BlueXP 勒索軟體保護文件

BlueXP ransomware protection

NetApp
March 22, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/bluexp-ransomware-protection/index.html on March 22, 2024. Always check docs.netapp.com for the latest.

目錄

BlueXP 勒索軟體保護文件

版本資訊： BlueXP 勒索軟體保護預覽的新功能

瞭解 BlueXP 勒索軟體保護預覽的新功能。

2024 年 3 月 5 日

此 BlueXP 勒索軟體保護的預覽版本包含下列更新：

- * 保護原則管理 * ：除了使用預先定義的原則之外、您現在還可以建立、變更及刪除原則。 "深入瞭解管理原則"。
- * 次要儲存設備（ DataLock ）的不可變性 * ：您現在可以使用物件存放區中的 NetApp DataLock 技術、在次要儲存設備中製作不可變的備份。 "深入瞭解如何建立保護原則"。
- * 自動備份至 NetApp StorageGRID * ：除了使用 AWS 之外、您現在可以選擇 StorageGRID 作為備份目的地。 "深入瞭解設定備份目的地"。
- * 調查潛在攻擊的其他功能 * ：您現在可以檢視更多鑑識詳細資料、以調查偵測到的潛在攻擊。 "深入瞭解如何回應偵測到的勒索軟體警示"。
- * 恢復程序 * 。恢復程序已增強。現在、您可以在單一工作流程中、依磁碟區、工作負載的所有磁碟區、甚至是磁碟區的數個檔案來還原磁碟區。 "深入瞭解如何從勒索軟體攻擊中恢復（在事件被消除之後）"。

"瞭解 BlueXP 勒索軟體保護"。

2023 年 10 月 6 日

BlueXP 勒索軟體保護服務是 SaaS 解決方案、可保護資料、偵測潛在攻擊、以及從勒索軟體攻擊中恢復資料。

對於預覽版本、此服務可保護 Oracle 、 MySQL 、 VM 資料存放區、內部部署 NAS 儲存設備上檔案共用的應用程式型工作負載、以及個別 BlueXP 帳戶上 Cloud Volumes ONTAP on AWS （使用 NFS 傳輸協定）、並將資料備份至 Amazon Web Services 雲端儲存設備。

BlueXP 勒索軟體保護服務可充分運用多項 NetApp 技術、讓您的資料安全管理員或安全營運工程師能夠達成下列目標：

- 一眼就能檢視所有工作負載的勒索軟體保護。
- 深入瞭解勒索軟體保護建議
- 根據 BlueXP 勒索軟體保護建議、改善保護狀態。
- 指派勒索軟體保護原則來保護您的主要工作負載和高風險資料、防範勒索軟體攻擊。
- 監控工作負載的健全狀況、防範尋找資料異常的勒索軟體攻擊。
- 快速評估勒索軟體事件對工作負載的影響。
- 透過還原資料並確保不會重新感染儲存的資料、以智慧方式從勒索軟體事件中恢復。

"瞭解 BlueXP 勒索軟體保護"。

開始使用

瞭解 BlueXP 勒索軟體保護預覽

勒索軟體攻擊可能會封鎖對您系統和資料的存取、攻擊者可能會要求勒索贖金、以換取資料的釋放或解密。根據 IDC 的調查、勒索軟體受害者經常遭受多種勒索軟體攻擊。攻擊可能會在一天到數週之間中斷資料存取。

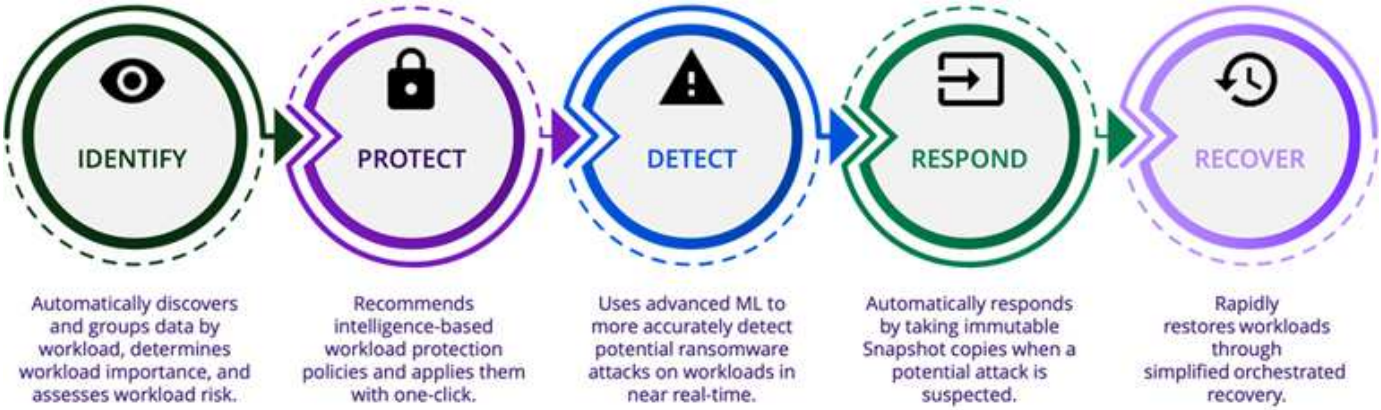
BlueXP 勒索軟體保護是一項協調服務、用於勒索軟體的保護、偵測及還原。對於預覽版本、此服務可保護 Oracle 、 MySQL 、 VM 資料存放區、 以及在內部部署 NAS 儲存設備上的檔案共用、以及在 Amazon Web Services （使用 NFS 傳輸協定）中跨 BlueXP 帳戶的 Cloud Volumes ONTAP 、並將資料備份至 Amazon Web Services 雲端儲存設備或 NetApp StorageGRID 。

> 本文件以技術預覽形式提供。 透過此預覽方案、 NetApp 保留在「一般供應」之前修改產品詳細資料、內容和時間表的權利。

BlueXP 勒索軟體保護的功能

BlueXP 勒索軟體保護服務可充分運用多項 NetApp 技術、讓您的儲存管理員、資料安全管理員或安全作業工程師能夠達成下列目標：

- * 識別 * 在 BlueXP 中、 BlueXP 帳戶、工作區和 BlueXP Connectors 中、透過 NFS 工作環境、在 NetApp 內部部署 NAS 中的所有應用程式型、檔案共用或 VMware 管理的工作負載。接著服務會將資料優先順序分類、並針對勒索軟體保護改善提供建議。
- * 在您的資料上啟用備份與 Snapshot 複本、以保護 * 您的工作負載。
- * 偵測 * 可能是勒索軟體攻擊的異常。
- * 自動啟動 NetApp ONTAP Snapshot 複本、以回應 * 可能的勒索軟體攻擊。
- * 恢復 * 您的工作負載可協調多項 NetApp 技術、協助加速工作負載正常運作時間。您可以選擇恢復磁碟區、資料夾或特定檔案。本服務針對最佳選項提供建議。



使用 **BlueXP** 勒索軟體保護的好處

BlueXP 勒索軟體保護提供下列優點：

- 探索工作負載和資料集、根據使用率指數分析優先順序、並將其相對重要性排名。
- 評估您的勒索軟體保護狀態、並將其顯示在易於理解的儀表板中。
- 根據探索和保護狀態分析、提供後續步驟的建議。
- 只需按一下滑鼠即可套用 AI / ML 導向的資料保護建議。
- 保護主要應用程式型工作負載中的資料、例如 MySQL 、 Oracle 、 VMware 資料存放區和檔案共用。
- 使用 AI 技術、在主要儲存設備上即時偵測勒索軟體對資料的攻擊。
- 建立 Snapshot 複本、並針對異常活動發出警示、以針對偵測到的潛在攻擊啟動自動化動作。
- 套用精心規劃的恢復、以符合 RPO 原則。BlueXP 勒索軟體保護利用多項 NetApp 恢復服務（包括 BlueXP 備份與還原（前身為雲端備份））來協調從勒索軟體事件中恢復的工作。

成本

使用 BlueXP 勒索軟體保護的預覽版本、 NetApp 不會向您收取費用。

授權

BlueXP 勒索軟體保護預覽本身不需要任何特殊授權。 所有預覽授權均為評估授權。

> 對於預覽版本、 NetApp 可協助您設定試用版和任何必要的授權。

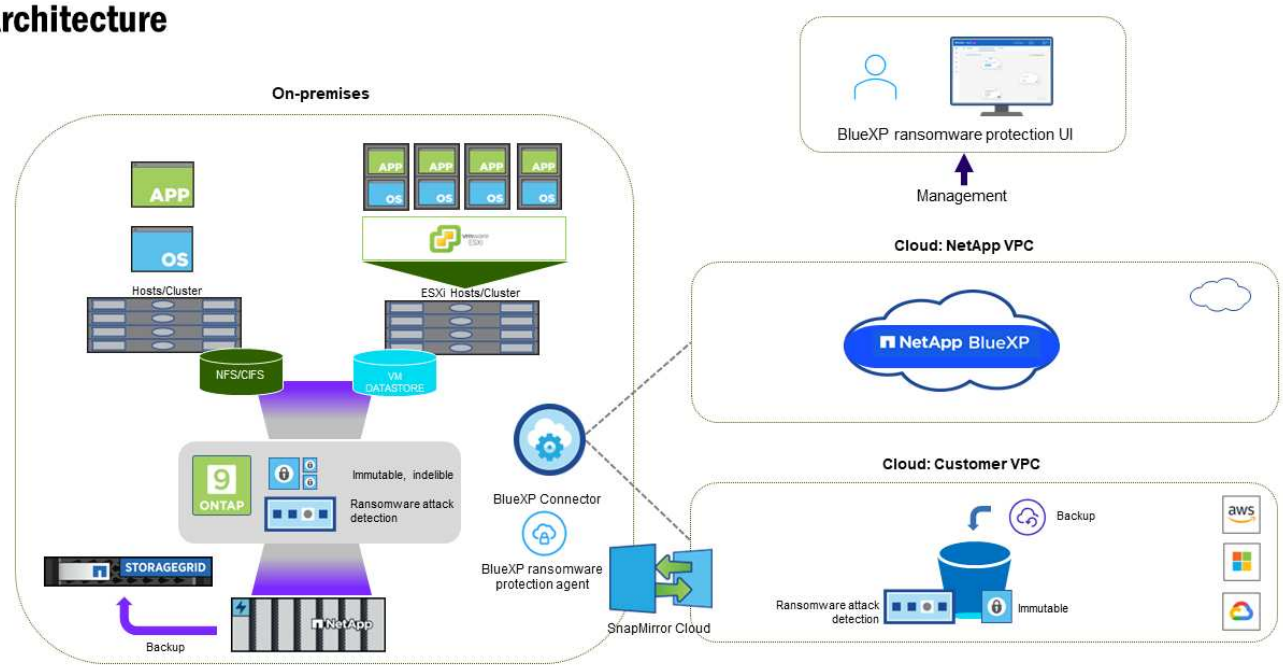
BlueXP 勒索軟體保護預覽需要下列授權：

- ONTAP
- NetApp 自主勒索軟體保護技術。請參閱 "自主勒索軟體保護總覽" 以取得詳細資料。
- BlueXP 備份與還原服務

BlueXP 勒索軟體保護的運作方式

在高階的 BlueXP 勒索軟體保護之下、其運作方式就像這樣。

Architecture



功能	說明
* 識別 *	• 尋找所有連線至 BlueXP 的客戶內部部署 NAS （ NFS 裝載）資料。 • 識別來自 ONTAP 服務 API 的客戶資料、並將其與工作負載相關聯。深入瞭解 "ONTAP" 和 "軟件SnapCenter"。 • 探索每個磁碟區目前的 NetApp Snapshot 複本和備份原則保護層級、以及任何隨裝即用的偵測功能。然後、該服務會使用 BlueXP 備份與還原、 BlueXP 數位顧問、 ONTAP 服務和 NetApp 技術（例如自主勒索軟體保護、 FPolicy 、備份原則和 Snapshot 原則）、將這種保護狀態與工作負載建立關聯。 深入瞭解 "自主勒索軟體保護" 和 "BlueXP 備份與還原"、 "BlueXP 數位顧問"和 "ONTAP FPolicy"。 • 根據自動探索到的保護層級、為每個工作負載指派業務優先順序、並根據工作負載的業務優先順序、建議保護原則。 • 勒索軟體保護也會學習原則關聯、並建議您針對類似的工作負載使用自訂原則。
* 保護 *	• 透過將原則套用至每個已識別的工作負載、主動監控工作負載、並協調 BlueXP 備份與還原及 ONTAP API 的使用。
* 偵測 *	• 利用整合式機器學習（ ML ）模式偵測潛在的攻擊、以偵測可能異常的加密和活動。 • 提供雙層偵測功能、從偵測主要儲存設備中可能發生的勒索軟體攻擊開始、並透過額外的自動 Snapshot 複本來建立最近的資料還原點來回應異常活動。這項服務可讓您更深入探索、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 、自主勒索軟體保護和 FPolicy 技術、判斷攻擊相關工作負載的特定可疑檔案和地圖。

功能	說明
* 回應 *	• 顯示相關資料、例如檔案活動、使用者活動和 Entropy 、以協助您完成攻擊的鑑識審查。 • 使用 NetApp 技術和產品（例如 ONTAP 、自主勒索軟體保護和 FPolicy ）來啟動快速 Snapshot 複本。
* 恢復 *	• 決定最佳的 Snapshot 或備份、並使用 BlueXP 備份與還原、 ONTAP 、自主勒索軟體保護及 FPolicy 技術與服務、建議最佳的實際還原點（ RPA ）。 • 協調工作負載的恢復、包括 VM 、檔案共用和資料庫、並確保應用程式一致性。

支援的備份目標、工作環境和資料來源

使用 BlueXP 勒索軟體保護預覽、瞭解您的資料對於下列類型的備份目標、工作環境和資料來源的網路攻擊有何彈性：

- 支援的備份目標 *
- Amazon Web Services （ AWS ） S3
- NetApp StorageGRID
- 支援的工作環境 *
- 內部部署 ONTAP NAS （使用 NFS 傳輸協定）
- ONTAP Select
- AWS 中的 Cloud Volumes ONTAP （使用 NFS 傳輸協定）
- 資料來源 *

對於預覽版本、此服務可保護下列應用程式型工作負載：

- NetApp 檔案共用
- VMware資料存放區
- 資料庫（適用於預覽版本、 Oracle 和 MySQL ）

有助於您保護勒索軟體的術語

瞭解與勒索軟體保護相關的一些術語、可能會讓您獲益良多。

- * 保護 * ： BlueXP 勒索軟體保護的保護、意味著使用保護原則、確保 Snapshot 和不可變備份定期發生在不同的安全網域。
- * 工作負載 * ： BlueXP 勒索軟體保護預覽中的工作負載可包括 MySQL 或 Oracle 資料庫、 VMware 資料存放區或檔案共用區。

BlueXP 勒索軟體保護先決條件

開始使用 BlueXP 勒索軟體保護、驗證您的作業環境、登入、網路存取和網頁瀏覽器是否

準備就緒。

若要使用 BlueXP 勒索軟體保護預覽版本、您需要具備下列先決條件：

- NetApp StorageGRID 或 AWS S3 中用於備份目標和存取權限集的帳戶

  請參閱 "AWS 權限清單" 以取得詳細資料。

- 更新版本ONTAP
  - 叢集管理 ONTAP 權限
  - NetApp 自主勒索軟體保護授權、由 BlueXP 勒索軟體保護所使用、可在內部部署 ONTAP 執行個體上啟用、視您使用的 ONTAP 版本而定。請參閱 "自主勒索軟體保護總覽"。

    如需更多授權詳細資料、請參閱 "瞭解 BlueXP 勒索軟體保護"。

- 在 BlueXP 中：
  - BlueXP 必須在 BlueXP 中設定每個虛擬私有雲（ VPC ）或內部部署區域的 BlueXP Connector 。請參閱 "設定 Connector 的 BlueXP 文件"。

    > ⓘ 如果您有多個 BlueXP Connectors 、服務將會掃描 BlueXP UI 目前所顯示以外的所有 Connectors 資料。

  - 在工作環境中啟用備份的 BlueXP 備份與還原服務
  - 採用 NetApp NAS 內部部署儲存設備的 BlueXP 工作環境
  - BlueXP 帳戶、至少有一個作用中的 Connector 連線至內部部署 ONTAP 叢集。所有來源和工作環境都必須位於相同的 BlueXP 帳戶。
  - 具備帳戶管理權限的 BlueXP 使用者帳戶、可用於探索資源
  - "標準 BlueXP 需求"

BlueXP 勒索軟體保護快速入門

以下概述開始使用 BlueXP 勒索軟體保護所需的步驟。每個步驟中的連結都會帶您前往提供更多詳細資料的頁面。

1 檢閱先決條件

"確保您的環境符合這些要求"。

2 設定勒索軟體保護服務

- "準備 NetApp StorageGRID 或 Amazon Web Services 作為備份目的地"。
- "在 BlueXP 中設定 Connector"。
- "設定備份目的地"。
- "探索 BlueXP 中的工作負載"。

3 接下來呢？

設定服務之後、接下來您可以做些什麼。

- "在儀表板上檢視工作負載保護健全狀況"。
- "保護工作負載"。
- "回應偵測可能的勒索軟體攻擊"。
- "從攻擊中恢復（在事件被消除之後）"。

設定 BlueXP 勒索軟體保護

若要使用 BlueXP 勒索軟體保護、請執行幾個步驟來設定。

開始之前、請先檢閱 "先決條件" 確保您的環境已準備就緒。

準備備份目的地

準備下列其中一個備份目的地：

- NetApp StorageGRID
- Amazon Web Services

在備份目的地本身設定選項之後、您稍後會在 BlueXP 勒索軟體保護服務中將其設定為備份目的地。

準備 **StorageGRID** 成為備份目的地

如果您想要使用 StorageGRID 做為備份目的地、請參閱 "本文檔StorageGRID" 如需 StorageGRID 的詳細資訊、

準備 **AWS** 成為備份目的地

- 在 AWS 中設定帳戶。
- 設定 "AWS權限" 在 AWS 中。

如需在 BlueXP 中管理 AWS 儲存設備的詳細資訊、請參閱 "管理您的Amazon S3儲存庫"。

設定 **BlueXP**

下一步是設定 BlueXP 和 BlueXP 勒索軟體保護服務。

檢閱 "標準 BlueXP 需求"。

在 **BlueXP** 中建立 **Connector**

您應該聯絡 NetApp 銷售代表、試用這項服務。然後、當您使用 BlueXP Connector 時、它會包含勒索軟體保護服務的適當功能。

若要在使用此服務之前在 BlueXP 中建立 Connector 、請參閱說明的 BlueXP 文件 "如何建立 BlueXP Connector"。

> 如果您有多個 BlueXP Connectors 、服務將會掃描 BlueXP UI 目前所顯示以外的所有 Connectors 資料。此服務會探索與此帳戶相關的所有工作區和所有 Connector 。

存取 **BlueXP** 勒索軟體保護

您可以使用 NetApp BlueXP 登入 BlueXP 勒索軟體保護服務。從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。

如需詳細資訊、請參閱 "存取 BlueXP 勒索軟體保護"。

在 **BlueXP** 勒索軟體保護中設定備份目的地

使用 BlueXP 勒索軟體保護備份目的地選項來設定備份目的地。如需詳細資訊、請參閱 "設定設定選項"。

存取 BlueXP 勒索軟體保護

您可以使用 NetApp BlueXP 登入 BlueXP 勒索軟體保護服務。

若要登入BlueXP、您可以使用NetApp 支援網站 您的不實證資料、也可以使用電子郵件和密碼註冊NetApp雲端登入。 "深入瞭解登入"。

步驟

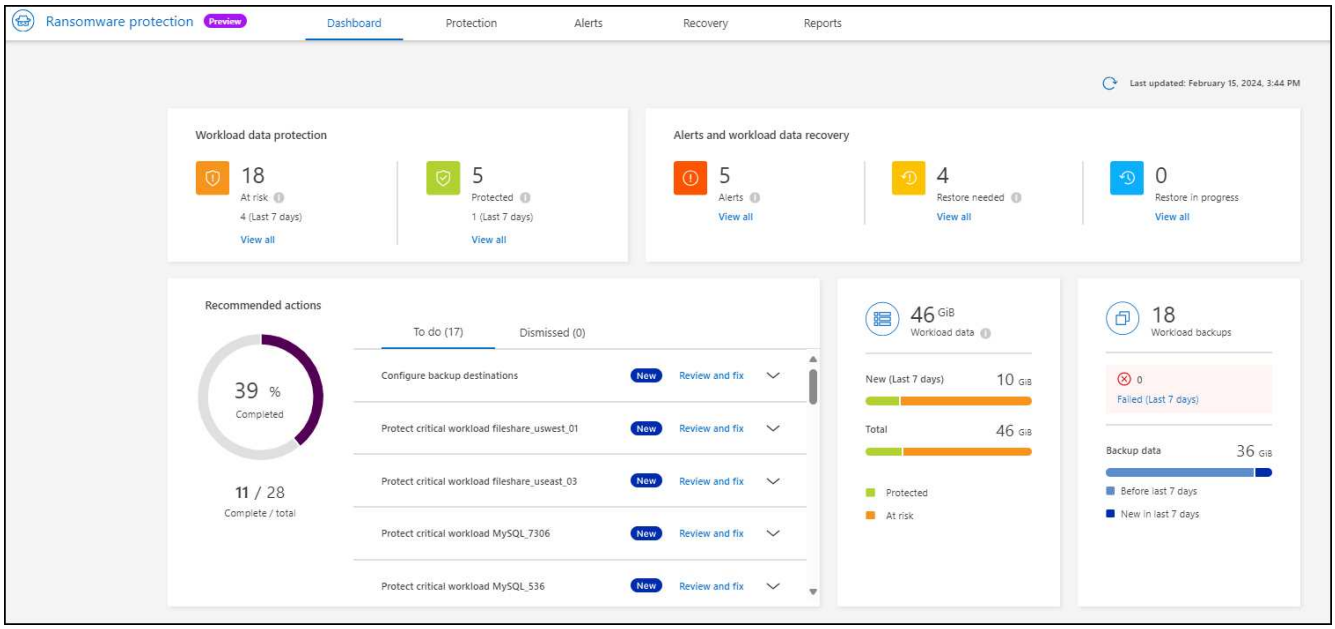
1. 開啟網頁瀏覽器、前往 "BlueXP主控台"。

   出現 NetApp BlueXP 登入頁面。

2. 登入 BlueXP 。
3. 從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。

   如果這是您第一次登入此服務、就會出現登陸頁面。

   否則、 BlueXP 勒索軟體保護儀表板就會出現。



4. 開始使用服務。
   - 如果您沒有 BlueXP Connector 、或不是此預覽的接頭、您可能需要聯絡 NetApp 支援或追蹤訊息、以註冊此預覽。
   - 如果您是 BlueXP 的新手、而且尚未使用任何 Connector 、當您選取「 * 勒索軟體保護 * 」時、會出現一則關於註冊的訊息。請繼續提交表單。NetApp 將會與您聯絡、告知您有關評估申請的資訊。
   - 如果您是具有現有 Connector 的 BlueXP 使用者、當您選取「 * 勒索軟體保護 * 」時、會出現一則關於註冊的訊息。
   - 如果您已經參與預覽、當您選取「 * 勒索軟體保護 * 」時、就可以繼續進行服務。如果您尚未選擇 * 探索工作負載 * 選項、請選擇此選項。

探索 BlueXP 勒索軟體保護的工作負載

若要使用 BlueXP 勒索軟體保護、服務必須先探索資料。在探索期間、 BlueXP 勒索軟體保護會分析所有 BlueXP Connector 和帳戶內工作空間中的所有工作環境中的所有磁碟區和檔案。

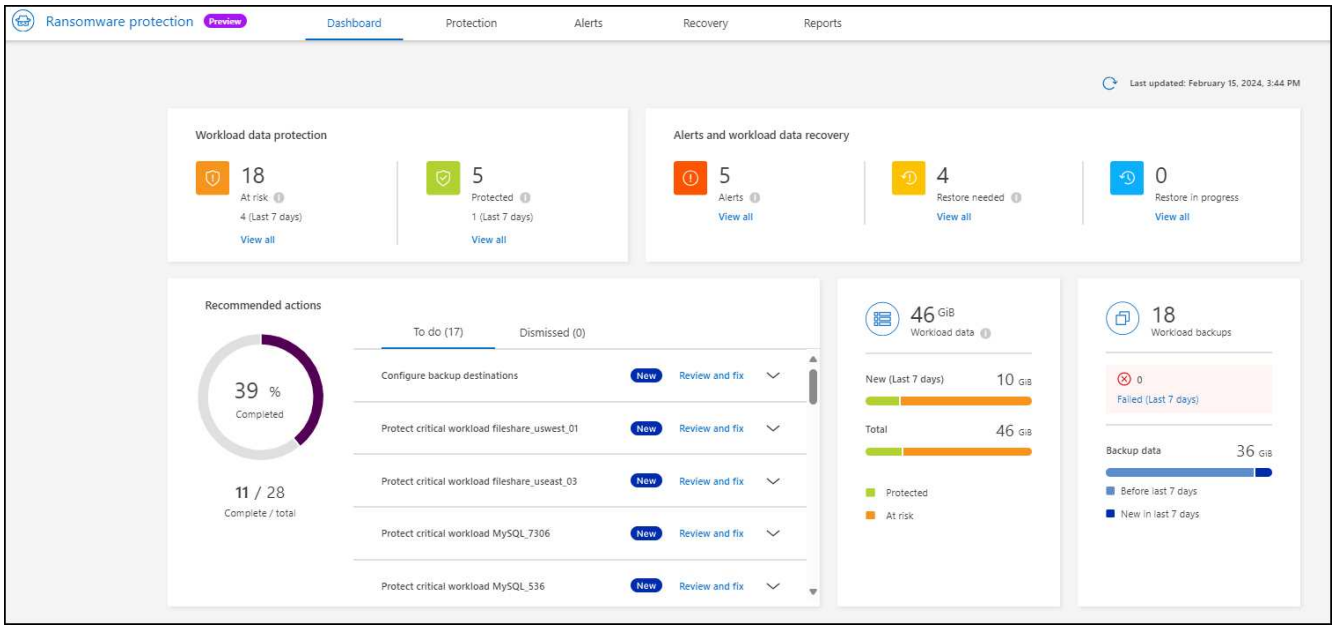
> 對於預覽版本、 BlueXP 勒索軟體保護會評估 MySQL 應用程式、 Oracle 應用程式、 VMware 資料存放區和檔案共用。

此服務會評估現有的保護層級、包括目前的備份保護、 Snapshot 複本和 NetApp 自主勒索軟體保護選項。根據評估結果、服務接著會建議如何改善勒索軟體的保護。

步驟

1. 從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。
2. 從初始登錄頁面中選擇 * 探索工作負載 * 。

   服務會探索工作負載資料、並在儀表板中顯示資料保護的健全狀況。



設定 BlueXP 勒索軟體保護設定

您可以檢閱儀表板上的建議、來設定備份目的地。

新增備份目的地

BlueXP 勒索軟體保護可識別尚未備份的工作負載、也可識別尚未指派任何備份目的地的工作負載。

若要保護這些工作負載、您應該新增備份目的地。您可以選擇下列其中一個備份目的地：

- NetApp StorageGRID
- Amazon Web Services（AWS）

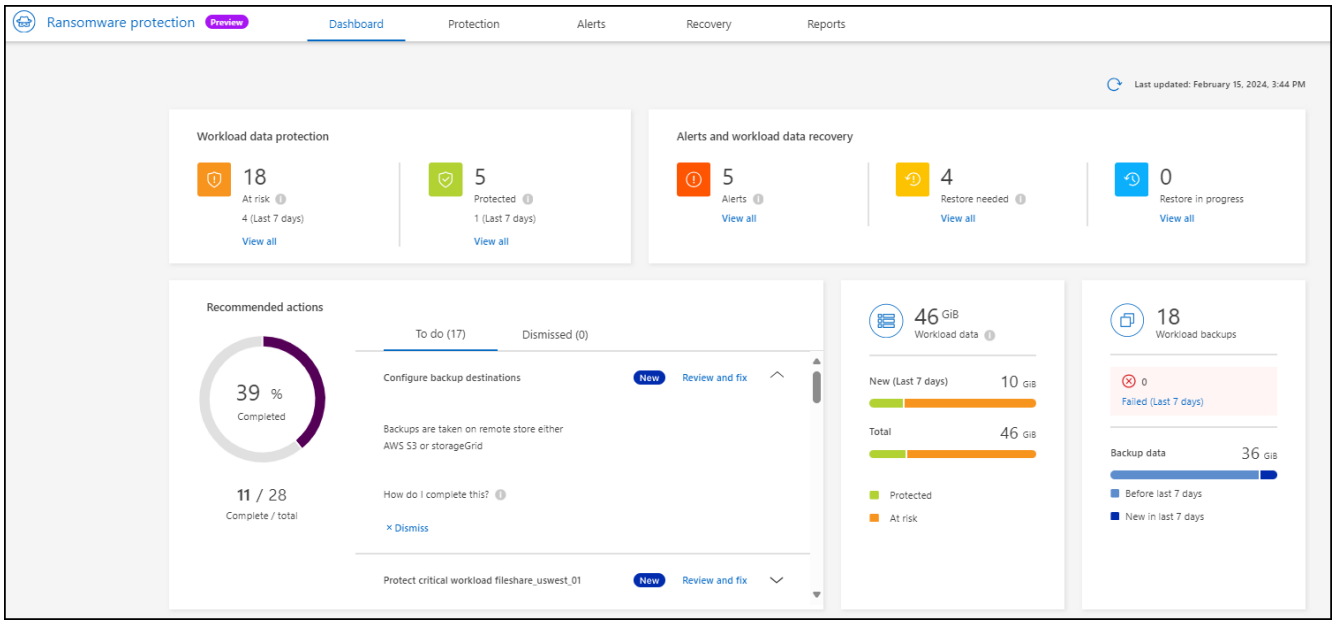
您可以根據儀表板的建議動作來新增備份目的地。

從儀表板的建議動作存取備份目的地選項

儀表板提供許多建議。其中一項建議可能是設定備份目的地。

步驟

1. 從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。
2. 檢閱儀表板的建議動作窗格。

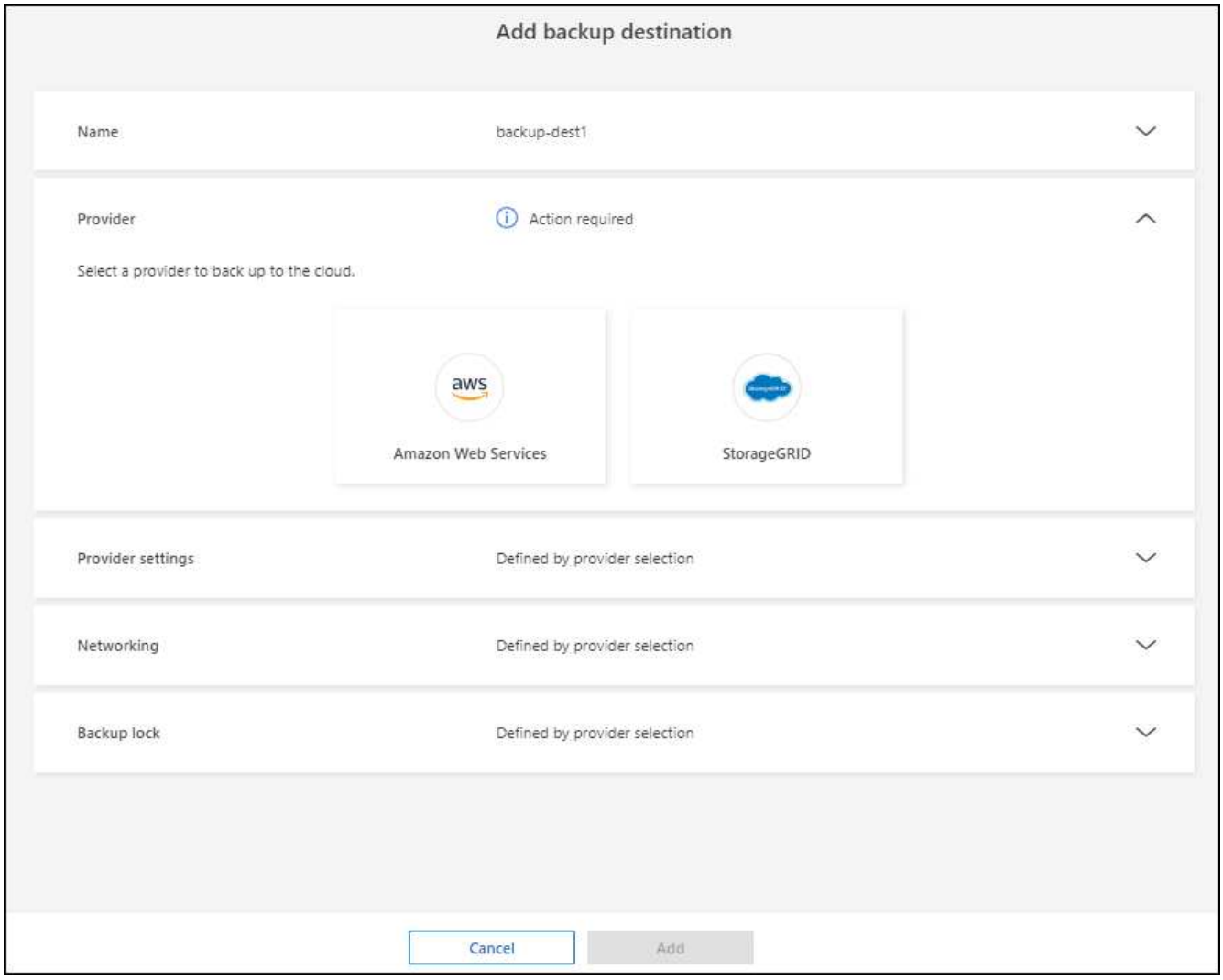


3. 在儀表板中、針對「設定備份目的地」的建議、選取 * 檢閱和修正 * 。
4. 根據備份供應商的不同、繼續執行相關指示。

將 StorageGRID 新增為備份目的地

若要將 NetApp StorageGRID 設定為備份目的地、請輸入下列資訊。

1. 在 * 設定 > 備份目的地 * 頁面中、選取 * 新增 * 。
2. 輸入備份目的地的名稱。



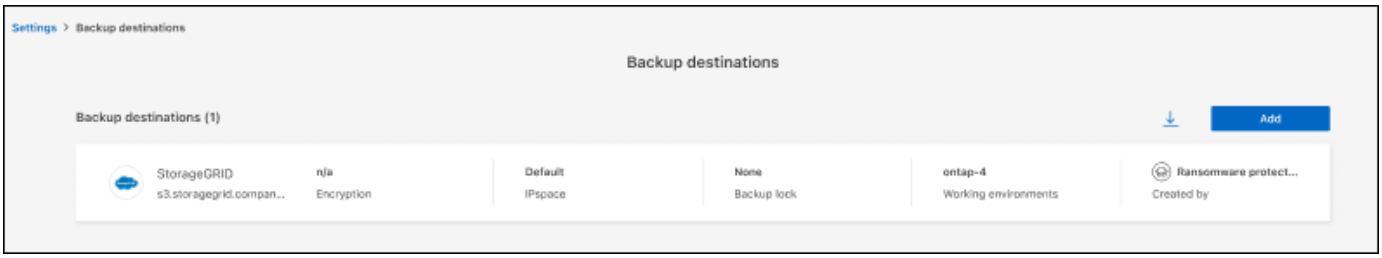
3. 選擇* StorageGRID 《》《*》。
4. 選取每個設定旁邊的向下箭頭、然後輸入或選取值：
   - * 供應商設定 * ：
     - 建立新的儲存庫或自帶儲存備份的儲存庫。
     - StorageGRID 閘道節點完整網域名稱、連接埠、 StorageGRID 存取金鑰和秘密金鑰認證。
   - * 網路 * ：選擇 IPspace 。
     - IPspace 是您要備份的磁碟區所在的叢集。此IPspace的叢集間生命體必須具有傳出網際網路存取。
   - * 備份鎖定 * ：選擇是否要讓服務保護備份不被修改或刪除。此選項使用 NetApp DataLock 技術。每個備份都會在保留期間內鎖定、或至少 30 天、再加上最多 14 天的緩衝期間。

     如果您現在設定備份鎖定設定、則無法在設定備份目的地之後再變更設定。

     - * 法規遵循模式 * ：使用者無法在保留期間覆寫或刪除受保護的備份檔案。
5. 選取*「Add*」。

結果

新的備份目的地會新增至備份目的地清單。

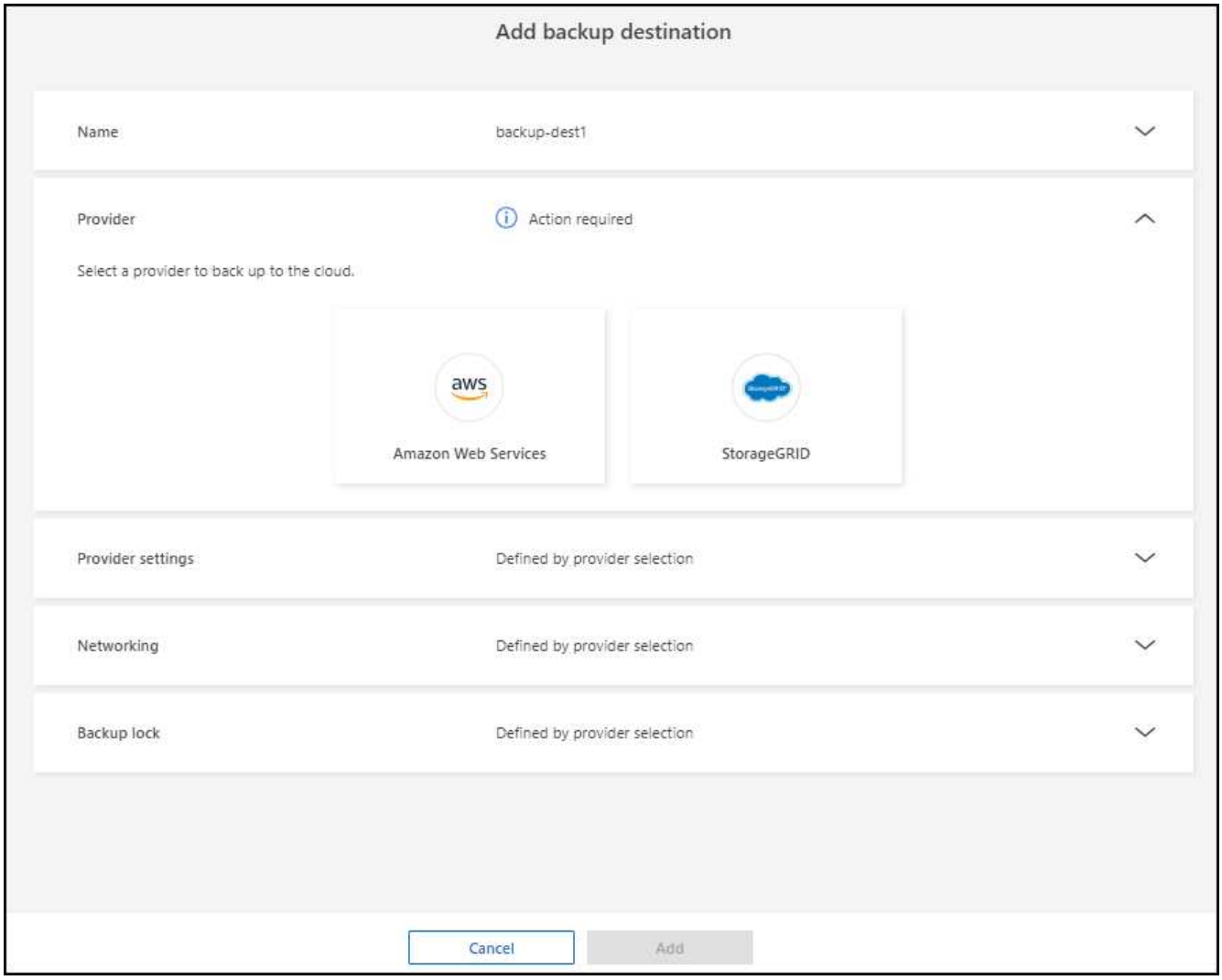


將 Amazon Web Services 新增為備份目的地

若要將 AWS 設定為備份目的地、請輸入下列資訊。

如需在 BlueXP 中管理 AWS 儲存設備的詳細資訊、請參閱 "管理您的Amazon S3儲存庫"。

1. 在 * 設定 > 備份目的地 * 頁面中、選取 * 新增 * 。
2. 輸入備份目的地的名稱。



3. 選擇* Amazon Web Services*。
4. 選取每個設定旁邊的向下箭頭、然後輸入或選取值：

- * 供應商設定 * ：
  - 建立新的儲存庫、如果 BlueXP 中已有現有儲存庫、請選取現有的儲存庫、或是自帶儲存備份的儲存庫。
  - AWS 帳戶、區域、存取金鑰和 AWS 認證的秘密金鑰

    "如果您想要自行攜帶貯體、請參閱新增 S3 貯體"。

- * 加密 * ：如果您要建立新的 S3 儲存區、請輸入供應商提供給您的加密金鑰資訊。如果您選擇現有的儲存區、則加密資訊已可供使用。

  根據預設、儲存區中的資料會使用 AWS 管理的金鑰進行加密。您可以繼續使用 AWS 管理的金鑰、或是使用自己的金鑰來管理資料加密。

- * 網路連線 * ：選擇 IPspace 、以及是否要使用私有端點。
  - IPspace 是您要備份的磁碟區所在的叢集。此IPspace的叢集間生命體必須具有傳出網際網路存取。
  - 您也可以選擇是否要使用先前設定的 AWS 私有端點（ Private Link ）。

    如果您想要使用 AWS Private Link 、請參閱 "適用於 Amazon S3 的 AWS Private Link"。

- * 備份鎖定 * ：選擇是否要讓服務保護備份不被修改或刪除。此選項使用 NetApp DataLock 技術。每個備份都會在保留期間內鎖定、或至少 30 天、再加上最多 14 天的緩衝期間。

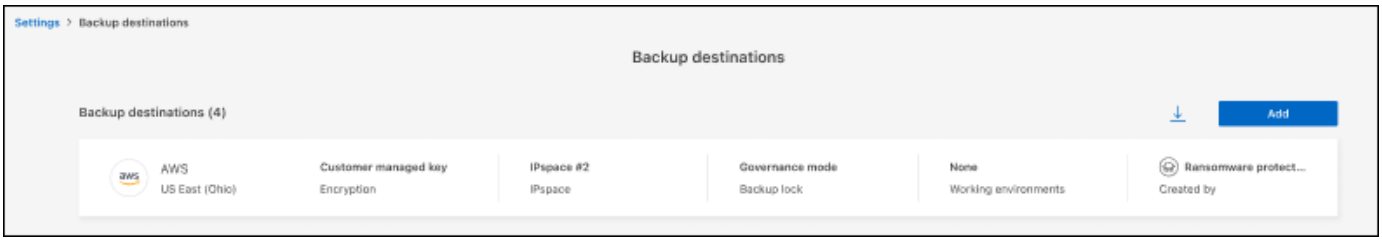
  ! 如果您現在設定備份鎖定設定、則無法在設定備份目的地之後再變更設定。

  - * 監管模式 * ：特定使用者（具有 S3 ： BypassGovernanceRetention 權限）可在保留期間覆寫或刪除受保護的檔案。
  - * 法規遵循模式 * ：使用者無法在保留期間覆寫或刪除受保護的備份檔案。

5. 選取*「Add*」。

結果

新的備份目的地會新增至備份目的地清單。



BlueXP 勒索軟體保護常見問題集

如果您只是想要快速回答問題、這個常見問題集就能幫上忙。

存取

- 什麼是 BlueXP 勒索軟體保護 URL ？ *
  對於 URL 、請在瀏覽器中輸入： "https://console.bluexp.netapp.com/" 存取 BlueXP 主控台。

- 您是否需要授權才能使用 BlueXP 勒索軟體保護？ *
  不需要 NetApp 授權檔案（NLF）。BlueXP 勒索軟體保護預覽本身不需要任何特殊授權。 所有預覽授權均為評估授權。

此服務的預覽版本需要 BlueXP 備份與還原服務授權。

> 對於預覽版本、 NetApp 可協助您設定試用版和任何必要的授權。

- 如何啟用 BlueXP 勒索軟體保護？ *
  BlueXP 勒索軟體保護不需要任何啟用。BlueXP 左側導覽會自動啟用勒索軟體保護選項。

如需預覽版本、您必須註冊或聯絡 NetApp 銷售代表、才能試用這項服務。然後、當您使用 BlueXP Connector 時、它會包含該服務的適當功能。

- BlueXP 勒索軟體保護是否適用於標準、受限和私有模式？ **
  目前、 BlueXP 勒索軟體保護僅適用於標準模式。敬請期待更多資訊。

如需所有 BlueXP 服務中這些模式的說明、請參閱 "BlueXP 部署模式"。

- 如何處理存取權限？ **
  只有帳戶管理員才能啟動服務並探索工作負載（因為這涉及使用資源）。後續互動可由任何角色執行。
- 哪種裝置解析度最佳？ **
  BlueXP 勒索軟體保護的建議裝置解析度為 1920x1080 或更高。
- 我應該使用哪個瀏覽器？ **
  任何現代化的瀏覽器都能正常運作。

與其他服務互動

- BlueXP 勒索軟體保護是否能感知 NetApp ONTAP 中的保護設定？ *
  是的、 BlueXP 勒索軟體保護會探索 ONTAP 中設定的 Snapshot 排程。
- 如果您使用 BlueXP 勒索軟體保護設定原則、您是否必須在未來僅在此服務中進行變更？ *
  我們建議您從 BlueXP 勒索軟體保護服務進行原則變更。

工作負載

- 工作負載的組成是什麼？ **
  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、部署在 ora3.host.com 上的 Oracle DB 執行個體、其資料和記錄可分別具有 vol1 和 vol2 。這些磁碟區一起構成 Oracle DB 執行個體的特定執行個體工作負載。
  - BlueXP 勒索軟體保護如何優先處理工作負載資料？ *
    預覽版本的資料優先順序取決於所製作的 Snapshot 複本和排程的備份。

工作負載優先順序由下列 Snapshot 頻率決定：

- * 關鍵 * ：每小時拍攝不到 1 份快照複本（極具挑戰性的保護排程）
- * 重要 * ：每天拍攝的快照複本少於 1 份、但每小時超過 1 份
- * 標準 * ：每天拍攝超過 1 份快照複本
  - 新增的 Volume 、但尚未顯示 **

如果您在環境中新增了新的磁碟區、請重新啟動探索、並套用保護原則來保護該新磁碟區。

- 儀表板不會顯示我所有的工作負載。可能出了什麼問題？ **
  目前僅支援 NFS 磁碟區。iSCSI 磁碟區、 CIFS 磁碟區和其他不受支援的組態會被篩選出來、不會出現在儀表板上。

保護原則

- BlueXP 勒索軟體原則是否與其他類型的工作負載原則共存？ *
  目前、 BlueXP 備份與還原（ Cloud Backup ）支援每個磁碟區一個備份原則。因此、 BlueXP 備份與還原以及 BlueXP 勒索軟體保護功能會共用備份原則。

Snapshot 複本不受限制、可與每項服務分開新增。

使用 BlueXP 勒索軟體保護

使用 BlueXP 勒索軟體保護

使用 BlueXP 勒索軟體保護、您可以檢視工作負載健全狀況並保護工作負載。

- "探索 BlueXP 勒索軟體保護的工作負載"。
- "從儀表板檢視保護和工作負載健全狀況"。
  - 審查勒索軟體保護建議並採取行動。
- "保護工作負載"：
  - 將勒索軟體保護原則指派給工作負載。
  - 加強應用程式保護、以防止未來的勒索軟體攻擊。
  - 建立、變更或刪除保護原則。
- "回應偵測可能的勒索軟體攻擊"。
- "從攻擊中恢復" （事件被消除之後）。
- "設定保護設定"。

使用儀表板一覽工作負載健全狀況

BlueXP 勒索軟體保護儀表板提供工作負載保護健全狀況的概覽資訊。您可以快速判斷面臨風險或受到保護的工作負載、識別受事件或恢復影響的工作負載、並查看有多少儲存設備受到保護或面臨風險、以評估保護程度。

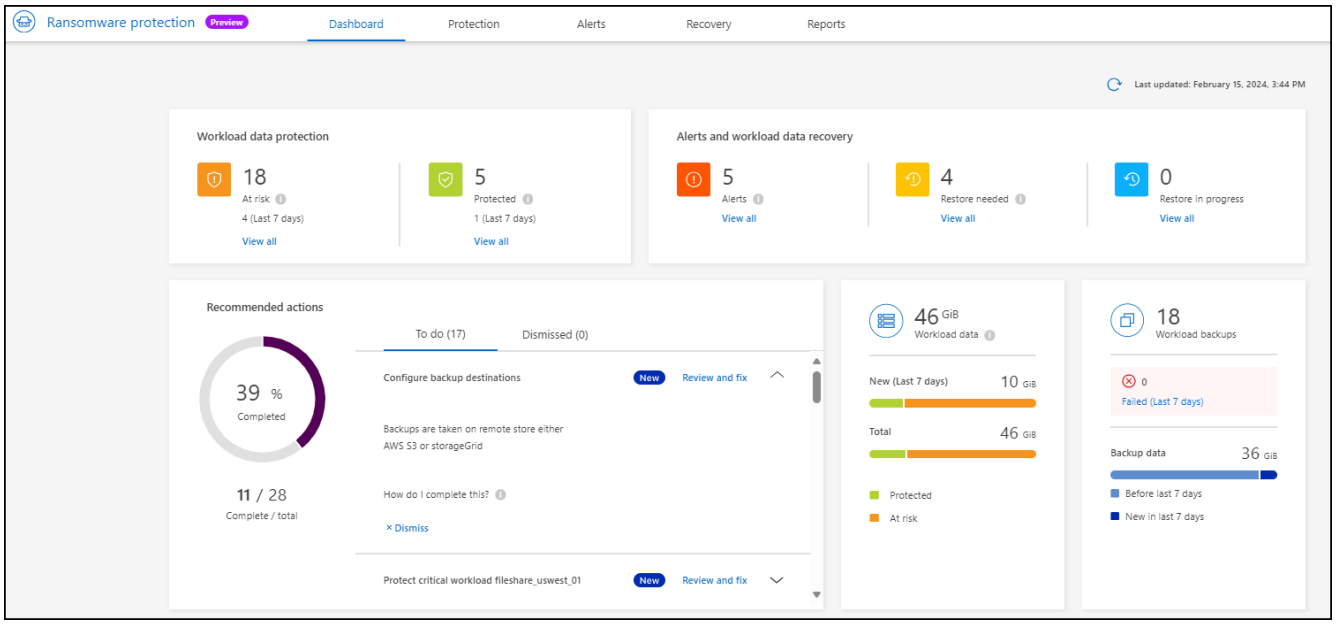
您也可以使用儀表板來檢閱及處理保護建議。

使用儀表板檢視工作負載健全狀況

步驟

1. 從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。

   探索之後、儀表板會顯示工作負載資料保護的健全狀況。



2. 在儀表板中、您可以在每個窗格中檢視及執行下列任何一項：

   - * 工作負載資料保護 * ：按一下 * 「檢視全部 * 」、即可在「保護」頁面上查看所有處於風險或受到保護的工作負載。當保護層級與保護原則不符時、工作負載就會面臨風險。請參閱 "保護工作負載"。
   - * 警示與工作負載資料恢復 * ：按一下 * 檢視全部 * 、即可查看影響工作負載的作用中事件、在事件失效或正在恢復後、準備好進行恢復。請參閱 "回應偵測到的警示"。

     事件分為下列其中一種狀態：

     - 受影響（顯示於警示頁面）
     - 準備好恢復（顯示在「恢復」頁面上）
     - 恢復（顯示在恢復頁面）
     - 恢復失敗（顯示在恢復頁面上）
     - 已恢復（顯示在「恢復」頁面）
   - * 建議行動 * ：若要加強保護、請檢閱每項建議、然後按一下 * 審查與修正 * 。

     請參閱 "檢閱儀表板上的保護建議" 或 "保護工作負載"。

     自您上次造訪儀表板後新增的任何建議、都會以「新增」表示至少 24 小時。行動會以優先順序列出、最重要的是在最頂端。您可以檢視並處理每個項目、或是將其關閉。

   行動總數不包括已駁回的行動。

   - * 工作負載資料 * ：監控過去 7 天的保護涵蓋範圍變更。
   - * 工作負載備份 * ：監控過去 7 天內服務失敗或成功完成的工作負載備份變更。

檢閱儀表板上的保護建議

BlueXP 勒索軟體保護可評估工作負載的保護、並建議採取行動來改善保護。

您可以檢閱建議並採取行動、將建議狀態變更為「完成」。或者、如果您想稍後再處理、您可以將其關閉。取消某項行動會將建議移至已駁回的行動清單、您可以稍後再加以審查。

以下是服務所提供建議的範例。

建議	說明	如何解決
新增勒索軟體保護原則	工作負載目前未受到保護。	指派原則給工作負載。 請參閱 "保護工作負載免受勒索軟體攻擊"。
設定備份目的地	工作負載目前沒有任何備份目的地。	將備份目的地新增至此工作負載以保護它。 請參閱 "設定保護設定"。
強化原則。	某些工作負載可能沒有足夠的保護。透過原則強化工作負載的保護。	增加保留、新增備份、強制執行不可變備份、封鎖可疑的副檔名、在次要儲存設備上啟用偵測等功能。 請參閱 "保護工作負載免受勒索軟體攻擊"。
保護關鍵或重要的應用程式工作負載、防範勒索軟體。	「保護」頁面會顯示不受保護的關鍵或重要（根據指派的優先順序層級）應用程式工作負載。	指派原則給這些工作負載。 請參閱 "保護工作負載免受勒索軟體攻擊"。
保護重要或重要的檔案共享工作負載、防範勒索軟體。	「保護」頁面會顯示檔案共用或資料存放區類型的關鍵或重要工作負載、這些工作負載並未受到保護。	為每個工作負載指派原則。 請參閱 "保護工作負載免受勒索軟體攻擊"。
檢閱新警示	存在新警示。	檢閱新警示。 請參閱 "回應偵測到的勒索軟體警示"。

步驟

1. 從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。
2. 從「建議的動作」窗格中、選取建議、然後選取 * 檢閱和修正 * 。
3. 若要在稍後關閉此動作、請選取 * 關閉 * 。

   建議會從「待辦事項」清單中清除、並顯示在「已解僱」清單中。

   您稍後可以將已解除的項目變更為待辦事項項目。當您將項目標記為已完成、或將已解除項目變更為待辦事項時、「總」動作會增加 1 。

4. 若要檢閱如何根據建議採取行動的資訊、請選取 * 資訊 * 圖示。

保護工作負載免受勒索軟體攻擊

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。

- 檢視現有的工作負載保護。
- 將原則指派給工作負載。

    - 提高應用程式保護能力、以防止未來的 RW 攻擊。
    - 變更先前在 RW 服務中受到保護的工作負載保護。
- 管理原則（僅限您建立的原則）。

BlueXP 勒索軟體保護會在探索期間為每個工作負載指派優先順序。工作負載優先順序由下列 Snapshot 頻率決定：

- * 關鍵 * ：每小時拍攝不到 1 份快照複本（極具挑戰性的保護排程）
- * 重要 * ：每天拍攝的快照複本少於 1 份、但每小時超過 1 份
- * 標準 * ：每天拍攝超過 1 份快照複本
- 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。
- * 風險 * ：不套用任何原則。
- * 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。
- 保護健全狀況 * ：工作負載可具有下列其中一種保護健全狀況狀態：
- * 健全 * ：工作負載已啟用保護、備份與 Snapshot 複本已完成。
- * 進行中 * ：正在進行備份或 Snapshot 複本。
- * 失敗 * ：備份或 Snapshot 複本尚未成功完成。
- **N/A** ：工作負載的保護功能未啟用或不足。

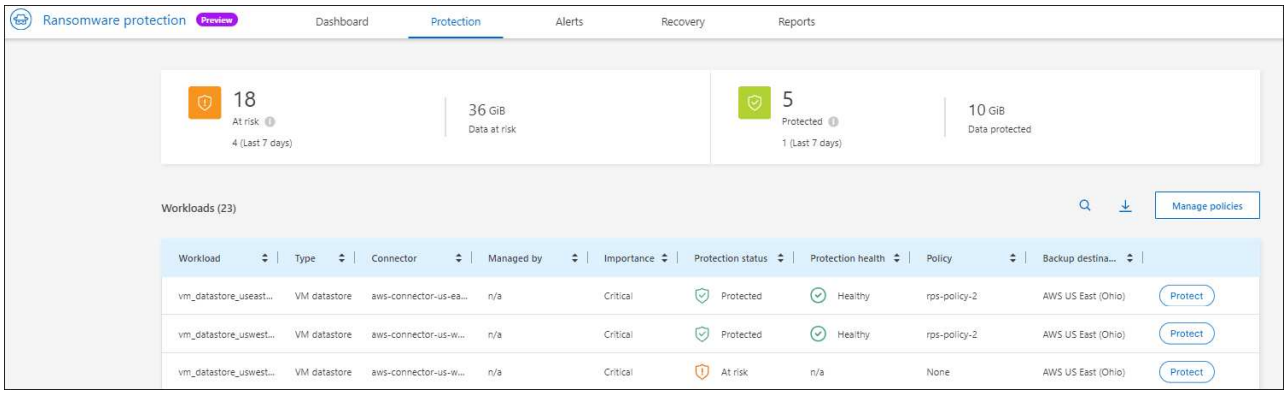
檢視工作負載勒索軟體保護

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：

- 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：
    - 從儀表板資料保護窗格中、選取 * 檢視全部 * 。
    - 從功能表中選取 * 保護 * 。



3. 在此頁面中、您可以將原則指派給工作負載。

將預先定義的保護原則指派給工作負載

為了協助保護資料、您可以將現有的勒索軟體保護原則指派給一或多個工作負載。您也可以將不同的原則指派給已有原則的工作負載。

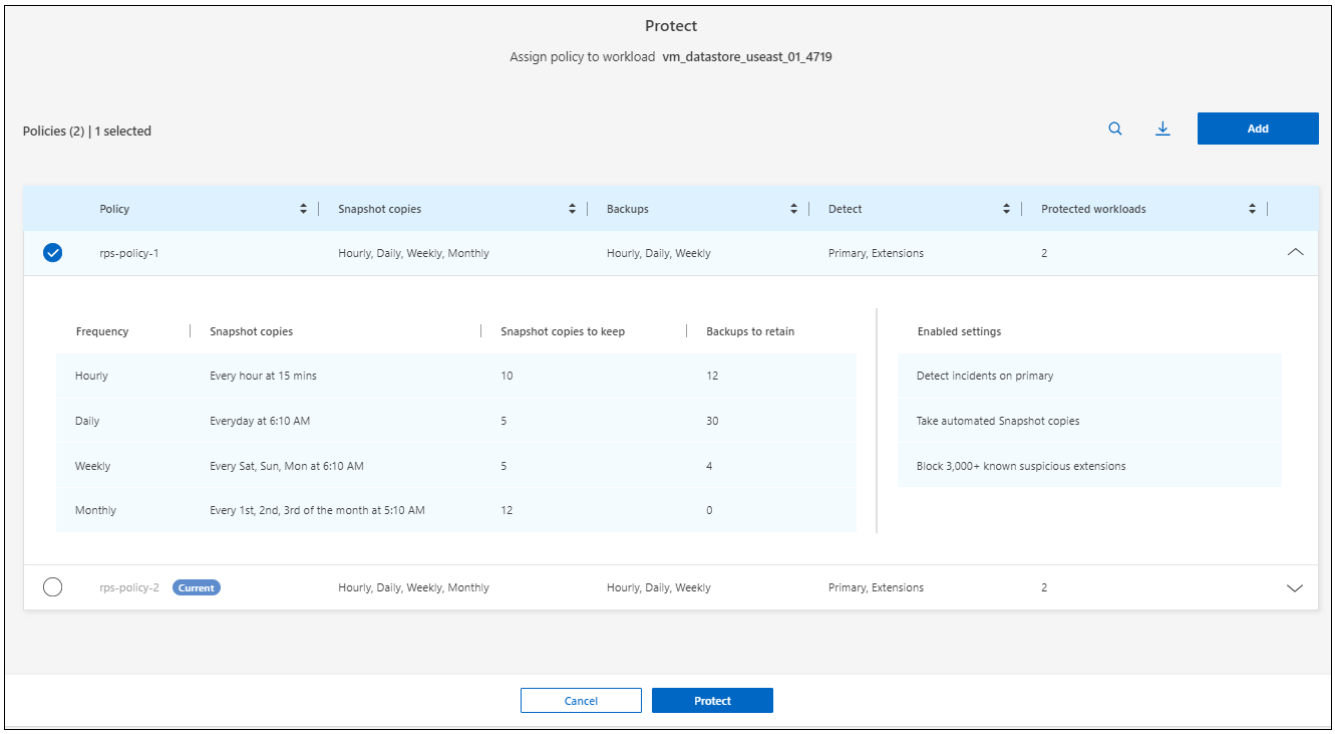
BlueXP 勒索軟體保護包括下列符合工作負載優先順序的預先定義原則：

原則層級	**Snapshot**	頻率	保留（天數）	**Snapshot** 複本數量	**Snapshot** 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
* 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 60 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

步驟

1. 從 BlueXP 勒索軟體保護中、執行下列其中一項：
    - 從儀表板資料保護窗格中、選取 * 檢視全部 * 。
    - 從「儀表板建議」窗格中、選取指派原則的建議、然後選取 * 檢閱和修正 * 。
    - 從功能表中選取 * 保護 * 。
2. 從「保護」頁面檢閱工作負載、然後選取工作負載旁的 * 保護 * 。

    隨即出現原則清單。



3. 若要查看詳細資料、請按一下原則的向下箭頭。
4. 選取要指派給工作負載的原則。
5. 選取 * 保護 * 。
6. 檢閱「儀表板建議動作」窗格、此窗格會將動作顯示為「已完成」。

建立保護原則

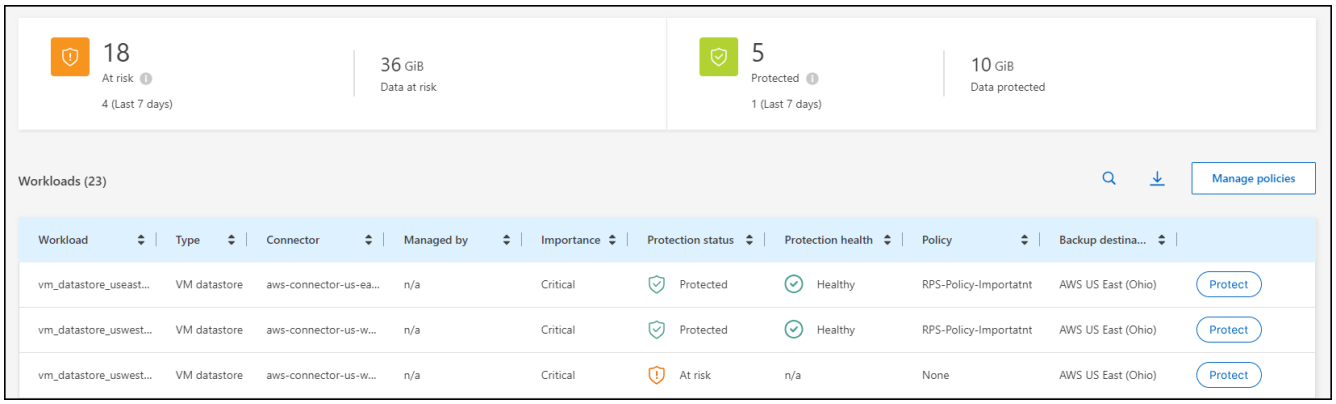
如果現有原則不符合您的業務需求、您可以建立新的保護原則。您可以從頭開始建立自己的原則、或使用現有原則並修改其設定。

您可以建立管理主要和次要儲存設備的原則、並以相同或不同的方式處理主要和次要儲存設備。

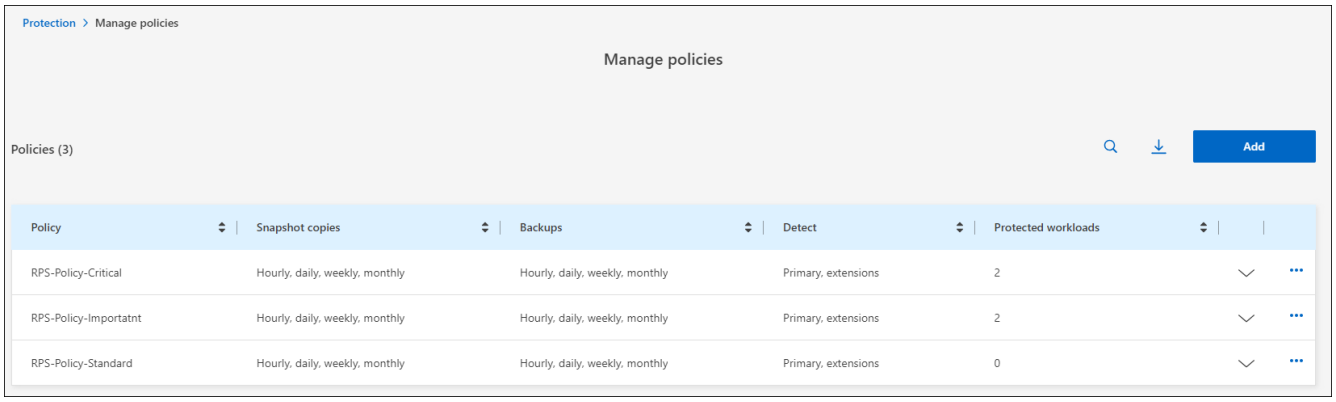
您可以在管理原則或將原則指派給工作負載的過程中建立原則。

在原則管理期間建立原則的步驟

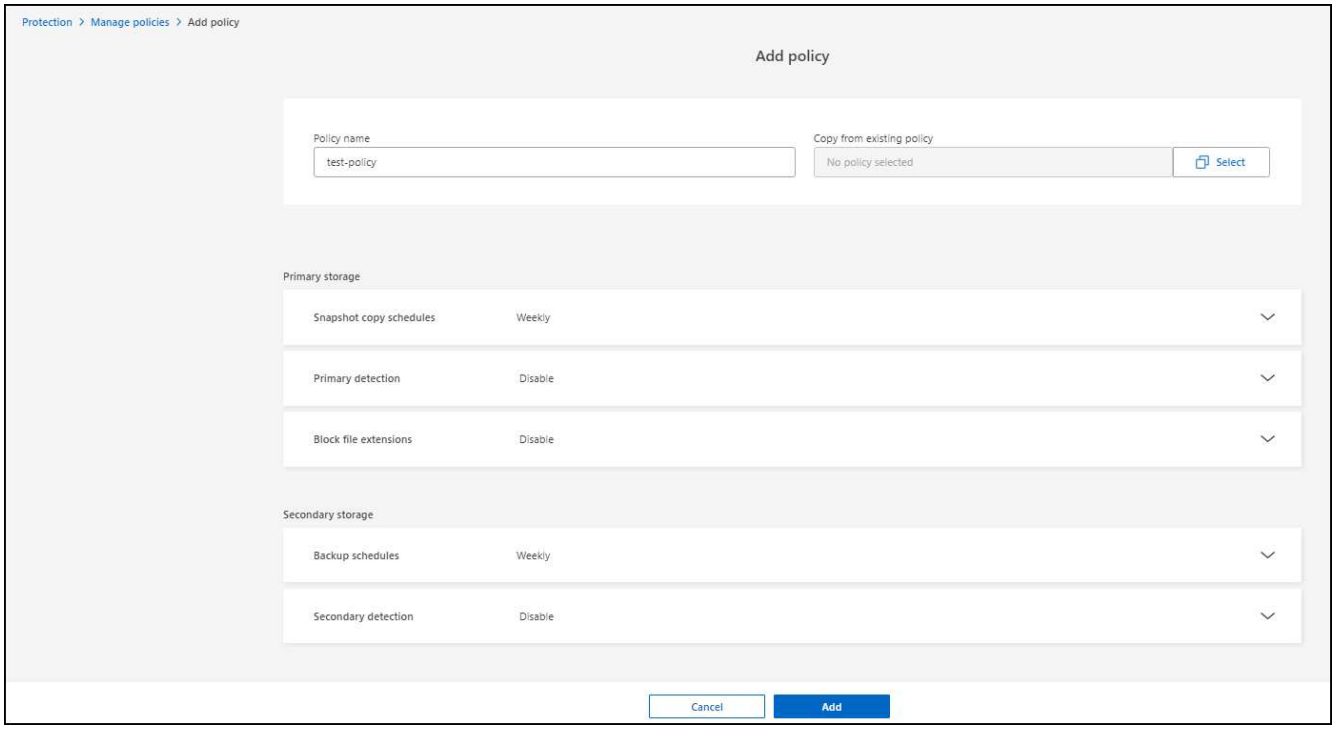
1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。



2. 從「保護」頁面選取 * 管理原則 * 。



3. 在「管理原則」頁面中、選取 * 新增 * 。



4. 輸入新的原則名稱、或輸入現有的原則名稱以進行複製。如果您輸入現有的原則名稱、請選擇要複製的原則。

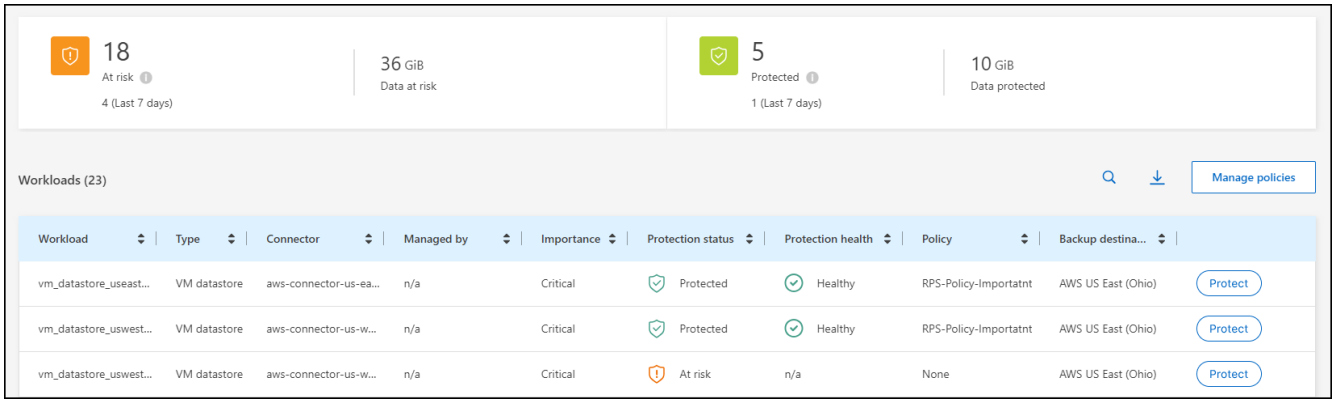
如果您選擇複製及修改現有原則、則必須變更至少一個設定、使其成為唯一的設定。

5. 針對每個項目、選取向下箭頭。
   - * 主儲存設備 * ：
     - * Snapshot 複製排程 * ：選擇排程選項、要保留的 Snapshot 複本數量、然後選擇以啟用排程。
     - * 主要偵測 * ：讓服務能夠偵測主要儲存設備上的勒索軟體事件。
     - * 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、服務會自動取得 Snapshot 複本。
   - * 次儲存設備 * ：
     - * 備份排程 * ：選擇次要儲存設備的排程選項並啟用排程。
     - * 次要偵測 * ：讓服務能夠偵測次要儲存設備上的勒索軟體事件。
     - * 鎖定備份 * ：選擇此選項可防止在一段時間內修改或刪除次要儲存設備上的備份。這也稱為 _immutable 儲存設備 _ 。

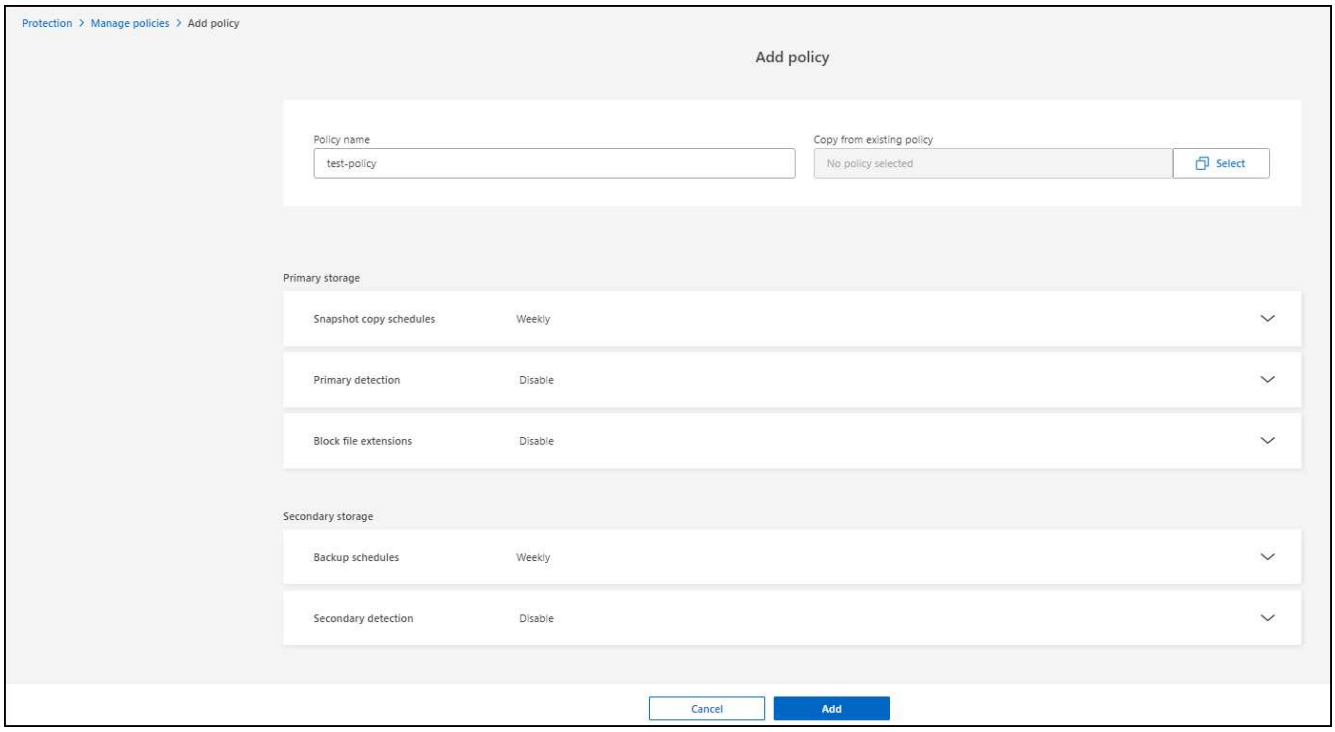
       此選項使用 NetApp DataLock 技術、可鎖定次要儲存設備上的備份。備份檔案被鎖定（並保留）的期間稱為DataLock保留期間。這是根據您定義的備份原則排程和保留設定、加上 14 天的緩衝區。任何少於30天的DataLock保留原則、最短四捨五入至30天。
6. 選取*「Add*」。

在保護原則指派期間建立原則的步驟

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 * 保護 * 。
3. 從「保護」頁面選取 * 新增 * 。



4. 完成此程序、就像從「管理原則」頁面建立原則一樣。

指派不同的保護原則

您可以為工作負載選擇不同的保護原則。
您可能想要透過變更保護原則來加強保護、以防止未來的勒索軟體攻擊。

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 * 。
3. 在「保護」頁面中、為工作負載選取不同的原則。
4. 若要變更原則的任何詳細資料、請選取右側的向下箭頭、然後變更詳細資料。
5. 選取 * 儲存 * 以完成變更。

編輯現有原則

只有當原則未與工作負載相關聯時、才能變更原則的詳細資料。

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 * 管理原則 * 。
3. 在「管理原則」頁面中、針對您要變更的原則選取 * 動作 * 選項。
4. 從「動作」功能表中、選取 * 編輯原則 * 。
5. 變更詳細資料。
6. 選取 * 儲存 * 以完成變更。

刪除原則

您可以刪除目前未與任何工作負載相關聯的保護原則。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
2. 從「保護」頁面選取 * 管理原則 * 。
3. 在「管理原則」頁面中、針對您要刪除的原則選取 * 動作 * 選項。
4. 從「動作」功能表中、選取 * 刪除原則 * 。

回應偵測到的勒索軟體警示

如果 BlueXP 勒索軟體防護偵測到可能的攻擊、 BlueXP 勒索軟體保護儀表板和右上角的 BlueXP 通知會出現警示、表示可能發生勒索軟體攻擊。服務也會立即啟動 Snapshot 複本。此時、您應該在 BlueXP 勒索軟體保護 * 警示 * 標籤中查看潛在風險。

若要開始恢復資料、請將警示標記為已準備好恢復、以便儲存管理員開始恢復程序。

每個警示可能會在不同磁碟區上有多個狀態不同的事件、因此請務必查看所有事件。

此服務提供的資訊稱為 _ 證據 _ 、說明導致發出警示的原因、例如：

- 檔案副檔名已建立或變更
- 檔案建立已完成、並以列出的百分比增加
- 檔案刪除已發生、並以列出的百分比增加

警示是以下列行為類型為基礎：

- * 潛在攻擊 * ：當自主勒索軟體保護偵測到新的延伸、且在過去 24 小時內重複發生超過 20 次（預設行為）時、就會發出警示。
- * 警告 * ：根據下列行為發出警告：
  - 偵測到新的擴充功能之前並未發現、相同的行為重複時間不足、無法將其宣告為攻擊。
  - 觀察到高 Entropy 。
  - 檔案讀取 / 寫入 / 重新命名 / 刪除作業的活動量超過基準線、達到 100% 激增。

證據是根據 ONTAP 中的自主勒索軟體保護所提供的資訊。如需詳細資訊、請參閱 "自主勒索軟體保護總覽"。

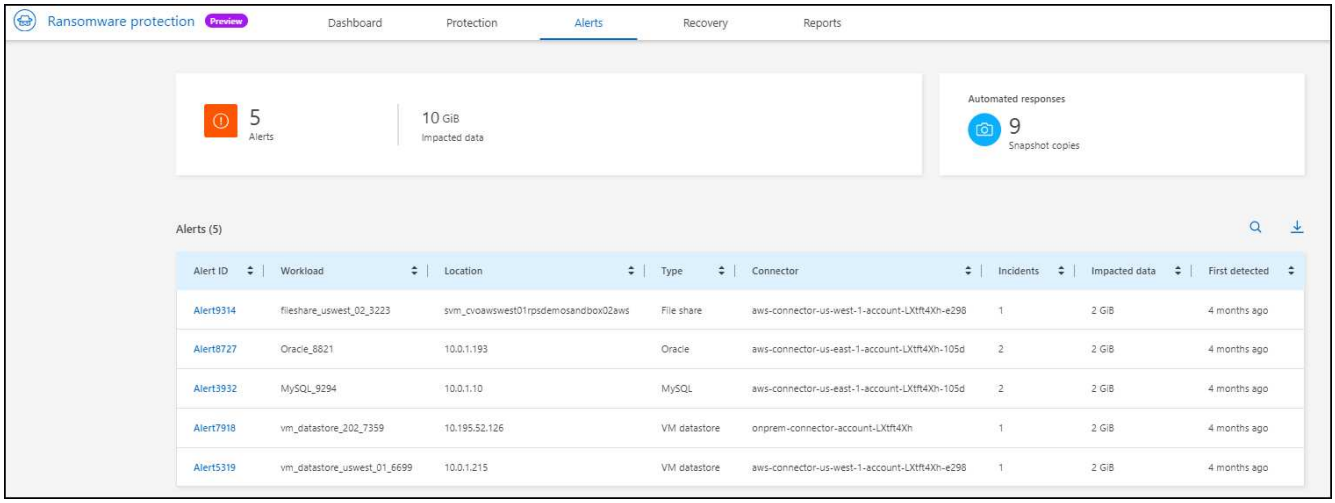
檢視警示

您可以從 BlueXP 勒索軟體保護儀表板或 * Alerts * 標籤存取警示。

步驟

1. 在 BlueXP 勒索軟體保護儀表板中、檢閱警示窗格。
2. 在其中一個雕像下方選取 * 檢視全部 * 。

3. 按一下警示、即可針對每個警示、檢閱每個磁碟區上的所有事件。
4. 若要檢閱其他警示、請按一下左上角階層的 * 警示 * 。
5. 檢閱「警示」頁面上的警示。



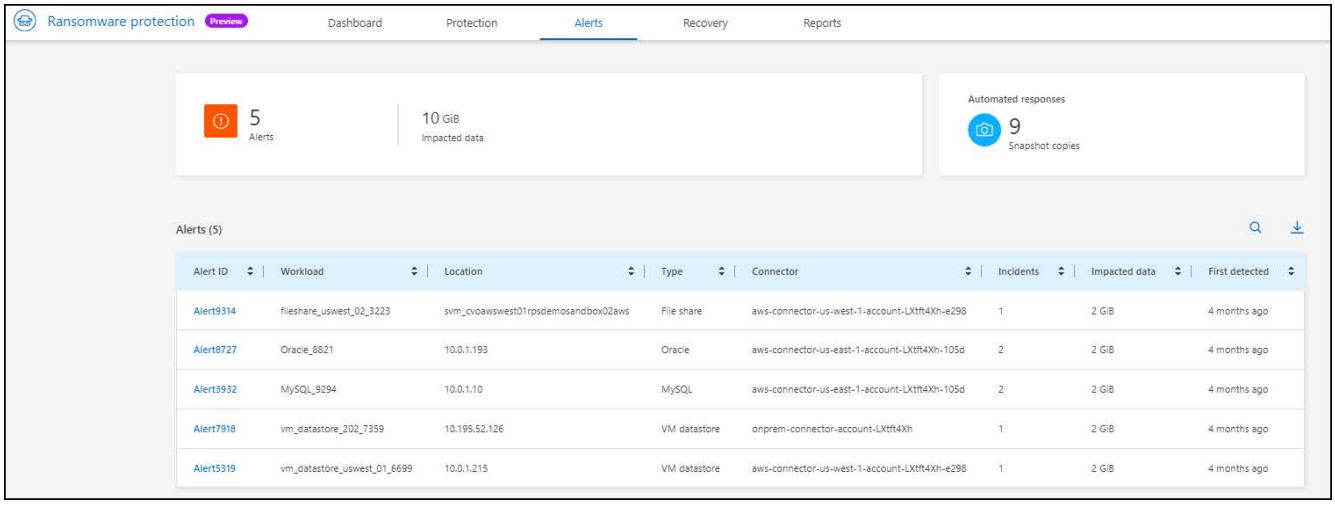
6. 繼續 [將勒索軟體事件標示為準備好進行恢復（在事件被消除之後）]。

將勒索軟體事件標示為準備好進行恢復（在事件被消除之後）

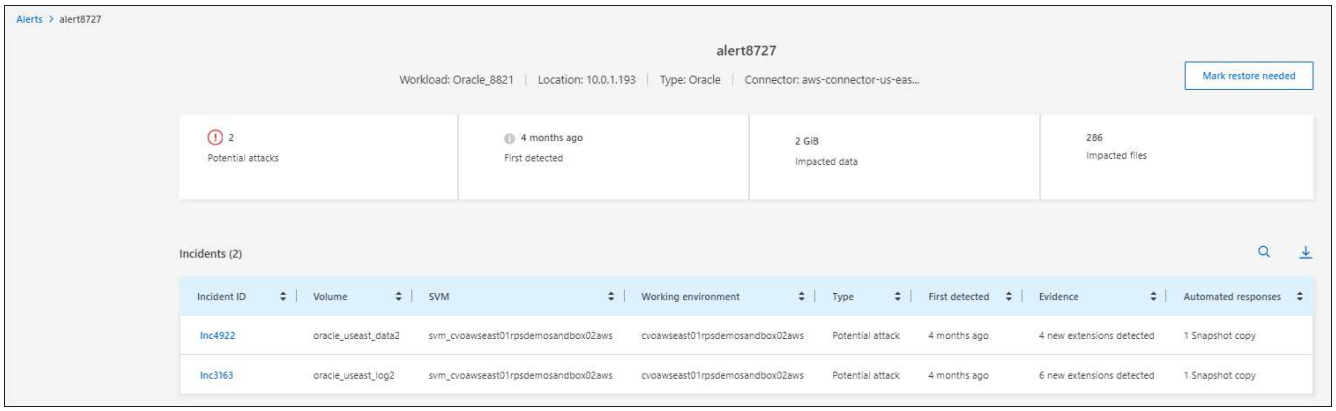
緩解攻擊並準備好恢復工作負載之後、您應該與儲存管理團隊溝通、告知資料已準備好進行恢復、以便開始恢復程序。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 警示 * 。



2. 在「警示」頁面中、選取警示。
3. 檢閱警示中的事件。



4. 如果您確定事件已準備好進行恢復，請選擇 *Mark restore 需求 * 。
5. 確認動作、然後選取 * 標示需要還原 * 。
6. 若要啟動工作負載恢復、請在訊息中選取 * 恢復 * 工作負載、或選取 * 恢復 * 索引標籤。

結果

警示標示為恢復後、警示會從警示索引標籤移至恢復索引標籤。

從勒索軟體攻擊中恢復（在事件被消除之後）

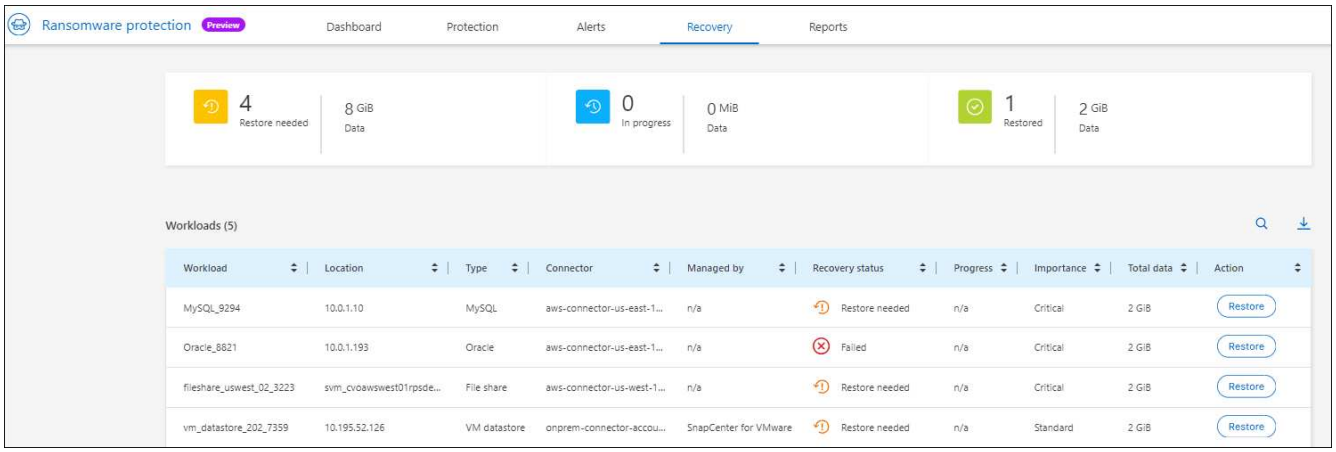
將工作負載標記為「準備好恢復」之後、 BlueXP 勒索軟體保護就會建議實際的還原點（ RPA ）、並協調工作流程以進行防損恢復。

檢視準備還原的工作負載

檢閱處於「還原所需」恢復狀態的工作負載。

步驟

1. 執行下列其中一項：
   - 在儀表板中、檢閱警示窗格中的「還原所需」總計、然後選取 * 檢視全部 * 。
   - 從功能表中選取 **Recovery** 。
2. 檢閱 * 恢復 * 頁面中的工作負載資訊。



恢復工作負載

使用 BlueXP 勒索軟體保護、儲存管理員可以決定如何從建議的還原點或其偏好的還原點、以最佳方式恢復工作負載。

安全儲存管理員可以在不同層級恢復資料：

- 恢復所有磁碟區
- 在磁碟區層級或檔案與資料夾層級復原應用程式。
- 在磁碟區層級、目錄或檔案 / 資料夾層級恢復檔案共用。
- 從 VM 層級的資料存放區恢復。

此程序會因工作負載類型而稍有不同。

步驟

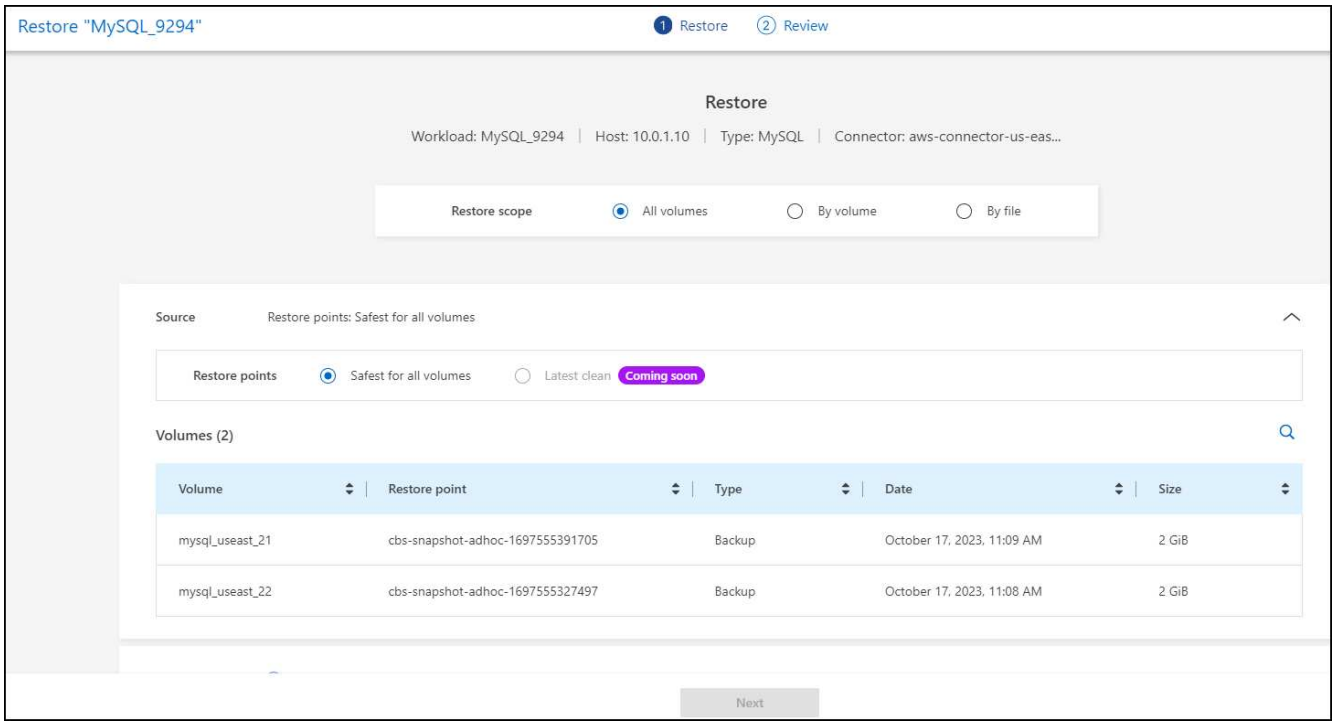
1. 從 BlueXP 勒索軟體保護功能表中、選取 * 回復 * 。
2. 檢閱 * 恢復 * 頁面中的工作負載資訊。
3. 選取處於「還原所需」狀態的工作負載。
4. 若要還原、請選取 * 還原 * 。
5. * 還原範圍 * ：選取您要完成的還原類型：
    - 所有磁碟區
    - 依 Volume
    - 依檔案：您可以指定要還原的資料夾或單一檔案。

    您最多可以選取 100 個檔案或單一資料夾。

6. 根據您選擇的是應用程式、磁碟區或檔案、繼續執行下列其中一個程序。

還原所有磁碟區

1. 在「還原」頁面的「還原」範圍中、選取 * 所有磁碟區 * 。



2. * 來源 * ：選取來源旁的向下箭頭以查看詳細資料。
   a. 選取您要用來還原資料的還原點。

> BlueXP 勒索軟體保護可將最佳還原點識別為事件發生前的最新備份、並顯示「所有磁碟區的安全性」指示。這表示所有磁碟區都會在第一次偵測到第一個磁碟區受到攻擊之前還原成複本。

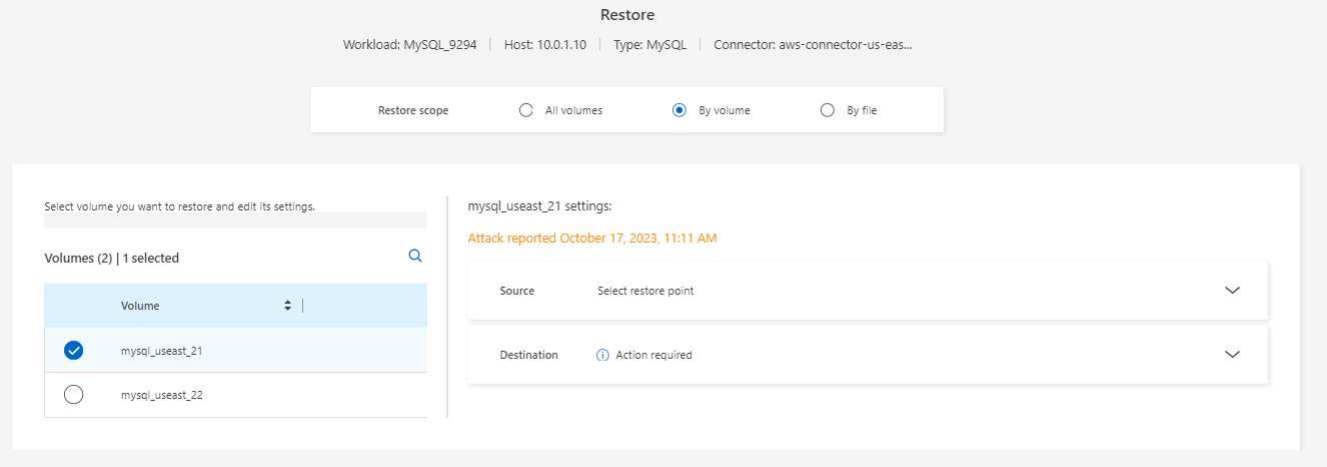
3. * 目的地 * ：選取目的地旁的向下箭頭以查看詳細資料。
   a. 選取工作環境。
   b. 選取儲存 VM 。
   c. 選取 Aggregate 。
   d. 變更要預先附加至所有新磁碟區的磁碟區前置碼。

> 新的磁碟區名稱會顯示為首碼 + 原始磁碟區名稱 + 備份名稱 + 備份日期。

4. 選擇*保存*。
5. 選擇*下一步*。
6. 檢閱您的選擇。
7. 選擇*還原*。
8. 從上方功能表中、選取 * 恢復 * 以檢閱恢復頁面上的工作負載、其中作業狀態會在狀態之間移動。

在磁碟區層級還原應用程式工作負載

1. 在「還原」頁面的「還原範圍」中、選取 * 依 Volume * 。



2. 在磁碟區清單中、選取您要還原的磁碟區。
3. * 來源 * ：選取來源旁的向下箭頭以查看詳細資料。
   a. 選取您要用來還原資料的還原點。

> BlueXP 勒索軟體保護可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 * ：選取目的地旁的向下箭頭以查看詳細資料。
   a. 選取工作環境。
   b. 選取儲存 VM 。
   c. 選取 Aggregate 。
   d. 檢閱新的 Volume 名稱。

> 新的磁碟區名稱會顯示為原始磁碟區名稱 + 備份名稱 + 備份日期。

5. 選擇*保存*。
6. 選擇*下一步*。
7. 檢閱您的選擇。
8. 選擇*還原*。
9. 從上方功能表中、選取 * 恢復 * 以檢閱恢復頁面上的工作負載、其中作業狀態會在狀態之間移動。

在檔案層級還原應用程式工作負載

1. 在「還原」頁面的「還原範圍」中、選取 * 依檔案 * 。
2. 在磁碟區清單中、選取您要還原的磁碟區。
3. * 來源 * ：選取來源旁的向下箭頭以查看詳細資料。
   a. 選取您要用來還原資料的還原點。

> BlueXP 勒索軟體保護可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。

b. 最多可選取 100 個檔案或單一資料夾進行還原。

4. * 目的地 * ：選取目的地旁的向下箭頭以查看詳細資料。

   a. 選擇要還原資料的位置：原始來源位置或您可以指定的替代位置。

   > 雖然還原的資料會覆寫原始檔案或目錄、但除非您指定新名稱、否則原始檔案和資料夾名稱將維持不變。

   b. 選取工作環境。

   c. 選取儲存 VM 。

   d. 也可以輸入路徑。

   > 如果您未指定還原路徑、檔案將會還原至最上層目錄的新磁碟區。

   e. 選取您要還原的檔案或目錄名稱與目前位置或不同名稱相同。

5. 選擇*保存*。

6. 選擇*下一步*。

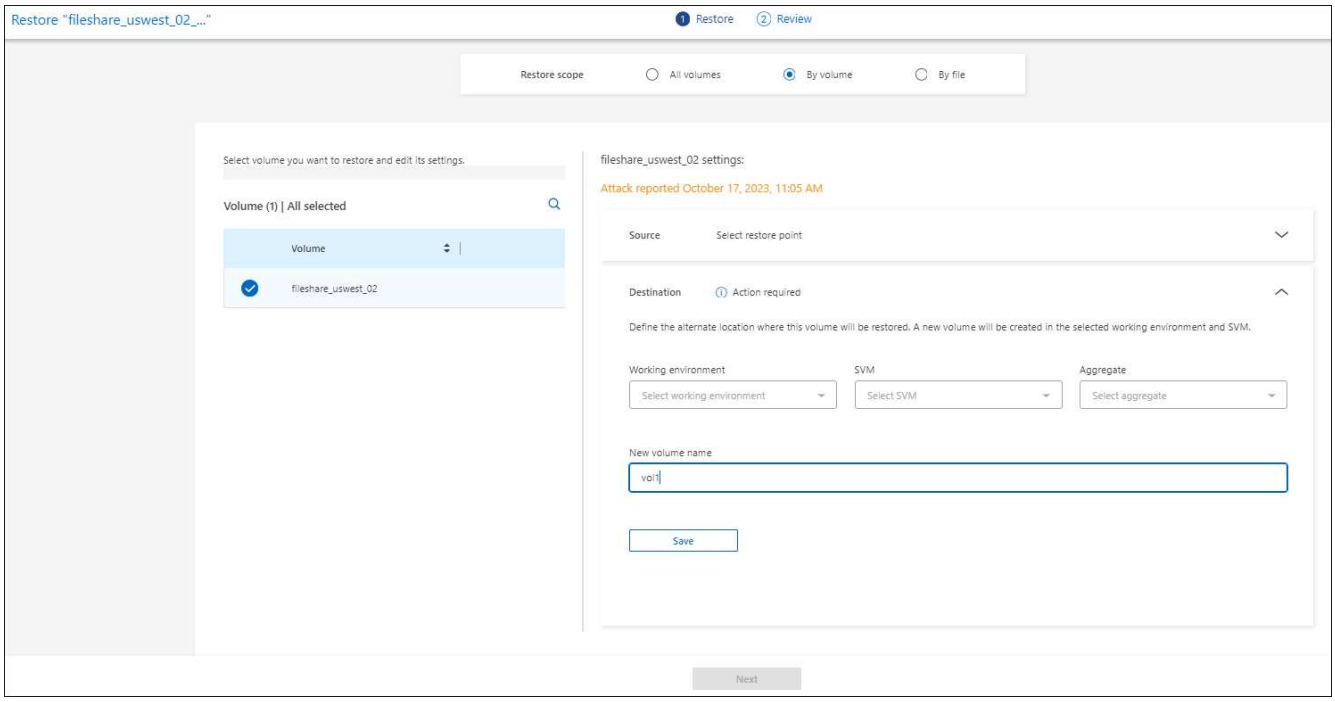
7. 檢閱您的選擇。

8. 選擇*還原*。

9. 從上方功能表中、選取 * 恢復 * 以檢閱恢復頁面上的工作負載、其中作業狀態會在狀態之間移動。

還原磁碟區或檔案層級的檔案共用區或資料存放區

1. 選取要還原的檔案共用區或資料存放區之後、在「還原」頁面的「還原」範圍中、選取 * 依 Volume * 或 * 依檔案 * 。



2. 在磁碟區清單中、選取您要還原的磁碟區。

3. * 來源 * ：選取來源旁的向下箭頭以查看詳細資料。
   a. 選取您要用來還原資料的還原點。

> BlueXP 勒索軟體保護可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 * ：選取目的地旁的向下箭頭以查看詳細資料。
   a. 選擇要還原資料的位置：原始來源位置或您可以指定的替代位置。

> 雖然還原的資料會覆寫原始檔案或目錄、但除非您指定新名稱、否則原始檔案和資料夾名稱將維持不變。

   b. 選取工作環境。
   c. 選取儲存 VM 。
   d. 也可以輸入路徑。

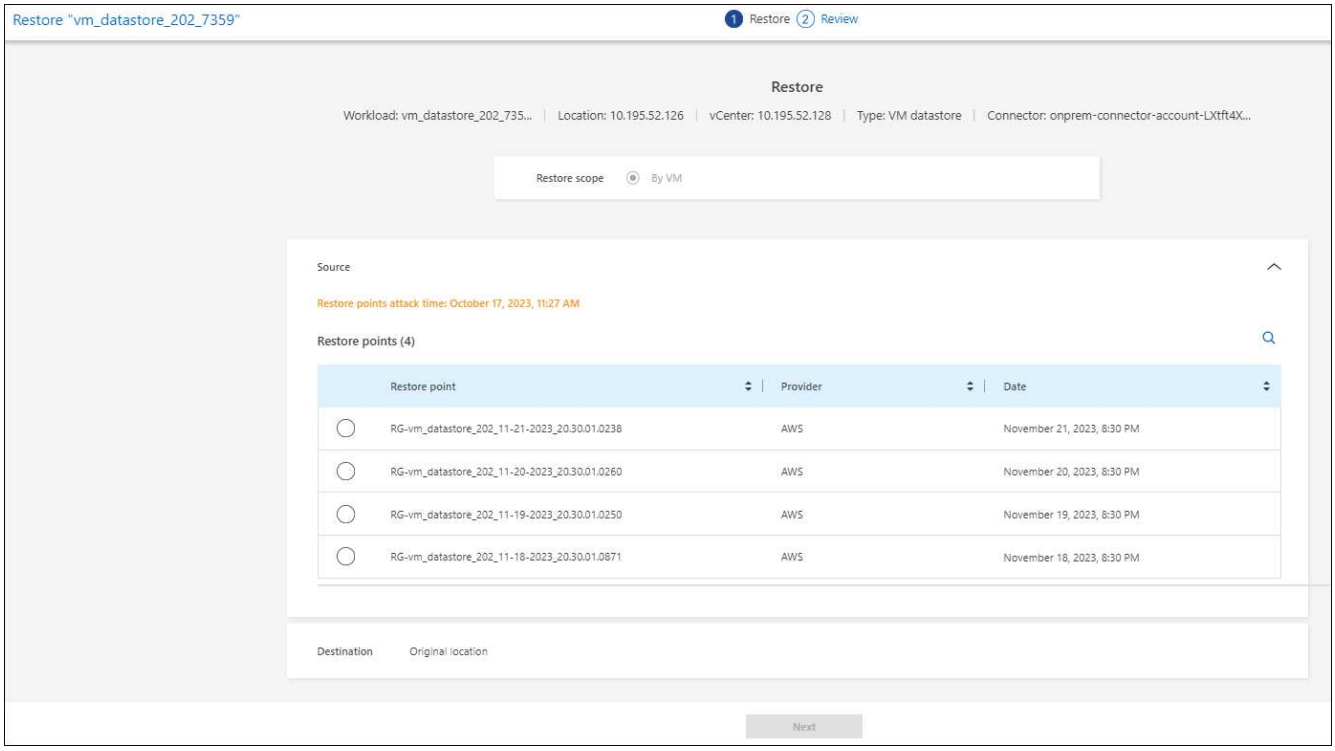
> 如果您未指定還原路徑、檔案將會還原至最上層目錄的新磁碟區。

5. 選擇*保存*。
6. 檢閱您的選擇。
7. 選擇*還原*。
8. 從功能表中、選取 * 恢復 * 以檢閱恢復頁面上的工作負載、其中作業狀態會在狀態之間移動。

在 **VM** 層級還原 **VM** 檔案共用

在您選取要還原的 VM 之後、請在「恢復」頁面上繼續執行這些步驟。

1. * 來源 * ：選取來源旁的向下箭頭以查看詳細資料。



2. 選取您要用來還原資料的還原點。
3. * 目的地 * ：至原始位置。
4. 選擇*下一步*。
5. 檢閱您的選擇。
6. 選擇*還原*。
7. 從功能表中、選取 * 恢復 * 以檢閱恢復頁面上的工作負載、其中作業狀態會在狀態之間移動。

知識與支援

註冊以取得支援

需要註冊支援、才能獲得 BlueXP 及其儲存解決方案與服務專屬的技術支援。也需要註冊支援、才能啟用 Cloud Volumes ONTAP 系統的重要工作流程。

註冊支援並不會啟用雲端供應商檔案服務的 NetApp 支援。如需雲端供應商檔案服務、其基礎架構或任何使用服務的解決方案的相關技術支援、請參閱該產品的 BlueXP 文件中的「取得說明」。

- "Amazon FSX for ONTAP Sf"
- "Azure NetApp Files"
- "適用於 Google Cloud Cloud Volumes Service"

支援登錄總覽

有兩種登錄形式可啟動支援服務權利：

- 註冊您的BlueXP帳戶ID支援訂閱（您的20位數960xxxxxxx序號位於BlueXP的「Support Resources（支援資源）」頁面）。

  這是您在BlueXP內任何服務的單一支援訂閱ID。每個BlueXP帳戶層級的支援訂閱都必須註冊。

- 在Cloud Volumes ONTAP 雲端供應商的市場中註冊與訂閱相關的支援服務序號（這些序號為20位數909601xxxxxxxx序號）。

  這些序號通常稱為「_PAYGO」序號、並在Cloud Volumes ONTAP 部署時由BlueXP產生。

註冊這兩種類型的序號、即可開啟支援服務單和自動建立個案。如下列所述、將 NetApp 支援網站 （ NSS ）帳戶新增至 BlueXP 即可完成登錄。

註冊您的 **BlueXP** 帳戶以取得 **NetApp** 支援

若要註冊以取得支援並啟動支援授權、 BlueXP 帳戶中的一位使用者必須將 NetApp 支援網站 帳戶與其 BlueXP 登入建立關聯。您如何註冊NetApp支援取決於您是否已擁有NetApp 支援網站 一個NetApp（NSS）帳戶。

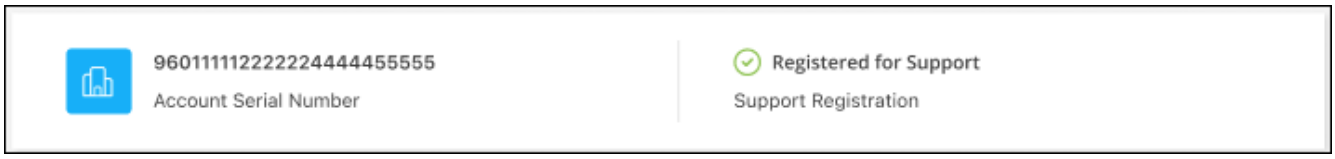
現有的客戶、擁有一個新服務客戶帳戶

如果您是擁有NSS帳戶的NetApp客戶、您只需透過BlueXP註冊即可獲得支援。

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 * 。
2. 選取 * 使用者認證 * 。
3. 選取 * 新增 NSS 認證 * 、然後遵循 NetApp 支援網站 （ NSS ）驗證提示。
4. 若要確認註冊程序是否成功、請選取「說明」圖示、然後選取 * 「支援 * 」。

   「 * 資源 * 」頁面應顯示您的帳戶已註冊以取得支援。



請注意、如果其他 BlueXP 使用者尚未將 NetApp 支援網站 帳戶與 BlueXP 登入建立關聯、則不會看到此相同的支援登錄狀態。不過、這並不表示您的 BlueXP 帳戶尚未註冊支援。只要帳戶中有一位使用者已遵循這些步驟、您的帳戶就已登錄。

現有客戶、但無**NSS.**帳戶

如果您是現有的 NetApp 客戶、擁有現有的授權和序號、但沒有 NSS_ 帳戶、則需要建立一個 NSS 帳戶、並將其與您的 BlueXP 登入建立關聯。

步驟

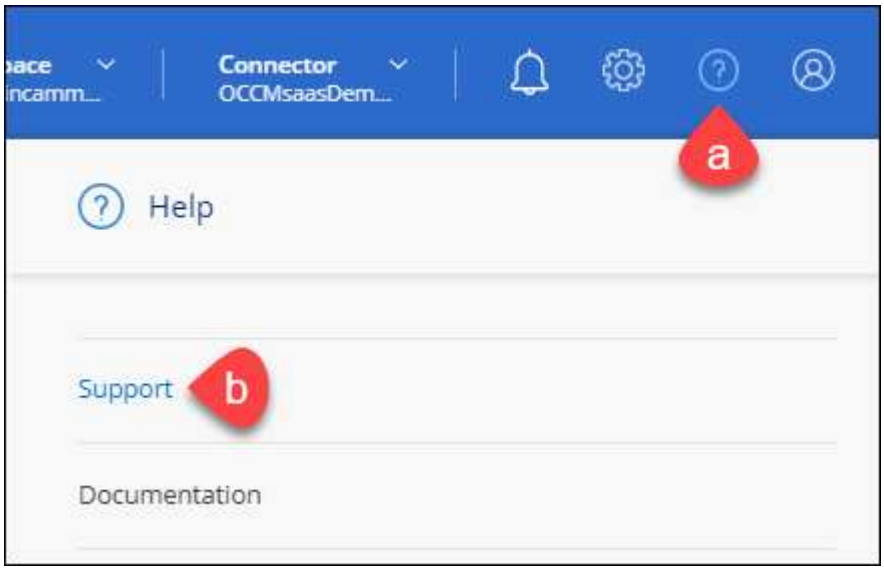
1. 完成建立NetApp 支援網站 一個不完善的帳戶 "《使用者登錄表》NetApp 支援網站"
   a. 請務必選擇適當的使用者層級、通常為* NetApp客戶/終端使用者*。
   b. 請務必複製上述序號欄位使用的BlueXP帳戶序號（960xxxx）。這將加速帳戶處理。
2. 完成下的步驟、將新的 NSS 帳戶與 BlueXP 登入建立關聯 [現有的客戶、擁有一個新服務客戶帳戶]。

NetApp全新推出

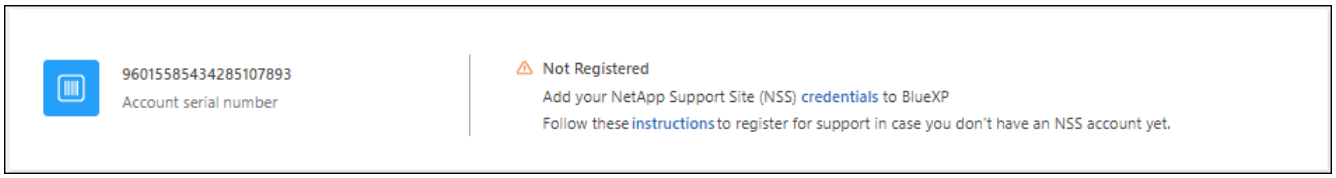
如果您是NetApp的新客戶、而且您沒有新的NSS帳戶、請依照下列每個步驟操作。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 * 「支援 * 」。



2. 從「Support Registration（支援註冊）」頁面找到您的帳戶ID序號。



3. 瀏覽至 "NetApp的支援註冊網站" 並選擇*我不是NetApp註冊客戶*。
4. 填寫必填欄位（紅色星號）。
5. 在*產品系列*欄位中、選取* Cloud Manager*、然後選取適用的帳單供應商。
6. 複製上述步驟2的帳戶序號、完成安全性檢查、然後確認您已閱讀NetApp的全球資料隱私權政策。

   系統會立即將電子郵件傳送至提供的信箱、以完成此安全交易。如果驗證電子郵件在幾分鐘內未送達、請務必檢查您的垃圾郵件資料夾。

7. 確認電子郵件中的行動。

   確認將您的申請提交給NetApp、並建議您建立NetApp 支援網站 一個申請表。

8. 完成建立NetApp 支援網站 一個不完善的帳戶 "《使用者登錄表》NetApp 支援網站"
   a. 請務必選擇適當的使用者層級、通常為* NetApp客戶/終端使用者*。
   b. 請務必複製上述序號欄位使用的帳戶序號（960xxxx）。這將加速帳戶處理。

完成後

在此過程中、NetApp應與您聯絡。這是新使用者的一次性就職練習。

擁有 NetApp 支援網站 帳戶後、請完成下的步驟、將帳戶與 BlueXP 登入建立關聯 [現有的客戶、擁有一個新服務客戶帳戶]。

建立 NSS 認證的關聯、以取得 Cloud Volumes ONTAP 支援

若要為 Cloud Volumes ONTAP 啟用下列關鍵工作流程、必須將 NetApp 支援網站 認證與 BlueXP 帳戶建立關聯：

- 註冊隨用隨付 Cloud Volumes ONTAP 系統以取得支援

  您必須提供您的NSS帳戶、才能啟動系統支援、並取得NetApp技術支援資源的存取權。

- 自帶授權（Cloud Volumes ONTAP BYOL）即可部署

  您必須提供您的NSS帳戶、才能讓BlueXP上傳授權金鑰、並啟用您所購買期間的訂閱。這包括定期續約的自動更新。

- 升級Cloud Volumes ONTAP 更新版的更新版

將 NSS 認證與 BlueXP 帳戶建立關聯、與 BlueXP 使用者登入相關的 NSS 帳戶不同。

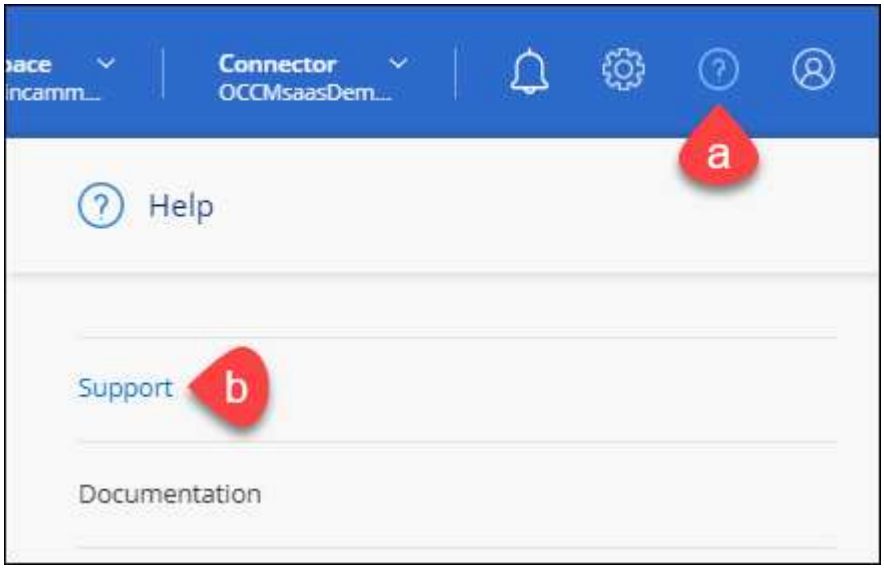
這些 NSS 認證會與您的特定 BlueXP 帳戶 ID 相關聯。屬於BlueXP帳戶的使用者可以從*支援> nss管理*存取這些認證資料。

- 如果您有客戶層級的帳戶、可以新增一或多個NSS帳戶。

- 如果您有合作夥伴或經銷商帳戶、您可以新增一或多個NSS帳戶、但這些帳戶無法與客戶層級帳戶一起新增。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 * 「支援 * 」。



2. 選取 **NSS Management > Add NSS Account** 。
3. 系統提示時、請選取 * 繼續 * 以重新導向至 Microsoft 登入頁面。

   NetApp 使用 Microsoft Entra ID 做為身分識別提供者、提供專為支援與授權所設計的驗證服務。

4. 在登入頁面上，提供您的 NetApp 支援網站註冊電子郵件地址和密碼，以執行身分驗證程序。

   這些行動可讓BlueXP將您的nssa帳戶用於授權下載、軟體升級驗證、以及未來的支援註冊等項目。

   請注意下列事項：

   - NSS-帳戶必須是客戶層級的帳戶（而非來賓帳戶或暫存帳戶）。您可以擁有多個客戶層級的NSS帳戶。
   - 如果該帳戶是合作夥伴層級帳戶、則只能有一個NSS帳戶。如果您嘗試新增客戶層級的NSS帳戶、但有合作夥伴層級的帳戶存在、您會收到下列錯誤訊息：

     「此帳戶不允許使用新增服務客戶類型、因為已經有不同類型的新增服務使用者。」

   如果您擁有預先存在的客戶層級的NSS帳戶、並嘗試新增合作夥伴層級的帳戶、情況也是如此。

   - 成功登入後、NetApp會儲存NSS.使用者名稱。

     這是系統產生的ID、會對應至您的電子郵件。在「* nssn*管理*」頁面上、您可以從顯示電子郵件 ••• 功能表。

   - 如果您需要重新整理登入認證憑證權杖、也可以在中使用*更新認證*選項 ••• 功能表。

     使用此選項會提示您重新登入。請注意、這些帳戶的權杖會在90天後過期。系統會張貼通知、提醒您注意此點。

取得協助

NetApp以多種方式支援BlueXP及其雲端服務。我們全年無休提供豐富的免費自助支援選項、例如知識庫（KB）文章和社群論壇。您的支援註冊包括透過網路票證提供遠端技術支援。

取得雲端供應商檔案服務的支援

如需雲端供應商檔案服務、其基礎架構或任何使用服務的解決方案的相關技術支援、請參閱該產品的 BlueXP 文件中的「取得說明」。

- "Amazon FSX for ONTAP Sf"
- "Azure NetApp Files"
- "適用於 Google Cloud Cloud Volumes Service"

若要獲得 BlueXP 及其儲存解決方案與服務的專屬技術支援、請使用下列支援選項。

使用自我支援選項

這些選項可供免費使用、一天24小時、一週7天：

- 文件

  您目前正在檢視的BlueXP文件。

- "知識庫"

  請搜尋BlueXP知識庫、找出有助於疑難排解問題的文章。

- "社群"

  歡迎加入BlueXP社群、以追蹤後續討論或建立新討論。

利用**NetApp**支援建立案例

除了上述的自我支援選項、您也可以在啟動支援之後、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 NetApp 支援網站 認證與 BlueXP 登入建立關聯。 "瞭解如何管理與 BlueXP 登入相關的認證"。
- 如果您要為具有序號的 ONTAP 系統開啟案例、則您的 NSS 帳戶必須與該系統的序號相關聯。

步驟

1. 在 BlueXP 中、選取 * 說明 > 支援 * 。
2. 在「資源」頁面上、選擇「技術支援」下的其中一個可用選項：

   a. 如果您想與電話上的某人通話、請選取 * 致電 * 。您將會被導向netapp.com上的頁面、其中列出您可以撥打的電話號碼。

b. 選擇 * 建立案例 * 、與 NetApp 支援專家一起開啟 Ticket ：

- 服務：選取問題相關的服務。例如、特定於服務工作流程或功能的技術支援問題的BlueXP。
- 工作環境：如果適用於儲存設備、請選取* Cloud Volumes ONTAP 《》或《內部部署*》、然後選取相關的工作環境。

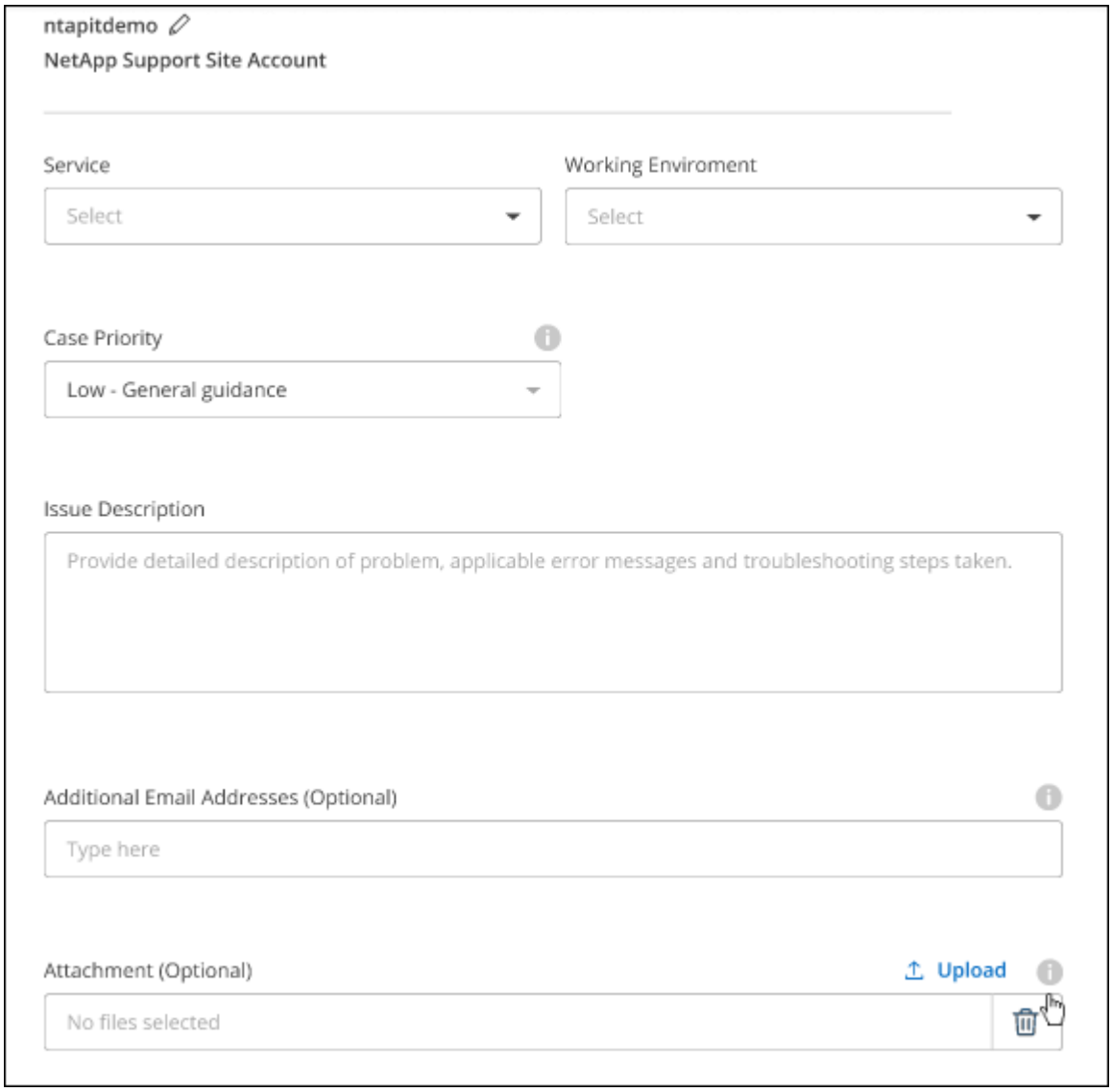
  工作環境清單位於您在服務的最上層橫幅中所選的BlueXP帳戶、工作區和Connector範圍內。

- 案例優先順序：選擇案例的優先順序、可以是低、中、高或嚴重。

  若要深入瞭解這些優先順序、請將滑鼠游標暫留在欄位名稱旁的資訊圖示上。

- 問題說明：提供問題的詳細說明、包括任何適用的錯誤訊息或您執行的疑難排解步驟。
- 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（選填） * ：上傳最多五個附件、一次上傳一個。

  每個檔案的附件上限為 25 MB 。支援下列副檔名： txt 、 log 、 pdf 、 jpg/jpeg 、 rtf 、 doc/dox 、 xls/xlsx 和 csv 。



完成後

您的支援案例編號會出現快顯視窗。NetApp支援專家將會審查您的案例、並盡快回覆您。

如需支援案例的記錄、您可以選取 * 設定 > 時間軸 * 、然後尋找名為「建立支援案例」的動作。 最右側的按鈕可讓您展開動作以查看詳細資料。

嘗試建立案例時、可能會遇到下列錯誤訊息：

"您無權針對所選服務建立案例"

此錯誤可能表示、與該帳戶相關聯的NSS帳戶及記錄公司與BlueXP帳戶序號的記錄公司不同（例如960xxxx)或工作環境序號。您可以使用下列其中一個選項尋求協助：

- 使用產品內對談
- 請至提交非技術案例 https://mysupport.netapp.com/site/help

管理支援案例（預覽）

您可以直接從BlueXP檢視及管理作用中和已解決的支援案例。您可以管理與您的NSS帳戶和貴公司相關的個案。

案例管理可透過預覽取得。我們計畫改善這項體驗、並在即將推出的版本中加入增強功能。請使用產品內建聊天功能、向我們傳送意見反應。

請注意下列事項：

- 頁面頂端的案例管理儀表板提供兩種檢視：
  - 左側檢視顯示您所提供的使用者nssc帳戶在過去3個月內開啟的個案總數。
  - 右側檢視顯示過去3個月內、貴公司層級根據您的使用者nssc帳戶所開啟的個案總數。

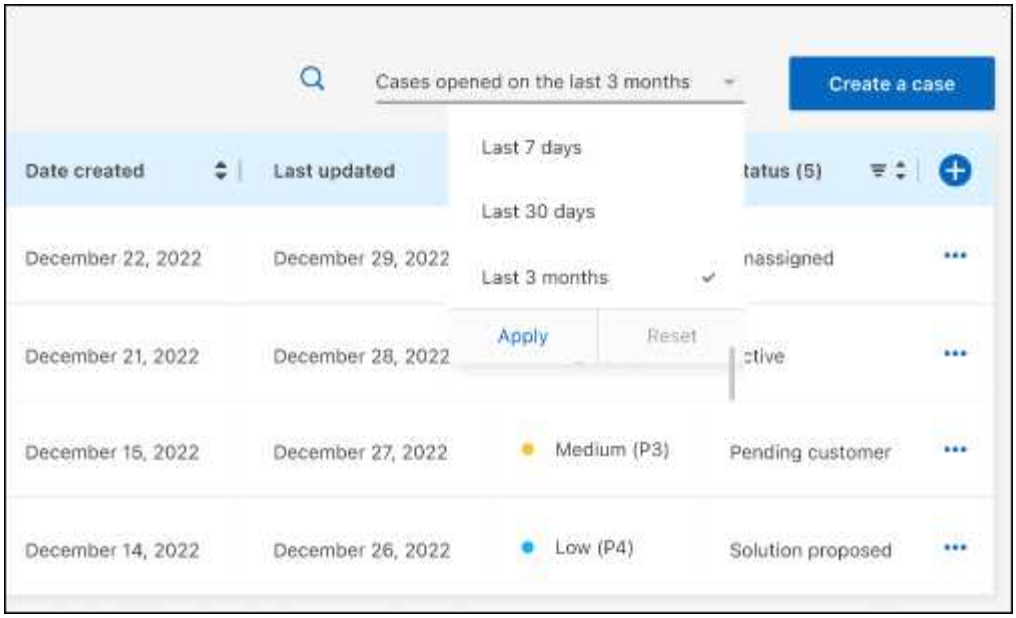
  表格中的結果會反映您所選檢視的相關個案。
- 您可以新增或移除感興趣的欄、也可以篩選優先順序和狀態等欄的內容。其他欄則只提供排序功能。

  如需詳細資料、請參閱下列步驟。
- 在個別案例層級、我們提供更新案例附註或關閉尚未處於「已結案」或「待結案」狀態的案例的功能。

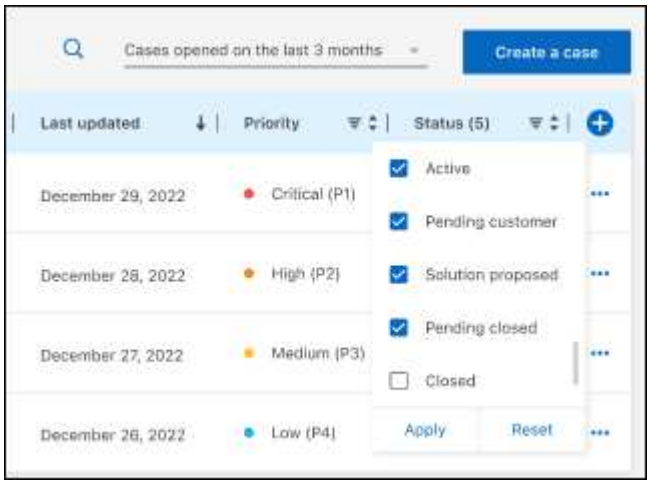
步驟

1. 在 BlueXP 中、選取 * 說明 > 支援 * 。
2. 選取 * 個案管理 * 、如果出現提示、請將您的 NSS 帳戶新增至 BlueXP 。

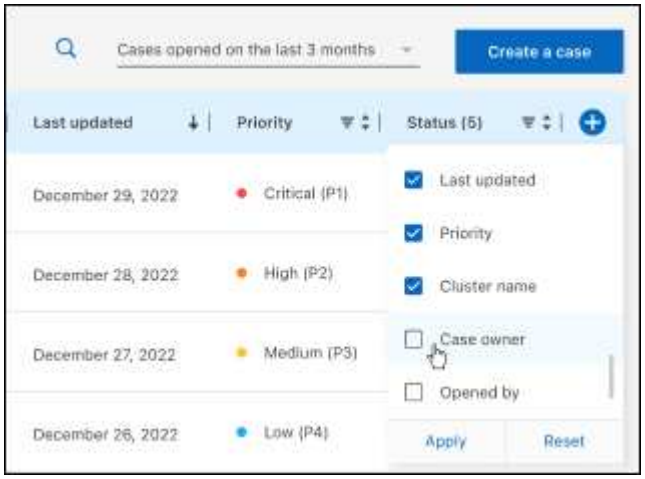
   「個案管理」頁面會顯示與您的BlueXP使用者帳戶相關聯的與NSS帳戶相關的未決個案。這是顯示在「* nssnmanagement *」頁面頂端的相同nss.帳戶。
3. （可選）修改表格中顯示的資訊：
   - 在 * 組織案例 * 下、選取 * 檢視 * 以檢視與貴公司相關的所有案例。
   - 選擇確切的日期範圍或選擇不同的時間範圍、以修改日期範圍。



- 篩選欄的內容。



- 選取以變更表格中顯示的欄 ⊕ 然後選擇您要顯示的欄。

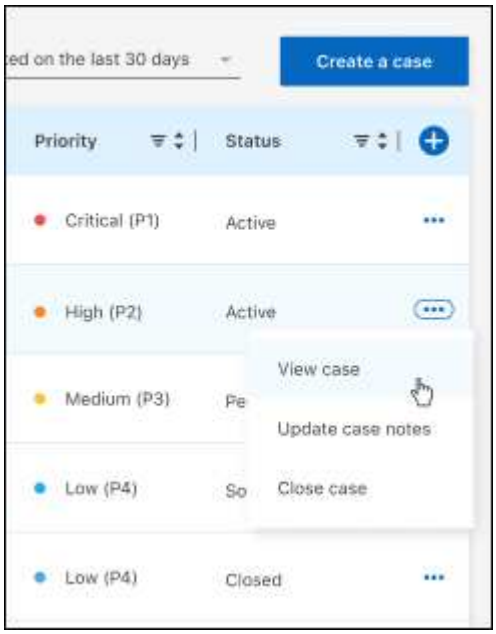


4. 選取以管理現有案例 ••• 並選擇其中一個可用選項：

- 檢視案例：檢視特定案例的完整詳細資料。
- * 更新案例附註 * ：提供問題的其他詳細資料、或選擇 * 上傳檔案 * 最多附加五個檔案。

  每個檔案的附件上限為 25 MB 。支援下列副檔名： txt 、 log 、 pdf 、 jpg/jpeg 、 rtf 、 doc/dox 、 xls/xlsx 和 csv 。

- * 結案案例 * ：提供結案原因的詳細資料、並選取 * 結案案例 * 。



法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

版權

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

商標

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

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

專利

如需最新的 NetApp 擁有專利清單、請參閱：

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

隱私權政策

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

開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

- "藍圖XP注意事項"

版權資訊

Copyright © 2024 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。