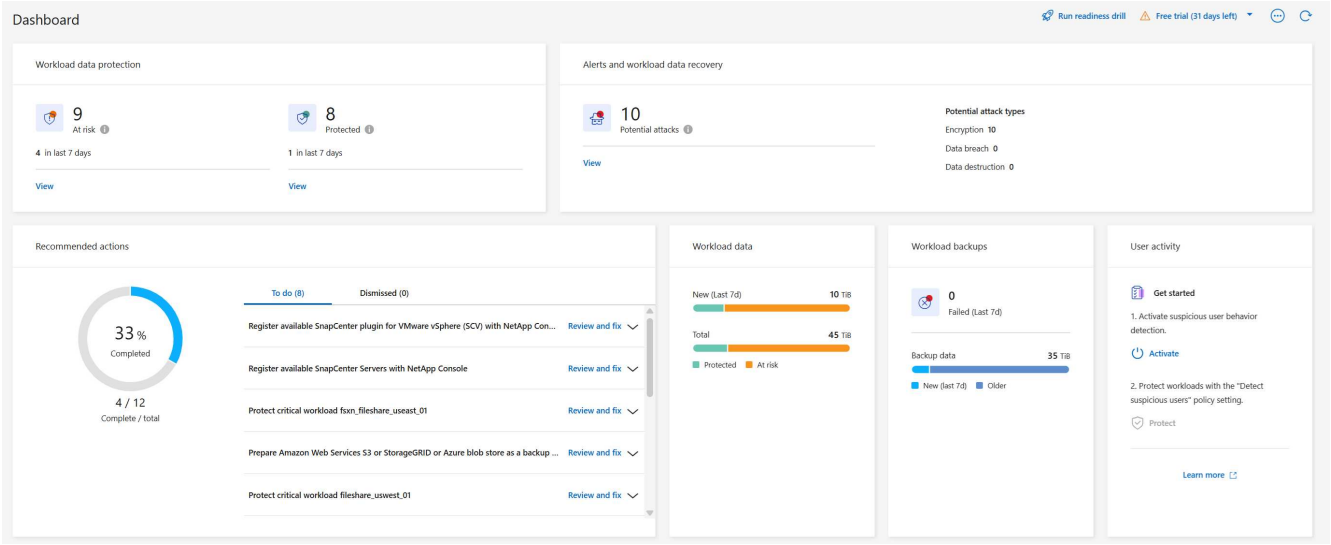
您只能從*報告*頁面下載準備情況演習報告。

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*。



2. 在儀錶板或其他頁面中，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”。