保護工作負載
BlueXP ransomware protection

NetApp
October 07, 2024

目錄

保護工作負載

使用勒索軟體策略保護工作負載

您可以使用 BlueXP 勒索軟體保護來完成下列動作、以保護工作負載免受勒索軟體攻擊。

- 啟用工作負載一致的保護功能、可與 SnapCenter 軟體或 SnapCenter Plug-in for VMware vSphere 搭配使用。
- 建立或管理勒索軟體保護策略、包括您為快照、備份和勒索軟體保護所建立的原則（稱為 _ 偵測原則 _ ）。
- 匯入策略並加以調整。
- 群組檔案共用、讓您更容易保護工作負載、而非個別保護工作負載。
- 刪除勒索軟體保護策略。
- 哪些服務用於保護？ *下列服務可用於管理保護原則。BlueXP 勒索軟體保護中會顯示這些服務的保護資訊：
- 檔案共用、 VM 檔案共用的 BlueXP 備份與還原
- 適用於 VMware 的 SnapCenter for VM 資料存放區
- SnapCenter for Oracle 和 MySQL

保護原則

您可能會發現檢閱有關您可以變更的保護原則、以及保護策略中的原則類型等資訊很有幫助。

- 您可以變更哪些保護原則？ *

您可以根據擁有的工作負載保護來變更保護原則：

- * 工作負載不受 NetApp 應用程式保護 * ：這些工作負載並非由 SnapCenter 、 SnapCenter Plug-in for VMware vSphere 或 BlueXP 備份與還原所管理。這些工作負載可能會將快照當成 ONTAP 或其他產品的一部分。如果 ONTAP FPolicy 保護已就緒、您可以使用 ONTAP 變更 FPolicy 保護。
- * 由 NetApp 應用程式提供現有保護的工作負載 * ：這些工作負載具有由 SnapCenter 、 SnapCenter for VMware vSphere 或 BlueXP 備份與還原所管理的備份或快照原則。
  - 如果快照或備份原則是由 SnapCenter 、 SnapCenter for VMware 或 BlueXP 備份與還原管理、則這些原則將繼續由這些應用程式管理。使用 BlueXP 勒索軟體保護、您也可以將勒索軟體偵測原則套用至這些工作負載。
  - 如果勒索軟體偵測原則是由 ONTAP 中的自主勒索軟體保護（ ARP ）和 FPolicy 管理、則這些工作負載會受到保護、並將繼續由 ARP 和 FPolicy 管理。
- 勒索軟體保護策略需要哪些政策？ *

勒索軟體保護策略需要下列原則：

- 勒索軟體偵測原則
- Snapshot原則

BlueXP 勒索軟體保護策略不需要備份原則。

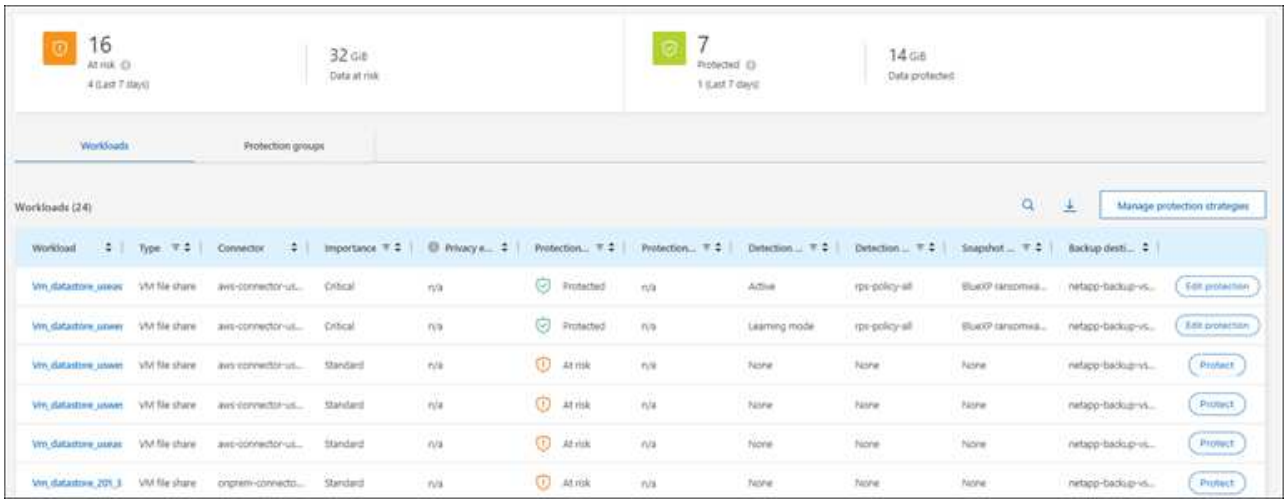
檢視工作負載的勒索軟體保護

保護工作負載的第一步之一、就是檢視您目前的工作負載及其保護狀態。您可以看到下列類型的工作負載：

- 應用程式工作負載
- VM 工作負載
- 檔案共用工作負載

步驟

1. 從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。
2. 執行下列其中一項：
   - 從儀表板的資料保護窗格中、選取 * 檢視全部 * 。
   - 從功能表中選取 * 保護 * 。



3. 您可以在此頁面檢視及變更工作負載的保護詳細資料。

> 對於已有 SnapCenter 或 BlueXP 備份與還原服務保護原則的工作負載、您無法編輯保護。對於這些工作負載、如果 BlueXP 勒索軟體已在其他服務中啟動、則 BlueXP 勒索軟體可啟用自動勒索軟體保護及 / 或 FPolicy 保護。深入瞭解 "自主勒索軟體保護"、 "BlueXP 備份與還原"和 "ONTAP FPolicy"。

保護詳細資料請參閱保護頁面

「保護」頁面顯示工作負載保護的下列資訊：

- 保護狀態 * ：工作負載可顯示下列其中一個保護狀態、以指出是否套用原則：
- * 受保護 * ：套用原則。所有與工作負載相關的磁碟區都會啟用 ARP 。
- * 風險 * ：不套用任何原則。如果工作負載未啟用主要偵測原則、即使已啟用快照和備份原則、也會有「風險」。
- * 進行中 * ：正在套用原則、但尚未完成。
- * 失敗 * ：套用原則但無法運作。

- 偵測狀態 * ：工作負載可具有下列其中一種勒索軟體偵測狀態：
- * 學習 * ：最近指派了勒索軟體偵測原則給工作負載、服務正在掃描工作負載。
- * Active * ：已指派勒索軟體偵測保護原則。
- * 未設定 * ：未指派勒索軟體偵測保護原則。
- * 錯誤 * ：已指派勒索軟體偵測原則、但服務發生錯誤。

在 BlueXP 勒索軟體保護中啟用保護功能時、警示偵測和報告會在勒索軟體偵測原則狀態從「學習」模式變更為「主動」模式後開始。

- 偵測原則 * ：如果已指派勒索軟體偵測原則、則會顯示該原則的名稱。如果尚未指派偵測原則、則會顯示「 N/A 」。
- Snapshot 與備份原則 * ：此欄顯示套用至工作負載的快照與備份原則、以及管理這些原則的產品或服務。
- 由 SnapCenter 管理
- 由 SnapCenter Plug-in for VMware vSphere 管理
- 由 BlueXP 備份與還原管理
- 管理快照和備份的勒索軟體保護原則名稱
- 無
- 工作負載重要性 *

BlueXP 勒索軟體保護會根據每個工作負載的分析、在探索期間為每個工作負載指派重要或優先順序。工作負載重要性取決於下列快照頻率：

- * 關鍵 * ：每小時拍攝超過 1 份快照複本（極具挑戰性的保護排程）
- * 重要 * ：快照複本每小時拍攝不到 1 份、但每天超過 1 份
- * 標準 * ：每天拍攝超過 1 份快照複本
- 預先定義的偵測原則 *

您可以選擇符合工作負載重要性的下列 BlueXP 勒索軟體保護預先定義原則之一：

原則層級	**Snapshot**	頻率	保留（天數）	快照複本數量	快照複本總數上限
* 關鍵工作負載原則 *	每季一次	每 15 分鐘	3.	288	309
	每日	每 1 天	14.	14.	309
	每週	每 1 週	35	5.	309
	每月	每 30 天	60	2.	309

原則層級	Snapshot	頻率	保留（天數）	快照複本數量	快照複本總數上限
* 重要工作負載原則 *	每季一次	每 30 分鐘一次	3.	144.	165
	每日	每 1 天	14.	14.	165
	每週	每 1 週	35	5.	165
	每月	每 30 天	60	2.	165
* 標準工作負載原則 *	每季一次	每 30 分鐘	3.	72.	93
	每日	每 1 天	14.	14.	93
	每週	每 1 週	35	5.	93
	每月	每 30 天	60	2.	93

使用 SnapCenter 實現應用程式或 VM 一致的保護

啟用應用程式或 VM 一致的保護功能、可協助您以一致的方式保護應用程式或 VM 工作負載、達到靜止且一致的狀態、以避免日後需要恢復時可能發生的資料遺失。

此程序會針對使用 BlueXP 備份與還原的虛擬機器、起始登錄適用於應用程式的 SnapCenter 軟體伺服器或適用於 VMware vSphere 的 SnapCenter 外掛程式。

啟用工作負載一致的保護之後、您就可以在 BlueXP 勒索軟體保護中管理保護策略。保護策略包括在其他地方管理的快照和備份原則、以及在 BlueXP 勒索軟體保護中管理的勒索軟體偵測原則。

若要深入瞭解如何使用 BlueXP 備份與還原為 VMware vSphere 註冊 SnapCenter 或 SnapCenter 外掛程式、請參閱下列資訊：

- "註冊 SnapCenter 伺服器軟體"
- "註冊SnapCenter VMware vSphere的VMware外掛程式"

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 儀表板 * 。
2. 從「建議」窗格中、找到下列其中一項建議、然後選取 * 「審查與修正」 * ：
    - 在 BlueXP 中註冊可用的 SnapCenter 伺服器
    - 在 BlueXP 中註冊 VMware vSphere （ SCV ）可用的 SnapCenter 外掛程式
3. 請依照相關資訊、使用 BlueXP 備份與還原、為 VMware vSphere 主機註冊 SnapCenter 或 SnapCenter 外掛程式。
4. 返回 BlueXP 勒索軟體保護。

5. 從 BlueXP 勒索軟體保護開始、請前往儀表板、再次啟動探索程序。
6. 從 BlueXP 勒索軟體保護中、選取 * 保護 * 以檢視保護頁面。
7. 檢閱「保護」頁面上「快照與備份原則」欄中的詳細資料、查看原則是否在其他地方受到管理。

新增勒索軟體保護策略

您可以為工作負載新增勒索軟體保護策略。執行方式取決於快照和備份原則是否已經存在：

- * 如果您沒有快照或備份原則、請建立勒索軟體保護策略 * 。如果工作負載上不存在快照或備份原則、您可以建立勒索軟體保護策略、其中包括您在 BlueXP 勒索軟體保護中建立的下列原則：
  - Snapshot原則
  - 備份原則
  - 勒索軟體偵測原則
- * 為已有快照和備份原則 * 的工作負載建立偵測原則、這些原則可在其他 NetApp 產品或服務中管理。偵測原則不會變更在其他產品中管理的原則。

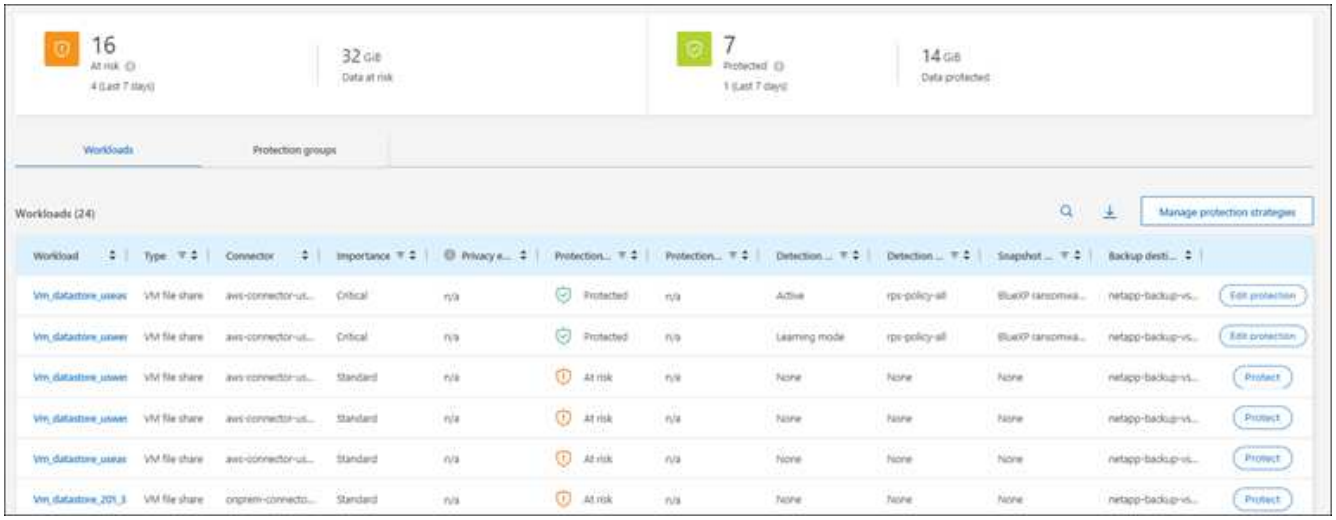
建立勒索軟體保護策略（如果您沒有快照或備份原則）

如果工作負載上不存在快照或備份原則、您可以建立勒索軟體保護策略、其中包括您在 BlueXP 勒索軟體保護中建立的下列原則：

- Snapshot原則
- 備份原則
- 勒索軟體偵測原則

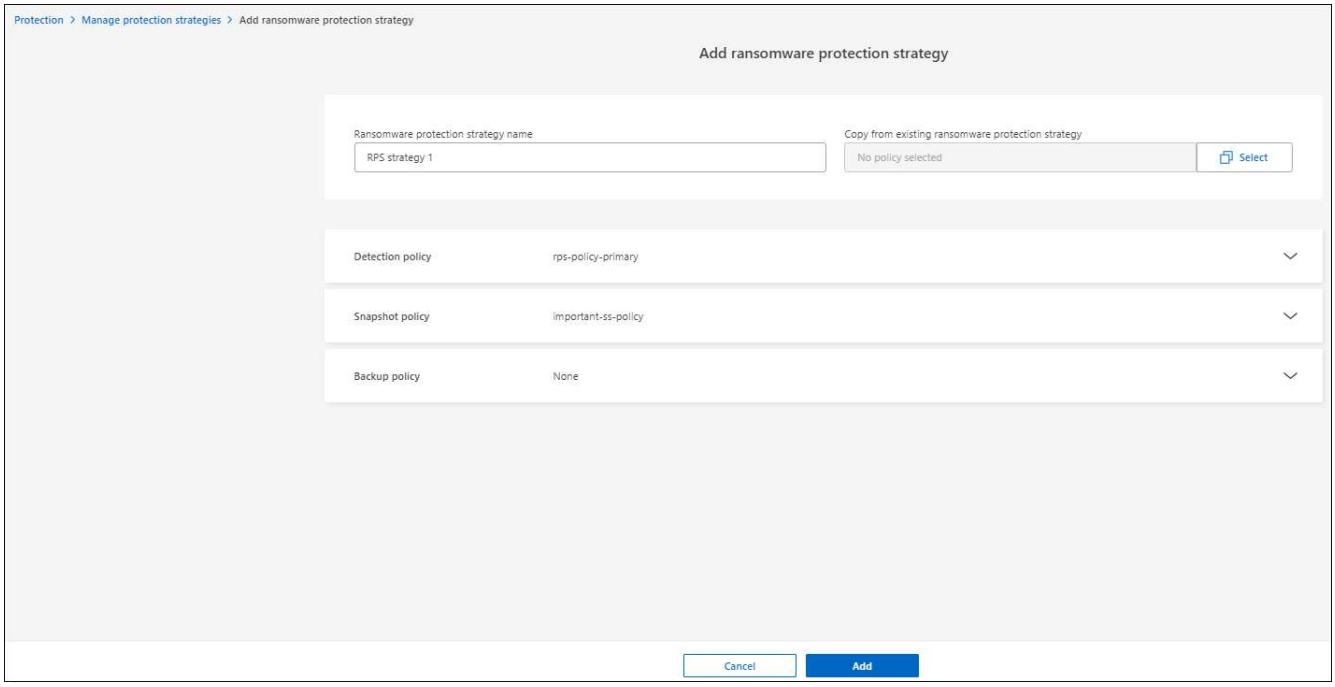
建立勒索軟體保護策略的步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。



2. 從「保護」頁面選取 * 管理保護策略 * 。

3. 從勒索軟體保護策略頁面、選取 * 新增 * 。



4. 輸入新的策略名稱、或輸入現有名稱以進行複製。如果您輸入現有名稱、請選擇要複製的名稱、然後選取 * 複製 * 。

> 如果您選擇複製及修改現有策略、服務會將「 _copy 」附加至原始名稱。您應該變更名稱和至少一個設定、使其成為唯一的。

5. 針對每個項目、選取 * 向下箭頭 * 。

   - * 偵測政策 * ：
     - * 原則 * ：選擇預先設計的偵測原則之一。
     - * 主要偵測 * ：啟用勒索軟體偵測功能、讓服務偵測可能的勒索軟體攻擊。
     - * 封鎖副檔名 * ：啟用此選項可讓服務封鎖已知可疑的副檔名。啟用主要偵測時、服務會自動擷取快照複本。

       如果您要變更封鎖的副檔名、請在 System Manager 中編輯副檔名。
   - * Snapshot 原則 * ：

- * Snapshot 原則基礎名稱 * ：選取原則或選取 * Create * 並輸入快照原則的名稱。
- * Snapshot 鎖定 * ：啟用此選項可鎖定主儲存設備上的快照複本、即使勒索軟體攻擊管理其通往備份儲存目的地的方式、仍無法在一段時間內修改或刪除快照複本。這也稱為 _immutable 儲存設備 _ 。如此可加快還原時間。

  快照鎖定時、磁碟區過期時間會設為快照複本的到期時間。

ONTAP 9.12.1 及更新版本均提供 Snapshot 複本鎖定功能。若要深入瞭解 SnapLock 、請參閱 "ONTAP 中的 SnapLock"。

- * Snapshot 排程 * ：選擇排程選項、要保留的快照複本數量、然後選取以啟用排程。

。* 備份原則 * ：

- * 備份原則基礎名稱 * ：輸入新名稱或選擇現有名稱。
- * 備份排程 * ：選擇次要儲存設備的排程選項並啟用排程。

若要在次要儲存設備上啟用備份鎖定、請使用 * 設定 * 選項來設定備份目的地。如需詳細資訊、請參閱 "設定"。

6. 選取*「Add*」。

將偵測原則新增至已有快照和備份原則的工作負載

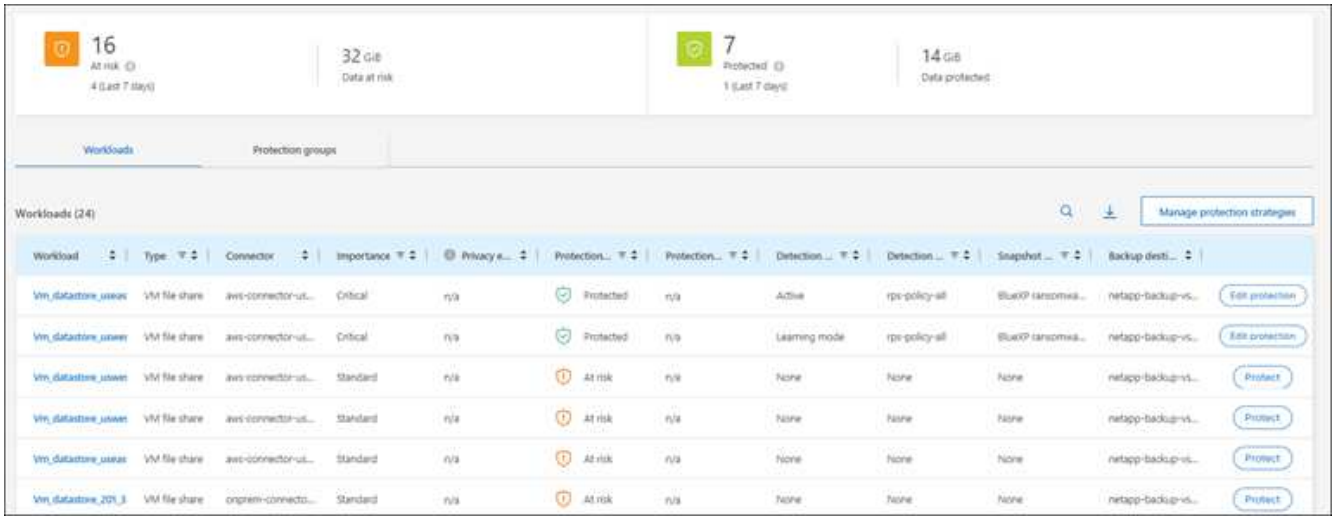
透過 BlueXP 勒索軟體保護、您可以將勒索軟體偵測原則指派給已有快照和備份原則的工作負載、這些原則是在其他 NetApp 產品或服務中管理的。偵測原則不會變更在其他產品中管理的原則。

其他服務（例如 BlueXP 備份與還原及 SnapCenter ）則使用下列類型的原則來管理工作負載：

- 管理快照的原則
- 管理複寫至次要儲存設備的原則
- 管理備份至物件儲存設備的原則

步驟

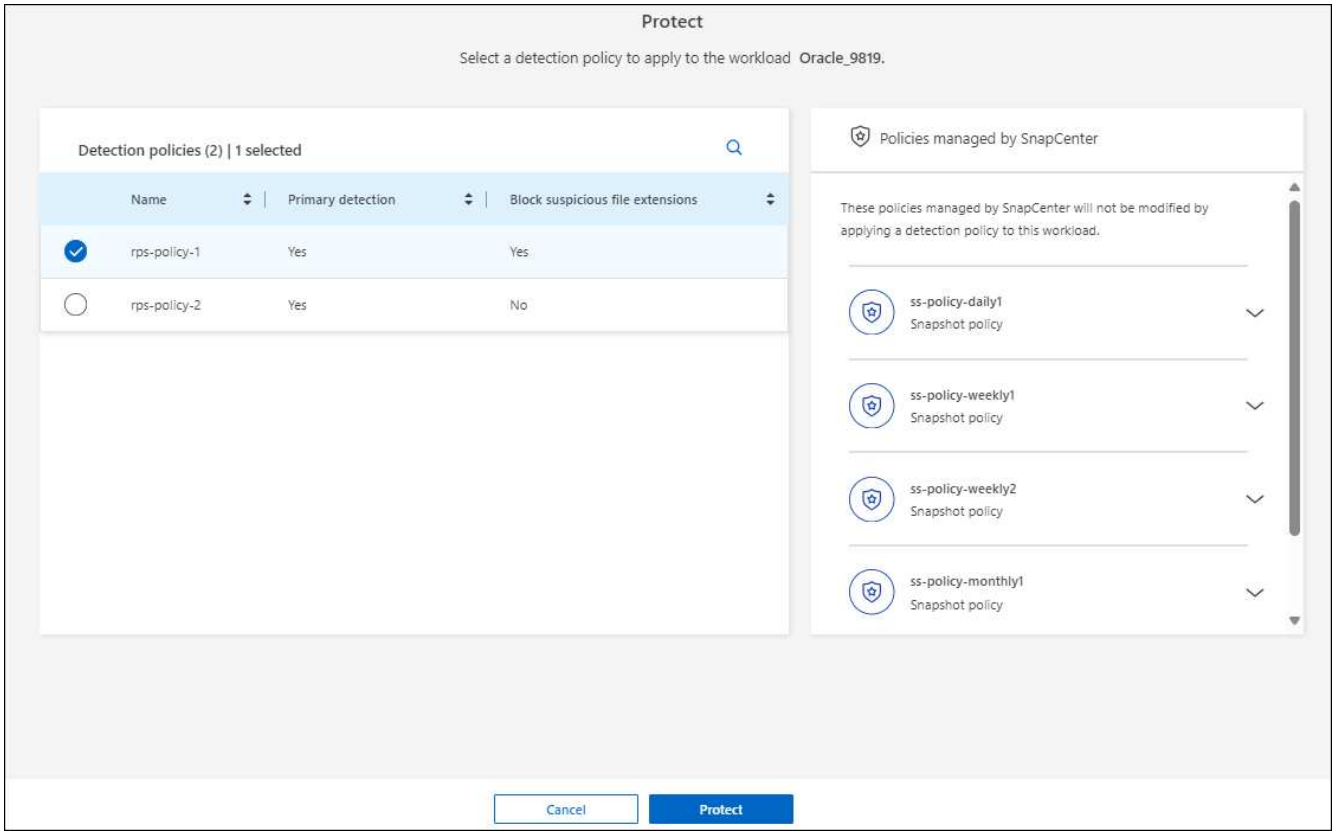
1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。



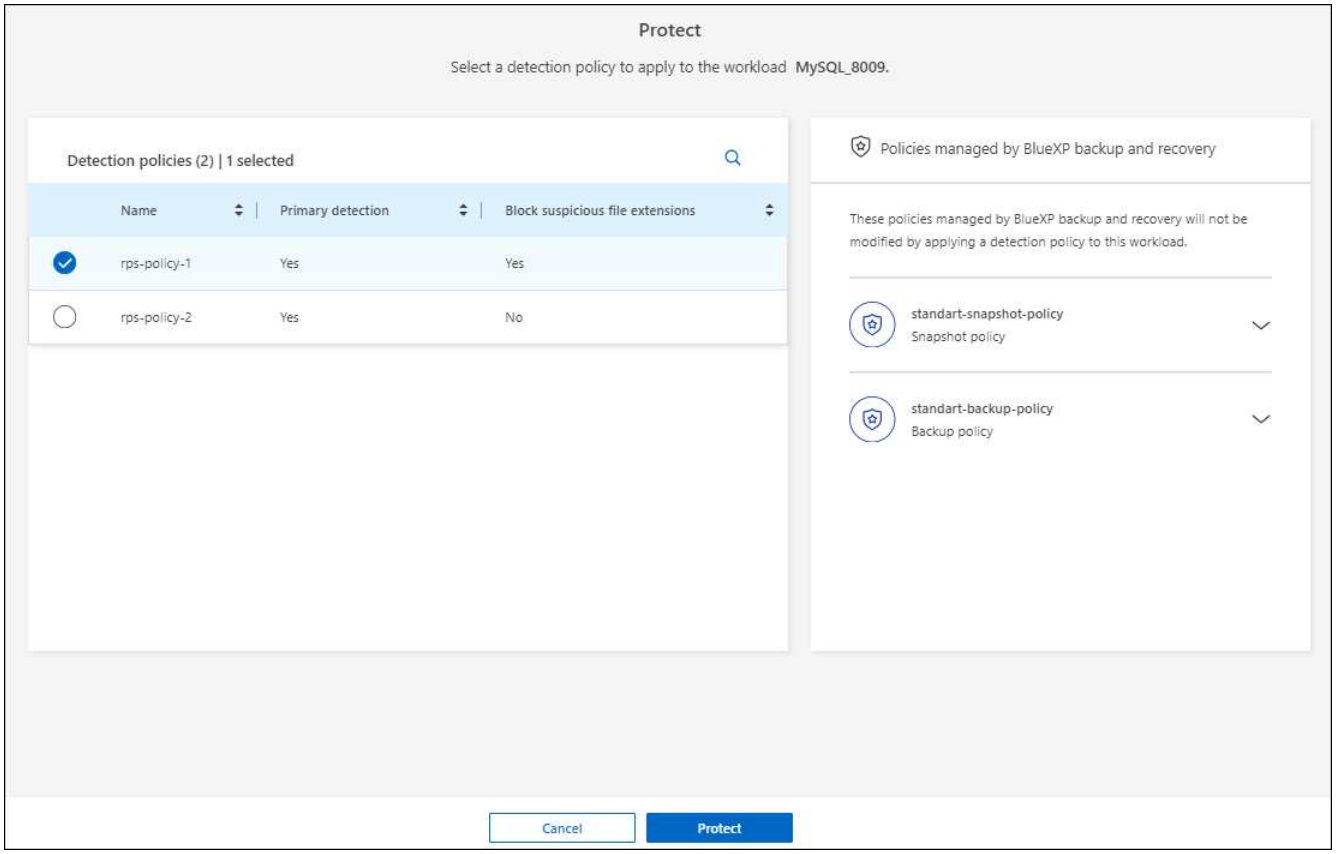
2. 從「保護」頁面選取工作負載、然後選取 * 保護 * 。

「保護」頁面會顯示由 SnapCenter 軟體、 SnapCenter for VMware vSphere 和 BlueXP 備份與還原所管理的原則。

下列範例顯示 SnapCenter 所管理的原則：



以下範例顯示 BlueXP 備份與還原所管理的原則：



3. 若要查看其他管理原則的詳細資料、請按一下 * 向下箭頭 * 。
4. 若要套用偵測原則、以及在其他地方管理的快照和備份原則、請選取偵測原則。
5. 選取 * 保護 * 。
6. 在「保護」頁面上、檢閱「偵測原則」欄、查看指派的「偵測原則」。此外、快照和備份原則欄也會顯示管理原則的產品或服務名稱。

指派不同的原則

您可以指派不同的保護原則來取代目前的保護原則。

步驟

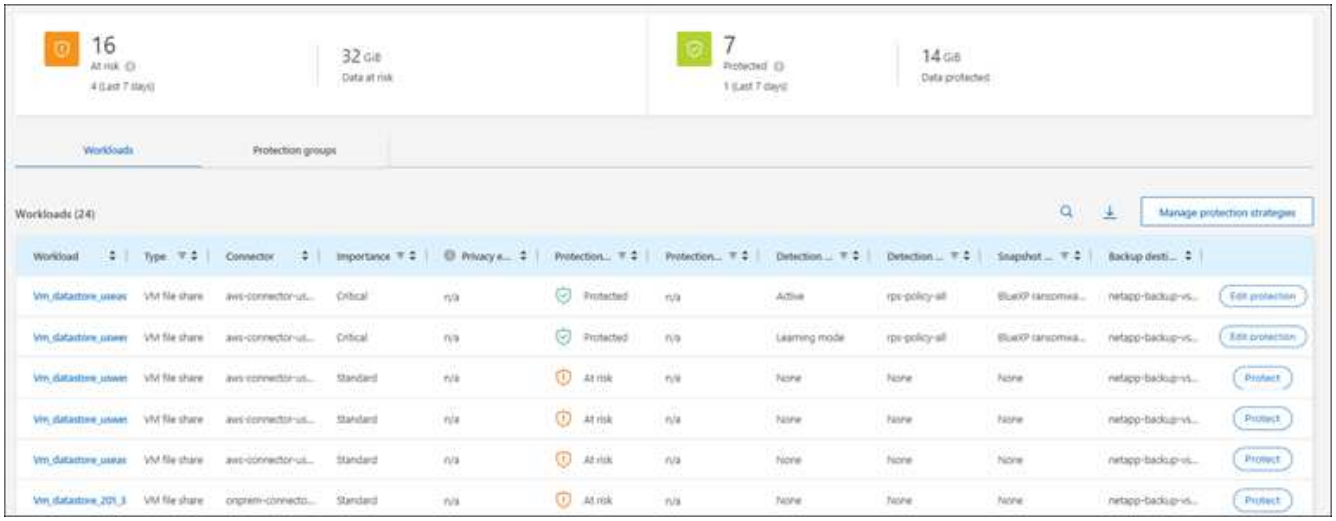
1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面的工作負載列中、選取 * 編輯保護 * 。
3. 在「原則」頁面中、按一下您要指派的原則向下箭頭、以檢閱詳細資料。
4. 選取您要指派的原則。
5. 選取 * 保護 * 以完成變更。

群組檔案共用以更容易保護

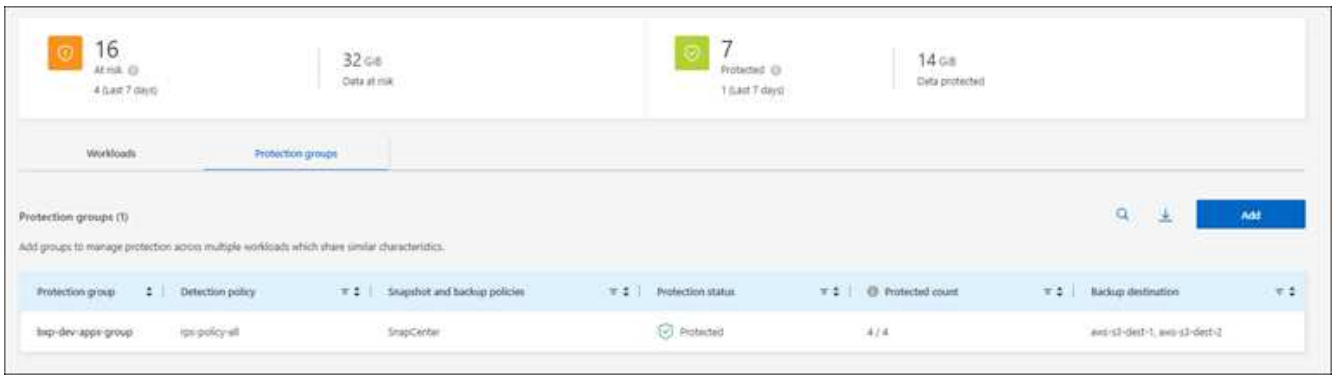
群組檔案共用可讓您更輕鬆地保護資料資產。此服務可同時保護群組中的所有磁碟區、而非分別保護每個磁碟區。

步驟

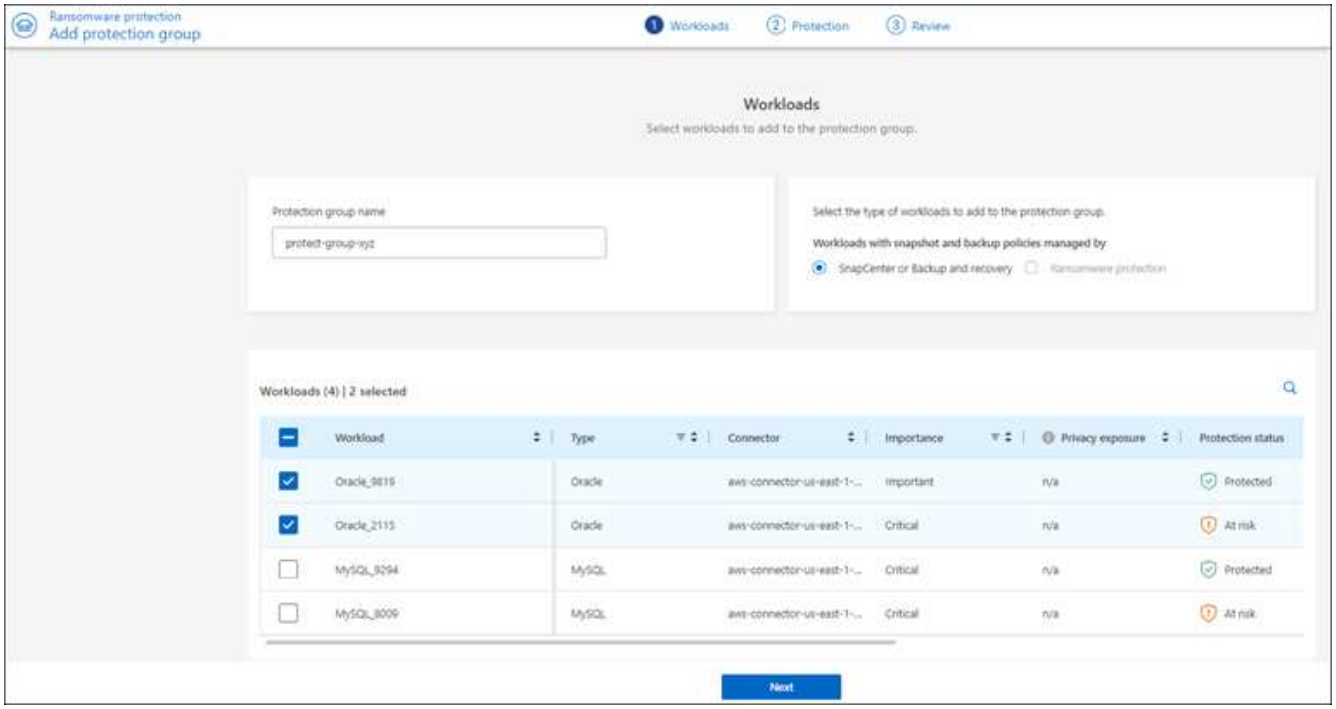
1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。



2. 從「保護」頁面中、選取 * 保護群組 * 索引標籤。



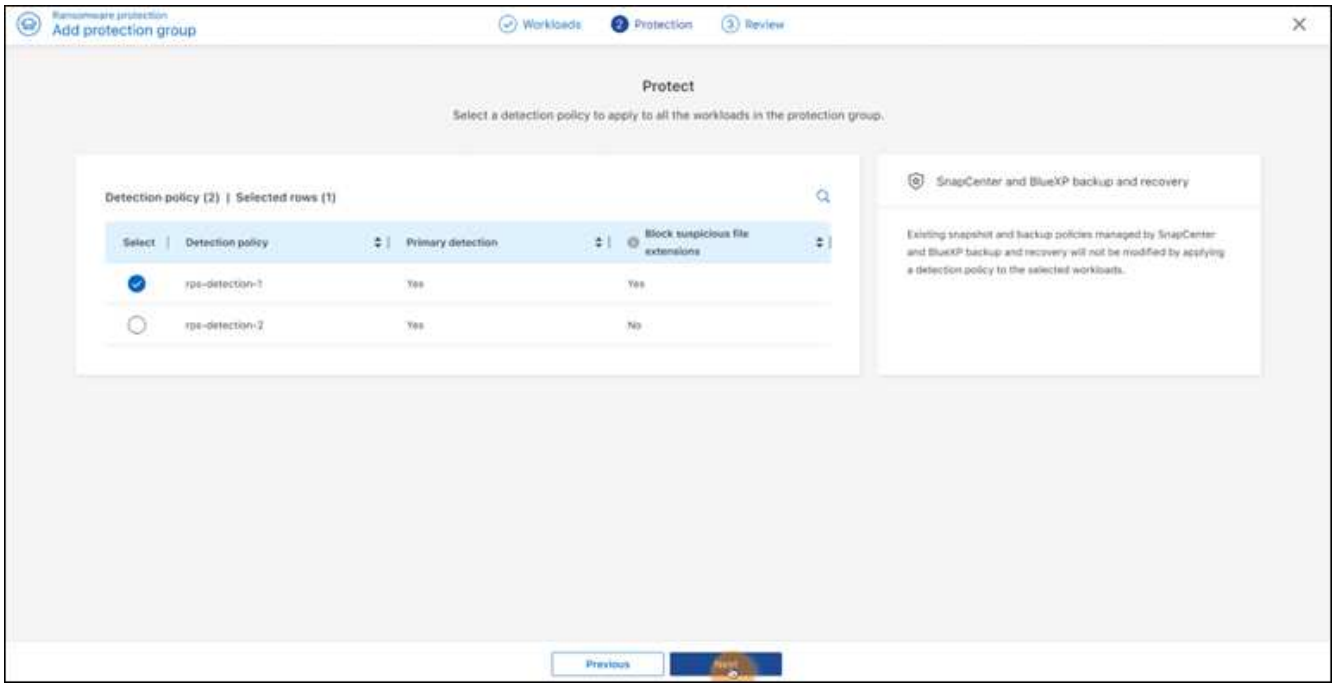
3. 選取*「Add*」。



4. 輸入保護群組的名稱。
5. 請完成下列其中一個步驟：
   a. 如果您已經有保護原則、請根據工作負載是否由下列其中一項管理、選擇是否要將其分組：
      - BlueXP 勒索軟體保護
      - SnapCenter 或 BlueXP 備份與還原
   b. 如果您尚未制定保護原則、頁面會顯示預先設定的勒索軟體保護策略。
      i. 選擇一個選項來保護您的群組、然後選取 * 下一步 * 。
      ii. 如果您選擇的工作負載在多個工作環境中都有磁碟區、請選取多個工作環境的備份目的地、以便將它們備份到雲端。
6. 選取要新增至群組的工作負載。

   若要查看工作負載的詳細資料、請向右捲動。

7. 選擇*下一步*。



8. 選取管理此群組保護的原則。
9. 選擇*下一步*。
10. 檢閱保護群組的選項。
11. 選取*「Add*」。

新增更多工作負載至群組

您稍後可能需要將更多工作負載新增至現有群組。

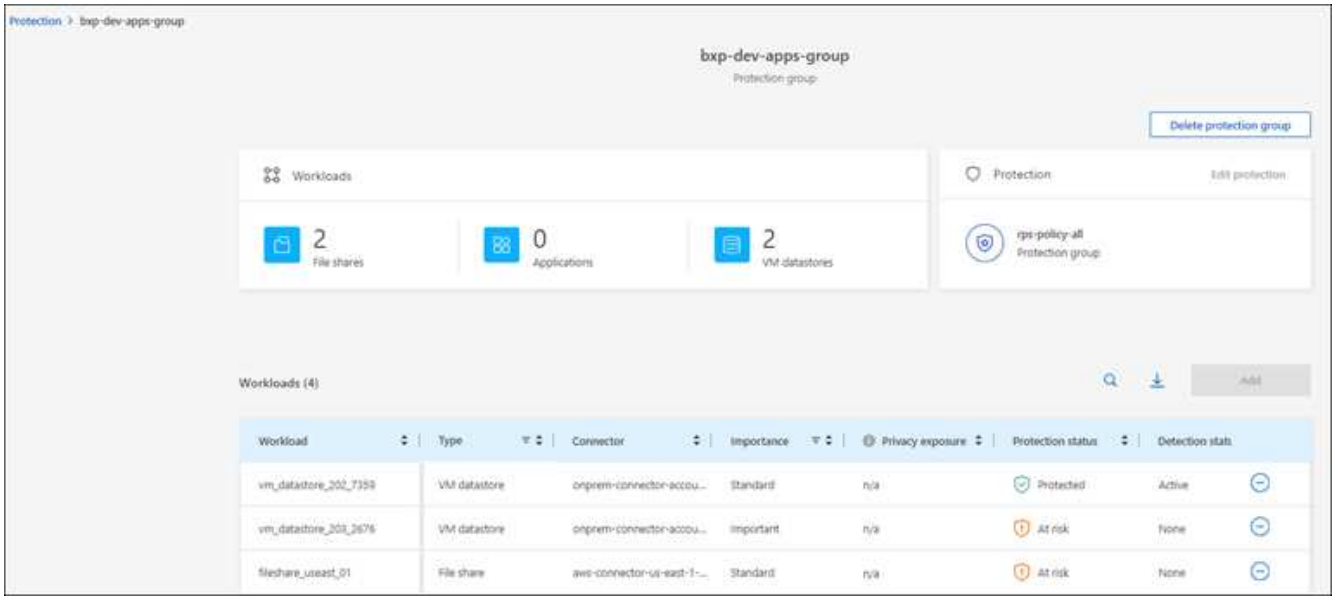
如果群組包含僅由 BlueXP 勒索軟體保護（而非由 SnapCenter 或 BlueXP 備份與還原管理）所管理的工作負載、則應針對僅由 BlueXP 勒索軟體保護所管理的工作負載、使用個別群組、而針對由其他服務管理的工作負

載、使用另一個群組。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面中、選取 * 保護群組 * 索引標籤。

3. 選取您要新增更多工作負載的群組。



4. 從選定的保護群組頁面中、選取 * 新增 * 。

   BlueXP 勒索軟體保護功能只會顯示群組中尚未使用與群組相同快照和備份原則的工作負載。

   頁面頂端會顯示維護快照、備份和偵測原則的服務。

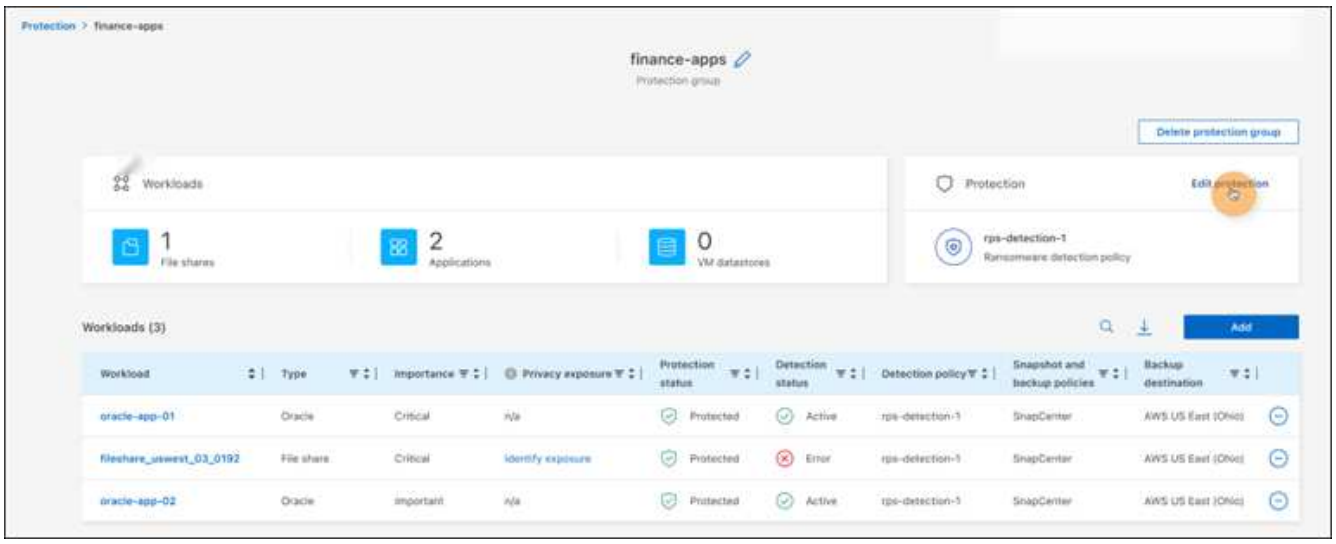
5. 選取應新增至群組的其他工作負載。
6. 選擇*保存*。

編輯群組保護

您可以變更現有群組上的偵測原則。如果尚未將偵測原則新增至此群組、您可以立即新增。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面中、選取 * 保護群組 * 索引標籤。



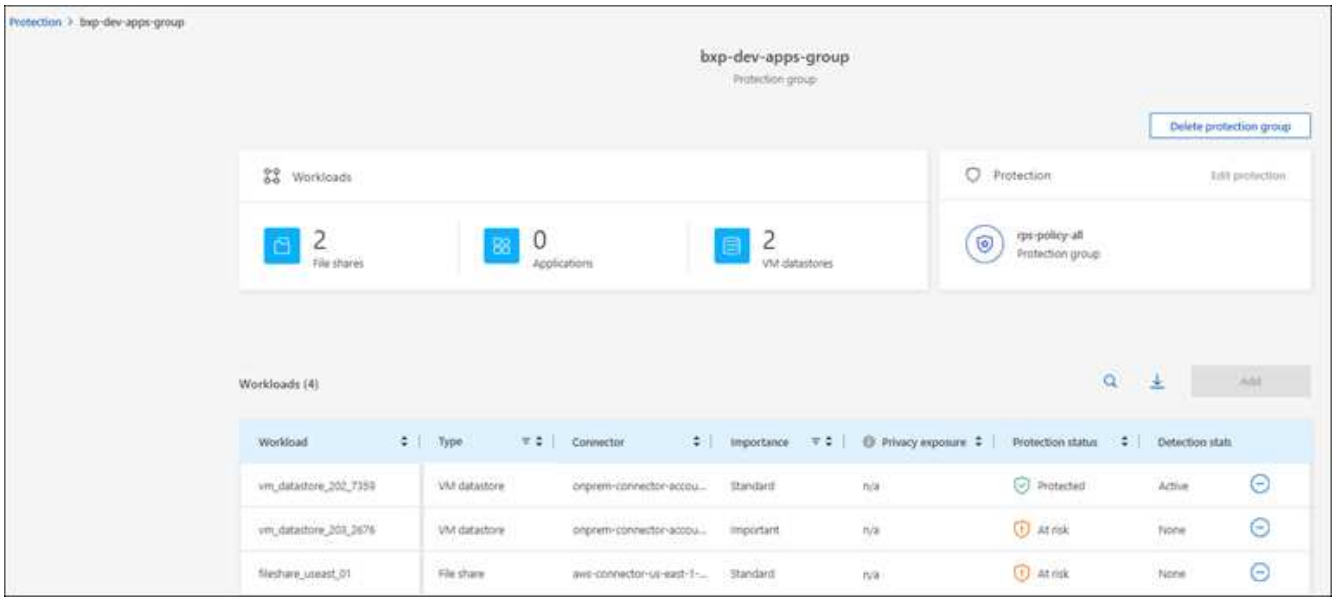
3. 從「保護」窗格中、選取 * 編輯保護 * 。
4. 選取或新增偵測原則至此群組。

移除群組中的工作負載

您稍後可能需要從現有群組移除工作負載。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面中、選取 * 保護群組 * 索引標籤。
3. 選取您要從中移除一或多個工作負載的群組。



4. 在選定的保護群組頁面中、選取您要從群組中移除的工作負載、然後選取 * 動作 * ••• 選項。

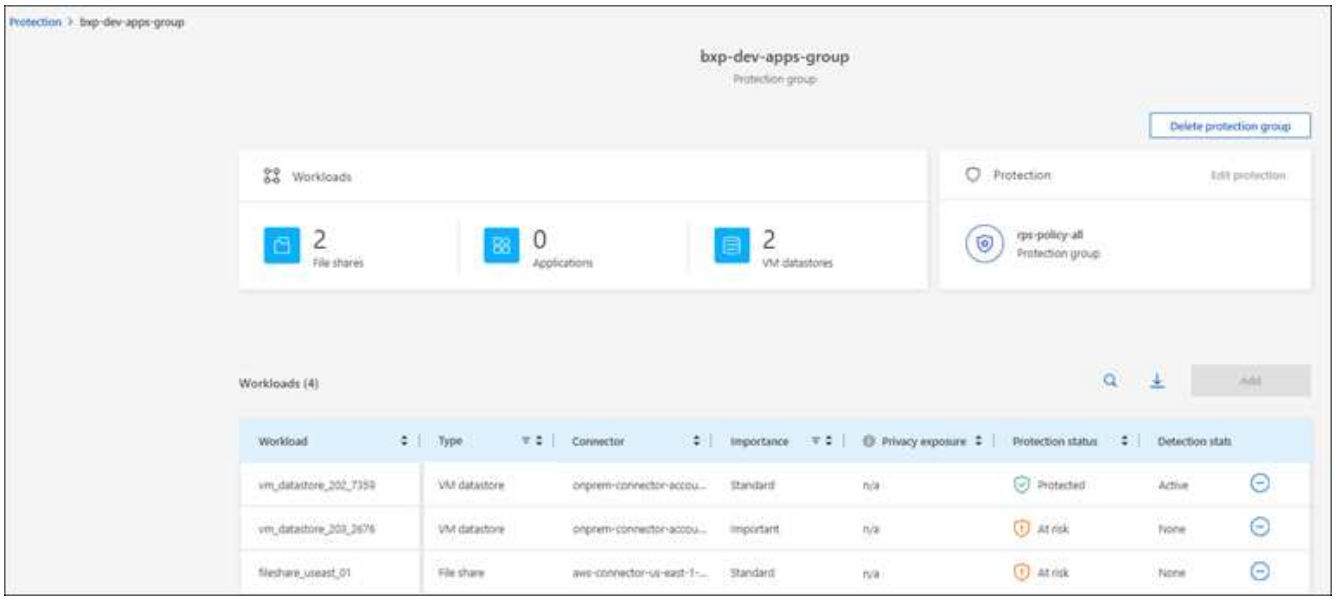
5. 從「動作」功能表中、選取 * 移除工作負載 * 。
6. 確認您要移除工作負載、然後選取 * 移除 * 。

刪除保護群組

刪除保護群組會移除群組及其保護、但不會移除個別工作負載。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面中、選取 * 保護群組 * 索引標籤。
3. 選取您要從中移除一或多個工作負載的群組。



4. 從選取的保護群組頁面右上角、選取 * 刪除保護群組 * 。
5. 確認您要刪除群組、然後選取 * 刪除 * 。

管理勒索軟體保護策略

您可以刪除勒索軟體策略。

檢視受勒索軟體保護策略保護的工作負載

刪除勒索軟體保護策略之前、您可能想要檢視哪些工作負載受到該策略的保護。

您可以從策略清單或編輯特定策略時、檢視工作負載。

檢視策略清單時的步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面選取 * 管理保護策略 * 。

   勒索軟體保護策略頁面會顯示策略清單。

3. 在勒索軟體保護策略頁面的受保護工作負載欄中、按一下列結尾的向下箭頭。

刪除勒索軟體保護策略

您可以刪除目前未與任何工作負載相關聯的保護策略。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面選取 * 管理保護策略 * 。
3. 在「管理策略」頁面中、針對您要刪除的策略選取 * 動作 * ••• 選項。
4. 從「動作」功能表中、選取 * 刪除原則 * 。