



使用**NetApp Backup and Recovery**

NetApp Backup and Recovery

NetApp
February 11, 2026

目錄

使用NetApp Backup and Recovery	1
在NetApp Backup and Recovery儀表板上查看保護健康狀況	1
查看保護摘要	1
查看職位摘要	1
查看還原摘要	2
建立和管理策略來管理NetApp Backup and Recovery中的備份	2
查看政策	2
創建策略	3
編輯策略	8
刪除策略	8
保護ONTAP磁碟區工作負載	8
使用NetApp Backup and Recovery保護您的ONTAP卷數據	9
使用NetApp Backup and Recovery規劃您的保護之旅	17
使用NetApp Backup and Recovery管理ONTAP磁碟區的備份策略	23
NetApp Backup and Recovery中的備份到物件原則選項	27
在NetApp Backup and Recovery和還原進階設定中管理備份到物件儲存選項	34
使用NetApp Backup and Recovery將Cloud Volumes ONTAP資料備份到 Amazon S3	37
使用NetApp Backup and Recovery將Cloud Volumes ONTAP資料備份到 Azure Blob 儲存	46
使用NetApp Backup and Recovery將Cloud Volumes ONTAP資料備份到 Google Cloud Storage	55
使用NetApp Backup and Recovery將本機ONTAP資料備份到 Amazon S3	65
使用NetApp Backup and Recovery將本機ONTAP資料備份到 Azure Blob 儲存	77
使用NetApp Backup and Recovery將本地ONTAP資料備份到 Google Cloud Storage	88
使用NetApp Backup and Recovery將本機ONTAP資料備份到ONTAP S3	99
使用NetApp Backup and Recovery將本機ONTAP資料備份到StorageGRID	108
在NetApp Backup and Recovery中使用SnapMirror將磁碟區遷移到 Cloud Resync	118
在暗站中恢復NetApp Backup and Recovery配置數據	122
使用NetApp Backup and Recovery管理ONTAP系統的備份	127
從ONTAP備份還原	134
保護 Microsoft SQL Server 工作負載	148
使用NetApp Backup and Recovery保護 Microsoft SQL 工作負載概述	148
從外掛程式服務匯入NetApp Backup and Recovery 的先決條件	150
發現 Microsoft SQL Server 工作負載並可選擇從NetApp Backup and Recovery中的SnapCenter匯入	152
使用NetApp Backup and RecoveryMicrosoft SQL Server 工作負載	156
使用NetApp Backup and RecoveryMicrosoft SQL Server 工作負載	159
使用NetApp Backup and RecoveryMicrosoft SQL Server 工作負載	163
使用NetApp Backup and Recovery管理 Microsoft SQL Server 庫存	167
使用NetApp Backup and Recovery管理 Microsoft SQL Server 快照	173
在NetApp Backup and Recovery中為 Microsoft SQL Server 工作負載建立報告	173
保護 VMware 工作負載（無需適用於 VMware 的 SnapCenter 外掛程式）	174

使用NetApp Backup and Recovery保護 VMware 工作負載概述	174
使用NetApp Backup and Recovery發現 VMware 工作負載	174
使用NetApp Backup and Recovery為 VMware 工作負載建立和管理保護群組	178
使用NetApp Backup and RecoveryVMware 工作負載	179
復原 VMware 工作負載	180
保護 KVM 工作負載（預覽版）	190
保護 KVM 工作負載概述	190
發現NetApp Backup and Recovery中的 KVM 工作負載	191
使用NetApp Backup and Recovery為 KVM 工作負載建立和管理保護群組	192
使用NetApp Backup and RecoveryKVM 工作負載	193
使用NetApp Backup and Recovery和還原還原 KVM 虛擬機	194
保護 Hyper-V 工作負載	196
保護 Hyper-V 工作負載概述	196
在NetApp Backup and Recovery中發現 Hyper-V 工作負載	197
使用NetApp Backup and Recovery為 Hyper-V 工作負載建立和管理保護群組	198
使用NetApp Backup and RecoveryHyper-V 工作負載	199
使用NetApp Backup and Recovery復原 Hyper-V 工作負載	200
保護 Oracle Database 工作負載（預覽版）	202
保護 Oracle 資料庫工作負載概述	202
在 NetApp Backup and Recovery 中探索 Oracle Database 工作負載	203
使用 NetApp Backup and Recovery 為 Oracle Database 工作負載建立及管理保護群組	204
使用 NetApp Backup and Recovery 備份 Oracle Database 工作負載	205
使用NetApp Backup and RecoveryOracle 資料庫	206
使用NetApp Backup and Recovery掛載和解除安裝 Oracle 資料庫復原點	209
保護 Kubernetes 工作負載（預覽版）	210
管理 Kubernetes 工作負載概覽	210
探索NetApp Backup and Recovery中的 Kubernetes 工作負載	211
新增和保護 Kubernetes 應用程式	213
恢復 Kubernetes 應用程式	222
管理 Kubernetes 集群	237
管理 Kubernetes 應用程式	237
管理適用於 Kubernetes 工作負載的NetApp Backup and Recovery執行掛鉤模板	238
監控NetApp Backup and Recovery中的作業	241
在作業監視器上查看作業狀態	241
檢討保留（備份生命週期）作業	243
在NetApp Console通知中心查看備份和還原警報	243
在控制台時間軸中查看操作活動	245
重新啟動NetApp Backup and Recovery	245

使用NetApp Backup and Recovery

在NetApp Backup and Recovery儀表板上查看保護健康狀況

監控工作負載的健康狀況可確保您了解工作負載保護的問題並採取措施解決這些問題。在NetApp Backup and Recovery儀表板上查看備份和復原的狀態。您可以查看系統摘要、保護摘要、作業摘要、復原摘要等。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員、備份和還原復原管理員、備份和還原複製管理員或備份和還原檢視器角色。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Console選單中，選擇 保護 > 備份和還原。
2. 選擇一個工作負載圖塊（例如，Microsoft SQL Server）。
3. 從備份和還原選單中，選擇*儀表板*。

您可以查看以下類型的信息：

- 發現的主機或虛擬機器的數量
- 發現的 Kubernetes 叢集數量
- 物件儲存上的備份目標數量
- vCenter 數量
- ONTAP中的儲存叢集數量

查看保護摘要

查看保護摘要中的以下資訊：

- 受保護和不受保護的資料庫、虛擬機器和資料儲存區的總數。



受保護的資料庫是已指派備份策略的資料庫。不受保護的資料庫是未分配備份策略的資料庫。

- 成功、出現警告或失敗的備份次數。
- 備份服務發現的總容量以及受保護的容量和不受保護的容量。將滑鼠懸停在「i」圖示上即可查看詳細資訊。

查看職位摘要

在作業摘要中查看已完成、正在執行或失敗的作業總數。

步驟

1. 對於每個作業分佈，變更篩選器以根據天數顯示失敗、正在執行和完成的摘要，例如過去 30 天、過去 7 天、過去 24 小時或過去 1 年。

2. 透過選擇「檢視作業監控」來查看失敗、正在運作和已完成作業的詳細資訊。

查看還原摘要

查看還原摘要中的以下資訊：

- 執行的恢復作業總數
- 已恢復的總容量
- 在本機、輔助和物件儲存上執行的復原作業的數量。將滑鼠懸停在圖表上即可查看詳細資訊。

建立和管理策略來管理NetApp Backup and Recovery中的備份

在NetApp Backup and Recovery中，建立您自己的策略來控制備份頻率、備份時間以及保留的備份檔案數量。



其中一些選項和配置部分並不適用於所有工作負載。

如果從SnapCenter匯入資源，您可能會發現SnapCenter中使用的策略與NetApp Backup and Recovery中使用的策略存在一些差異。看["SnapCenter與NetApp Backup and Recovery之間的策略差異"](#)。

您可以實現以下與政策相關的目標：

- 建立本機快照策略
- 建立複製到輔助儲存的策略
- 為對象儲存設定建立策略
- 配置進階策略設定
- 編輯策略（不適用於 VMware 預覽工作負載）
- 刪除策略

查看政策

1. 從NetApp Backup and Recovery選單中，選擇 策略。
2. 查看這些政策詳情。
 - 工作負載：範例包括 Microsoft SQL Server、Volumes、VMware、KVM、Hyper-V、Oracle Database 或 Kubernetes。
 - 備份類型：例如完整備份和日誌備份。
 - 架構：範例包括本機快照、扇出、級聯、磁碟到磁碟和磁碟到物件儲存。
 - 受保護的資源：顯示該工作負載的總資源中有多少資源受到保護。
 - 勒索軟體保護：顯示策略是否包含本機快照上的快照鎖定、二級儲存上的快照鎖定或物件儲存上的 DataLock 鎖定。

創建策略

您可以建立策略來管理本機快照、複製到二級儲存以及備份到物件儲存。3-2-1 策略的一部分包括建立主儲存系統上的實例、資料庫、應用程式或虛擬機器的快照。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

開始之前

如果您打算複製到二級儲存並希望在本機快照或遠端ONTAP二級儲存上使用快照鎖定，則首先需要在叢集層級初始化ONTAP合規時脈。這是在政策中啟用快照鎖定的要求。

有關如何執行此操作的說明，請參閱 ["在ONTAP中初始化合規性時鐘"](#)。

有關快照鎖定的一般信息，請參閱 ["ONTAP中的快照鎖定"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 策略。
2. 在「策略」頁面中，選擇「建立新策略」。
3. 在「策略」頁面中，提供以下資訊。

◦ ***詳細資訊***部分：

- 工作負載類型：選擇將使用該策略的工作負載。
- 輸入策略名稱。



若要查看要避免的角色列表，請參閱懸停提示。

- 從*代理*清單中選擇一個控制台代理。

◦ ***備份架構***部分：選擇向下箭頭並選擇備份的資料流，例如 3-2-1 扇出、3-2-1 級聯或磁碟到磁碟。

- **3-2-1 fanout**：主儲存（磁碟）到輔助儲存（磁碟）到雲端（物件儲存）。在不同的儲存系統之間建立多個資料副本，例如 ONTAP 到 ONTAP 以及 ONTAP 到物件儲存的配置。這可以是雲端超大規模物件儲存或私有物件儲存。這些配置有助於實現最佳的資料保護和災難復原。



此選項不適用於Amazon FSx for NetApp ONTAP。

對於 VMware 工作負載，這會在主資料儲存或虛擬機器上配置本機快照，並從主磁碟儲存複製到輔助磁碟儲存以及從主儲存複製到雲端物件儲存。

- **3-2-1 級聯**：（不適用於 Kubernetes 工作負載）主儲存（磁碟）到輔助儲存（磁碟）以及主儲存（磁碟）到雲端儲存（物件儲存）。這可以是雲端超大規模物件儲存或私有物件儲存 - StorageGRID。這會在多個系統之間建立資料複製鏈，以確保冗餘和可靠性。



此選項不適用於Amazon FSx for NetApp ONTAP。

對於 VMware 工作負載，這會在主儲存上的資料儲存區或虛擬機器上配置本機快照，以及從主磁碟儲存到輔助磁碟儲存再到雲端物件儲存的級聯。

- 磁碟到磁碟：（不適用於 Kubernetes 工作負載）主儲存（磁碟）到輔助儲存（磁碟）。ONTAP 到ONTAP資料保護策略在兩個ONTAP系統之間複製數據，以確保高可用性和災難復原。這通常是使用SnapMirror實現的，它支援同步和非同步複製。此方法可確保您的資料持續更新並可在多個位置使用，從而提供強大的資料遺失保護。

對於 VMware 工作負載，這會在主儲存系統上的資料儲存或 VMware 上配置本機快照，然後將資料從主磁碟儲存系統複製到輔助磁碟儲存系統。

- 磁碟到物件儲存：主儲存（磁碟）到雲端（物件儲存）。這會將資料從ONTAP系統複製到物件儲存系統，例如 AWS S3、Azure Blob Storage 或StorageGRID。這通常是使用SnapMirror Cloud 實現的，它透過在初始基線傳輸後僅傳輸更改的資料區塊來提供永久增量備份。這可以是雲端超大規模物件儲存或私有物件儲存 - StorageGRID。此方法非常適合長期資料保留和存檔，為資料保護提供了經濟高效且可擴展的解決方案。

對於 VMWare 工作負載，這會在主資料儲存或虛擬機器上配置本機快照，並從主磁碟儲存到雲端物件儲存進行複製。

- 磁碟到磁碟扇出：（不適用於 Kubernetes 工作負載）主儲存（磁碟）到輔助儲存（磁碟）以及主儲存（磁碟）到輔助儲存（磁碟）。



您可以為磁碟到磁碟扇出選項配置多個輔助設定。

對於 VMware 工作負載，這會將主磁碟儲存配置為輔助磁碟存儲，並將主磁碟儲存複製到輔助磁碟儲存。

- 本機快照：所選磁碟區上的本機快照（Microsoft SQL Server）。本機快照是資料保護策略的關鍵組成部分，可以擷取特定時間點的資料狀態。這將建立工作負載正在運行的生產卷的唯讀、時間點副本。快照佔用的儲存空間極小，且產生的效能開銷可以忽略不計，因為它僅記錄自上次快照以來檔案的變更。您可以使用本機快照來還原資料遺失或損壞，以及為災難復原目的建立備份。

對於 VMware 工作負載，這會在主儲存系統上的資料儲存或虛擬機器上配置本機快照。

建立本機快照策略

提供本地快照的資訊。

- 選擇“新增計劃”選項來選擇快照計劃或計劃。您最多可以有 5 個時間表。
- 快照頻率：選擇每小時、每天、每週、每月或每年的頻率。Kubernetes 工作負載沒有年度頻率。
- 快照保留：輸入要保留的快照數量。
- 啟用日誌備份：（僅適用於 Microsoft SQL Server 工作負載和 Oracle 資料庫工作負載。）啟用此選項可備份日誌並設定日誌備份的頻率和保留。為此，您必須已經配置了日誌備份。看["配置日誌目錄"](#)。
 - 備份後修剪存檔日誌：（僅限 Oracle 資料庫工作負載）如果啟用了日誌備份，您可以選擇啟用此功能來限制備份和還原保留 Oracle 存檔日誌的時間。您可以選擇保留期限以及備份和還原應刪除存檔日誌的位置。
- 提供者：（僅限 Kubernetes 工作負載）選擇託管 Kubernetes 應用程式資源的儲存提供者。

為輔助設定建立策略（複製到輔助儲存）

提供複製到輔助儲存的資訊。本機快照設定的計畫資訊會顯示在輔助設定中。這些設定不適用於 Kubernetes 工作負載。

- 備份：選擇每小時、每天、每週、每月或每年的頻率。
- 備份目標：選擇二級儲存上用於備份的目標系統。
- 保留：輸入要保留的快照數量。
- 啟用快照鎖定：選擇是否要啟用防篡改快照。
- 快照鎖定期限：輸入您想要鎖定快照的天數、月數或年數。
- 轉入中學：
 - 預設情況下，選擇 * ONTAP傳輸計畫 - 內嵌* 選項，表示快照會立即傳輸到二級儲存系統。您不需要安排備份。
 - 其他選項：如果您選擇延期轉帳，則轉帳不是立即進行的，您可以設定時間表。
- * SnapMirror和SnapVault SMAS 二級關係*：對 SQL Server 工作負載使用SnapMirror和SnapVault SMAS 二級關係。

為對象儲存設定建立策略

提供備份到物件儲存的資訊。這些設定被稱為 Kubernetes 工作負載的「備份設定」。



出現的欄位會根據所選的提供者和架構而有所不同。

為 AWS 物件儲存建立策略

在這些欄位中輸入資訊：

- 提供者：選擇*AWS*。
- **AWS 帳戶**：選擇 AWS 帳戶。
- 備份目標：選擇已註冊的 S3 物件儲存目標。確保目標在您的備份環境中可存取。
- **IPspace**：選擇用於備份作業的 IP 空間。如果您有多個 IP 空間並想要控制哪一個用於備份，這將非常有用。
- 計畫設定：選擇為本機快照設定的計畫。您可以刪除計畫，但不能新增計畫，因為計畫是根據本機快照計畫設定的。
- 保留副本：輸入要保留的快照數量。
- 運行於：選擇ONTAP傳輸計畫將資料備份到物件儲存。
- 將備份從物件儲存分層到檔案儲存：如果您選擇將備份分層到檔案儲存（例如，AWS Glacier），請選擇層選項和存檔天數。
- 啟用完整性掃描：（不適用於 Kubernetes 工作負載）選擇是否要在物件儲存上啟用完整性掃描（快照鎖定）。這可確保備份有效並可成功復原。完整性掃描頻率預設為 7 天。為了保護您的備份不被修改或刪除，請選擇*完整性掃描*選項。掃描僅發生在最新的快照上。您可以對最新快照啟用或停用完整性掃描。

為 Microsoft Azure 物件儲存裝置建立策略

在這些欄位中輸入資訊：

- 提供者：選擇*Azure*。
- **Azure 訂閱**：從發現的 Azure 訂閱中選擇。

- **Azure 資源組**：從發現的資源組中選擇 Azure 資源組。
- **備份目標**：選擇已註冊的物件儲存目標。確保目標在您的備份環境中可存取。
- **IPspace**：選擇用於備份作業的 IP 空間。如果您有多個 IP 空間並想要控制哪一個用於備份，這將非常有用。
- **計畫設定**：選擇為本機快照設定的計畫。您可以刪除計畫，但不能新增計畫，因為計畫是根據本機快照計畫設定的。
- **保留副本**：輸入要保留的快照數量。
- **運行於**：選擇ONTAP傳輸計畫將資料備份到物件儲存。
- **將備份從物件儲存分層到檔案儲存**：如果您選擇將備份分層到檔案存儲，請選擇層選項和存檔天數。
- **啟用完整性掃描**：（不適用於 Kubernetes 工作負載）選擇是否要在物件儲存上啟用完整性掃描（快照鎖定）。這可確保備份有效並可成功復原。完整性掃描頻率預設為 7 天。為了保護您的備份不被修改或刪除，請選擇*完整性掃描*選項。掃描僅發生在最新的快照上。您可以對最新快照啟用或停用完整性掃描。

為StorageGRID物件儲存建立策略

在這些欄位中輸入資訊：

- **提供者**：選擇* StorageGRID*。
- *** StorageGRID憑證***：從發現的憑證中選擇StorageGRID憑證。這些憑證用於存取StorageGRID物件儲存系統，並在「設定」選項中輸入。
- **備份目標**：選擇已註冊的 S3 物件儲存目標。確保目標在您的備份環境中可存取。
- **IPspace**：選擇用於備份作業的 IP 空間。如果您有多個 IP 空間並想要控制哪一個用於備份，這將非常有用。
- **計畫設定**：選擇為本機快照設定的計畫。您可以刪除計畫，但不能新增計畫，因為計畫是根據本機快照計畫設定的。
- **保留副本**：輸入每個頻率保留的快照數量。
- **物件儲存的傳輸計畫**：（不適用於 Kubernetes 工作負載）選擇ONTAP傳輸計畫將資料備份到物件儲存。
- **啟用完整性掃描**：（不適用於 Kubernetes 工作負載）選擇是否要在物件儲存上啟用完整性掃描（快照鎖定）。這可確保備份有效並可成功復原。完整性掃描頻率預設為 7 天。為了保護您的備份不被修改或刪除，請選擇*完整性掃描*選項。掃描僅發生在最新的快照上。您可以對最新快照啟用或停用完整性掃描。
- **將備份從物件儲存分層到檔案儲存**：（不適用於 Kubernetes 工作負載）如果您選擇將備份分層到檔案存儲，請選擇層選項和存檔天數。

在策略中配置進階設定

您也可以選擇在策略中配置進階設定。這些設定適用於所有備份架構，包括本機快照、複製到二級儲存以及備份到物件儲存。這些設定不適用於 Kubernetes 工作負載。可用的進階設定將根據您在頁面頂部選擇的工作負載而有所不同，因此此處所述的進階設定可能不適用於所有工作負載。為 Kubernetes 工作負載配置策略時，進階設定不可用。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 策略。
2. 在「策略」頁面中，選擇「建立新策略」。

3. 在「策略 > 進階」設定部分中，選擇「選擇進階操作」選單，從進階設定清單中進行選擇。

4. 啟用您想要查看或更改的任何設置，然後選擇*接受*。

5. 提供以下資訊：

- 僅複製備份：（僅適用於 Microsoft SQL Server 工作負載）如果您需要使用其他備份應用程式備份資源，請選擇僅複製備份（一種 Microsoft SQL Server 備份）。
- 可用性群組設定：（僅適用於 Microsoft SQL Server 工作負載）選擇首選備份副本或指定特定副本。如果您有 SQL Server 可用性群組並且想要控制用於備份的副本，則此設定很有用。
- 最大傳輸速率：若不設定頻寬使用限制，請選擇*無限制*。如果要限制傳輸速率，請選擇*限制*，並選擇指派給將備份上傳到物件儲存的 1 到 1,000 Mbps 之間的網路頻寬。預設情況下，ONTAP 可以使用無限量的頻寬將備份資料從系統中的磁碟區傳輸到物件儲存。如果您注意到備份流量影響了正常的使用者工作負載，請考慮減少傳輸過程中使用的網路頻寬量。
- 備份重試：（不適用於 VMware 工作負載）若要在發生故障或中斷時重試作業，請選擇*啟用故障期間的作業重試*。輸入快照和備份作業重試的最大次數以及重試時間間隔。重新計票數必須少於 10。如果您想要確保在發生故障或中斷時重試備份作業，此設定很有用。



如果快照頻率設定為 1 小時，則最大延遲以及重試次數不應超過 45 分鐘。

- 啟用虛擬機器一致性快照：選擇是否啟用虛擬機器一致性快照。這樣可以確保新建立的快照與建立快照時虛擬機器的狀態保持一致。這有助於確保備份能夠成功恢復，並且資料處於一致狀態。這不適用於現有快照。
- 勒索軟體掃描：選擇是否要在每個儲存桶上啟用勒索軟體掃描。這需要對物件儲存進行 DataLock 鎖定。輸入掃描頻率（以天為單位）。此選項適用於 AWS 和 Microsoft Azure 物件儲存。請注意，此選項可能會產生額外費用，具體取決於雲端提供者。
- 備份驗證：（不適用於 VMware 工作負載）選擇是否要啟用備份驗證以及是否立即或稍後進行。此功能可確保備份有效並可成功復原。我們建議您啟用此選項以確保備份的完整性。預設情況下，如果配置了輔助存儲，則備份驗證從輔助存儲運行。如果未配置輔助存儲，則備份驗證從主存儲運行。

此外，配置以下選項：

- 每日、每週、*每月*或*每年*驗證：如果您選擇*稍後*作為備份驗證，請選擇備份驗證的頻率。這可確保定期檢查備份的完整性並可成功復原。
- 備份標籤：輸入備份的標籤。此標籤用於識別系統中的備份，並可用於追蹤和管理備份。
- 資料庫一致性檢查：（不適用於 VMware 工作負載）選擇是否要啟用資料庫一致性檢查。此選項可確保資料庫在備份之前處於一致狀態，這對於確保資料完整性至關重要。
- 驗證日誌備份：（不適用於 VMware 工作負載）選擇是否要驗證日誌備份。選擇驗證伺服器。如果您選擇磁碟到磁碟或 3-2-1，也請選擇驗證儲存位置。此選項可確保日誌備份有效並可成功恢復，這對於維護資料庫的完整性非常重要。
- 網路：選擇用於備份作業的網路介面。如果您有多個網路介面並想要控制哪一個用於備份，這將非常有用。
 - **IPspace**：選擇用於備份作業的 IP 空間。如果您有多個 IP 空間並想要控制哪一個用於備份，這將非常有用。
 - 私有端點配置：如果您使用私有端點進行物件存儲，請選擇用於備份作業的私有端點配置。如果您想確保備份透過專用網路連線安全傳輸，這將非常有用。
- 通知：選擇是否要為備份操作啟用電子郵件通知。如果您希望在備份作業開始、完成或失敗時收到通知，這將非常有用。

- 獨立磁碟：（僅適用於 VMware 工作負載）選取此項目可將任何包含暫存資料的獨立磁碟資料儲存包含在備份中。獨立磁碟是未包含在 VMware 快照中的 VM 磁碟。
- * SnapMirror磁碟區和快照格式*：（選用）在管理 Microsoft SQL Server 工作負載備份的政策中輸入您的快照名稱。輸入格式和自訂文字。如果您選擇備份到二級存儲，您還可以添加SnapMirror卷前綴和後綴。

編輯策略

您可以編輯備份架構、備份頻率、保留策略和策略的其他設定。

您可以在編輯策略時新增另一個保護級別，但不能刪除保護級別。例如，如果策略僅保護本機快照，則可以將複製新增至輔助儲存或將備份新增至物件儲存。如果您有本機快照和複製，則可以新增物件儲存。但是，如果您有本機快照、複製和物件存儲，則不能刪除其中一個層級。

如果您正在編輯備份到物件儲存的策略，則可以啟用存檔。

如果您從SnapCenter匯入資源，您可能會遇到SnapCenter中使用的政策與NetApp Backup and Recovery中使用的策略之間的一些差異。看["SnapCenter與NetApp Backup and Recovery之間的策略差異"](#)。

所需的**NetApp Console**角色

備份和恢復超級管理員。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 在NetApp Console中，前往 保護 > 備份和還原。
2. 選擇*政策*選項。
3. 選擇要編輯的策略。
4. 選擇*操作*  圖標，然後選擇*編輯*。

刪除策略

如果您不再需要某個策略，則可以將其刪除。



您無法刪除與工作負載關聯的策略。

步驟

1. 在控制台中，前往*保護*>*備份和還原*。
2. 選擇*政策*選項。
3. 選擇要刪除的策略。
4. 選擇*操作*  圖標，然後選擇*刪除*。
5. 確認操作，然後選擇*刪除*。

保護ONTAP磁碟區工作負載

使用NetApp Backup and Recovery保護您的ONTAP卷數據

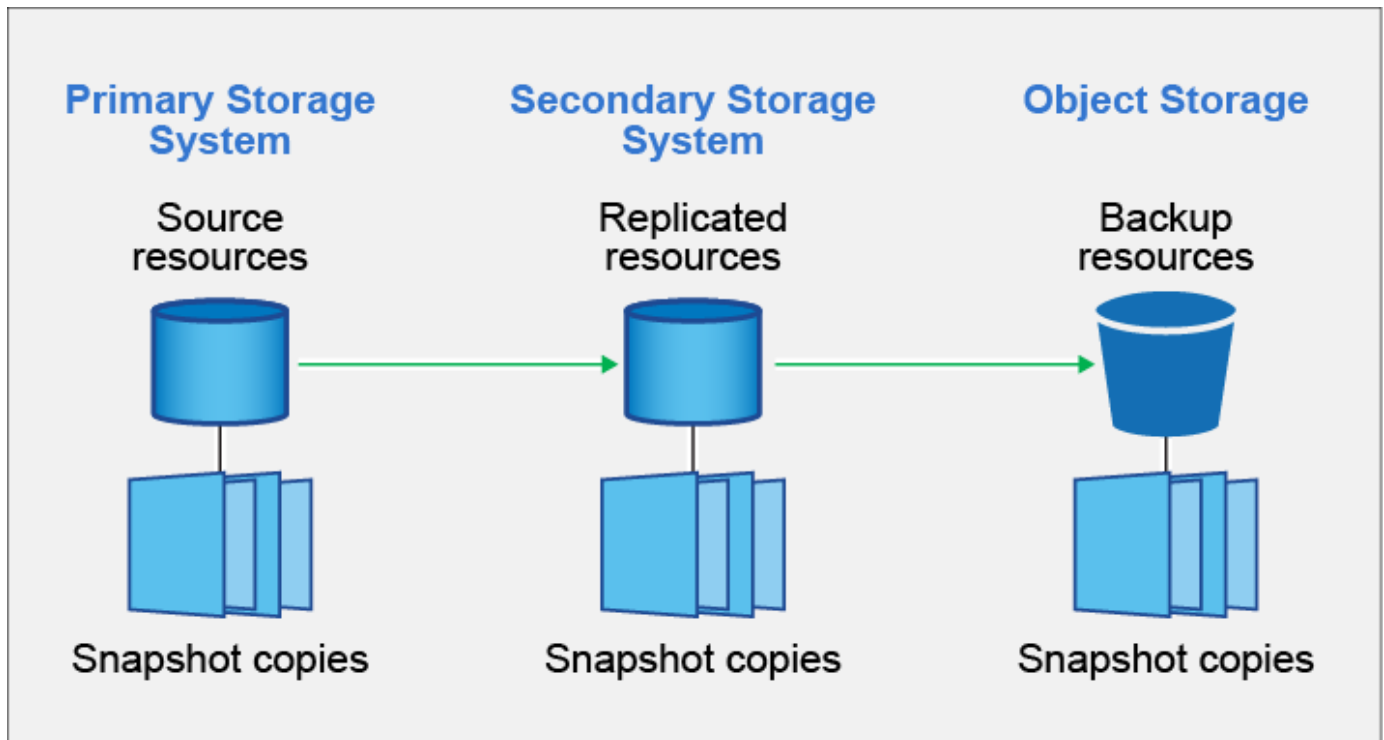
NetApp Backup and Recovery功能，用於保護和長期存檔您的ONTAP磁碟區資料。您可以實施 3-2-1 策略，即在 2 個不同的儲存系統上保留 3 個來源資料副本，並在雲端中保留 1 個副本。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

啟動後，備份和復原會建立區塊級、增量永久備份，這些備份儲存在另一個ONTAP叢集和雲端中的物件儲存中。除了來源磁碟區之外，您還將擁有：

- 來源系統上磁碟區的快照
- 不同儲存系統上的複製卷
- 物件儲存中的磁碟區備份



NetApp Backup and Recovery利用 NetApp 的SnapMirror資料複製技術，透過建立快照並將其傳輸到備份位置，確保所有備份完全同步。

3-2-1 方法的優點包括：

- 多個資料副本可防止內部和外部網路安全威脅。
- 如果一種媒體發生故障，使用不同類型的媒體可以幫助您恢復。
- 您可以從現場副本快速恢復，如果現場副本受到損害，則可以使用異地副本。

必要時，您可以將整個磁碟區、資料夾或一個或多個檔案從任何備份副本還原到相同或不同的系統。

特徵

複製功能：

- 在ONTAP儲存系統之間複製資料以支援備份和災難復原。
- 透過高可用性確保您的 DR 環境的可靠性。
- 透過兩個系統之間的預先共用金鑰 (PSK) 設定的本機ONTAP動態加密。
- 複製的資料是不可變的，直到您使其可寫入並可供使用為止。
- 如果傳輸失敗，複製可以自我修復。
- 與.....相比 ["NetApp Replication"](#)，NetApp Backup and Recovery中的複製包括以下功能：
 - 一次將多個FlexVol磁碟區複製到輔助系統。
 - 使用 UI 將複製的磁碟區還原到來源系統或其他系統。

看["ONTAP磁碟區的複製限制"](#)了解NetApp Backup and Recovery for ONTAP磁碟區不可用的複製功能清單。

備份到物件功能：

- 將資料卷的獨立副本備份到低成本的物件儲存。
- 將單一備份策略套用至群集中的所有捲，或為具有唯一還原點目標的磁碟區指派不同的備份策略。
- 建立備份策略，以應用於叢集中建立的所有未來磁碟區。
- 製作不可變的備份文件，以便在保留期內鎖定和保護它們。
- 掃描備份檔案以查找可能的勒索軟體攻擊 - 並自動刪除/替換受感染的備份。
- 將較舊的備份文件分層到檔案儲存以節省成本。
- 刪除備份關係，以便您可以存檔不需要的來源卷，同時保留磁碟區備份。
- 從雲端備份到雲，從本機系統備份到公有雲或私有雲。
- 備份資料在靜態時透過 AES-256 位元加密保護，在動態時透過 TLS 1.2 HTTPS 連線保護。
- 使用您自己的客戶管理金鑰進行資料加密，而不是使用雲端提供者提供的預設加密金鑰。
- 支援單一磁碟區最多 4,000 個備份。

恢復功能：

- 從物件儲存中的本機快照、複製磁碟區或備份磁碟區還原特定時間點的資料。
- 將磁碟區、資料夾或單一檔案還原到來源系統或其他系統。
- 將資料還原到使用不同訂閱/帳戶或位於不同區域的系統。
- 將磁碟區從雲端儲存快速還原到Cloud Volumes ONTAP系統或本機系統；非常適合需要盡快提供對磁碟區的存取的災難復原情況。
- 在區塊層級恢復數據，將資料直接放置在您指定的位置，同時保留原始 ACL。
- 瀏覽和搜尋檔案目錄，輕鬆選擇單一資料夾和檔案進行單一檔案復原。

支援備份和復原作業的系統

NetApp Backup and Recovery支援ONTAP系統以及公有和私有雲供應商。

支援的區域

NetApp Backup and Recovery在許多 Amazon Web Services、Microsoft Azure 和 Google Cloud 區域中均支援Cloud Volumes ONTAP。

["使用全球區域地圖了解更多信息"](#)

支援的備份目標

NetApp Backup and Recovery讓您能夠將ONTAP磁碟區從下列來源系統備份到下列輔助系統以及公有雲和私有雲供應商中的物件儲存。快照保留在來源系統上。

來源系統	輔助系統（複製）	目標物件儲存（備份）
AWS 中的Cloud Volumes ONTAP	AWS 本機ONTAP系統中的Cloud Volumes ONTAP	亞馬遜 S3
Azure 中的Cloud Volumes ONTAP	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP	Azure Blob
Google 的Cloud Volumes ONTAP	Google 本機ONTAP系統中的Cloud Volumes ONTAP	Google 雲端儲存
本地ONTAP系統	Cloud Volumes ONTAP本地ONTAP系統	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID ONTAP S3

支援的還原目標

您可以將ONTAP資料從位於輔助系統（複製磁碟區）或物件儲存（備份檔案）中的備份檔案還原到下列系統。快照位於來源系統上，並且只能還原到同一系統。

備份檔案位置		目的地系統
物件儲存（備份）	輔助系統（複製）	
亞馬遜 S3	AWS 本機ONTAP系統中的Cloud Volumes ONTAP	AWS 本機ONTAP系統中的Cloud Volumes ONTAP
Azure Blob	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP
Google 雲端儲存	Google 本機ONTAP系統中的Cloud Volumes ONTAP	Google 本機ONTAP系統中的Cloud Volumes ONTAP
NetAppStorageGRID	本機ONTAP系統Cloud Volumes ONTAP	本地ONTAP系統
ONTAP S3	本機ONTAP系統Cloud Volumes ONTAP	本地ONTAP系統

請注意，「本地ONTAP系統」包括FAS、AFF和ONTAP Select系統。

支持的捲

NetApp Backup and Recovery支援以下類型的磁碟區：

- FlexVol讀寫卷
- FlexGroup磁碟區（需要ONTAP 9.12.1 或更高版本）
- SnapLock Enterprise磁碟區（需要ONTAP 9.11.1 或更高版本）
- 適用於本地磁碟區的SnapLock Compliance（需要ONTAP 9.14 或更高版本）
- SnapMirror資料保護 (DP) 目標卷



NetApp Backup and Recovery不支援FlexCache磁碟區的備份。

請參閱["ONTAP磁碟區的備份和還原限制"](#)了解其他要求和限制。

成本

使用NetApp Backup and Recovery與ONTAP系統相關的成本有兩種：資源費用和服務費用。這兩項費用均針對服務的對象部分備份。

建立快照或複製磁碟區不收取任何費用—除了儲存快照和複製磁碟區所需的磁碟空間。

資源費用

資源費用是向雲端提供者支付的，用於物件儲存容量以及將備份檔案寫入和讀取到雲端。

- 對於備份到對象儲存，您需要向雲端提供者支付對象儲存費用。

由於NetApp Backup and Recovery保留了來源磁碟區的儲存效率，因此您需要向雲端提供者物件儲存支付ONTAP效率之後的資料費用（針對應用程式重複資料刪除和壓縮後的較少量的資料）。

- 對於使用「搜尋和還原」還原數據，您的雲端提供者會提供某些資源，並且您的搜尋要求掃描的數據量會產生每 TiB 成本。（瀏覽和恢復不需要這些資源。）
 - 在 AWS 中，["亞馬遜雅典娜"](#)和 ["AWS Glue"](#)資源部署在新的 S3 儲存桶中。
 - 在 Azure 中，["Azure Synapse 工作區"](#)和 ["Azure 資料湖儲存"](#)在您的儲存帳戶中配置以儲存和分析您的資料。
 - 在 Google 中，部署了一個新的儲存桶，並且 ["Google Cloud BigQuery 服務"](#)在帳戶/項目層級進行配置。
- 如果您打算從已移動到檔案物件儲存的備份檔案中恢復磁碟區數據，則雲端提供者會收取額外的每 GiB 檢索費用和每個請求費用。
- 如果您打算在恢復磁碟區資料的過程中掃描備份檔案中的勒索軟體（如果您已為雲端備份啟用了 DataLock 和勒索軟體復原功能），那麼您還將產生來自雲端提供者的額外出口成本。

服務費

服務費用支付給NetApp，涵蓋建立物件儲存備份的成本以及從這些備份中還原磁碟區或檔案的成本。您只需為物件儲存中保護的資料付費，該費用會根據備份到物件儲存的ONTAP磁碟區的來源邏輯使用容量（ONTAP效率之前）計算。此容量也稱為前端兆位元組 (FETB)。

有三種方式可以支付備份服務費用。第一個選項是從您的雲端供應商訂閱，這樣您就可以按月付費。第二種選擇是簽訂年度合約。第三種選擇是直接從NetApp購買授權。

授權

NetApp Backup and Recovery適用於以下消費模式：

- **BYOL**：從NetApp購買的許可證，可與任何雲端提供者一起使用。
- **PAYGO**：從您的雲端供應商市場按小時訂閱。
- **年度**：來自雲端提供者市場的年度合約。

僅當從物件儲存進行備份和還原時才需要備份許可證。建立快照和複製磁碟區不需要許可證。

自備駕照

BYOL 是基於期限（1、2 或 3 年）和容量的，以 1 TiB 為增量。您向NetApp付費以使用該服務一段時間（例如 1 年）以及最大容量（例如 10 TiB）。

您將收到一個序號，請在NetApp Console中輸入該序號以啟用該服務。當達到任一限制時，您都需要更新許可證。備份 BYOL 授權適用於與您的NetApp Console組織或帳號關聯的所有來源系統。

["了解如何管理您的 BYOL 許可證"](#)。

按需付費訂閱

NetApp Backup and Recovery以按需付費模式提供基於消費的授權。透過雲端供應商的市場訂閱後，您需要按 GiB 為備份資料付費 - 無需預付款。您的雲端提供者將透過每月帳單向您收費。

["了解如何設定即用即付訂閱"](#)。

請注意，當您首次註冊 PAYGO 訂閱時，可以享受 30 天的免費試用。

年度合約

使用 AWS 時，有兩種年度合約可供選擇，期限分別為 1 年、2 年或 3 年：

- 「雲端備份」計畫可讓您備份Cloud Volumes ONTAP資料和本機ONTAP資料。
- 「CVO Professional」計畫可讓您捆綁Cloud Volumes ONTAP和NetApp Backup and Recovery。這包括根據此許可證收費的Cloud Volumes ONTAP磁碟區的無限備份（備份容量不計入許可證）。

使用 Azure 時，有兩種年度合約可供選擇，分別為 1 年、2 年或 3 年：

- 「雲端備份」計畫可讓您備份Cloud Volumes ONTAP資料和本機ONTAP資料。
- 「CVO Professional」計畫可讓您捆綁Cloud Volumes ONTAP和NetApp Backup and Recovery。這包括根據此許可證收費的Cloud Volumes ONTAP磁碟區的無限備份（備份容量不計入許可證）。

當您使用 GCP 時，您可以向NetApp要求私人優惠，然後在NetApp Backup and Recovery啟動期間從 Google Cloud Marketplace 訂閱時選擇該計劃。

["了解如何制定年度合約"](#)。

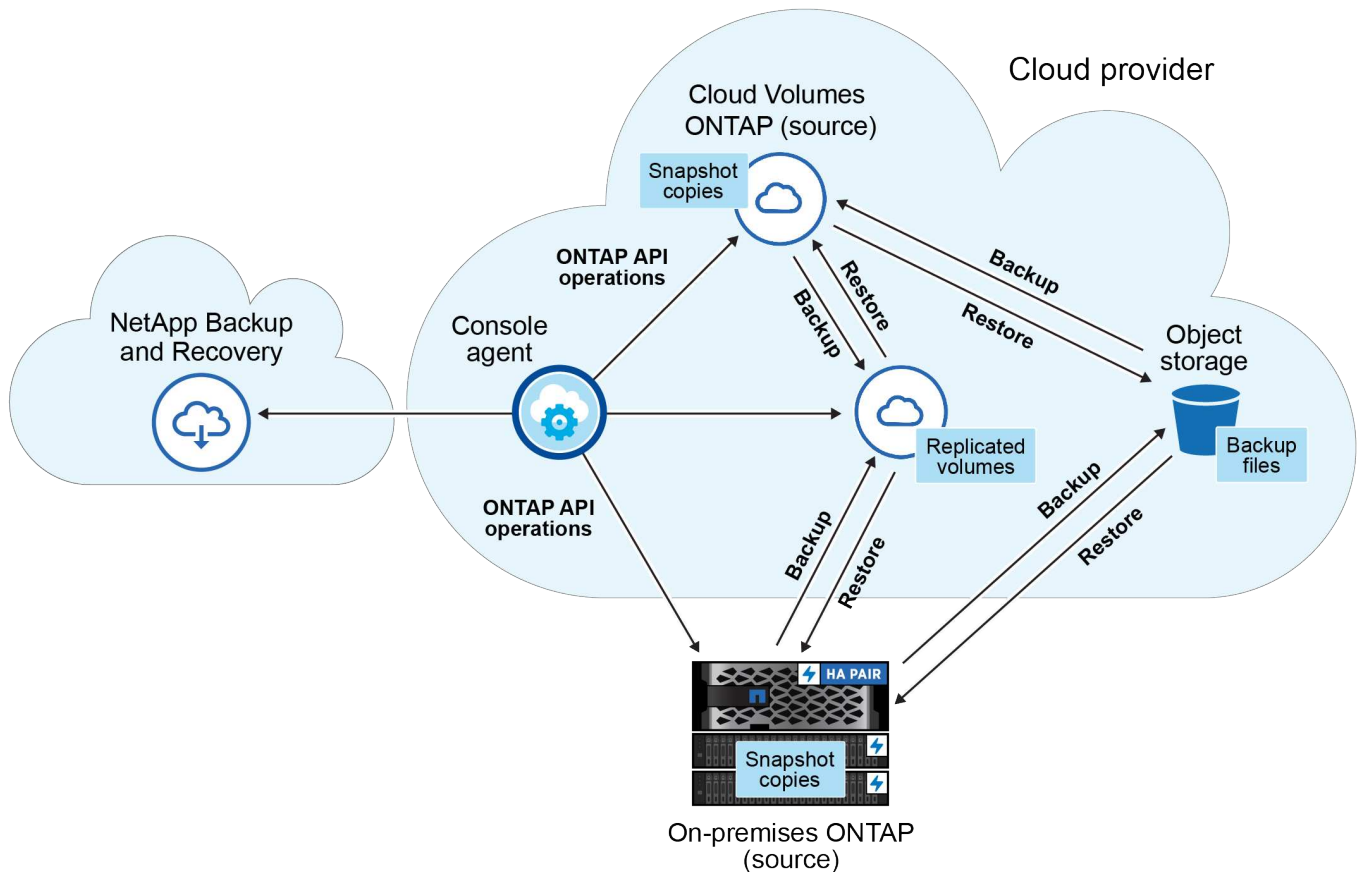
NetApp Backup and Recovery的工作原理

當您在Cloud Volumes ONTAP或本機ONTAP系統上啟用NetApp Backup and Recovery時，本服務會對您的資料執行完整備份。初始備份之後，所有附加備份都是增量的，這意味著只備份更改的區塊和新區塊。這使得網路流量保持最低限度。物件儲存備份建立在 "[NetApp SnapMirror雲端技術](#)"。



直接從您的雲端提供者環境採取的任何管理或更改雲端備份檔案的操作都可能損壞檔案並導致不受支援的配置。

下圖顯示了各個組件之間的關係：



此圖顯示磁碟區被複製到Cloud Volumes ONTAP系統，但磁碟區也可以複製到本機ONTAP系統。

備份所在位置

根據備份類型，備份位於不同的位置：

- 快照儲存在來源系統的來源磁碟區上。
- 複製磁碟區駐留在二級儲存系統上 - Cloud Volumes ONTAP或本機ONTAP系統。
- 備份副本儲存在控制台在您的雲端帳戶中建立的物件儲存中。每個集群/系統有一個物件存儲，控制台將物件存儲命名為：「netapp-backup-clusteruid」。請確保不要刪除此物件存儲。
 - 在 AWS 中，控制台可以實現 "[Amazon S3 阻止公共存取功能](#)" 在 S3 鏟斗上。
 - 在 Azure 中，控制台使用新的或現有的資源群組，並為 Blob 容器指派儲存帳戶。主機 "[阻止公眾存取您的 Blob 數據](#)" 預設情況下。

- 在 GCP 中，控制台使用具有 Google Cloud Storage 儲存桶儲存帳戶的新專案或現有專案。
- 在StorageGRID中，控制台使用現有的租用戶帳戶來管理 S3 儲存桶。
- 在ONTAP S3 中，控制台使用 S3 儲存桶的現有使用者帳戶。

如果您將來想要更改叢集的目標物件存儲，則需要["取消註冊系統的NetApp Backup and Recovery"](#)，然後使用新的雲端供應商資訊啟用NetApp Backup and Recovery。

可自訂的備份計劃和保留設置

當您為系統啟用NetApp Backup and Recovery時，您最初選擇的所有磁碟區都會使用您選擇的策略進行備份。您可以為快照、複製磁碟區和備份檔案選擇不同的策略。如果您想要為具有不同復原點目標 (RPO) 的某些磁碟區指派不同的備份策略，則可以為該叢集建立其他策略，並在啟動NetApp Backup and Recovery後將這些原則指派給其他磁碟區。

您可以選擇所有捲的每小時、每天、每週、每月和每年備份的組合。對於物件備份，您還可以選擇系統定義的策略之一，提供 3 個月、1 年和 7 年的備份和保留。您使用ONTAP System Manager 或ONTAP CLI 在叢集上建立的備份保護原則也會作為選擇出現。這包括使用自訂SnapMirror標籤建立的策略。



應用於磁碟區的快照策略必須具有您在複製策略和備份到物件策略中使用的標籤之一。如果未找到符合的標籤，則不會建立備份檔案。例如，如果您想要建立「每週」複製磁碟區和備份文件，則必須使用建立「每週」快照的快照策略。

一旦達到某個類別或間隔的最大備份數量，較舊的備份就會被刪除，以便您始終擁有最新的備份（因此過時的備份不會繼續佔用空間）。



資料保護磁碟區備份的保留期與來源SnapMirror關係中定義的保留期相同。如果您願意，可以使用 API 來變更此設定。

備份檔案保護設定

如果您的叢集使用ONTAP 9.11.1 或更高版本，您可以保護物件儲存中的備份免於刪除和勒索軟體攻擊。每個備份策略都為_DataLock 和勒索軟體復原_提供了一個部分，可以在特定時間段（即_保留期_）內應用於您的備份檔案。

- *DataLock* 保護您的備份檔案不被修改或刪除。
- 勒索軟體保護 會在建立備份檔案時以及恢復備份檔案中的資料時掃描您的備份檔案以查找勒索軟體攻擊的證據。

預設啟用計劃的勒索軟體防護掃描。掃描頻率的預設為 7 天。掃描僅發生在最新的快照上。可以停用計劃掃描以降低成本。您可以透過「進階設定」頁面上的選項，啟用或停用最新快照上的計畫勒索軟體掃描。如果啟用它，則預設每週執行一次掃描。您可以將該計劃更改為幾天或幾週，或停用它，以節省成本。

備份保留期與備份計畫保留期相同，再加上最多 31 天的緩衝期。例如，每週備份保留 5 份副本，每個備份檔案將鎖定 5 週。每月備份保留 6 份副本，每個備份檔案將鎖定 6 個月。

當您的備份目標是 Amazon S3、Azure Blob 或NetApp StorageGRID時，目前可獲得支援。未來版本中將新增其他儲存提供者目的地。

欲了解更多詳細信息，請參閱以下信息：

- ["DataLock 和勒索軟體保護的工作原理"](#)。
- ["如何在「進階設定」頁面中更新勒索軟體防護選項"](#)。



如果您將備份分層到檔案存儲，則無法啟用 DataLock。

舊備份文件的存檔存儲

使用某些雲端儲存時，您可以在一定天數後將較舊的備份檔案移至較便宜的儲存類別/存取層。您也可以選擇立即將備份檔案傳送到檔案存儲，而無需寫入標準雲端儲存。請注意，如果您啟用了 DataLock，則無法使用檔案儲存。

- 在 AWS 中，備份從「標準」儲存類別開始，並在 30 天後轉換到「標準-不頻繁存取」儲存類別。

如果您的叢集使用的是 ONTAP 9.10.1 或更高版本，您可以選擇在一定天數後將舊備份分層到 NetApp Backup and Recovery UI 中的“S3 Glacier”或“S3 Glacier Deep Archive”存儲，以進一步優化成本。["了解有關 AWS 檔案儲存的更多信息"](#)。

- 在 Azure 中，備份與 *Cool* 存取層相關聯。

如果您的叢集使用的是 ONTAP 9.10.1 或更高版本，您可以選擇在一定天數後將舊備份分層到 NetApp Backup and Recovery UI 中的“Azure Archive”存儲，以進一步優化成本。["了解有關 Azure 檔案儲存的更多信息"](#)。

- 在 GCP 中，備份與 *Standard* 儲存類別相關聯。

如果您的叢集使用的是 ONTAP 9.12.1 或更高版本，您可以選擇在一定天數後將舊備份分層到 NetApp Backup and Recovery UI 中的「Archive」儲存中，以進一步最佳化成本。["詳細了解 Google 歸檔存儲"](#)。

- 在 StorageGRID 中，備份與 *Standard* 儲存類別相關聯。

如果您的本機叢集使用的是 ONTAP 9.12.1 或更高版本，而您的 StorageGRID 系統使用的是 11.4 或更高版本，則可以在一定天數後將較舊的備份檔案存檔到公有雲存檔儲存。目前支援 AWS S3 Glacier/S3 Glacier Deep Archive 或 Azure Archive 儲存層。["了解有關從 StorageGRID 歸檔備份檔案的更多信息"](#)。

有關存檔舊備份文件的詳細信息，請參閱 [xref:./prev-ontap-policy-object-options.html](#)。

FabricPool 分層策略注意事項

當您要備份的磁碟區位於 FabricPool 聚合上，並且指派了分層策略時，您需要注意以下幾點 *none*：

- FabricPool 分層磁碟區的第一次備份需要讀取所有本機和所有分層資料（從物件儲存）。備份作業不會「重新加熱」物件儲存中分層的冷資料。

此操作可能會導致從雲端供應商讀取資料的成本一次性增加。

- 後續備份是增量的，不會產生這種影響。
- 如果在最初建立磁碟區時將分層策略指派給磁碟區，則您將不會看到此問題。

- 在分配之前考慮備份的影響 `all` 對磁碟區進行分層策略。由於資料是立即分層的，NetApp Backup and Recovery 將從雲層而不是本地層讀取資料。由於並發備份操作共享與雲端物件儲存的網路鏈接，因此如果網路資源飽和，可能會出現效能下降。在這種情況下，您可能需要主動配置多個網路介面 (LIF) 來減少這種類

型的網路飽和。

使用NetApp Backup and Recovery規劃您的保護之旅

NetApp Backup and Recovery使您能夠建立最多三個來源磁碟區副本來保護您的資料。在磁碟區上啟用備份和還原時，您可以選擇許多選項，因此您應該檢查您的選擇以做好準備。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

我們將討論以下選項：

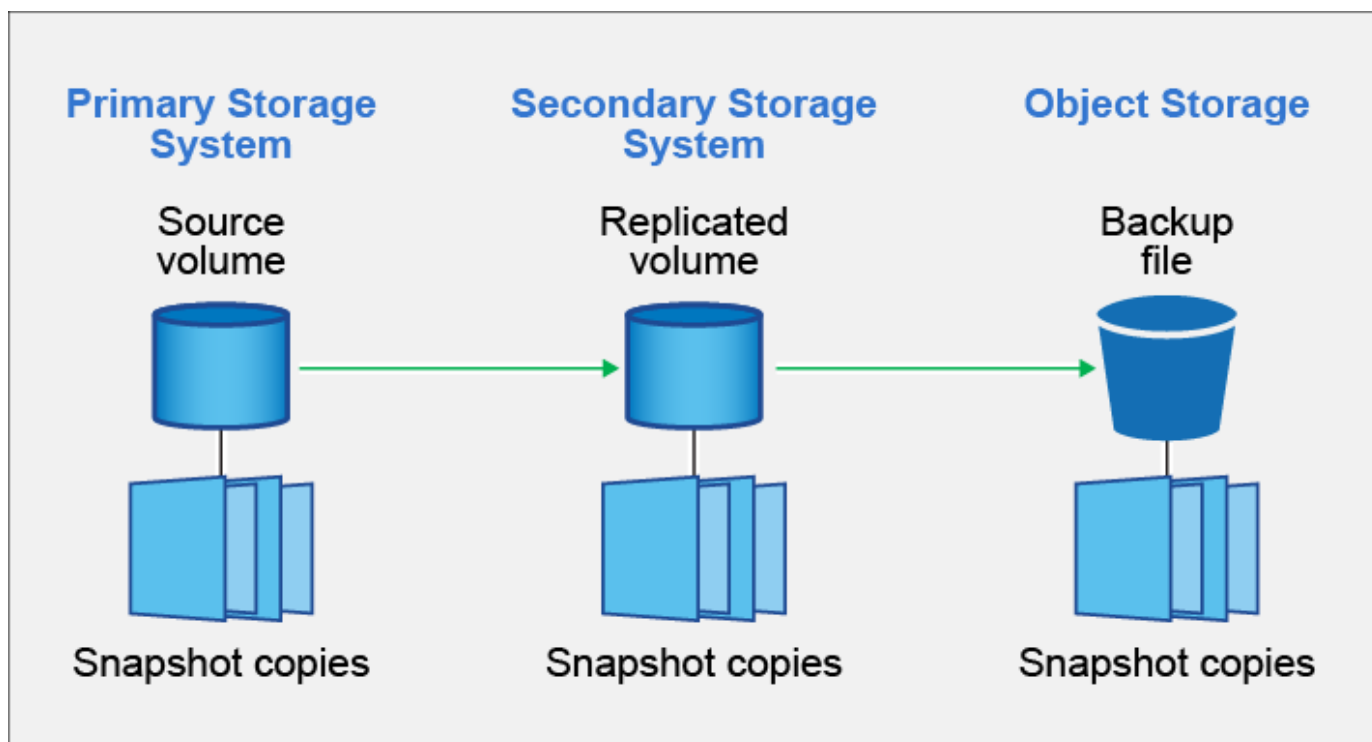
- 您將使用哪些保護功能：快照、複製磁碟區和/或雲端備份
- 您將使用哪種備份架構：磁碟區的級聯備份還是磁軌備份
- 您是否會使用預設備份策略，還是需要建立自訂策略
- 您希望服務為您建立雲端儲存桶，還是希望在開始之前建立物件儲存容器
- 您使用哪種控制台代理部署模式（標準、受限或私有模式）

您將使用哪些保護功能

在您選擇要使用的功能之前，這裡先簡單介紹一下每個功能的作用以及它提供的保護類型。

備份類型	描述
快照	建立來源磁碟區中某個磁碟區的唯一、時間點映像作為快照。您可以使用快照來還原單一文件，或還原整個磁碟區的內容。
複製	在另一個ONTAP儲存系統上建立資料的輔助副本並不斷更新輔助資料。您的資料將保持最新狀態，並在您需要時隨時可用。
雲端備份	將您的資料備份到雲端，以進行保護並用於長期存檔。如果需要，您可以將磁碟區、資料夾或單一檔案從備份還原到相同或不同的系統。

快照是所有備份方法的基礎，是使用備份和還原服務的必要條件。快照是磁碟區的唯一、時間點影像。此映像佔用極少的儲存空間，由於它只記錄自上次快照建立以來檔案發生的更改，因此效能開銷可以忽略不計。在磁碟區上建立的快照用於保持複製磁碟區和備份檔案與來源磁碟區所做的變更保持同步—如圖所示。



您可以選擇在另一個ONTAP儲存系統上建立複製卷，並在雲端中建立備份檔案。或者您可以選擇僅建立複製磁碟區或備份檔案 - 這是您的選擇。

總而言之，這些是您可以為ONTAP系統中的磁碟區建立的有效保護流程：

- 來源磁碟區 → 快照 → 複製磁碟區 → 備份文件
- 來源磁碟區 → 快照 → 備份文件
- 來源卷 → 快照 → 複製卷



複製磁碟區或備份檔案的初始建立包括來源資料的完整副本 - 這稱為「基線傳輸」。後續傳輸僅包含來源資料的差異副本（快照）。

不同備份方法的比較

下表顯示了三種備份方法的總體比較。雖然物件儲存空間通常比本地磁碟儲存便宜，但如果您認為您可能會頻繁地從雲端恢復數據，那麼雲端提供者的出口費用可能會減少您的一些節省。您需要確定需要多久從雲端中的備份檔案還原資料。

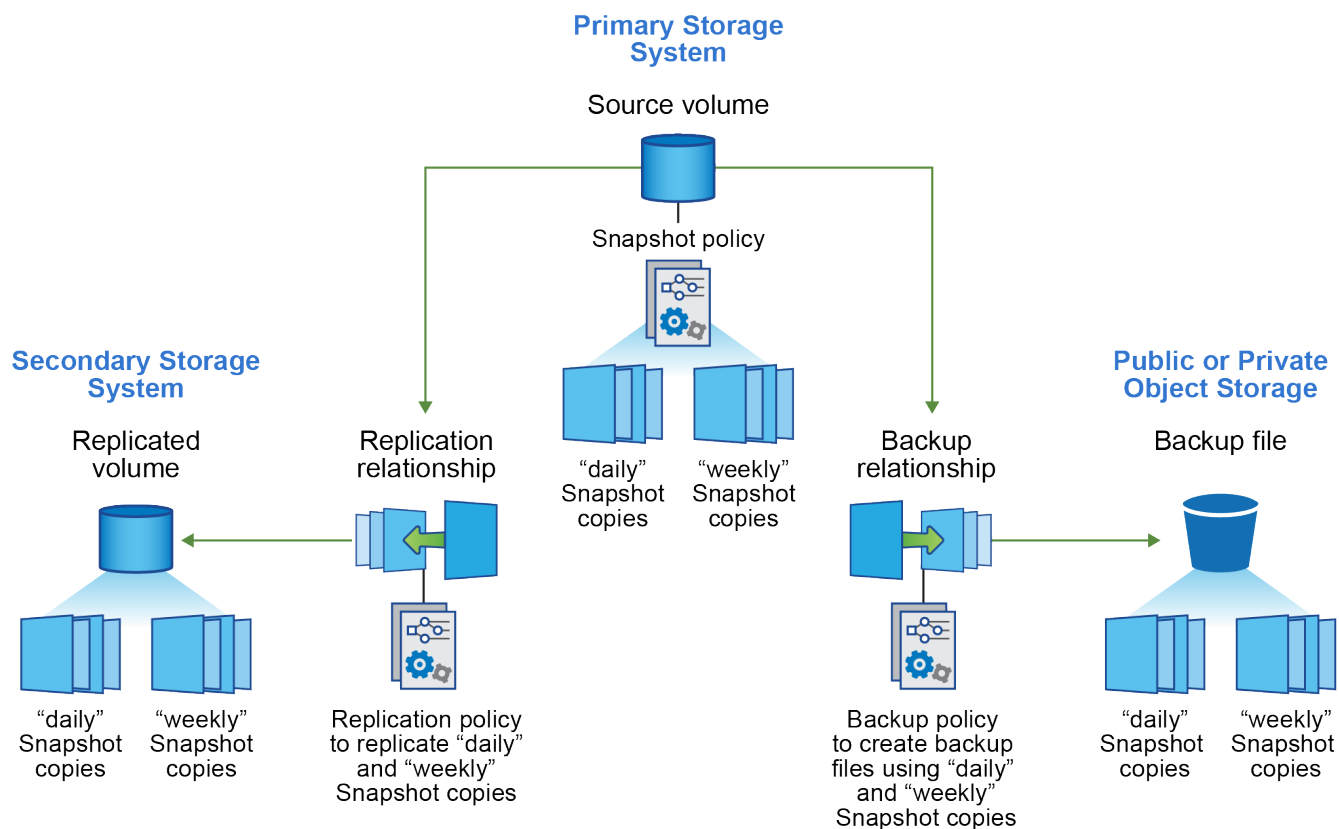
除了此標準之外，如果您使用 DataLock 和勒索軟體復原功能，雲端儲存還可以提供額外的安全性選項，並且透過為舊備份檔案選擇存檔儲存類別可以節省額外的成本。["了解有關 DataLock 和勒索軟體保護以及檔案儲存設定的更多信息"](#)。

備份類型	備份速度	備份成本	恢復速度	恢復成本
快照	高的	低（磁碟空間）	高的	低的
複製	中等的	中等（磁碟空間）	中等的	中（網路）
雲端備份	低的	低（物體空間）	低的	高（提供者費用）

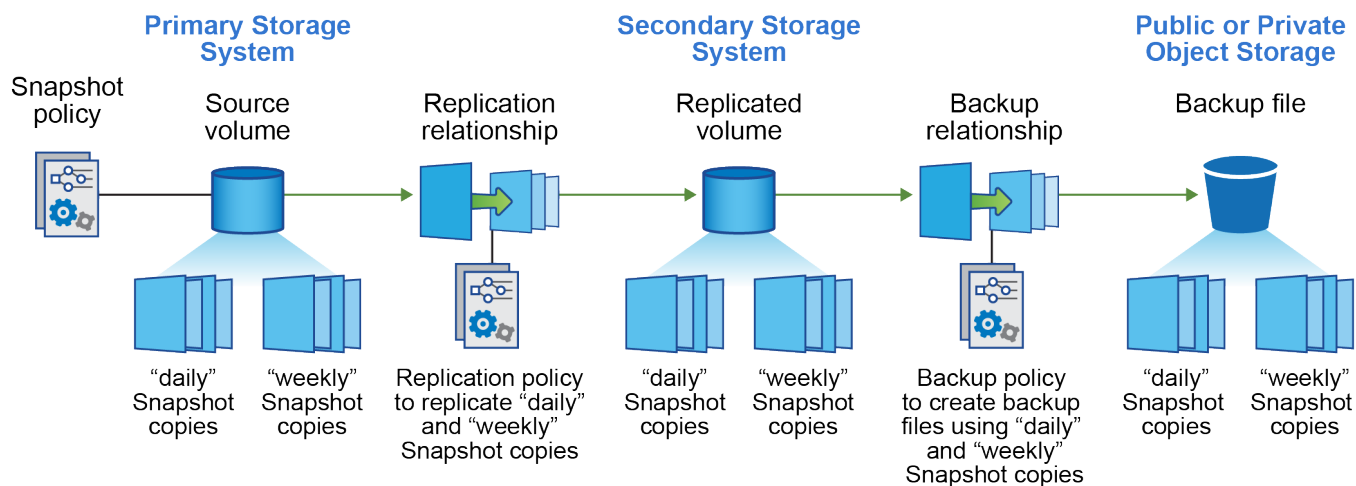
您將使用哪種備份架構

在建立複製磁碟區和備份檔案時，您可以選擇磁軌或級聯架構來備份磁碟區。

扇出式架構將快照獨立傳輸到目標儲存系統和雲端備份物件。



級聯架構首先將快照傳輸到目標儲存系統，然後該系統將副本傳輸到雲端的備份物件。



不同架構選擇的比較

此表提供了扇出型和級聯型架構的比較。

扇出	級聯
由於來源系統需要向兩個不同的系統發送快照，因此對來源系統的效能影響很小。	對來源儲存系統的效能影響較小，因為它只發送一次快照。
更易於設置，因為所有策略、網路和ONTAP配置都在來源系統上完成	還需要從輔助系統完成一些網路和ONTAP配置。

您是否會使用快照、複製和備份的預設策略

您可以使用NetApp提供的預設策略來建立備份，也可以建立自訂策略。當您使用啟動精靈為您的磁碟區啟用備份和復原服務時，您可以從預設原則和系統中已經存在的任何其他策略（Cloud Volumes ONTAP或本機ONTAP系統）中進行選擇。如果您想使用與現有策略不同的策略，您可以在開始之前或使用啟動精靈時建立該策略。

- 預設快照策略會建立每小時、每天和每週快照，保留 6 個每小時快照、2 個每天快照和 2 個每週快照。
- 預設複製策略複製每日和每週快照，保留 7 個每日快照和 52 個每週快照。
- 預設備份策略複製每日和每週快照，保留 7 個每日快照和 52 個每週快照。

如果您為複製或備份建立自訂策略，則策略標籤（例如「每日」或「每週」）必須與快照策略中存在的標籤匹配，否則將不會建立複製的磁碟區和備份檔案。

您可以在NetApp Backup and RecoveryUI 中建立快照、複製和備份到物件儲存策略。請參閱["新增新的備份策略"](#)了解詳情。

除了使用NetApp Backup and Recovery建立自訂策略之外，您還可以使用 System Manager 或ONTAP命令列介面 (CLI)：

- ["使用 System Manager 或ONTAP CLI 建立快照策略"](#)
- ["使用 System Manager 或ONTAP CLI 建立複製策略"](#)

注意：使用系統管理員時，選擇*非同步*作為複製策略的策略類型，並選擇*非同步*和*備份到雲端*作為備份到物件策略。

以下是一些ONTAP CLI 命令範例，如果您要建立自訂策略，這些命令可能會有所幫助。請注意，您必須使用_admin_ vservice（儲存虛擬機器）作為`<vservice\_name>`在這些命令中。

政策描述	命令
簡單快照策略	<code>snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vservice ClusterA -snapmirror-label1 weekly</code>
簡單備份到雲端	<code>snapmirror policy create -policy <policy_name> -transfer -priority normal -vservice <vservice_name> -create -snapshot-on-source false -type vault snapmirror policy add-rule -policy <policy_name> -vservice <vservice_name> -snapmirror-label <snapmirror_label> -keep</code>

政策描述	命令
使用 DataLock 和勒索軟體保護功能備份到雲端	<pre> snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name> snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days </pre>
使用歸檔儲存類別備份到雲端	<pre> snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>
簡單複製到另一個儲存系統	<pre> snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name> snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>



只有保險庫策略可用於備份到雲端關係。

我的政策在哪裡？

根據您計劃使用的備份架構，備份策略位於不同的位置：扇出式或級聯式。複製策略和備份策略的設計方式不同，因為複製將兩個ONTAP儲存系統配對，而物件備份使用儲存提供者作為目標。

- 快照策略始終駐留在主儲存系統上。
- 複製策略始終駐留在輔助儲存系統上。
- 備份到物件策略是在來源磁碟區所在的系統上建立的 - 這是扇出配置的主集群，也是級聯配置的輔助集群。

這些差異如表所示。

架構	快照策略	複製策略	備份策略
扇出	基本的	次要	基本的
級聯	基本的	次要	次要

因此，如果您計劃在使用級聯架構時建立自訂策略，則需要在將建立複製磁碟區的輔助系統上建立複製和備份到物件策略。如果您打算在使用扇出架構時建立自訂策略，則需要在將建立複製磁碟區的輔助系統上建立複製策略，並在主系統上備份到物件原則。

如果您使用所有ONTAP系統上存在的預設策略，那麼一切就都設定好了。

你想建立自己的物件儲存容器嗎

當您在系統的物件儲存中建立備份檔案時，預設情況下，備份和復原服務會在您配置的物件儲存帳戶中為備份檔案建立容器（儲存桶或儲存帳戶）。AWS 或 GCP 儲存桶預設為「netapp-backup-<uuid>」。Azure Blob 儲存帳戶名稱為「netappbackup<uuid>」。

如果您想要使用某個前綴或指派特殊屬性，您可以在物件提供者帳戶中自行建立容器。如果您想建立自己的容器，則必須在啟動啟動精靈之前建立它。NetApp Backup and Recovery可以使用任何儲存桶並共用儲存桶。備份啟動精靈將自動發現所選帳戶和憑證的設定容器，以便您選擇要使用的容器。

您可以從控制台或雲端提供者建立儲存桶。

- ["從控制台建立 Amazon S3 儲存桶"](#)
- ["從控制台建立 Azure Blob 儲存體帳戶"](#)
- ["從控制台建立 Google Cloud Storage 儲存桶"](#)

如果您打算使用與「netapp-backup-xxxxxx」不同的儲存桶前綴，則需要修改控制台代理 IAM 角色的 S3 權限。

進階儲存桶設定

如果您打算將較舊的備份檔案移至檔案存儲，或者如果您打算啟用 DataLock 和勒索軟體保護來鎖定備份檔案並掃描其中是否存在可能的勒索軟體，則需要使用某些設定來建立容器：

- 目前，當您在叢集上使用ONTAP 9.10.1 或更高版本軟體時，AWS S3 儲存裝置支援您自己的儲存桶上的存檔儲存。預設情況下，備份從 S3 *Standard* 儲存類別開始。確保使用適當的生命週期規則建立儲存桶：
 - 30 天後將整個儲存桶範圍內的物件移至 S3 *Standard-IA*。
 - 將標籤「smc_push_to_archive: true」的物件移到_Glacier Flexible Retrieval_（以前稱為 S3 Glacier）
- 當叢集上使用ONTAP 9.11.1 或更高版本軟體時，AWS 儲存支援 DataLock 和勒索軟體保護；當使用ONTAP 9.12.1 或更高版本軟體時，Azure 儲存支援 DataLock 和勒索軟體保護。
 - 對於 AWS，您必須使用 30 天的保留期在儲存桶上啟用物件鎖定。
 - 對於 Azure，您需要建立具有版本級不變性支援的儲存體類別。

您正在使用哪種控制台代理部署模式

如果您已經使用控制台來管理您的存儲，那麼控制台代理已經安裝。如果您打算將相同的控制台代理與NetApp Backup and Recovery一起使用，那麼一切就緒了。如果您需要使用不同的控制台代理，則需要在開始備份和還原實作之前安裝它。

NetApp Console提供多種部署模式，讓您能夠以滿足業務和安全要求的方式使用控制台。_標準模式_利用控制台 SaaS 層提供全部功能，而_限制模式_和_私人模式_適用於有連線限制的組織。

["了解有關NetApp Console部署模式的更多信息"](#)。

支援具有完整網路連線的網站

當在具有完全互聯網連接（也稱為_標準模式_或_SaaS 模式_）的網站中使用NetApp Backup and Recovery時，您可以在控制台管理的任何本地ONTAP或Cloud Volumes ONTAP系統上建立複製卷，並且可以在任何受支援的雲端提供者的物件儲存上建立備份檔案。["查看受支援的備份目標的完整列表"](#)。

有關有效控制台代理位置的列表，請參閱您計劃建立備份檔案的雲端提供者的以下備份程式之一。存在一些限制，控制台代理必須手動安裝在 Linux 機器上或部署在特定的雲端提供者中。

- ["將Cloud Volumes ONTAP資料備份到 Amazon S3"](#)
- ["將Cloud Volumes ONTAP資料備份到 Azure Blob"](#)

- "將Cloud Volumes ONTAP資料備份到 Google Cloud"
- "將本地ONTAP資料備份到 Amazon S3"
- "將本機ONTAP資料備份到 Azure Blob"
- "將本地ONTAP資料備份到 Google Cloud"
- "將本地ONTAP資料備份到StorageGRID"
- "將本地ONTAP備份到ONTAP S3"

支援網路連線有限的網站

NetApp Backup and Recovery可用於網際網路連線受限的網站（也稱為「受限模式」）來備份磁碟區資料。在這種情況下，您需要在目標雲端區域部署控制台代理程式。

- 您可以將資料從本機ONTAP系統或安裝在 AWS 商業區域的Cloud Volumes ONTAP系統備份到 Amazon S3。"將Cloud Volumes ONTAP資料備份到 Amazon S3"。
- 您可以將資料從本機ONTAP系統或安裝在 Azure 商業區域中的Cloud Volumes ONTAP系統備份到 Azure Blob。"將Cloud Volumes ONTAP資料備份到 Azure Blob"。

支援沒有網路連線的網站

NetApp Backup and Recovery可用於沒有網路連線的網站（也稱為_私有模式_或_暗站_）來備份磁碟區資料。在這種情況下，您需要在同一網站的 Linux 主機上部署控制台代理程式。



BlueXP私有模式（傳統BlueXP介面）通常用於沒有網路連線的本機環境和安全雲端區域，其中包括 AWS Secret Cloud、AWS Top Secret Cloud 和 Azure IL6。NetApp繼續透過傳統的BlueXP介面支援這些環境。有關舊版BlueXP介面中的私人模式文檔，請參閱 ["BlueXP私人模式的 PDF 文檔"](#)。

- 您可以將資料從本機ONTAP系統備份到本機NetApp StorageGRID系統。"將本地ONTAP資料備份到StorageGRID"。
- 您可以將資料從本機ONTAP系統備份到本機ONTAP系統或為 S3 物件儲存配置的Cloud Volumes ONTAP系統。"將本地ONTAP資料備份到ONTAP S3"。

使用NetApp Backup and Recovery管理ONTAP磁碟區的備份策略

使用NetApp Backup and Recovery，使用NetApp提供的預設備份策略來建立備份，或建立自訂策略。策略控制備份頻率、備份時間以及保留的備份檔案數量。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

當您使用啟動精靈為您的磁碟區啟用備份和復原服務時，您可以從預設原則和系統中已經存在的任何其他策略（Cloud Volumes ONTAP或本機ONTAP系統）中進行選擇。如果您想使用與現有策略不同的策略，您可以在使用啟動精靈之前或使用啟動精靈時建立該策略。

若要了解提供的預設備份策略，請參閱["規劃您的保育之旅"](#)。

NetApp Backup and Recovery提供三種類型的ONTAP資料備份：快照、複製和物件儲存備份。根據您使用的架

構和備份類型，它們的策略位於不同的位置：

架構	快照策略儲存位置	複製策略儲存位置	備份到物件策略儲存位置
扇出	基本的	次要	基本的
級聯	基本的	次要	次要

根據您的環境、偏好和保護類型，使用以下工具建立備份策略：

- NetApp Console 介面
- 系統管理器使用者介面
- ONTAP 命令列介面



使用系統管理員時，選擇*非同步*作為複製策略的策略類型，並選擇*非同步*和*備份到雲端*作為備份到物件策略。

查看系統的策略

1. 在控制台 UI 中，選擇 磁碟區 > 備份設定。
 2. 從備份設定頁面，選擇系統，選擇*操作*  圖標，然後選擇*策略管理*。
- 出現「策略管理」頁面。預設顯示快照策略。
3. 若要查看系統中存在的其他策略，請選擇「複製策略」或「備份策略」。如果現有策略可用於您的備份計劃，則一切就緒。如果您需要具有不同特徵的策略，您可以從此頁面建立新策略。

創建策略

您可以建立策略來管理物件儲存的快照、複製和備份：

- [\[啟動快照之前建立快照策略\]](#)
- [\[在啟動複製之前建立複製策略\]](#)
- [\[在啟動備份之前建立備份到物件儲存策略\]](#)

啟動快照之前建立快照策略

3-2-1 策略的一部分包括建立主儲存系統上磁碟區的快照。

策略創建過程的一部分涉及識別表示計劃和保留的快照和 SnapMirror 標籤。您可以使用預定義標籤或建立自己的標籤。

步驟

1. 在控制台 UI 中，選擇 磁碟區 > 備份設定。
 2. 從備份設定頁面，選擇系統，選擇*操作*  圖標，然後選擇*策略管理*。
- 出現「策略管理」頁面。
3. 在策略頁面中，選擇*建立策略* > 建立快照策略。

4. 指定策略名稱。
5. 選擇一個或多個快照計劃。您最多可以有 5 個標籤。或者，建立一個時間表。
6. 如果您選擇建立時間表：
 - a. 選擇每小時、每天、每週、每月或每年的頻率。
 - b. 指定表示計劃和保留的快照標籤。
 - c. 輸入拍攝快照的時間和頻率。
 - d. 保留：輸入要保留的快照數量。
7. 選擇“創建”。

使用級聯架構的快照策略範例

此範例建立具有兩個叢集的快照策略：

1. 集群 1：
 - a. 在策略頁面上選擇集群 1。
 - b. 忽略複製和備份到物件策略部分。
 - c. 建立快照策略。
2. 集群 2：
 - a. 在策略頁面上選擇集群 2。
 - b. 忽略快照策略部分。
 - c. 配置複製和備份到物件策略。

在啟動複製之前建立複製策略

您的 3-2-1 策略可能包括在不同的儲存系統上複製磁碟區。複製策略位於*輔助*儲存系統上。

步驟

1. 在「策略」頁面中，選擇「建立策略」>「建立複製策略」。
2. 在「策略詳細資料」部分中，指定策略名稱。
3. 指定SnapMirror標籤（最多 5 個）以表示每個標籤的保留。
4. 指定傳輸時間表。
5. 選擇“創建”。

在啟動備份之前建立備份到物件儲存策略

您的 3-2-1 策略可能包括將磁碟區備份到物件儲存。

根據備份架構，此儲存策略位於不同的儲存系統位置：

- 扇出：主儲存系統
- 級聯：二級儲存系統

步驟

1. 在策略管理頁面中，選擇*建立策略* > 建立備份策略。
2. 在「策略詳細資料」部分中，指定策略名稱。
3. 指定SnapMirror標籤（最多 5 個）以表示每個標籤的保留。
4. 指定設置，包括傳輸計劃和何時存檔備份。
5. （可選）要在一定天數後將較舊的備份檔案移至較便宜的儲存類別或存取層，請選擇*存檔*選項並指示存檔資料之前應經過的天數。輸入 0 作為「存檔天數」以將備份檔案直接傳送到存檔儲存。

["了解有關檔案存儲設置的更多信息"](#)。

6. （可選）為保護您的備份不被修改或刪除，請選擇*DataLock 和勒索軟體保護*選項。

如果您的叢集使用的是ONTAP 9.11.1 或更高版本，您可以選擇透過設定「DataLock」和「勒索軟體保護」來保護您的備份免於刪除。

["了解有關可用 DataLock 設定的更多信息"](#)。

7. 選擇“創建”。

編輯策略

您可以編輯自訂快照、複製或備份策略。

更改備份策略會影響所有使用該策略的磁碟區。

步驟

1. 在策略管理頁面中，選擇策略，選擇*操作*  圖標，然後選擇*編輯策略*。



複製和備份策略的過程相同。

2. 在「編輯策略」頁面中進行變更。
3. 選擇*儲存*。

刪除策略

您可以刪除與任何磁碟區均不關聯的策略。

如果某個策略與某個磁碟區關聯，並且您想要刪除該策略，則必須先從該磁碟區中刪除該策略。

步驟

1. 在策略管理頁面中，選擇策略，選擇*操作*  圖標，然後選擇*刪除快照策略*。
2. 選擇*刪除*。

查找更多信息

有關使用 System Manager 或ONTAP CLI 建立政策的說明，請參閱下列內容：

["使用 System Manager 建立 Snapshot 策略"](#) ["使用ONTAP CLI 建立 Snapshot 策略"](#) ["使用 System Manager 建](#)

NetApp Backup and Recovery中的備份到物件原則選項

NetApp Backup and Recovery讓您能夠為本機ONTAP和Cloud Volumes ONTAP系統建立具有各種設定的備份策略。



這些策略設定僅與備份到物件儲存相關。這些設定都不會影響您的快照或複製策略。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

備份計畫選項

NetApp Backup and Recovery使您能夠為每個系統（叢集）建立具有唯一計劃的多個備份策略。您可以為具有不同復原點目標 (RPO) 的磁碟區指派不同的備份策略。

每個備份策略都提供了一個「標籤和保留」部分，您可以將其套用至備份檔案。請注意，應用於磁碟區的 Snapshot 策略必須是NetApp Backup and Recovery識別的策略之一，否則將不會建立備份檔案。

該計劃分為兩部分：標籤和保留值：

- 標籤 定義了從磁碟區建立（或更新）備份檔案的頻率。您可以從以下標籤類型中進行選擇：
 - 您可以選擇*每小時*、每天、每週、*每月*和*每年*時間範圍中的一個或多個組合。
 - 您可以選擇系統定義的策略之一，提供 3 個月、1 年或 7 年的備份和保留。
 - 如果您已使用ONTAP System Manager 或ONTAP CLI 在叢集上建立了自訂備份保護策略，則可以選擇其中一個原則。
- *保留*值定義每個標籤（時間範圍）保留多少個備份檔案。一旦達到某個類別或間隔內的最大備份數量，較舊的備份就會被刪除，以便您始終擁有最新的備份。這還可以節省您的儲存成本，因為過時的備份不會繼續佔用雲端中的空間。

例如，假設您建立備份策略，該策略會建立 7 個 每週 備份和 12 個 每月 備份：

- 每周和每月都會為卷創建一個備份文件
- 在第 8 週，刪除第一個每週備份，並新增第 8 週的新每週備份（最多保留 7 個每週備份）
- 在第 13 個月，刪除第一個月度備份，並新增第 13 個月的新月度備份（最多保留 12 個月度備份）

年度備份在傳輸到物件儲存後會自動從來源系統中刪除。可以在系統的進階設定頁面中變更此預設行為。

DataLock 和勒索軟體保護選項

NetApp Backup and Recovery為您的磁碟區備份提供 DataLock 和勒索軟體保護支援。這些功能使您能夠鎖定備份檔案並對其進行掃描以偵測備份檔案上可能存在的勒索軟體。這是一個可選設置，當您希望為叢集的磁碟區備份提供額外保護時，可以在備份策略中定義它。

這兩個功能都可以保護您的備份文件，以便在您的備份遭受勒索軟體攻擊時，您始終擁有一個有效的備份文件來恢復資料。滿足某些監管要求也很有幫助，在這些要求中，備份需要被鎖定並保留一段時間。啟用 DataLock 和

勒索軟體復原選項後，作為NetApp Backup and Recovery啟動的一部分配置的雲端儲存桶將啟用物件鎖定和物件版本控制。

此功能不會為您的來源磁碟區提供保護；僅為這些來源磁碟區的備份提供保護。使用一些 ["ONTAP提供的反勒索軟體保護"](#)保護您的來源磁碟區。



- 如果您打算使用 DataLock 和勒索軟體保護，則可以在建立第一個備份策略並為該叢集啟動NetApp Backup and Recovery時啟用它。您可以稍後使用NetApp Backup and Recovery進階設定啟用或停用勒索軟體掃描。
- 當控制台在恢復磁碟區資料時掃描備份檔案中的勒索軟體時，您將產生來自雲端提供者的額外出口成本以存取備份檔案的內容。

什麼是DataLock

借助此功能，您可以鎖定透過SnapMirror複製到雲端的雲端快照，還可以啟用該功能來偵測勒索軟體攻擊並恢復物件儲存上快照的一致副本。此功能在 AWS、Azure、Google Cloud Platform 和StorageGRID上均支援。

DataLock 可保護您的備份檔案在一定時間內不被修改或刪除 - 也稱為_不可變儲存_。此功能使用物件儲存提供者的技術進行「物件鎖定」。

雲端提供者使用保留截止日期 (RUD)，它是根據快照保留期計算的。快照保留期是根據備份策略中定義的標籤和保留計數計算的。

最短快照保留期為 30 天。讓我們看一些例子來了解它的工作原理：

- 如果您選擇保留計數為 20 的 **Daily** 標籤，則快照保留期為 20 天，預設為最短 30 天。
- 如果您選擇保留計數為 4 的 **每週** 標籤，則快照保留期為 28 天，預設為最短 30 天。
- 如果您選擇保留計數為 3 的「**每月**」標籤，則快照保留期為 90 天。
- 如果您選擇保留計數為 1 的 **每年** 標籤，則快照保留期為 365 天。

什麼是保留截止日期 (RUD)？如何計算？

保留截止日期 (RUD) 根據快照保留期確定。保留截止日期是透過將快照保留期與緩衝區相加來計算的。

- 緩衝為轉移時間緩衝（3天）+成本最佳化緩衝（28天），總計31天。
- 最短保留截止日期為 30 天 + 31 天緩衝期 = 61 天。

以下是一些範例：

- 如果您建立具有 12 個保留的每月備份計劃，則您的備份將被鎖定 12 個月（加 31 天），然後才會被刪除（由下一個備份檔案取代）。
- 如果您建立的備份策略建立 30 個每日備份、7 個每週備份和 12 個每月備份，則有三個鎖定保留期：
 - 「每日 30 次」備份將保留 61 天（30 天加上 31 天緩衝），
 - 「每週 7 次」備份保留 11 週（7 週加 31 天），且
 - 「12 個月」備份將保留 12 個月（加 31 天）。
- 如果您建立具有 24 個保留的每小時備份計劃，您可能會認為備份已鎖定 24 小時。但是，由於該時間少於 30 天的最低限制，因此每個備份將被鎖定並保留 61 天（30 天加上 31 天的緩衝時間）。



舊備份將在 DataLock 保留期到期後刪除，而不是在備份策略保留期到期後刪除。

DataLock 保留設定將覆蓋備份策略中的策略保留設定。這可能會影響您的儲存成本，因為您的備份檔案將在物件儲存中保存更長時間。

啟用 **DataLock** 和勒索軟體保護

您可以在建立策略時啟用 DataLock 和勒索軟體保護。建立策略後，您無法啟用、修改或停用此功能。

1. 建立策略時，展開「DataLock 和勒索軟體彈性」部分。
2. 選擇下列選項之一：
 - 無：DataLock 保護和勒索軟體復原功能已停用。
 - 已解鎖：DataLock 保護和勒索軟體復原功能已啟用。具有特定權限的使用者可以在保留期內覆蓋或刪除受保護的備份檔案。
 - 已鎖定：DataLock 保護和勒索軟體復原功能已啟用。在保留期內，任何使用者都不能覆蓋或刪除受保護的備份檔案。這滿足了完全的監管合規性。

參考["如何在「進階設定」頁面中更新勒索軟體防護選項"](#)。

什麼是勒索軟體保護

勒索軟體防護會掃描您的備份檔案以尋找勒索軟體攻擊的證據。勒索軟體攻擊的偵測是使用校驗和比較來執行的。如果在新的備份檔案與先前的備份檔案中發現潛在的勒索軟體，則該較新的備份檔案將被未顯示任何勒索軟體攻擊跡象的最新備份檔案取代。（被判定為遭受勒索軟體攻擊的檔案在被替換1天後被刪除。）

掃描發生在以下情況：

- 雲端備份物件傳輸到雲端物件儲存後，很快就會啟動雲端備份物件的掃描。當備份檔案首次寫入雲端儲存時，不會執行掃描，而是在寫入下一個備份檔案時執行掃描。
- 當選擇備份進行復原程序時，可以啟動勒索軟體掃描。
- 可以隨時按需進行掃描。

恢復過程如何進行？

當偵測到勒索軟體攻擊時，該服務使用 Active Data Console 代理 Integrity Checker REST API 來啟動復原程序。資料物件最舊的版本是事實來源，並作為復原過程的一部分轉換為當前版本。

讓我們看看它是如何運作的：

- 如果發生勒索軟體攻擊，該服務會嘗試覆蓋或刪除儲存桶中的物件。
- 由於雲端儲存支援版本控制，它會自動建立備份物件的新版本。如果在啟用版本控制的情況下刪除對象，則會將其標記為已刪除，但仍可檢索。如果物件被覆蓋，則會儲存並標記先前的版本。
- 當啟動勒索軟體掃描時，將驗證兩個物件版本的校驗和並進行比較。如果校驗和不一致，則表示偵測到了潛在的勒索軟體。
- 恢復過程涉及恢復到最後一個已知的良好副本。

支援的系統和對象儲存提供者

在下列公有和私有雲供應商中使用物件儲存時，您可以從下列系統在ONTAP磁碟區上啟用 DataLock 和勒索軟體保護。

來源系統	備份檔案目標位置
AWS 中的Cloud Volumes ONTAP	亞馬遜 S3
Azure 中的Cloud Volumes ONTAP	Azure Blob
Google Cloud 中的Cloud Volumes ONTAP	Google雲
本地ONTAP系統	Amazon S3 Azure Blob Google Cloud NetApp StorageGRID

要求

- 對於 AWS：
 - 您的叢集必須執行ONTAP 9.11.1 或更高版本
 - 控制台代理可以部署在雲端或您的本地
 - 以下 S3 權限必須是提供控制台代理權限的 IAM 角色的一部分。它們位於資源「arn:aws:s3:::netapp-backup-*」的「backupS3Policy」部分：

AWS S3 權限

- s3:取得物件版本標記
- s3：取得儲存桶物件鎖配置
- s3:取得物件版本Acl
- s3：PutObjectTagging
- s3：刪除對象
- s3：刪除物件標記
- s3：取得對象保留
- s3：刪除物件版本標記
- s3：Put對象
- s3：獲取對象
- s3:PutBucketObjectLock配置
- s3:獲取生命週期配置
- s3：取得儲存桶標記
- s3：刪除物件版本
- s3：列出儲存桶版本
- s3：列表桶
- s3：PutBucket標記
- s3:取得物件標記
- s3：PutBucket版本控制
- s3：PutObjectVersionTagging
- s3：取得儲存桶版本
- s3：取得儲存桶Acl
- s3：繞過治理保留
- s3：PutObjectRetention
- s3：取得儲存桶位置
- s3：取得物件版本

"[查看策略的完整 JSON 格式](#)，您可以在其中複製並貼上所需的權限"。

- 對於 Azure：
 - 您的叢集必須執行ONTAP 9.12.1 或更高版本
 - 控制台代理可以部署在雲端或您的本地
- 對於 Google Cloud：
 - 您的叢集必須執行ONTAP 9.17.1 或更高版本

- 控制台代理可以部署在雲端或您的本地
- 對於StorageGRID：
 - 您的叢集必須執行ONTAP 9.11.1 或更高版本
 - 您的StorageGRID系統必須執行 11.6.0.3 或更高版本
 - 控制台代理必須部署在您的場所（可以安裝在有或沒有網路存取的網站）
 - 以下 S3 權限必須是提供控制台代理權限的 IAM 角色的一部分：

StorageGRID S3 權限

- s3:取得物件版本標記
- s3：取得儲存桶物件鎖配置
- s3:取得物件版本Acl
- s3：PutObjectTagging
- s3：刪除對象
- s3：刪除物件標記
- s3：取得對象保留
- s3：刪除物件版本標記
- s3：Put對象
- s3：獲取對象
- s3:PutBucketObjectLock配置
- s3:獲取生命週期配置
- s3：取得儲存桶標記
- s3：刪除物件版本
- s3：列出儲存桶版本
- s3：列表桶
- s3：PutBucket標記
- s3:取得物件標記
- s3：PutBucket版本控制
- s3：PutObjectVersionTagging
- s3：取得儲存桶版本
- s3：取得儲存桶Acl
- s3：PutObjectRetention
- s3：取得儲存桶位置
- s3：取得物件版本

限制

- 如果您在備份策略中配置了檔案存儲，則 DataLock 和勒索軟體保護功能不可用。
- 啟動 NetApp Backup and Recovery 時選擇的 DataLock 選項必須用於該叢集的所有備份策略。
- 您無法在單一叢集上使用多種 DataLock 模式。
- 如果啟用 DataLock，所有磁碟區備份都將被鎖定。您不能為單一叢集混合鎖定和非鎖定磁碟區備份。
- DataLock 和勒索軟體保護適用於使用啟用了 DataLock 和勒索軟體保護的備份策略的新磁碟區備份。您可以稍後使用進階設定選項啟用或停用這些功能。
- 只有在使用 ONTAP 9.13.1 或更高版本時，FlexGroup 磁碟區才能使用 DataLock 和勒索軟體保護。

如何降低 DataLock 成本的技巧

您可以啟用或停用勒索軟體掃描功能，同時保持 DataLock 功能處於活動狀態。為了避免額外費用，您可以停用計劃的勒索軟體掃描。這使您可以自訂安全設定並避免產生雲端提供者的費用。

即使停用了計劃的勒索軟體掃描，您仍然可以在需要時執行按需掃描。

您可以選擇不同等級的保護：

- 無需勒索軟體掃描的 **DataLock**：為目標儲存中的備份資料提供保護，可以處於治理模式或合規模式。
 - 治理模式：為管理員提供覆蓋或刪除受保護資料的彈性。
 - 合規模式：在保留期到期之前提供完全不可磨滅性。這有助於滿足嚴格監管環境中最嚴格的資料安全要求。資料在其生命週期內無法被覆蓋或修改，為您的備份副本提供最強大的保護等級。



Microsoft Azure 使用鎖定和解鎖模式。

- 具有勒索軟體掃描的 **DataLock**：為您的資料提供額外的安全保護。此功能有助於檢測任何更改備份副本的嘗試。如果進行任何嘗試，則會謹慎地建立新版本的資料。掃描頻率可以變更為 1、2、3、4、5、6 或 7 天。如果將掃描設定為每 7 天一次，則成本會顯著降低。

有關降低 DataLock 成本的更多提示，請參閱 <https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475>

此外，您還可以造訪以下網站以取得與 DataLock 相關的成本估算：["NetApp Backup and Recovery 總擁有成本 \(TCO\) 計算器"](#)。

檔案存儲選項

使用 AWS、Azure 或 Google 雲端儲存時，您可以在一定天數後將較舊的備份檔案移至較便宜的存檔儲存類別或存取層。您也可以選擇立即將備份檔案傳送到檔案存儲，而無需寫入標準雲端儲存。只需輸入 0 作為「幾天後存檔」即可將備份檔案直接傳送到檔案儲存。對於很少需要存取雲端備份資料的用戶或正在替換磁帶備份解決方案的用戶來說，這尤其有用。

存檔層中的資料在需要時無法立即訪問，並且需要更高的檢索成本，因此在決定存檔備份檔案之前，您需要考慮需要多久從備份檔案中還原一次資料。



- 即使您選擇「0」將所有資料區塊傳送到檔案雲端存儲，元資料區塊也始終寫入標準雲端儲存。
- 如果您啟用了 DataLock，則無法使用檔案儲存。
- 選擇 0 天（立即存檔）後，您無法變更存檔策略。

每個備份策略都提供了一個「存檔策略」部分，您可以將其套用至備份檔案。

- 在 AWS 中，備份從「標準」儲存類別開始，並在 30 天後轉換到「標準-不頻繁存取」儲存類別。

如果您的叢集使用的是 ONTAP 9.10.1 或更高版本，您可以將較舊的備份分層到 *S3 Glacier* 或 *S3 Glacier Deep Archive* 儲存。"[了解有關 AWS 檔案儲存的更多信息](#)"。

- 如果您在啟動 NetApp Backup and Recovery 時在第一個備份策略中未選擇任何存檔層，那麼 *S3 Glacier* 將是您未來策略的唯一存檔選項。
 - 如果您在第一個備份策略中選擇了“S3 Glacier”，那麼您可以將該叢集的未來備份策略變更為“S3 Glacier Deep Archive”層。
 - 如果您在第一個備份策略中選擇“S3 Glacier Deep Archive”，則該層將是該叢集未來備份策略唯一可用的存檔層。
- 在 Azure 中，備份與 *Cool* 存取層相關聯。

如果您的叢集使用的是 ONTAP 9.10.1 或更高版本，則可以將舊備份分層到 *Azure Archive* 儲存。"[了解有關 Azure 檔案儲存的更多信息](#)"。

- 在 GCP 中，備份與 *Standard* 儲存類別相關聯。

如果您的本地叢集使用的是 ONTAP 9.12.1 或更高版本，您可以選擇在一定天數後將舊備份分層到 NetApp Backup and Recovery UI 中的「Archive」儲存中，以進一步最佳化成本。"[詳細了解 Google 歸檔存儲](#)"。

- 在 StorageGRID 中，備份與 *Standard* 儲存類別相關聯。

如果您的本地叢集使用 ONTAP 9.12.1 或更高版本，並且您的 StorageGRID 系統使用 11.4 或更高版本，則可以將較舊的備份檔案存檔到公有雲檔案儲存。

- 對於 AWS，您可以將備份分層儲存到 AWS *S3 Glacier* 或 *S3 Glacier Deep Archive* 儲存中。"[了解有關 AWS 檔案儲存的更多信息](#)"。
- 對於 Azure，您可以將較舊的備份分層儲存到 *Azure Archive* 儲存體中。"[了解有關 Azure 檔案儲存的更多信息](#)"。

在 NetApp Backup and Recovery 和還原進階設定中管理備份到物件儲存選項

您可以使用「進階設定」頁面變更在為每個 ONTAP 系統啟動 NetApp Backup and Recovery 時設定的叢集等級、備份到物件儲存設定。您也可以修改一些作為「預設」備份設定的設定。這包括更改備份到物件儲存的傳輸速率、是否將歷史快照匯出為備份文件，以及啟用或停用系統的勒索軟體掃描。



這些設定僅適用於備份到物件儲存。這些設定都不會影響您的快照或複製設定。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

您可以在進階設定頁面中變更以下選項：

- 變更授予ONTAP系統存取物件儲存權限的儲存金鑰
- 變更連接到物件儲存的ONTAP IP 空間
- 使用「最大傳輸速率」選項變更指派給上傳備份到物件儲存的網路頻寬
- 更改是否將歷史快照匯出為備份檔案並將其包含在未來磁碟區的初始基線備份檔案中
- 更改是否從來源系統中刪除“年度”快照
- 啟用或停用系統的勒索軟體掃描，包括計畫掃描

查看叢集等級備份設定

您可以查看每個系統的叢集級系統設定和提供者設定。

步驟

1. 從控制台選單中，選擇*保護>備份和還原*。
2. 從*Volumes*選項卡中，選擇*Backup Settings*。
3. 在「備份設定」頁面中，選擇... 選擇「配置進階設定 > 系統設定」檢視系統設置，選擇「配置進階設定 > 提供者設定」查看提供者設定。

產生的頁面會顯示該系統的目前設定。查看提供者設定時，顯示的提供者設定與您在頁面頂部選擇的儲存桶相關。

請注意，根據來源叢集上的ONTAP版本和備份所在的雲端供應商目標位置，某些選項不可用。

變更可用於將備份上傳到物件儲存的網路頻寬

當您為系統啟動NetApp Backup and Recovery時，預設情況下，ONTAP可以使用無限量的頻寬將備份資料從系統中的磁碟區傳送到物件儲存。如果您注意到備份流量影響了正常的使用者工作負載，您可以使用「進階設定」頁面中的最大傳輸速率選項來限制傳輸過程中使用的網路頻寬量。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 在「備份設定」頁面中，按一下... 在系統中，選擇「配置進階設定 > 系統設定」。
3. 在進階設定頁面中，展開*最大傳輸速率*部分。
4. 選擇 1 到 1,000 Mbps 之間的值作為最大傳輸速率。
5. 選擇*Limited*單選按鈕並輸入可使用的最大頻寬，或選擇*Unlimited*表示沒有限制。
6. 選擇*應用*。

此設定不會影響分配給系統中磁碟區配置的任何其他複製關係的頻寬。

更改是否將歷史快照匯出為備份文件

如果存在與本系統中使用的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則可以將這些歷史快照匯出到物件儲存作為備份檔案。這樣，您就可以透過將較舊的快照移至基準備份副本中來初始化雲端備份。

請注意，此選項僅適用於新讀/寫卷的新備份文件，並且不支援資料保護 (DP) 磁碟區。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 在「備份設定」頁面中，按一下 ... 在系統中，選擇「配置進階設定 > 系統設定」。
3. 在「進階設定」頁面中，展開「匯出現有快照副本」部分。
4. 選擇是否要匯出現有快照。
5. 選擇*應用*。

更改是否從來源系統中刪除“年度”快照

當您為任何磁碟區選擇「年度」備份策略標籤時，建立的快照將非常大。預設情況下，這些年度快照在傳輸到物件儲存後會自動從來源系統中刪除。您可以從「年度快照刪除」部分變更此預設行為。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 在「備份設定」頁面中，按一下 ... 在系統中，選擇「配置進階設定 > 系統設定」。
3. 在進階設定頁面中，展開*年度快照刪除*部分。
4. 選擇“停用”以在來源系統上保留年度快照。
5. 選擇*應用*。

啟用或停用勒索軟體掃描

預設啟用勒索軟體防護掃描。掃描頻率的預設為 7 天。掃描僅發生在最新的快照上。

有關 DataLock 和勒索軟體恢復選項的詳細信息，請參閱["DataLock 和勒索軟體復原選項"](#)。

您可以將該計劃更改為幾天或幾週，或停用它，以節省成本。



根據雲端提供者的不同，啟用勒索軟體掃描將產生額外費用。

如果停用計劃的勒索軟體掃描，您仍然可以執行按需掃描，並且恢復操作期間的掃描仍會發生。

參考["管理政策"](#)有關管理實施勒索軟體檢測的政策詳細資訊。

啟用或停用系統的勒索軟體掃描

您可以為叢集啟用或停用勒索軟體掃描。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。

2. 在「備份設定」頁面中，按一下 ... 在系統中，選擇「配置進階設定 > 系統設定」。
3. 在出現的頁面中，展開「勒索軟體掃描」部分。
4. 啟用或停用*勒索軟體掃描*。
5. 選擇*計劃勒索軟體掃描*。
6. 或者，將每週預設掃描更改為幾天或幾週。
7. 設定掃描運作的頻率（以天數或週數為單位）。
8. 選擇*應用*。

啟用或停用提供者的勒索軟體掃描

您可以透過提供者設定頁面在提供者層級啟用或停用勒索軟體掃描。頁面上的設定與您在頁面頂部選擇的儲存桶相關。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 在「備份設定」頁面中，按一下 ... 在系統中，選擇「配置進階設定 > 提供者設定」。
3. 在出現的頁面頂部，選擇需要變更設定的儲存桶。
4. 展開「勒索軟體掃描」部分。
5. 啟用或停用*勒索軟體掃描*。
6. 選擇*計劃勒索軟體掃描*。
7. 或者，將每週預設掃描更改為幾天或幾週。
8. 設定掃描運作的頻率（以天數或週數為單位）。
9. 選擇*應用*。

使用NetApp Backup and Recovery將Cloud Volumes ONTAP資料備份到 Amazon S3

完成NetApp Backup and Recovery中的幾個步驟即可開始將磁碟區資料從Cloud Volumes ONTAP系統備份到 Amazon S3。



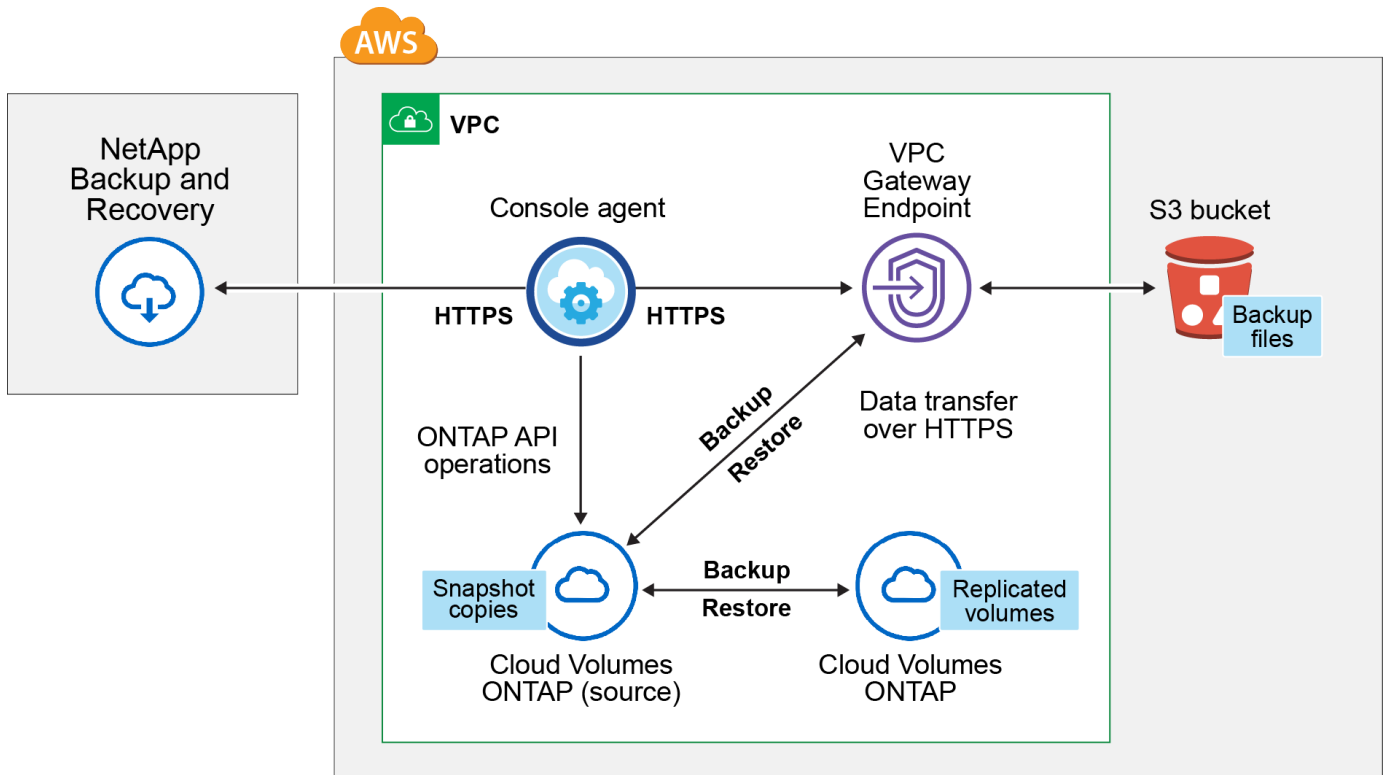
若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

驗證對您的配置的支持

在開始將磁碟區備份到 S3 之前，請閱讀以下要求以確保您具有受支援的配置。

下圖顯示了每個組件以及您需要在它們之間準備的連接。

或者，您也可以使用公用或私有連線連線到用於複製磁碟區的輔助ONTAP系統。



VPC 閘道端點必須已經存在於您的 VPC 中。 ["了解有關網關端點的更多信息"](#)。

支援的 **ONTAP** 版本

最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。

使用客戶管理的密鑰進行資料加密所需的信息

您可以在啟動精靈中選擇自己的客戶管理金鑰進行資料加密，而不是使用預設的 Amazon S3 加密金鑰。在這種情況下，您需要設定加密管理金鑰。 ["了解如何使用自己的密鑰"](#)。

驗證許可證要求

對於NetApp Backup and Recovery PAYGO 許可，可在 AWS Marketplace 中訂閱控制台，從而支援部署Cloud Volumes ONTAP和NetApp Backup and Recovery。你需要 ["訂閱此NetApp Console"](#)在啟用NetApp Backup and Recovery之前。 NetApp Backup and Recovery的計費透過此訂閱完成。

對於允許您備份Cloud Volumes ONTAP資料和本地ONTAP資料的年度合同，您需要從 ["AWS Marketplace 頁面"](#) 進而 ["將訂閱與您的 AWS 憑證關聯"](#)。

對於允許您捆綁Cloud Volumes ONTAP和NetApp Backup and Recovery 的年度合同，您必須在建立Cloud Volumes ONTAP系統時設定年度合約。此選項不允許您備份本機資料。

對於NetApp Backup and Recovery BYOL 許可，您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用該服務。["了解如何管理您的 BYOL 許可證"](#)。當控制台代理程式和Cloud Volumes ONTAP系統部署在暗站時，您必須使用 BYOL 授權。

並且您需要有一個 AWS 帳戶，用於儲存備份所在的儲存空間。

準備控制台代理

控制台代理必須安裝在具有完全或有限網路存取權限（「標準」或「受限」模式）的 AWS 區域。["有關詳細信息，請參閱NetApp Console部署模式"](#)。

- ["了解控制台代理"](#)
- ["在 AWS 中以標準模式（完全網路存取）部署控制台代理"](#)
- ["以受限模式安裝控制台代理程式（限制出站存取）"](#)

驗證或新增控制台代理的權限

為控制台提供權限的 IAM 角色必須包含最新的 S3 權限 ["控制台策略"](#)。如果策略不包含所有這些權限，請參閱 ["AWS 文件：編輯 IAM 原則"](#)。

以下是該政策的具體權限：

```

{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "athena:StartQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryExecution",
    "glue:GetDatabase",
    "glue:GetTable",

```



```

    "glue:CreateTable",
    "glue:CreateDatabase",
    "glue:GetPartitions",
    "glue:BatchCreatePartition",
    "glue:BatchDeletePartition"
  ],
  "Resource": [
    "arn:aws:s3:::netapp-backup-*"
  ]
}

```



在 AWS 中國區域建立備份時，您需要將 IAM 政策中所有 `_Resource_` 部分下的 AWS 資源名稱「arn」從「aws」變更為「aws-cn」；例如 `arn:aws-cn:s3:::netapp-backup-*`。

所需的 **AWS Cloud Volumes ONTAP** 權限

當您的 Cloud Volumes ONTAP 系統執行 ONTAP 9.12.1 或更高版本的軟體時，為該系統提供權限的 IAM 角色必須包含一組新的 S3 權限，專門用於 NetApp Backup and Recovery，從最新的 ["Cloud Volumes ONTAP 策略"](#)。

如果您使用控制台版本 3.9.23 或更高版本建立了 Cloud Volumes ONTAP 系統，則這些權限應該已經是 IAM 角色的一部分。否則您將需要新增缺少的權限。

支援的 **AWS** 區域

所有 AWS 區域（包括 AWS GovCloud 區域）均支援 NetApp Backup and Recovery。

在不同的 **AWS** 帳戶中建立備份所需的設置

預設情況下，使用與 Cloud Volumes ONTAP 系統相同的帳戶建立備份。如果您想要使用不同的 AWS 帳戶進行備份，則必須：

- 驗證權限「s3:PutBucketPolicy」和「s3:PutBucketOwnershipControls」是否屬於為控制台代理提供權限的 IAM 角色的一部分。
- 在控制台新增目標 AWS 帳戶憑證。["了解如何操作"](#)。
- 在第二個帳戶的使用者憑證中新增下列權限：

```

"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"

```

建立您自己的儲存桶

預設情況下，該服務會為您建立儲存桶。如果您想使用自己的儲存桶，您可以在啟動備份啟動精靈之前建立它們，然後在精靈中選擇這些儲存桶。

["了解有關創建您自己的存儲桶的更多信息"](#)。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。
- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。["查看ONTAP文件中的叢集對等前提條件"](#)。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。
- 要在不同子網路中的兩個Cloud Volumes ONTAP系統之間複製數據，子網路必須一起路由（這是預設）。

在Cloud Volumes ONTAP上啟用NetApp Backup and Recovery

啟用NetApp Backup and Recovery非常簡單。根據您擁有的是現有Cloud Volumes ONTAP系統還是新系統，步驟略有不同。

在新系統上啟用NetApp Backup and Recovery

NetApp Backup and Recovery在系統精靈中預設為啟用。確保該選項保持啟用狀態。

看 ["在 AWS 中啟動Cloud Volumes ONTAP"](#)了解建立Cloud Volumes ONTAP系統的需求和詳細資訊。

步驟

1. 從控制台*系統*頁面，選擇*新增系統*，選擇雲端提供者，然後選擇*新增*。選擇「建立Cloud Volumes ONTAP」。
2. 選擇*Amazon Web Services*作為雲端提供者，然後選擇單節點或 HA 系統。
3. 填寫詳細資料和憑證頁面。
4. 在服務頁面上，保持服務啟用並選擇*繼續*。
5. 完成精靈中的頁面以部署系統。

結果

系統上已啟用NetApp Backup and Recovery。在這些Cloud Volumes ONTAP系統上建立磁碟區後，啟動NetApp Backup and Recovery和["在您想要保護的每個磁碟區上啟動備份"](#)。

在現有系統上啟用NetApp Backup and Recovery

隨時直接從控制台在現有系統上啟用NetApp Backup and Recovery。

步驟

1. 從控制台*系統*頁面中，選擇叢集並選擇右側面板中備份和還原旁邊的*啟用*。

如果備份的 Amazon S3 目標在 系統 頁面上以叢集形式存在，則可以將該叢集拖曳到 Amazon S3 系統上以啟動設定精靈。

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- [\[選擇要備份的捲\]](#)
- [\[定義備份策略\]](#)
- [\[檢查您的選擇\]](#)

您還可以[顯示 API 命令](#)在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：

- 從控制台*系統*頁面中，選擇系統，然後選擇右側面板中備份和還原旁邊的*啟用>備份磁碟區*。

如果備份的 AWS 目標作為系統存在於控制台 系統 頁面上，則可以將ONTAP叢集拖曳到 AWS 物件儲存上。

- 在備份和復原欄中選擇“磁碟區”。在「卷」標籤中，選擇「操作」。  圖示選項，選擇“啟動 3-2-1 保護”，適用於單一磁碟區（尚未啟用複製或備份到物件儲存）。

精靈的介紹頁面顯示保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您還沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何["啟動系統中附加磁碟區的備份"](#)（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。
 - 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
 - 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區（FlexGroup磁碟區一次只能選擇一個）。若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
 - 若要備份單一卷，請選取每個卷對應的複選框。
2. 選擇“下一步”。

定義備份策略

定義備份策略涉及設定以下選項：

- 您是否需要一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構
- 本機快照策略
- 複製目標和策略



如果您選擇的磁碟區具有與您在此步驟中選擇的策略不同的快照和複製策略，則現有策略將被覆寫。

- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：
 - 本機快照：如果您正在執行複製或備份到物件存儲，則必須建立本機快照。
 - 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
 - 備份：將磁碟區備份到物件儲存。在選擇現有儲存桶或配置新儲存桶時，每個叢集最多可備份 6 個儲存桶中的磁碟區。
2. 架構：如果您選擇複製和備份，請選擇下列資訊流之一：
 - 級聯：資訊從主儲存系統流向輔助儲存系統，再從輔助儲存系統流向物件儲存。
 - 扇出：資訊從主儲存系統流向輔助儲存系統，再從主儲存系統流向物件儲存。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。
3. 本機快照：選擇現有的快照原則或建立新的快照策略。



若要在啟動快照之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- a. 輸入策略的名稱。
- b. 選擇最多五個時間表，通常頻率不同。
- c. 選擇“創建”。

4. 複製：設定以下選項：

- 複製目標：選擇目標系統和儲存虛擬機器。（可選）選擇目標聚合或多個聚合，以及要新增至複製磁碟區名稱的前綴或後綴。
- 複製策略：選擇現有的複製策略或建立一個。



若要建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- i. 輸入策略的名稱。
- ii. 選擇最多五個時間表，通常頻率不同。
- iii. 選擇“創建”。

5. 備份：設定以下選項：

- 提供者：選擇*Amazon Web Services*。
- 提供者設定：輸入提供者詳細資料和儲存備份的區域。

輸入用於儲存備份的 AWS 帳戶。這可以是與Cloud Volumes ONTAP系統所在的帳戶不同的帳戶。

如果您想要使用不同的 AWS 帳戶進行備份，則必須在控制台中新增目標 AWS 帳戶憑證，並將權限「s3：PutBucketPolicy」和「s3：PutBucketOwnershipControls」新增至為控制台提供權限的 IAM 角色。

選擇儲存備份的區域。這可能與Cloud Volumes ONTAP系統所在的區域不同。

建立新儲存桶或選擇現有儲存桶。

- 加密：如果您建立了一個新的儲存桶，請輸入提供者提供給您的加密金鑰資訊。您可以選擇使用預設的 AWS 加密金鑰，或從您的 AWS 帳戶中選擇您自己的客戶管理金鑰來管理資料的加密。（["了解如何使用您自己的加密金鑰"](#)）。

如果您選擇使用自己的客戶管理金鑰，請輸入金鑰保管庫和金鑰資訊。



如果您選擇了現有的儲存桶，加密資訊已經可用，因此您現在無需輸入。

- 網路：配置此提供者的網路選項。
- 備份策略：選擇現有的備份到物件儲存策略或建立一個。



若要在啟動備份之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- i. 輸入策略的名稱。
 - ii. 選擇最多五個時間表，通常頻率不同。
 - iii. 對於備份到物件策略，設定 DataLock 和 Ransomware Resilience 設定。有關 DataLock 和勒索軟體恢復的詳細信息，請參閱["備份到對象策略設置"](#)。
 - iv. 選擇“創建”。
- 。匯出現有快照：如果此系統中存在與您剛剛為此系統選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此框，即可將所有歷史快照複製到物件儲存作為備份文件，以確保您的磁碟區得到最全面的保護。

6. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取此複選框可「自動修復本機快照、複製和備份中不符的標籤」。這將建立與快照、複製和備份策略中的標籤相符的標籤的快照。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括主儲存系統資料的完整副本。後續傳輸包含快照中包含的主儲存系統資料的差異副本。

在目標叢集中建立一個複製卷，該卷將與主儲存卷同步。

在您輸入的 S3 存取金鑰和金鑰指示的服務帳戶中建立一個 S3 儲存桶，並將備份檔案儲存在那裡。

顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用["作業監控頁面"](#)。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

使用NetApp Backup and Recovery將Cloud Volumes ONTAP資料備份到 Azure Blob 存儲

完成NetApp Backup and Recovery中的幾個步驟，開始將磁碟區資料從Cloud Volumes ONTAP系統備份到 Azure Blob 儲存體。



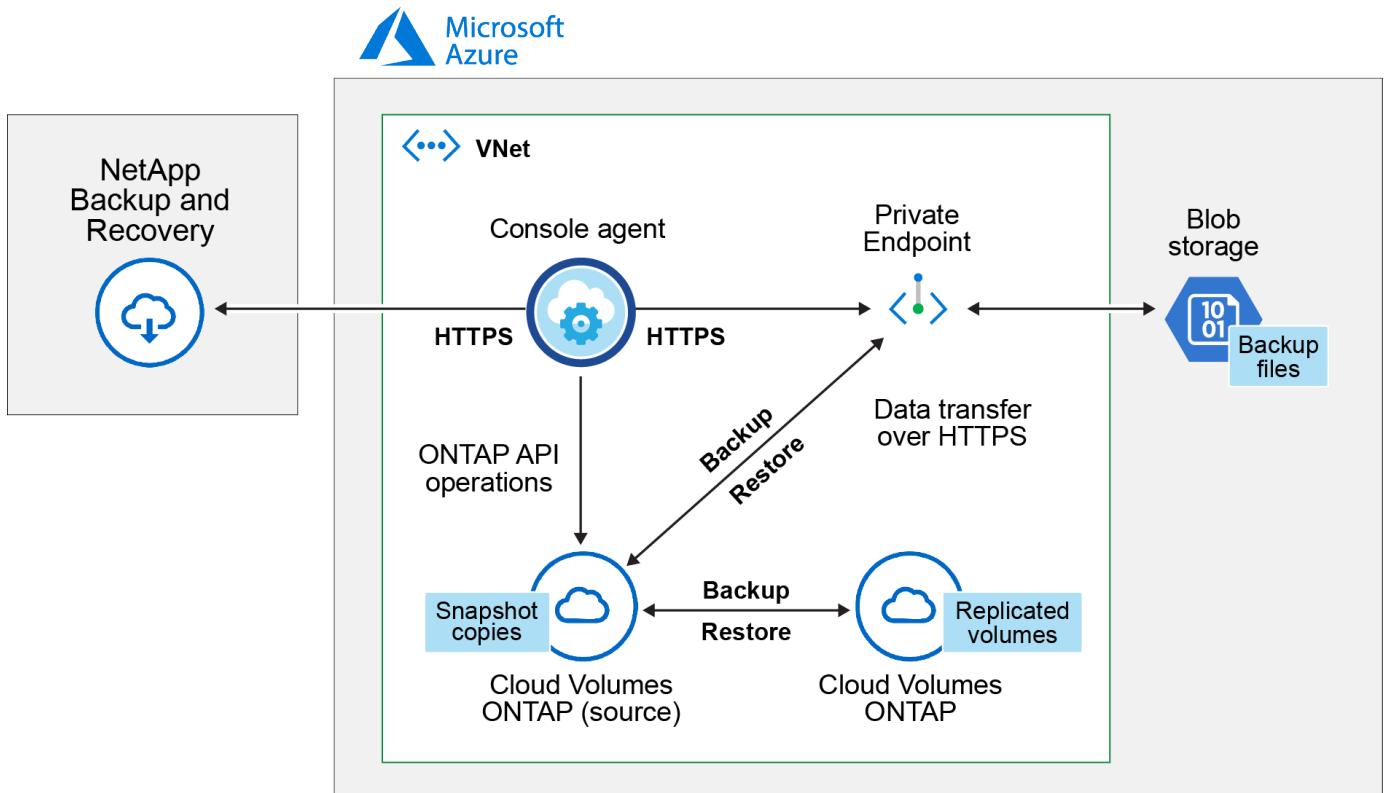
若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

驗證對您的配置的支持

在開始將磁碟區備份到 Azure Blob 儲存體之前，請閱讀下列要求以確保您具有支援的設定。

下圖顯示了每個組件以及您需要在它們之間準備的连接。

或者，您也可以使用公用或私有連線連線到用於複製磁碟區的輔助ONTAP系統。



支援的 **ONTAP** 版本

最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。

支援的 **Azure** 區域

所有 Azure 區域（包括 Azure 政府區域）都支援NetApp Backup and Recovery。

預設情況下，NetApp Backup and Recovery為 Blob 容器提供本機冗餘 (LRS) 以優化成本。如果您想要確保資料在不同區域之間複製，則可以在啟動NetApp Backup and Recovery後將此設定變更為區域冗餘 (ZRS)。請參閱 Microsoft 說明 ["變更儲存帳戶的複製方式"](#)。

在不同的 **Azure** 訂閱中建立備份所需的設置

預設情況下，使用與Cloud Volumes ONTAP系統相同的訂閱來建立備份。

驗證許可證要求

對於NetApp Backup and Recovery PAYGO 許可，在啟用NetApp Backup and Recovery之前，需要透過 Azure Marketplace 進行訂閱。NetApp Backup and Recovery的計費透過此訂閱完成。["您可以從系統精靈的「詳細資](#)

[料和憑證」頁面進行訂閱](#)。

對於NetApp Backup and Recovery BYOL 許可，您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用該服務。["了解如何管理您的 BYOL 許可證"](#)。當控制台代理程式和Cloud Volumes ONTAP系統部署在暗站（「私有模式」）時，您必須使用 BYOL 授權。

並且您需要訂閱 Microsoft Azure 以取得備份所在的儲存空間。

準備控制台代理

控制台代理可以安裝在具有完全或有限網際網路存取權限（「標準」或「受限」模式）的 Azure 區域。["有關詳細信息，請參閱NetApp Console部署模式"](#)。

- ["了解控制台代理"](#)
- ["在 Azure 中以標準模式（完全網際網路存取）部署控制台代理"](#)
- ["以受限模式安裝控制台代理程式（限制出站存取）"](#)

驗證或新增控制台代理的權限

要使用NetApp Backup and Recovery搜尋和還原功能，您需要在控制台代理程式的角色中擁有特定權限，以便它可以存取 Azure Synapse 工作區和資料湖儲存帳戶。請參閱下面的權限，如果需要修改策略，請依照下列步驟操作。

開始之前

- 您必須向您的訂閱註冊 Azure Synapse Analytics 資源提供者（稱為「Microsoft.Synapse」）。["了解如何為您的訂閱註冊此資源提供程序"](#)。您必須是訂閱*擁有者*或*貢獻者*才能註冊資源提供者。
- 必須開啟連接埠 1433 才能實現控制台代理程式和 Azure Synapse SQL 服務之間的通訊。

步驟

1. 確定指派給控制台代理虛擬機器的角色：
 - a. 在 Azure 入口網站中，開啟虛擬機器服務。
 - b. 選擇控制台代理虛擬機器。
 - c. 在“設定”下，選擇“身份”。
 - d. 選擇“Azure 角色分配”。
 - e. 記下指派給控制台代理虛擬機器的自訂角色。
2. 更新自訂角色：
 - a. 在 Azure 入口網站中，開啟你的 Azure 訂閱。
 - b. 選擇“存取控制 (IAM)”>“角色”。
 - c. 選擇自訂角色的省略號 (...)，然後選擇*編輯*。
 - d. 選擇 **JSON** 並新增以下權限：

```

"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"

```

["查看策略的完整 JSON 格式"](#)

e. 選擇*審核 + 更新*，然後選擇*更新*。

使用客戶管理的密鑰進行資料加密所需的信息

您可以在啟動精靈中使用自己的客戶管理金鑰進行資料加密，而不是使用預設的 Microsoft 管理加密金鑰。在這種情況下，您將需要有 Azure 訂閱、Key Vault 名稱和金鑰。"[了解如何使用自己的密鑰](#)"。

NetApp Backup and Recovery支援 Azure 存取策略、Azure 基於角色的存取控制 (Azure RBAC) 權限模型和託管硬體安全模型 (HSM) (請參閱 "[什麼是 Azure Key Vault 託管 HSM ?](#)")。

建立 Azure Blob 儲存體帳戶

預設情況下，該服務會為您建立儲存帳戶。如果您想使用自己的儲存帳戶，您可以在啟動備份啟動精靈之前建立它們，然後在精靈中選擇這些儲存帳戶。

["了解有關創建自己的儲存帳戶的更多信息"](#)。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。
- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。"[查看ONTAP文件中的叢集對等前提條件](#)"。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。
- 要在不同子網路中的兩個Cloud Volumes ONTAP系統之間複製數據，子網路必須一起路由（這是預設）。

在Cloud Volumes ONTAP上啟用NetApp Backup and Recovery

啟用NetApp Backup and Recovery非常簡單。根據您擁有的是現有Cloud Volumes ONTAP系統還是新系統，步驟略有不同。

在新系統上啟用NetApp Backup and Recovery

NetApp Backup and Recovery在系統精靈中預設為啟用。確保該選項保持啟用狀態。

看 "[在 Azure 中啟動Cloud Volumes ONTAP](#)"了解建立Cloud Volumes ONTAP系統的需求和詳細資訊。



如果您想要選擇資源組的名稱，請在部署Cloud Volumes ONTAP時*停用* NetApp Backup and Recovery。

步驟

1. 從控制台*系統*頁面，選擇*新增系統*，選擇雲端提供者，然後選擇*新增*。選擇「建立Cloud Volumes

ONTAP」。

2. 選擇 **Microsoft Azure** 作為雲端供應商，然後選擇單一節點或 HA 系統。
3. 在「定義 Azure 憑證」頁面中，輸入憑證名稱、用戶端 ID、用戶端金鑰和目錄 ID，然後選擇「繼續」。
4. 填寫「詳細資料和憑證」頁面並確保已訂閱 Azure 市場，然後選擇「繼續」。
5. 在服務頁面上，保持服務啟用並選擇*繼續*。
6. 完成精靈中的頁面以部署系統。

結果

系統上已啟用NetApp Backup and Recovery。在這些Cloud Volumes ONTAP系統上建立磁碟區後，啟動NetApp Backup and Recovery和[在您想要保護的每個磁碟區上啟動備份](#)。

在現有系統上啟用NetApp Backup and Recovery

隨時直接從系統啟用NetApp Backup and Recovery。

步驟

1. 從控制台*系統*頁面中，選擇系統並選擇右側面板中備份和還原旁邊的*啟用*。

如果備份的 Azure Blob 目標作為系統存在於控制台*系統*頁面上，則可以將叢集拖曳到 Azure Blob 系統上以啟動設定精靈。

2. 完成精靈中的頁面以部署NetApp Backup and Recovery。
3. 當您想要啟動備份時，請繼續[啟動ONTAP磁碟區上的備份](#)。

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- [\[選擇要備份的捲\]](#)
- [\[定義備份策略\]](#)
- [\[檢查您的選擇\]](#)

您還可以[顯示 API 命令](#)在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：
 - 從控制台*系統*頁面中，選擇系統，然後選擇右側面板中備份和還原旁邊的*啟用>備份磁碟區*。

如果備份的 Azure 目標作為系統存在於 系統 頁面上，則可以將ONTAP叢集拖曳到 Azure Blob 物件儲存體上。

- 在備份和復原欄中選擇*卷*。從磁碟區選項卡中，選擇*操作*  圖示並選擇單一磁碟區（尚未啟用複製或備份到物件儲存）的*啟動備份*。

精靈的介紹頁面顯示保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您還沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何"[啟動系統中附加磁碟區的備份](#)"（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。
 - 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
 - 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區。（一次只能選擇一個FlexGroup磁碟區。）若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
 - 若要備份單一卷，請選取每個卷對應的複選框。
2. 選擇“下一步”。

定義備份策略

定義備份策略涉及設定以下選項：

- 您是否需要一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構
- 本機快照策略
- 複製目標和策略



如果您選擇的磁碟區具有與您在此步驟中選擇的策略不同的快照和複製策略，則現有策略將被覆寫。

- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：

- 本機快照：如果您正在執行複製或備份到物件儲存，則必須建立本機快照。
- 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
- 備份：將磁碟區備份到物件儲存。

2. 架構：如果您選擇複製和備份，請選擇下列資訊流之一：

- 級聯：資訊從主儲存系統流向輔助儲存系統，再從輔助儲存系統流向物件儲存。
- 扇出：資訊從主儲存系統流向輔助儲存系統，再從主儲存系統流向物件儲存。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。

3. 本機快照：選擇現有的快照原則或建立一個。



若要在啟動快照之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

4. 複製：設定以下選項：

- 複製目標：選擇目標系統和 SVM。或者，選擇將新增至複製磁碟區名稱的目標聚合或聚合以及前綴或後綴。
- 複製策略：選擇現有的複製策略或建立一個。



若要在啟動複製之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

5. 備份到物件：如果您選擇了*備份*，請設定以下選項：

- 提供者：選擇*Microsoft Azure*。
- 提供者設定：輸入提供者詳細資料。

輸入儲存備份的區域。這可能與Cloud Volumes ONTAP系統所在的區域不同。

建立一個新的儲存帳戶或選擇一個現有的儲存帳戶。

輸入用於儲存備份的 Azure 訂閱。這可能是與Cloud Volumes ONTAP系統所在的訂閱不同的訂閱。

建立自己的管理 Blob 容器的資源群組，或選擇資源組類型和群組。



如果您想保護備份檔案不被修改或刪除，請確保建立儲存帳戶時啟用了 30 天保留期的不可變儲存。

- 加密金鑰：如果您建立了新的 Azure 儲存體帳戶，請輸入提供者提供給您的加密金鑰資訊。選擇是否使用預設 Azure 加密金鑰，或從 Azure 帳戶中選擇您自己的客戶管理金鑰來管理資料加密。

如果您選擇使用自己的客戶管理金鑰，請輸入金鑰保管庫和金鑰資訊。"[了解如何使用自己的密鑰](#)"。



如果您選擇了現有的 Microsoft 儲存帳戶，加密資訊已經可用，因此您現在無需輸入。

- 網路：選擇 IP 空間，以及是否使用私有端點。預設情況下，私有端點是禁用的。
 - i. 您要備份的磁碟區所在的 ONTAP 叢集中的 IP 空間。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
 - ii. 或者，選擇是否使用先前設定的 Azure 專用終端點。"[了解如何使用 Azure 專用終端點](#)"。
- 備份策略：選擇現有的備份到物件儲存策略。



若要在啟動備份之前建立自訂策略，請參閱"[創建策略](#)"。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 對於備份到物件策略，設定 DataLock 和 Ransomware Resilience 設定。有關 DataLock 和勒索軟體恢復的詳細信息，請參閱"[備份到對象策略設置](#)"。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。
- 將現有快照匯出至物件儲存作為備份副本：如果此系統中存在與您剛剛為此系統選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此方塊可將所有歷史快照複製到物件儲存作為備份文件，以確保對您的磁碟區進行最全面的保護。

6. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取核取方塊*自動將快照原則標籤與複製和備份策略標籤同步*。這將建立具有與複製和備份策略中的標籤相符的標籤的快照。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery 開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括主儲存系統資料的完整副本。後續傳輸包含快照中包含的主儲存資料的差異副本。

在目標群集中建立一個複製卷，該複製卷將與主卷同步。

在您輸入的資源組中建立一個 Blob 儲存容器，並將備份檔案儲存在那裡。

預設情況下，NetApp Backup and Recovery 為 Blob 容器提供本機冗餘 (LRS) 以優化成本。如果您想確保資料在不同區域之間複製，則可以將此設定變更為區域冗餘 (ZRS)。請參閱 Microsoft 說明 "[變更儲存帳戶的複製方式](#)"。

顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用"[作業監控頁面](#)"。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

下一步是什麼？

- 您可以"[管理您的備份檔案和備份策略](#)"。這包括啟動和停止備份、刪除備份、新增和更改備份計劃等。
- 您可以"[管理叢集級備份設定](#)"。這包括更改 ONTAP 用於存取雲端儲存的儲存金鑰、更改可用於將備份上傳到物件儲存的網路頻寬、更改未來磁碟區的自動備份設定等等。
- 您還可以"[從備份文件還原磁碟區、資料夾或單一文件](#)"到 AWS 中的 Cloud Volumes ONTAP 系統，或到本機 ONTAP 系統。

使用 NetApp Backup and Recovery 將 Cloud Volumes ONTAP 資料備份到 Google Cloud Storage

完成 NetApp Backup and Recovery 中的幾個步驟，開始將磁碟區資料從 Cloud Volumes ONTAP 系統備份到 Google Cloud Storage。



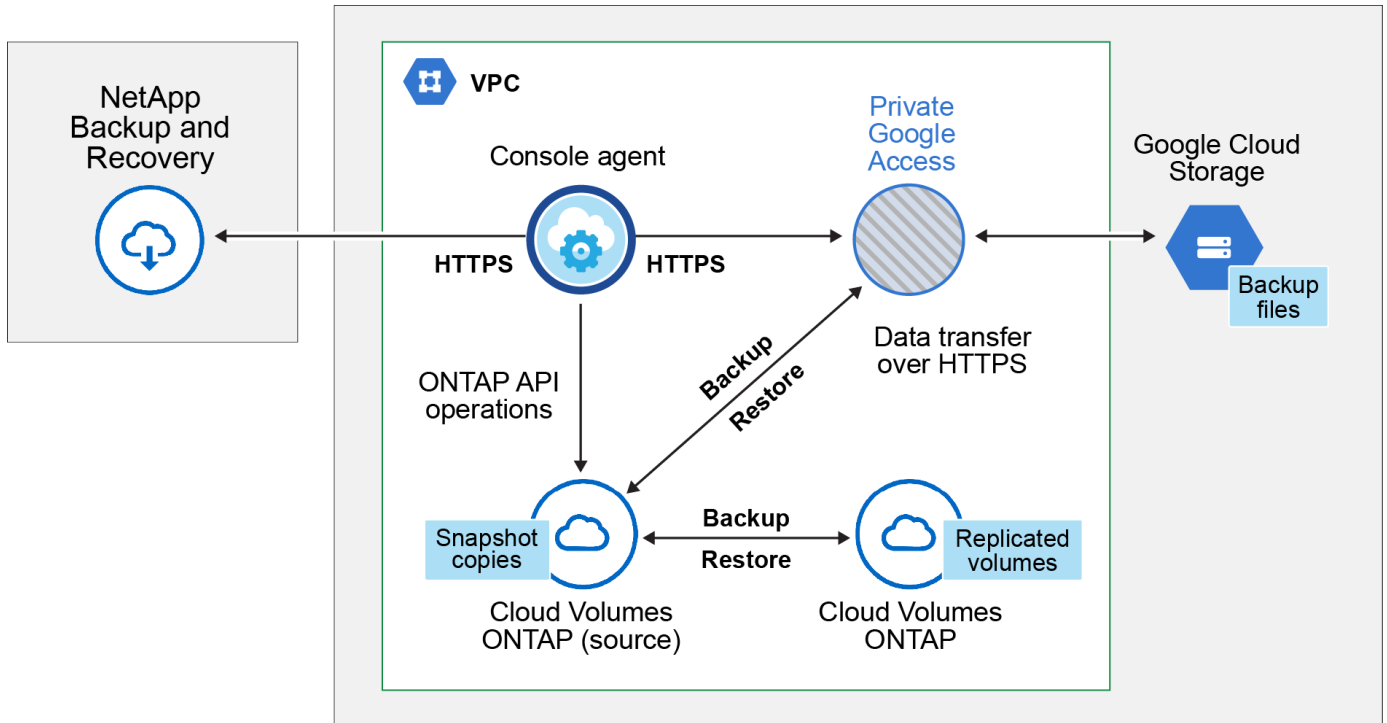
若要切換至 NetApp Backup and Recovery 工作負載，請參閱"[切換到不同的 NetApp Backup and Recovery 工作負載](#)"。

驗證對您的配置的支持

在開始將磁碟區備份到 Google Cloud Storage 之前，請閱讀以下要求以確保您具有受支援的配置。

下圖顯示了每個組件以及您需要在它們之間準備的連接。

或者，您也可以使用公用或私有連線連線到用於複製磁碟區的輔助 ONTAP 系統。



支援的 **ONTAP** 版本

最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。

支援的 **GCP** 區域

所有 GCP 區域均支援NetApp Backup and Recovery。

GCP 服務帳戶

您需要在 Google Cloud 專案中擁有一個具有自訂角色的服務帳戶。["了解如何建立服務帳號"](#)。



啟用NetApp Backup and Recovery來存取 Google Cloud Storage 儲存桶的服務帳戶不再需要儲存管理員角色。

驗證許可證要求

對於NetApp Backup and Recovery PAYGO 許可，可在 Google Marketplace 中訂閱控制台，從而實現Cloud Volumes ONTAP和NetApp Backup and Recovery 的部署。你需要 ["訂閱此控制台訂閱"](#)在啟用NetApp Backup and Recovery之前。NetApp Backup and Recovery的計費透過此訂閱完成。["您可以從系統精靈的「詳細資料和憑證」頁面進行訂閱"](#)。

對於NetApp Backup and RecoveryBYOL 許可，您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用該服務。["了解如何管理您的 BYOL 許可證"](#)。

並且您需要向 Google 訂閱用於儲存備份的儲存空間。

準備控制台代理

控制台代理必須安裝在可以存取網路的 Google 區域。

- ["了解控制台代理"](#)
- ["在 Google Cloud 中部署控制台代理"](#)

驗證或新增控制台代理的權限

要使用 NetApp Backup and Recovery 的「搜尋和復原」功能，您需要在控制台代理的角色中擁有特定權限，以便它可以存取 Google Cloud BigQuery 服務。請參閱下面的權限，如果需要修改策略，請依照下列步驟操作。

步驟

1. 在 ["Google 雲端控制台"](#)，轉到*角色*頁面。
2. 使用頁面頂部的下拉列表，選擇包含要編輯的角色的項目或組織。
3. 選擇自訂角色。
4. 選擇*編輯角色*來更新角色的權限。
5. 選擇*新增權限*為角色新增下列新權限。

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. 選擇*更新*以儲存編輯的角色。

使用客戶管理的加密金鑰 (CMEK) 所需的信息

您可以使用自己的客戶管理金鑰進行資料加密，而不是使用預設的 Google 管理加密金鑰。跨區域和跨項目密鑰均受支持，因此您可以為存儲桶選擇與 CMEK 密鑰的項目不同的項目。如果您打算使用自己的客戶管理金鑰：

- 您需要有密鑰環和密鑰名稱，以便可以在啟動精靈中新增此資訊。 ["了解有關客戶管理加密金鑰的更多信息"](#)。
- 您需要驗證控制台代理程式的角色是否包含這些必要的權限：

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 您需要驗證您的專案中是否啟用了 Google「雲端金鑰管理服務 (KMS)」API。查看 ["Google Cloud 文件：啟用 API"](#) 了解詳情。

CMEK 注意事項：

- 支援 HSM（硬體支援）和軟體產生的金鑰。
- 支援新建立或匯入的 Cloud KMS 金鑰。
- 僅支援區域密鑰；不支援全域密鑰。
- 目前僅支援“對稱加密/解密”目的。
- NetApp Backup and Recovery 為與儲存帳戶關聯的服務代理程式指派了「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM 角色。

建立您自己的儲存桶

預設情況下，該服務會為您建立儲存桶。如果您想使用自己的儲存桶，您可以在啟動備份啟動精靈之前建立它們，然後在精靈中選擇這些儲存桶。

["了解有關創建您自己的存儲桶的更多信息"](#)。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。
- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。["查看ONTAP文件中的叢集對等前提條件"](#)。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。
- 要在不同子網路中的兩個Cloud Volumes ONTAP系統之間複製數據，子網路必須一起路由（這是預設）。

在Cloud Volumes ONTAP上啟用NetApp Backup and Recovery

啟用NetApp Backup and Recovery步驟略有不同，具體取決於您擁有的是現有Cloud Volumes ONTAP系統還是新系統。

在新系統上啟用NetApp Backup and Recovery

當您完成系統精靈以建立新的Cloud Volumes ONTAP系統時，可以啟用NetApp Backup and Recovery。

您必須已經配置了服務帳戶。如果在建立Cloud Volumes ONTAP系統時未選擇服務帳戶，則需要關閉系統並從GCP 控制台將服務帳戶新增至Cloud Volumes ONTAP。

看 ["在 GCP 中啟動Cloud Volumes ONTAP"](#) 了解建立Cloud Volumes ONTAP系統的需求和詳細資訊。

步驟

1. 從控制台*系統*頁面，選擇*新增系統*，選擇雲端提供者，然後選擇*新增*。選擇「建立Cloud Volumes ONTAP」。
2. 選擇位置：選擇*Google Cloud Platform*。
3. 選擇類型：選擇* Cloud Volumes ONTAP*（單節點或高可用性）。
4. 詳細資料和憑證：輸入以下資訊：
 - a. 如果您要使用的項目與預設項目（控制台代理程式所在的項目）不同，請按一下「編輯項目」並選擇新項目。
 - b. 指定叢集名稱。
 - c. 啟用*服務帳戶*開關並選擇具有預先定義儲存管理員角色的服務帳戶。這是啟用備份和分層所必需的。
 - d. 指定憑證。

確保已訂閱 GCP Marketplace。

5. 服務：保持NetApp Backup and Recovery處於啟用狀態，然後按一下*繼續*。
6. 完成精靈中的頁面以部署系統，如中所述 ["在 GCP 中啟動Cloud Volumes ONTAP"](#)。

結果

系統上已啟用NetApp Backup and Recovery。在這些Cloud Volumes ONTAP系統上建立磁碟區後，啟動NetApp Backup and Recovery和["在您想要保護的每個磁碟區上啟動備份"](#)。

在現有系統上啟用NetApp Backup and Recovery

您可以隨時直接從系統啟用NetApp Backup and Recovery。

步驟

1. 從控制台*系統*頁面中，選擇系統並選擇右側面板中備份和還原旁邊的*啟用*。

如果您的備份的 Google Cloud Storage 目標作為系統存在於控制台*系統*頁面上，則可以將叢集拖曳到 Google Cloud Storage 系統上以啟動設定精靈。

準備 Google Cloud Storage 作為備份目標

準備 Google Cloud Storage 作為備份目標涉及以下步驟：

- 設定權限。
- (可選) 創建您自己的儲存桶。(如果您願意，該服務將為您建立儲存桶。)
- (可選) 設定客戶管理的金鑰以進行資料加密

設定權限

您需要使用自訂角色為具有特定權限的服務帳戶提供儲存存取金鑰。服務帳戶使NetApp Backup and Recovery能夠驗證和存取用於儲存備份的 Cloud Storage 儲存桶。需要金鑰，以便 Google Cloud Storage 知道誰在發出請求。

步驟

1. 在 ["Google 雲端控制台"](#)，轉到*角色*頁面。
2. ["創建新角色"](#)具有以下權限：

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. 在 Google Cloud 控制台中，["前往服務帳戶頁面"](#)。
4. 選擇您的雲端項目。
5. 選擇*建立服務帳戶*並提供所需資訊：
 - a. 服務帳戶詳細資料：輸入名稱和描述。
 - b. 授予此服務帳戶存取項目的權限：選擇您剛剛建立的自訂角色。
 - c. 選擇*完成*。
6. 前往 ["GCP 儲存設定"](#)並為服務帳戶建立存取金鑰：
 - a. 選擇一個項目，然後選擇*互通性*。如果您還沒有這樣做，請選擇*啟用互通性存取*。
 - b. 在*服務帳戶的存取金鑰*下，選擇*為服務帳戶建立金鑰*，選擇剛剛建立的服務帳戶，然後按一下*建立金鑰*。

稍後設定備份服務時，您需要在NetApp Backup and Recovery中輸入金鑰。

建立您自己的儲存桶

預設情況下，該服務會為您建立儲存桶。或者，如果您想使用自己的儲存桶，您可以在啟動備份啟動精靈之前建立它們，然後在精靈中選擇這些儲存桶。

["了解有關創建您自己的存儲桶的更多信息"](#)。

設定客戶管理的加密金鑰 (CMEK) 以進行資料加密

您可以使用自己的客戶管理金鑰進行資料加密，而不是使用預設的 Google 管理加密金鑰。跨區域和跨項目密鑰均受支持，因此您可以為儲存桶選擇與 CMEK 密鑰的項目不同的項目。

如果您打算使用自己的客戶管理金鑰：

- 您需要有密鑰環和密鑰名稱，以便可以在啟動精靈中新增此資訊。 ["了解有關客戶管理加密金鑰的更多信息"](#)。
- 您需要驗證控制台代理程式的角色是否包含這些必要的權限：

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 您需要驗證您的專案中是否啟用了 Google「雲端金鑰管理服務 (KMS)」API。查看 ["Google Cloud 文件：啟用 API"](#) 了解詳情。

CMEK 注意事項：

- 支援 HSM（硬體支援）和軟體產生的金鑰。
- 支援新建立或匯入的 Cloud KMS 金鑰。
- 僅支援區域密鑰，不支援全域密鑰。
- 目前僅支援“對稱加密/解密”目的。
- NetApp Backup and Recovery 為與儲存帳戶關聯的服務代理程式指派了「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM 角色。

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- [\[選擇要備份的捲\]](#)
- [\[定義備份策略\]](#)

- [\[檢查您的選擇\]](#)

您還可以[顯示 API 命令](#)在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：

- 從控制台*系統*頁面*中，選擇系統並選擇右側面板中備份和還原旁邊的*啟用>備份磁碟區*。

如果備份的 GCP 目標作為系統存在於控制台*系統*頁面上，則可以將ONTAP叢集拖曳到 GCP 物件儲存上。

- 在備份和復原欄中選擇*卷*。從磁碟區選項卡中，選擇*操作*  圖示並選擇單一磁碟區（尚未啟用複製或備份到物件儲存）的*啟動備份*。

精靈的介紹頁面顯示保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您還沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何"[啟動系統中附加磁碟區的備份](#)"（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

請注意，如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。

- 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
- 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區（FlexGroup磁碟區一次只能選擇一個）。若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
- 若要備份單一卷，請選取每個卷對應的複選框。

2. 選擇“下一步”。

定義備份策略

定義備份策略涉及設定以下選項：

- 您是否需要一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構
- 本機快照策略
- 複製目標和策略



如果您選擇的磁碟區具有與您在此步驟中選擇的策略不同的快照和複製策略，則現有策略將被覆寫。

- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：

- 本機快照：如果您正在執行複製或備份到物件存儲，則必須建立本機快照。
- 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
- 備份：將磁碟區備份到物件儲存。

2. 架構：如果您選擇複製和備份，請選擇下列資訊流之一：

- 級聯：資訊從主儲存系統流向輔助儲存系統，再從輔助儲存系統流向物件儲存。
- 扇出：資訊從主儲存系統流向輔助儲存系統，再從主儲存系統流向物件儲存。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。

3. 本機快照：選擇現有的快照原則或建立一個。



若要在啟動備份之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 對於備份到物件策略，設定 Datalock 和 Ransomware Resilience。有關 Datalock 和勒索軟體復原的詳細信息，請參閱["備份到對象策略設置"](#)。
- 選擇“創建”。

4. 複製：設定以下選項：

- 複製目標：選擇目標系統和 SVM。或者，選擇將新增至複製磁碟區名稱的目標聚合或聚合以及前綴或後綴。
- 複製策略：選擇現有的複製策略或建立一個。



若要在啟動複製之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

5. 備份到物件：如果您選擇了*備份*，請設定以下選項：

- 提供者：選擇*Google Cloud*。
- 提供者設定：輸入提供者詳細資料和儲存備份的區域。

建立新儲存桶或選擇現有儲存桶。

- 加密金鑰：如果您建立了新的 Google 儲存桶，請輸入提供者提供給您的加密金鑰資訊。選擇是否使用預設的 Google Cloud 加密金鑰，或從您的 Google 帳戶中選擇您自己的客戶管理金鑰來管理您的資料加密。

如果您選擇使用自己的客戶管理金鑰，請輸入金鑰保管庫和金鑰資訊。



如果您選擇了現有的 Google Cloud 儲存桶，則加密資訊已經可用，因此您現在無需輸入。

- 備份策略：選擇現有的備份到物件儲存策略或建立一個。



若要在啟動備份之前建立自訂策略，請參閱[“創建策略”](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。
- 將現有快照匯出至物件儲存作為備份副本：如果此系統中存在與您剛剛為此系統選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此方塊可將所有歷史快照複製到物件儲存作為備份文件，以確保對您的磁碟區進行最全面的保護。

6. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取核取方塊*自動將快照原則標籤與複製和備份策略標籤同步*。這將建立具有與複製和備份策略中的標籤相符的標籤的快照。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括主儲存系統

資料的完整副本。後續傳輸包含快照中包含的主儲存系統資料的差異副本。

在目標群集中建立一個複製卷，該卷將與主儲存系統卷同步。

在您輸入的 Google 存取金鑰和金鑰所指示的服務帳戶中建立一個 Google Cloud Storage 儲存桶，並將備份檔案儲存在那裡。

預設情況下，備份與 [Standard](#) 儲存類別相關聯。您可以使用成本較低的 [Nearline](#)、[Coldline](#) 或 [Archive](#) 儲存類別。但是，您透過 Google 設定儲存類，而不是透過 NetApp Backup and Recovery UI。請參閱 Google 主題 ["更改儲存桶的預設儲存類別"](#) 了解詳情。

顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用 ["作業監控頁面"](#)。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

下一步是什麼？

- 您可以["管理您的備份檔案和備份策略"](#)。這包括啟動和停止備份、刪除備份、新增和更改備份計劃等。
- 您可以["管理叢集級備份設定"](#)。這包括更改 ONTAP 用於存取雲端儲存的儲存金鑰、更改可用於將備份上傳到物件儲存的網路頻寬、更改未來磁碟區的自動備份設定等等。
- 您還可以["從備份文件還原磁碟區、資料夾或單一文件"](#)到 AWS 中的 Cloud Volumes ONTAP 系統，或到本機 ONTAP 系統。

使用 NetApp Backup and Recovery 將本機 ONTAP 資料備份到 Amazon S3

完成 NetApp Backup and Recovery 中的幾個步驟，開始將磁碟區資料從本機 ONTAP 系統備份到二級儲存系統和 Amazon S3 雲端儲存。



「本地 ONTAP 系統」包括 FAS、AFF 和 ONTAP Select 系統。



若要切換至 NetApp Backup and Recovery 工作負載，請參閱["切換到不同的 NetApp Backup and Recovery 工作負載"](#)。

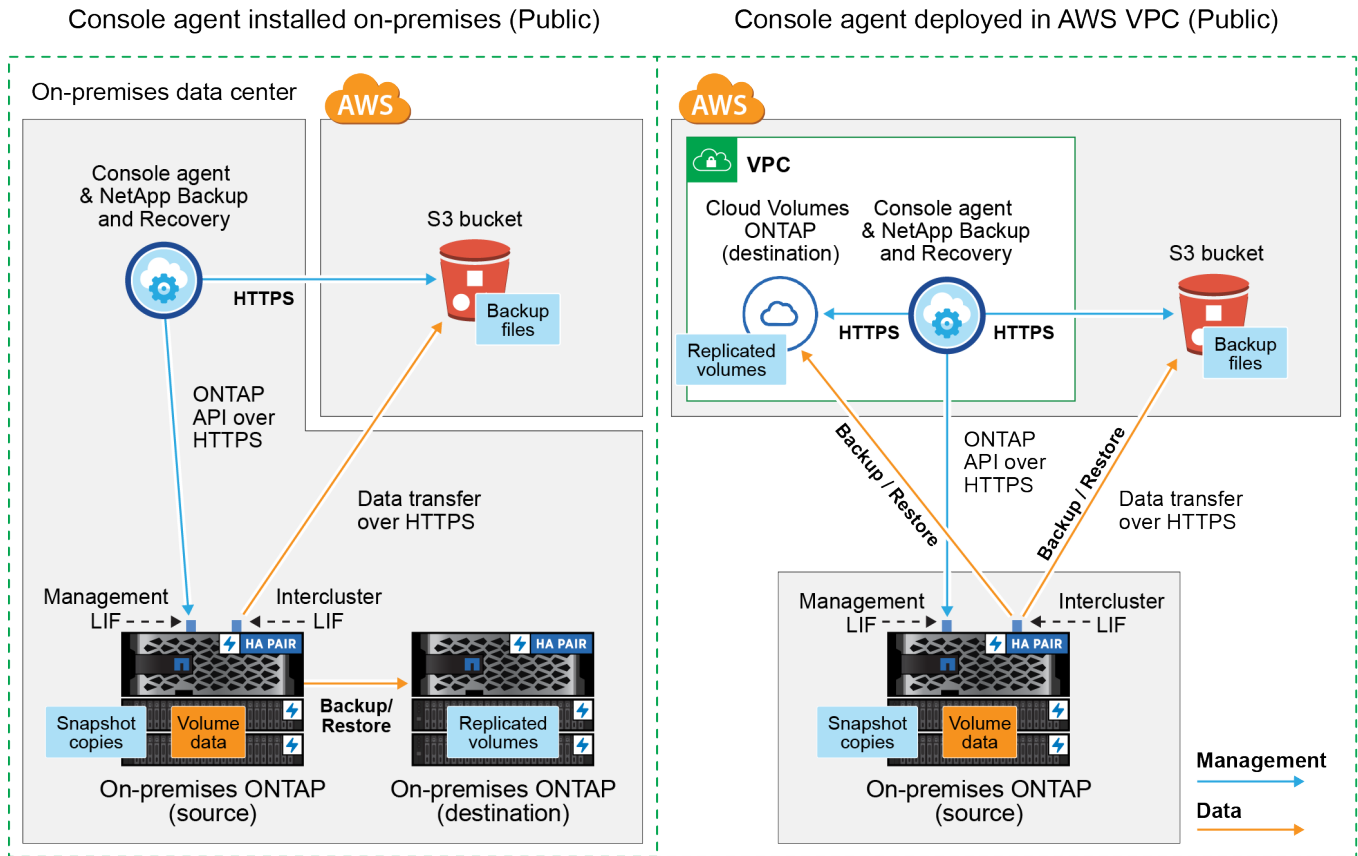
識別連接方法

選擇在配置從本機 ONTAP 系統到 AWS S3 的備份時要使用的兩種連接方法中的哪一種。

- 公用連線 - 使用公用 S3 端點將 ONTAP 系統直接連接到 AWS S3。
- 私人連線 - 使用 VPN 或 AWS Direct Connect 並透過使用私人 IP 位址的 VPC Endpoint 介面路由流量。

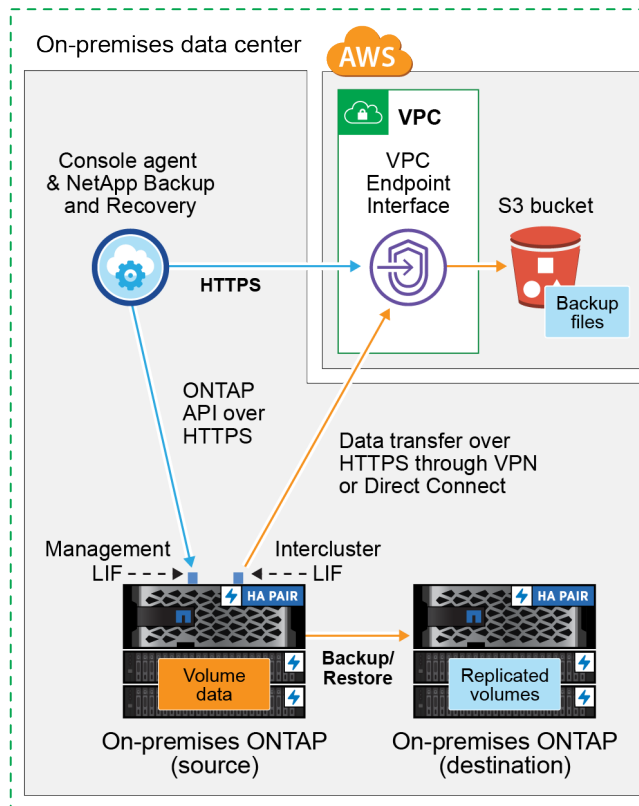
或者，您也可以使用公用或私有連線連線到用於複製磁碟區的輔助ONTAP系統。

下圖顯示了*公共連接*方法以及您需要在組件之間準備的連接。您可以使用在您的場所安裝的控制台代理，或在AWS VPC 中部署的控制台代理。

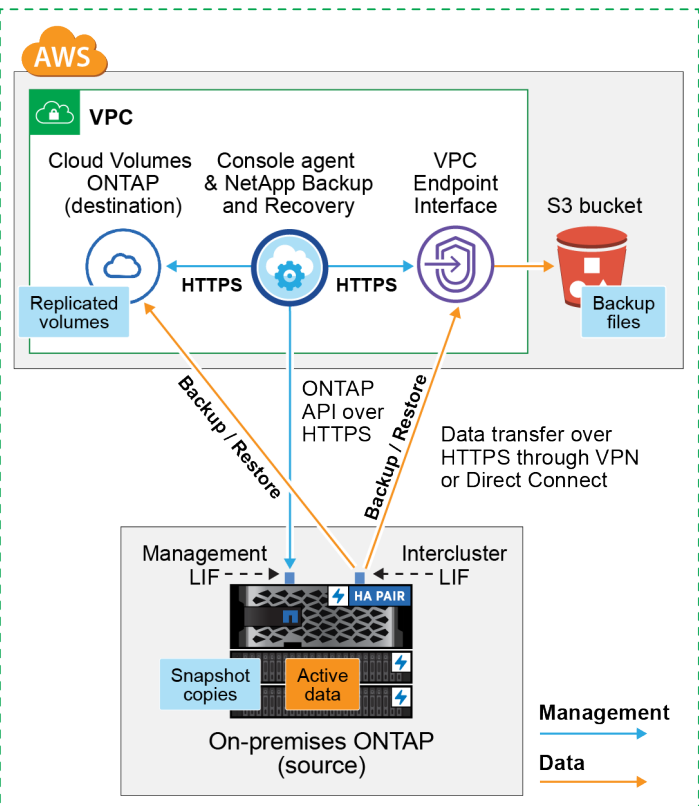


下圖顯示了*私有連接*方法以及您需要在元件之間準備的連接。您可以使用在您的場所安裝的控制台代理，或在AWS VPC 中部署的控制台代理。

Console agent installed on-premises (Private)



Console agent deployed in AWS VPC (Private)



準備控制台代理

控制台代理程式是NetApp Console功能的主要軟體。需要控制台代理程式來備份和還原您的ONTAP資料。

建立或切換控制台代理

如果您已經在 AWS VPC 或您的場所部署了控制台代理，那麼一切就緒了。

如果沒有，那麼您需要在其中一個位置建立控制台代理，以將ONTAP資料備份到 AWS S3 儲存。您不能使用部署在其他雲端提供者的控制台代理程式。

- ["了解控制台代理"](#)
- ["在 AWS 中安裝控制台代理"](#)
- ["在您的場所安裝控制台代理"](#)
- ["在 AWS GovCloud 區域安裝控制台代理"](#)

當控制台代理部署在雲端時（而不是安裝在您的場所中），NetApp Backup and Recovery在 GovCloud 區域受支援。此外，您必須從 AWS Marketplace 部署控制台代理程式。您無法從NetApp Console SaaS 網站在政府區域部署控制台代理程式。

準備控制台代理網路要求

確保符合以下網路要求：

- 確保安裝控制台代理程式的網路啟用以下連線：
 - 透過連接埠 443 建立到NetApp Backup and Recovery以及 S3 物件儲存的 HTTPS 連接(["查看端點列表"](#))
 - 透過連接埠 443 建立到ONTAP叢集管理 LIF 的 HTTPS 連接
 - AWS 和 AWS GovCloud 部署需要額外的入站和出站安全群組規則。看 ["AWS 中的控制台代理程式規則"](#) 了解詳情。
- 如果您有從ONTAP叢集到 VPC 的 Direct Connect 或 VPN 連接，且您希望控制台代理程式和 S3 之間的通訊保持在 AWS 內部網路（*私有*連線）中，則需要啟用至 S3 的 VPC 端點介面。[使用 VPC 終端節點介面配置系統以進行私有連接](#)。

驗證許可證要求

您需要驗證 AWS 和NetApp Console的授權需求：

- 在為叢集啟動NetApp Backup and Recovery之前，您需要訂閱 AWS 提供的即用即付 (PAYGO) NetApp Console Marketplace，或從NetApp購買並啟用NetApp Backup and Recovery BYOL 授權。這些許可證適用於您的帳戶，可以在多個系統中使用。
 - 對於NetApp Backup and Recovery PAYGO 許可，您需要訂閱 ["AWS Marketplace 提供的NetApp Console"](#)。NetApp Backup and Recovery的計費透過此訂閱完成。
 - 對於NetApp Backup and RecoveryBYOL 許可，您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用該服務。
- 您需要訂閱用於儲存備份的物件儲存空間的 AWS。

支援地區

您可以在所有區域（包括 AWS GovCloud 區域）中從本機系統建立到 Amazon S3 的備份。您在設定服務時指定儲存備份的區域。

準備ONTAP集群

準備來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統。

準備ONTAP集群涉及以下步驟：

- 在NetApp Console中發現您的ONTAP系統
- 驗證ONTAP系統要求
- 驗證ONTAP網路要求以將資料備份到對象存儲
- 驗證ONTAP複製卷的網路要求

在NetApp Console中發現您的ONTAP系統

您的來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統都必須在NetApp Console*系統*頁面上可用。

您需要知道叢集管理 IP 位址和管理員使用者帳戶的密碼才能新增叢集。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>[["了解如何發現集群"](#)]。

驗證ONTAP系統要求

確保您的ONTAP系統符合以下要求：

- 最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。
- SnapMirror許可證（包含在高級捆綁包或資料保護捆綁包中）。
- *注意：*使用NetApp Backup and Recovery時不需要「混合雲端捆綁包」。

了解如何 ["管理您的叢集許可證"](#)。

- 時間和時區設定正確。了解如何 ["配置叢集時間"](#)。
- 如果您複製數據，請檢查來源系統和目標系統是否要執行相容的ONTAP版本。

["查看與SnapMirror關係相容的ONTAP版本"](#)。

驗證ONTAP網路要求以將資料備份到對象存儲

您必須在連接到物件儲存的系統上配置以下要求。

- 對於扇出備份架構，請在主系統上配置以下設定。
- 對於級聯備份架構，請在_輔助_系統上設定下列設定。

需滿足以下ONTAP集群網路需求：

- 叢集需要從控制台代理到叢集管理 LIF 的入站 HTTPS 連線。
- 每個託管要備份的磁碟區的ONTAP節點上都需要一個叢集間 LIF。這些群集間 LIF 必須能夠存取物件儲存。

叢集透過連接埠 443 啟動從叢集間 LIF 到 Amazon S3 儲存的出站 HTTPS 連接，以執行備份和還原作業。ONTAP從物件儲存讀取和寫入資料 - 物件儲存從不啟動，它只是回應。

- 群集間 LIF 必須與ONTAP用於連接物件儲存的 *IPspace* 相關聯。 ["了解有關 IP 空間的更多信息"](#)。

當您設定NetApp Backup and Recovery時，系統會提示您輸入要使用的 IP 空間。您應該選擇與這些 LIF 關聯的 IP 空間。這可能是「預設」IP 空間或您建立的自訂 IP 空間。

如果您使用的 IP 空間與「預設」不同，那麼您可能需要建立靜態路由來存取物件儲存。

IP 空間內的所有叢集間 LIF 都必須具有物件儲存的存取權限。如果您無法為目前 IP 空間配置此功能，則需要建立一個專用 IP 空間，其中所有群集間 LIF 都可以存取物件儲存。

- 必須為磁碟區所在的儲存虛擬機器設定 DNS 伺服器。了解如何 ["為 SVM 配置 DNS 服務"](#)。
- 如有必要，請更新防火牆規則，以允許NetApp Backup and Recovery透過連接埠 443 從ONTAP連接到物件儲存，並透過連接埠 53（TCP/UDP）從儲存虛擬機器到 DNS 伺服器的名稱解析流量。
- 如果您在 AWS 中使用私有 VPC 介面端點進行 S3 連接，那麼為了使用 HTTPS/443，您需要將 S3 端點憑證載入到ONTAP叢集中。 [使用 VPC 終端節點介面配置系統以進行私有連接](#)。
- 確保您的ONTAP叢集有權存取 S3 儲存桶。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。
- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。"[查看ONTAP文件中的叢集對等前提條件](#)"。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。

準備 Amazon S3 作為備份目標

準備 Amazon S3 作為備份目標涉及以下步驟：

- 設定 S3 權限。
- （可選）創建您自己的 S3 儲存桶。（如果您願意，該服務將為您建立儲存桶。）
- （可選）設定客戶管理的 AWS 金鑰以進行資料加密。
- （可選）使用 VPC 終端節點介面配置系統以進行私人連接。

設定 S3 權限

您需要設定兩組權限：

- 控制台代理程式建立和管理 S3 儲存桶的權限。
- 本地ONTAP叢集的權限，以便它可以讀取和寫入 S3 儲存桶的資料。

步驟

1. 確保控制台代理具有所需的權限。有關詳細信息，請參閱 "[NetApp Console策略權限](#)"。



在 AWS 中國區域建立備份時，您需要將 IAM 政策中所有 _Resource_ 部分下的 AWS 資源名稱「arn」從「aws」變更為「aws-cn」；例如 `arn:aws-cn:s3:::netapp-backup-*`。

2. 當您啟動服務時，備份精靈會提示您輸入存取金鑰和金鑰。這些憑證會傳遞到ONTAP集群，以便ONTAP可以將資料備份和還原到 S3 儲存桶。為此，您需要建立具有以下權限的 IAM 使用者。

請參閱 "[AWS 文件：建立角色以將權限委託給 IAM 用戶](#)"。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}

```

建立您自己的儲存桶

預設情況下，該服務會為您建立儲存桶。或者，如果您想使用自己的儲存桶，您可以在啟動備份啟動精靈之前建立它們，然後在精靈中選擇這些儲存桶。

["了解有關創建您自己的存儲桶的更多信息"](#)。

如果您建立自己的儲存桶，則應使用儲存桶名稱「netapp-backup」。如果需要使用自訂名稱，請編輯 `ontapcloud-instance-policy-netapp-backup` 為現有 CVO 新增 IAMRole，並將下列 JSON 區塊新增至 S3 權限中 `Statement` 大批。您需要包括 `"Resource": "arn:aws:s3:::\*"` 並分配與儲存桶關聯的所有必要權限。

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

設定客戶管理的 AWS 金鑰以進行資料加密

如果您想使用預設的 Amazon S3 加密金鑰來加密您的本機叢集和 S3 儲存桶之間傳遞的數據，那麼您已經完成了所有設置，因為預設安裝使用這種類型的加密。

如果您想使用自己的客戶管理金鑰進行資料加密而不是使用預設金鑰，那麼您需要在啟動 NetApp Backup and Recovery 精靈之前設定加密管理金鑰。

"請參閱如何在Cloud Volumes ONTAP中使用您自己的 Amazon 加密金鑰"。

"請參閱如何在NetApp Backup and Recovery中使用您自己的 Amazon 加密金鑰"。

使用 VPC 終端節點介面配置系統以進行私有連接

如果您想使用標準公共互聯網連接，那麼所有權限都由控制台代理設置，您無需執行任何其他操作。

如果您希望透過網路從本機資料中心到 VPC 建立更安全的連接，則可以在備份啟動精靈中選擇 AWS PrivateLink 連接。如果您打算使用 VPN 或 AWS Direct Connect 透過使用私人 IP 位址的 VPC 終端節點介面連接您的本機系統，則需要它。

步驟

1. 使用 Amazon VPC 控制台或命令列建立介面終端節點配置。"請參閱有關使用 AWS PrivateLink for Amazon S3 的詳細信息"。
2. 修改與控制台代理程式關聯的安全性群組配置。您必須將策略變更為"自訂"（從"完全存取"），並且您必須從備份策略新增 S3 權限如前所示。

如果您使用連接埠 80（HTTP）與私有端點進行通信，則一切就緒。現在您可以在叢集上啟用NetApp Backup and Recovery。

如果您使用連接埠 443（HTTPS）與私有端點通信，則必須從 VPC S3 端點複製憑證並將其新增至您的ONTAP集群，如接下來的 4 個步驟所示。

3. 從 AWS 控制台取得端點的 DNS 名稱。
4. 從 VPC S3 端點取得憑證。你可以透過以下方式做到這一點 "登入託管控制台代理的虛擬機"並運行以下命令。輸入端點的 DNS 名稱時，在開頭新增"bucket"，取代"*"：

```
openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

5. 從此指令的輸出中，複製 S3 憑證的資料（BEGIN / END CERTIFICATE 標籤之間（包括 BEGIN / END CERTIFICATE 標籤）的所有資料）：

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
...
...
GqvboZ/0O2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. 登入ONTAP叢集 CLI 並使用以下命令套用您複製的憑證（取代您自己的儲存虛擬機器名稱）：

```
cluster1::> security certificate install -vserver cluster1 -type server-  
ca  
Please enter Certificate: Press <Enter> when done
```

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- [\[選擇要備份的捲\]](#)
- [\[定義備份策略\]](#)
- [\[檢查您的選擇\]](#)

您還可以[顯示 API 命令](#)在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：

- 從控制台*系統*頁面中，選擇系統，然後選擇右側面板中備份和還原旁邊的*啟用>備份磁碟區*。

如果備份的 Amazon S3 目標作為系統存在於控制台*系統*頁面上，則可以將ONTAP叢集拖曳到 Amazon S3 物件儲存上。

- 在備份和復原欄中選擇*卷*。從磁碟區選項卡中，選擇*操作*  圖示並選擇單一磁碟區（尚未啟用複製或備份到物件儲存）的*啟動備份*。

精靈的介紹頁面顯示保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您還沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何[啟動系統中附加磁碟區的備份](#)（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。
 - 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
 - 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區（FlexGroup磁碟區一次只能選擇一個）。若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
 - 若要備份單一卷，請選取每個卷對應的複選框。
2. 選擇“下一步”。

定義備份策略

定義備份策略涉及設定以下選項：

- 您是否需要一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構
- 本機快照策略
- 複製目標和策略



如果您選擇的磁碟區具有與您在此步驟中選擇的策略不同的快照和複製策略，則現有策略將被覆寫。

- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：
 - 本機快照：如果您正在執行複製或備份到物件存儲，則必須建立本機快照。
 - 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
 - 備份：將磁碟區備份到物件儲存。
2. 架構：如果您選擇複製和備份，請選擇下列資訊流之一：
 - 級聯：資訊從主存儲流向輔助存儲，再流向物件存儲，再從輔助存儲流向物件存儲。
 - 扇出：資訊從主存儲流向輔助存儲，再從主存儲流向物件存儲。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。

3. 本機快照：選擇現有的快照原則或建立原則。



若要在啟動快照之前建立自訂策略，請參閱["創建策略"](#)。

4. 若要建立策略，請選擇「建立新策略」並執行下列操作：
 - 輸入策略的名稱。
 - 選擇最多五個時間表，通常頻率不同。

- 對於備份到物件策略，設定 DataLock 和 Ransomware Resilience 設定。有關 DataLock 和勒索軟體恢復的詳細信息，請參閱["備份到對象策略設置"](#)。

- 選擇“創建”。

5. 複製：設定以下選項：

- 複製目標：選擇目標系統和 SVM。或者，選擇將新增至複製磁碟區名稱的目標聚合或聚合以及前綴或後綴。
- 複製策略：選擇現有的複製策略或建立策略。



若要在啟動複製之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

6. 備份到物件：如果您選擇了*備份*，請設定以下選項：

- 提供者：選擇*Amazon Web Services*。
- 提供者設定：輸入提供者詳細資訊和將儲存備份的 AWS 區域。

存取金鑰和金鑰適用於您建立的 IAM 用戶，用於授予 ONTAP 叢集對 S3 儲存桶的存取權限。

- 儲存桶：選擇現有的 S3 儲存桶或建立一個新的。參考 ["添加 S3 儲存桶"](#)。
- 加密金鑰：如果您建立了新的 S3 儲存桶，請輸入提供者提供給您的加密金鑰資訊。選擇是否使用預設的 Amazon S3 加密金鑰，或從您的 AWS 帳戶中選擇您自己的客戶管理金鑰來管理資料的加密。



如果您選擇了現有的儲存桶，加密資訊已經可用，因此您現在無需輸入。

- 網路：選擇 IP 空間，以及是否使用私有端點。預設情況下，私有端點是禁用的。
 - i. 您要備份的磁碟區所在的 ONTAP 叢集中的 IP 空間。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
 - ii. 或者，選擇是否使用您先前配置的 AWS PrivateLink。 ["查看有關將 AWS PrivateLink 用於 Amazon S3 的詳細信息"](#)。
- 備份策略：選擇現有的備份策略或建立策略。



若要在啟動備份之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。
- 將現有快照匯出至物件儲存作為備份副本：如果此系統中存在與您剛剛為此系統選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此方塊可將所有歷史快照

複製到物件儲存作為備份文件，以確保對您的磁碟區進行最全面的保護。

7. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取核取方塊*自動將快照原則標籤與複製和備份策略標籤同步*。這將建立具有與複製和備份策略中的標籤相符的標籤的快照。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括主儲存系統資料的完整副本。後續傳輸包含快照中所含主資料的差異副本。

在目標叢集中建立一個複製卷，該卷將與主儲存卷同步。

S3 儲存桶在您輸入的 S3 存取金鑰和金鑰指示的服務帳戶中創建，並且備份檔案儲存在那裡。顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用["作業監控頁面"](#)。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

使用NetApp Backup and Recovery將本機ONTAP資料備份到 Azure Blob 儲存

完成NetApp Backup and Recovery中的幾個步驟，開始將磁碟區資料從本機ONTAP系統備份到二級儲存系統和 Azure Blob 儲存體。



「本地ONTAP系統」包括FAS、AFF和ONTAP Select系統。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

識別連接方法

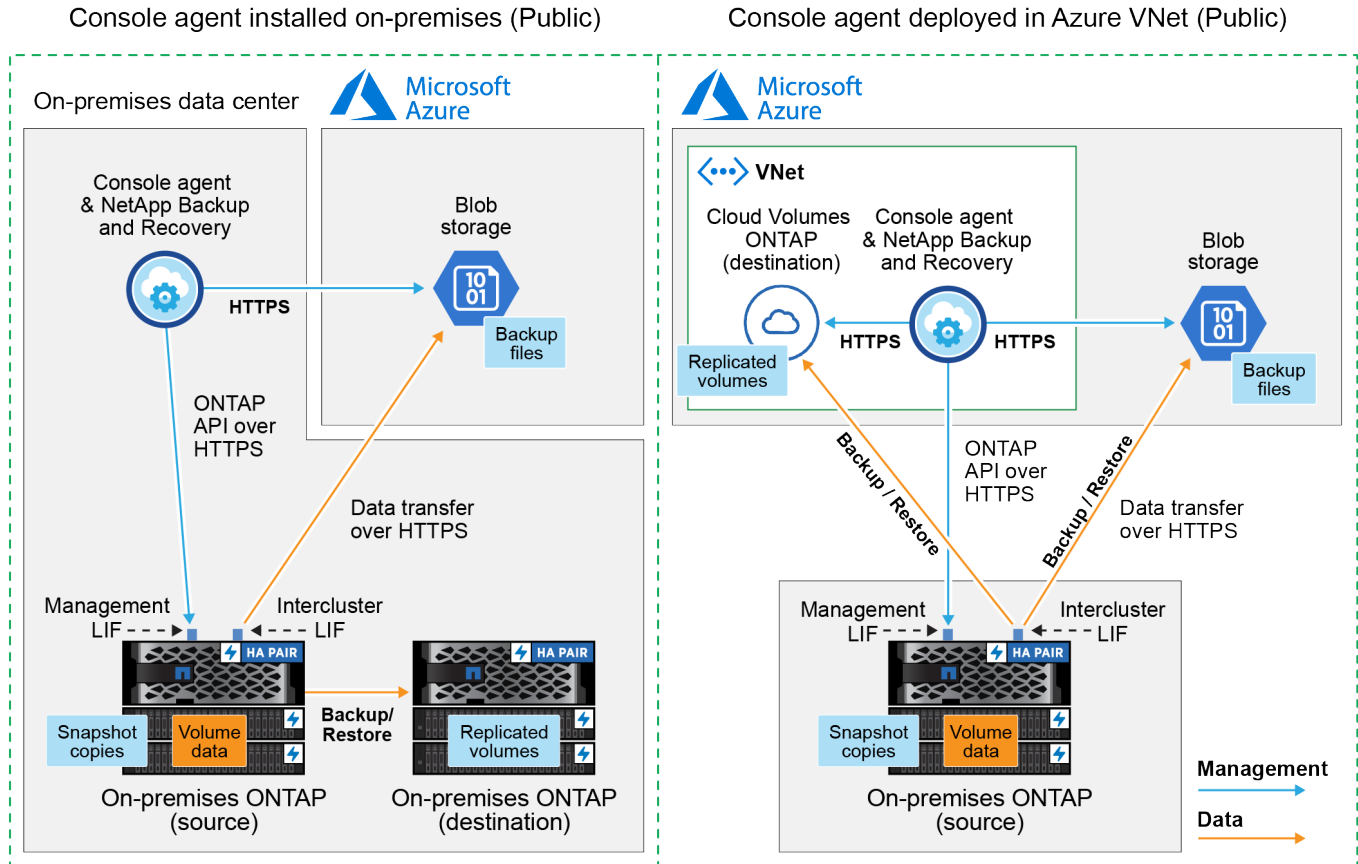
選擇在設定從本機ONTAP系統到 Azure Blob 的備份時要使用的兩種連接方法中的哪一種。

- 公用連線 - 使用公用 Azure 端點將ONTAP系統直接連接到 Azure Blob 儲存體。

- 私人連線 - 使用 VPN 或 ExpressRoute 並透過使用私人 IP 位址的 VNet 私人端點路由流量。

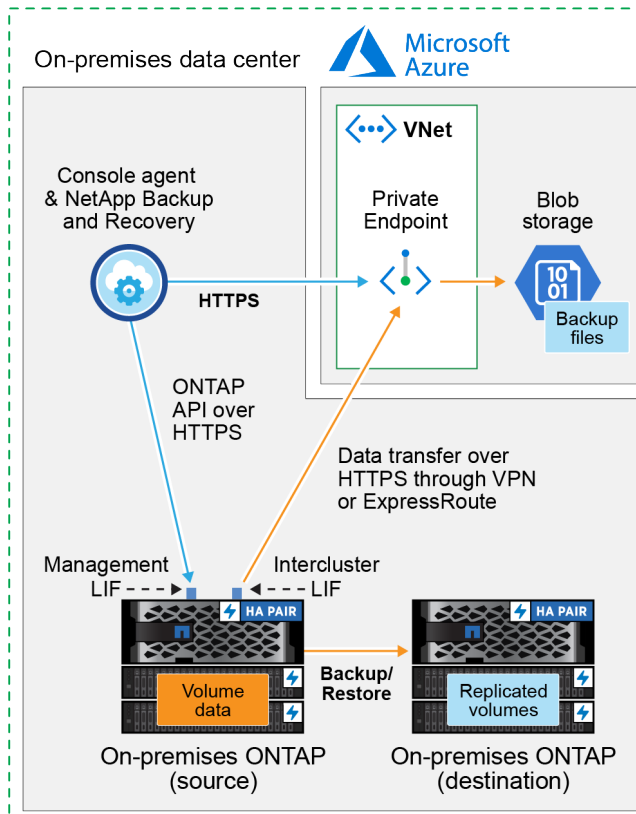
或者，您也可以使用公用或私有連線連線到用於複製磁碟區的輔助ONTAP系統。

下圖顯示了*公共連接*方法以及您需要在組件之間準備的連接。您可以使用已在本機安裝的控制台代理，或已在 Azure VNet 中部署的控制台代理程式。

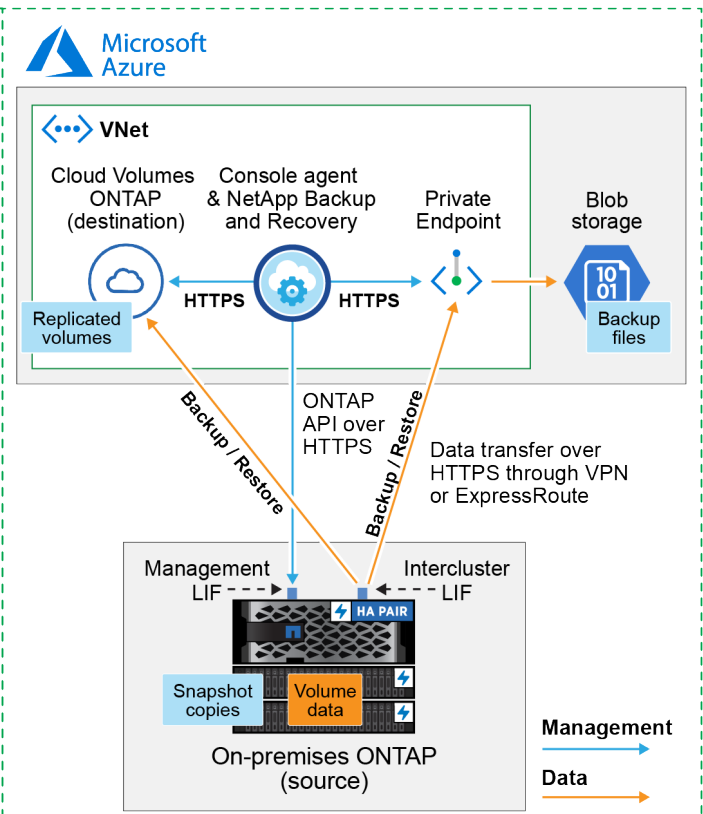


下圖顯示了*私有連接*方法以及您需要在元件之間準備的連接。您可以使用已在本機安裝的控制台代理，或已在 Azure VNet 中部署的控制台代理程式。

Console agent installed on-premises (Private)



Console agent deployed in Azure VNet (Private)



準備控制台代理

控制台代理程式是NetApp Console功能的主要軟體。需要控制台代理程式來備份和還原您的ONTAP資料。

建立或切換控制台代理

如果您已經在 Azure VNet 或本機部署了控制台代理，那麼一切就緒了。

如果沒有，那麼您需要在其中一個位置建立一個控制台代理，以將ONTAP資料備份到 Azure Blob 儲存體。您不能使用部署在其他雲端提供者的控制台代理程式。

- ["了解控制台代理"](#)
- ["在 Azure 中安裝控制台代理"](#)
- ["在您的場所安裝控制台代理"](#)
- ["在 Azure 政府區域安裝控制台代理"](#)

當控制台代理部署在雲端時（而不是安裝在您的場所），Azure 政府區域支援NetApp Backup and Recovery。此外，您必須從 Azure 市場部署控制台代理程式。您無法從 Console SaaS 網站在政府區域部署 Console 代理程式。

為控制台代理準備網路

確保控制台代理程式具有所需的網路連線。

步驟

1. 確保安裝控制台代理程式的網路啟用以下連線：
 - 透過連接埠 443 建立到 NetApp Backup and Recovery 以及 Blob 物件儲存的 HTTPS 連接(["查看端點列表"](#))
 - 透過連接埠 443 建立到 ONTAP 叢集管理 LIF 的 HTTPS 連接
 - 為了讓 NetApp Backup and Recovery 搜尋與還原功能正常運作，必須開啟連接埠 1433 以便控制台代理程式和 Azure Synapse SQL 服務之間進行通訊。
 - Azure 和 Azure 政府部署需要額外的入站安全性群組規則。看 ["Azure 中的控制台代理程式規則"](#) 了解詳情。
2. 啟用 VNet 專用終端點到 Azure 儲存體。如果您有從 ONTAP 叢集到 VNet 的 ExpressRoute 或 VPN 連接，並且希望控制台代理程式和 Blob 儲存之間的通訊保持在虛擬專用網路（*專用*連接）中，則需要這樣做。

驗證或新增控制台代理的權限

要使用 NetApp Backup and Recovery 搜尋和還原功能，您需要在控制台代理程式的角色中擁有特定權限，以便它可以存取 Azure Synapse 工作區和資料湖儲存帳戶。請參閱下面的權限，如果需要修改策略，請依照下列步驟操作。

開始之前

您必須向您的訂閱註冊 Azure Synapse Analytics 資源提供者（稱為「Microsoft.Synapse」）。 ["了解如何為您的訂閱註冊此資源提供程序"](#)。您必須是訂閱*擁有者*或*貢獻者*才能註冊資源提供者。

步驟

1. 確定指派給控制台代理虛擬機器的角色：
 - a. 在 Azure 入口網站中，開啟虛擬機器服務。
 - b. 選擇控制台代理虛擬機器。
 - c. 在*設定*下，選擇*身份*。
 - d. 選擇“Azure 角色分配”。
 - e. 記下指派給控制台代理虛擬機器的自訂角色。
2. 更新自訂角色：
 - a. 在 Azure 入口網站中，開啟你的 Azure 訂閱。
 - b. 選擇“存取控制 (IAM)”>“角色”。
 - c. 選擇自訂角色的省略號 (...)，然後選擇*編輯*。
 - d. 選擇 **JSON** 並新增以下權限：

```

"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"

```

["查看策略的完整 JSON 格式"](#)

e. 選擇*審核 + 更新*，然後選擇*更新*。

驗證許可證要求

您需要驗證 Azure 和控制台的授權需求：

- 在為叢集啟動NetApp Backup and Recovery之前，您需要訂閱 Azure 提供的即用即付 (PAYGO) 主機市場，或從NetApp購買並啟用NetApp Backup and Recovery BYOL 授權。這些許可證適用於您的帳戶，可以在多個系統中使用。
 - 對於NetApp Backup and Recovery PAYGO 許可，您需要訂閱 ["Azure 市場提供的NetApp Console"](#)。NetApp Backup and Recovery的計費透過此訂閱完成。
 - 對於NetApp Backup and Recovery BYOL 許可，您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用該服務。["了解如何管理您的 BYOL 許可證"](#)。
- 您需要對用於儲存備份的物件儲存空間進行 Azure 訂閱。

支援地區

您可以在所有區域（包括 Azure 政府區域）中建立從本機系統到 Azure Blob 的備份。您在設定服務時指定儲存備份的區域。

準備ONTAP集群

準備來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統。

準備ONTAP集群涉及以下步驟：

- 在NetApp Console中發現您的ONTAP系統
- 驗證ONTAP系統要求
- 驗證ONTAP網路要求以將資料備份到對象存儲
- 驗證ONTAP複製卷的網路要求

在NetApp Console中發現您的ONTAP系統

您的來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統都必須在NetApp Console*系統*頁面上可用。

您需要知道叢集管理 IP 位址和管理員使用者帳戶的密碼才能新增叢集。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>["了解如何發現集群"^]。

驗證ONTAP系統要求

確保您的ONTAP系統符合以下要求：

- 最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。
- SnapMirror許可證（包含在高級捆綁包或資料保護捆綁包中）。

*注意：*使用NetApp Backup and Recovery時不需要「混合雲端捆綁包」。

了解如何 ["管理您的叢集許可證"](#)。

- 時間和時區設定正確。了解如何 ["配置叢集時間"](#)。

- 如果您複製數據，請檢查來源系統和目標系統是否要執行相容的ONTAP版本。

["查看與SnapMirror關係相容的ONTAP版本"](#)。

驗證ONTAP網路要求以將資料備份到對象存儲

您必須在連接到物件儲存的系統上配置以下要求。

- 對於扇出備份架構，請在主系統上配置以下設定。
- 對於級聯備份架構，請在_輔助_系統上設定下列設定。

需滿足以下ONTAP集群網路需求：

- ONTAP叢集透過連接埠 443 啟動從叢集間 LIF 到 Azure Blob 儲存體的 HTTPS 連接，以執行備份和還原作業。

ONTAP從物件儲存讀取和寫入資料。物件儲存從不啟動，它只是響應。

- ONTAP需要從控制台代理到叢集管理 LIF 的入站連線。控制台代理程式可以駐留在 Azure VNet 中。
- 每個託管要備份的磁碟區的ONTAP節點上都需要一個叢集間 LIF。LIF 必須與ONTAP用於連接物件儲存的 *IPspace* 相關聯。["了解有關 IP 空間的更多信息"](#)。

當您設定NetApp Backup and Recovery時，系統會提示您輸入要使用的 IP 空間。您應該選擇與每個 LIF 關聯的 IP 空間。這可能是「預設」IP 空間或您建立的自訂 IP 空間。

- 節點和叢集間 LIF 能夠存取物件儲存。
- 已為磁碟區所在的儲存虛擬機器設定 DNS 伺服器。了解如何 ["為 SVM 配置 DNS 服務"](#)。
- 如果您使用的 IP 空間與預設 IP 空間不同，則可能需要建立靜態路由才能存取物件儲存。
- 如有必要，請更新防火牆規則，以允許NetApp Backup and Recovery服務透過連接埠 443 從ONTAP連接到物件存儲，並透過連接埠 53 (TCP/UDP) 從儲存虛擬機器到 DNS 伺服器的名稱解析流量。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。
- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。["查看ONTAP文件中的叢集對等前提條件"](#)。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。

準備 Azure Blob 作為備份目標

1. 您可以在啟動精靈中使用自己的自訂管理金鑰進行資料加密，而不是使用預設的 Microsoft 管理加密金鑰。在這種情況下，您將需要有 Azure 訂閱、Key Vault 名稱和金鑰。"[了解如何使用自己的密鑰](#)"。

請注意，備份和復原支援_Azure 存取策略_作為權限模型。目前不支援 Azure 基於角色的存取控制 (Azure RBAC) 權限模型。

2. 如果您希望透過公共網際網路從本機資料中心到 VNet 建立更安全的連接，則可以在啟動精靈中設定 Azure 專用端點。在這種情況下，您需要了解此連接的 VNet 和子網路。"[請參閱有關使用私有端點的詳細信息](#)"。

建立 Azure Blob 儲存體帳戶

預設情況下，該服務會為您建立儲存帳戶。如果您想使用自己的儲存帳戶，您可以在啟動備份啟動精靈之前建立它們，然後在精靈中選擇這些儲存帳戶。

"[了解有關創建自己的儲存帳戶的更多信息](#)"。

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- [\[選擇要備份的捲\]](#)
- [\[定義備份策略\]](#)
- [\[檢查您的選擇\]](#)

您還可以[顯示 API 命令](#)在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：

- 從控制台*系統*頁面中，選擇系統並選擇右側面板中備份和還原服務旁邊的*啟用>備份磁碟區*。

如果控制台*系統*頁面上存在備份的 Azure 目標，則可以將ONTAP叢集拖曳到 Azure Blob 物件儲存體上。

- 在備份和復原欄中選擇*卷*。從磁碟區選項卡中，選擇*操作*圖示並選擇單一磁碟區（尚未啟用複製或備份到物件儲存）的*啟動備份*。

精靈的介紹頁面顯示保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您還沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何[啟動系統中附加磁碟區的備份](#)（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

請注意，如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。
 - 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
 - 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區（FlexGroup磁碟區一次只能選擇一個）。若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
 - 若要備份單一卷，請選取每個卷對應的複選框。
2. 選擇“下一步”。

定義備份策略

定義備份策略涉及設定以下選項：

- 您是否需要一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構
- 本機快照策略
- 複製目標和策略



如果您選擇的磁碟區具有與您在此步驟中選擇的策略不同的快照和複製策略，則現有策略將被覆寫。

- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：
 - 本機快照：如果您正在執行複製或備份到物件存儲，則必須建立本機快照。
 - 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
 - 備份：將磁碟區備份到物件儲存。
2. 架構：如果您選擇複製和備份，請選擇下列資訊流之一：
 - 級聯：資訊從主存儲流向輔助存儲，再從輔助存儲流向物件存儲。
 - 扇出：資訊從主存儲流向輔助存儲，再從主存儲流向物件存儲。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。

3. 本機快照：選擇現有的快照原則或建立新的快照策略。



若要在啟動快照之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

4. 複製：設定以下選項：

- 複製目標：選擇目標系統和 SVM。或者，選擇將新增至複製磁碟區名稱的目標聚合或聚合以及前綴或後綴。
- 複製策略：選擇現有的複製策略或建立新的複製策略。



若要在啟動複製之前建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

5. 備份到物件：如果您選擇了*備份*，請設定以下選項：

- 提供者：選擇*Microsoft Azure*。
- 提供者設定：輸入提供者詳細資料和儲存備份的區域。

建立一個新的儲存帳戶或選擇一個現有的儲存帳戶。

建立自己的管理 Blob 容器的資源群組，或選擇資源組類型和群組。



如果您想保護備份檔案不被修改或刪除，請確保建立儲存帳戶時啟用了 30 天保留期的不可變儲存。



如果您要將較舊的備份檔案分層到 Azure 存檔儲存體以進一步最佳化成本，請確保儲存帳戶具有適當的生命週期規則。

- 加密金鑰：如果您建立了新的 Azure 儲存體帳戶，請輸入提供者提供給您的加密金鑰資訊。選擇是否使用預設 Azure 加密金鑰，或從 Azure 帳戶中選擇您自己的客戶管理金鑰來管理資料加密。

如果您選擇使用自己的客戶管理金鑰，請輸入金鑰保管庫和金鑰資訊。



如果您選擇了現有的 Microsoft 儲存帳戶，加密資訊已經可用，因此您現在無需輸入。

- 網路：選擇 IP 空間，以及是否使用私有端點。預設情況下，私有端點是禁用的。
 - i. 您要備份的磁碟區所在的ONTAP叢集中的 IP 空間。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。
 - ii. 或者，選擇是否使用先前設定的 Azure 專用終端點。"[了解如何使用 Azure 專用終結點](#)"。
- 備份策略：選擇現有的備份到物件儲存策略或建立新的策略。



若要在啟動備份之前建立自訂策略，請參閱"[創建策略](#)"。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
 - 選擇最多五個時間表，通常頻率不同。
 - 對於備份到物件策略，設定 DataLock 和 Ransomware Resilience 設定。有關 DataLock 和勒索軟體恢復的詳細信息，請參閱"[備份到對象策略設置](#)"。
 - 選擇“創建”。
- 將現有快照匯出至物件儲存作為備份副本：如果此系統中存在與您剛剛為此系統選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此方塊可將所有歷史快照複製到物件儲存作為備份文件，以確保對您的磁碟區進行最全面的保護。

6. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取核取方塊*自動將快照原則標籤與複製和備份策略標籤同步*。這將建立具有與複製和備份策略中的標籤相符的標籤的快照。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括主儲存系統資料的完整副本。後續傳輸包含快照中包含的主儲存系統資料的差異副本。

在目標群集中建立一個複製卷，該複製卷將與主卷同步。

在您輸入的資源組中建立一個 Blob 儲存帳戶，並將備份檔案儲存在那裡。顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用"[作業監控頁面](#)"。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

使用NetApp Backup and Recovery將本地ONTAP資料備份到 Google Cloud Storage

完成NetApp Backup and Recovery中的幾個步驟，開始將磁碟區資料從本機主ONTAP系統備份到二級儲存系統和 Google Cloud Storage。



「本地ONTAP系統」包括FAS、AFF和ONTAP Select系統。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

識別連接方法

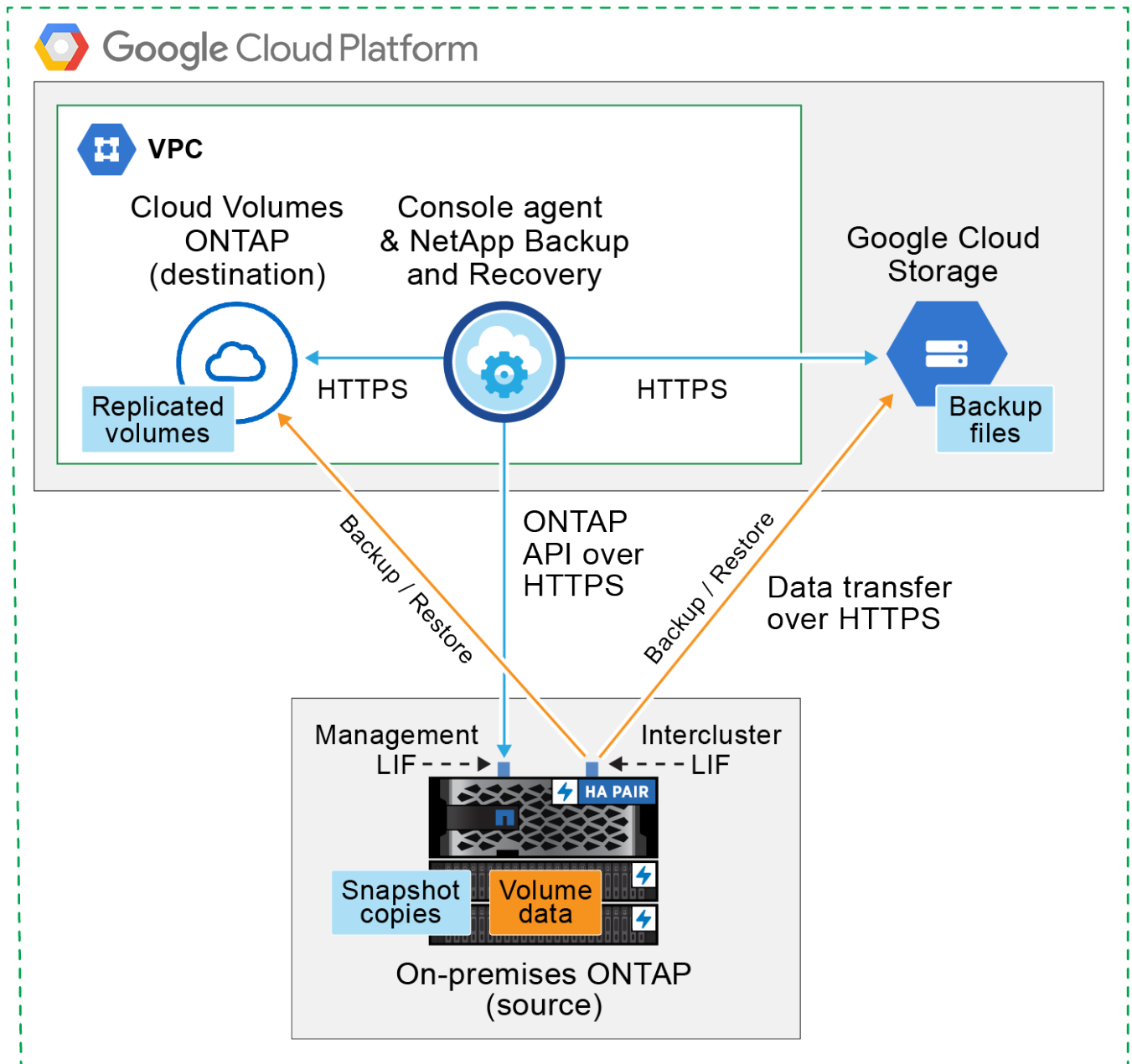
選擇在設定從本機ONTAP系統到 Google Cloud Storage 的備份時要使用的兩種連接方法中的哪一種。

- 公共連線 - 使用公共 Google 端點將ONTAP系統直接連接到 Google Cloud Storage。
- 私人連接 - 使用 VPN 或 Google Cloud Interconnect 並透過使用私人 IP 位址的私人 Google Access 介面路由流量。

或者，您也可以使用公用或私有連線連線到用於複製磁碟區的輔助ONTAP系統。

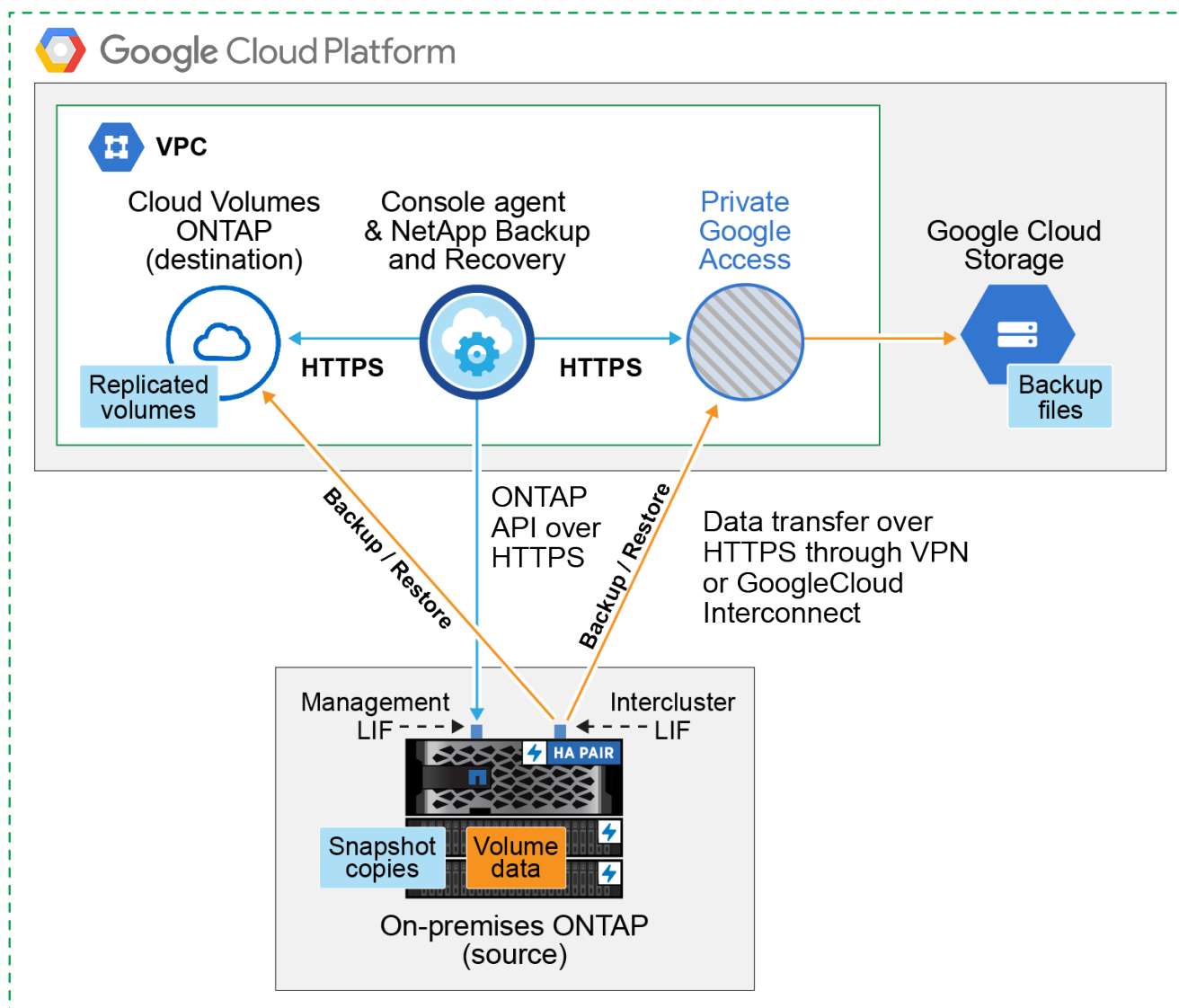
下圖顯示了*公共連接*方法以及您需要在組件之間準備的連接。控制台代理程式必須部署在 Google Cloud Platform VPC 中。

Console agent deployed in Google Cloud VPC (Public)



下圖顯示了*私有連接*方法以及您需要在元件之間準備的連接。控制台代理程式必須部署在 Google Cloud Platform VPC 中。

Console agent deployed in Google Cloud VPC (Private)



準備控制台代理

控制台代理程式是控制台功能的主要軟體。需要控制台代理程式來備份和還原您的ONTAP資料。

建立或切換控制台代理

如果您已經在 Google Cloud Platform VPC 中部署了控制台代理，那麼一切就緒了。

如果沒有，那麼您需要在該位置建立一個控制台代理，以將ONTAP資料備份到 Google Cloud Storage。您不能使用部署在其他雲端提供者或本機的控制台代理程式。

- ["了解控制台代理"](#)
- ["在 GCP 中安裝控制台代理"](#)

為控制台代理準備網絡

確保控制台代理程式具有所需的網路連線。

步驟

1. 確保安裝控制台代理程式的網路啟用以下連線：

- 透過連接埠 443 建立到NetApp Backup and Recovery以及您的 Google Cloud 儲存的 HTTPS 連接(["查看端點列表"](#))
- 透過連接埠 443 建立到ONTAP叢集管理 LIF 的 HTTPS 連接

2. 在您規劃部署控制台代理程式的子網路上啟用私人 Google Access（或私人服務連線）。"[私人 Google 存取權限](#)"或者 "[私人服務連接](#)"如果您有從ONTAP叢集到 VPC 的直接連接，並且希望控制台代理程式和 Google Cloud Storage 之間的通訊保持在虛擬專用網路（*專用*連接）中，則需要。

請按照 Google 說明設定這些私人存取選項。確保您的 DNS 伺服器已配置為指向 `www.googleapis.com` 和 `storage.googleapis.com` 到正確的內部（私有）IP 位址。

驗證或新增控制台代理的權限

要使用NetApp Backup and Recovery的「搜尋和復原」功能，您需要在控制台代理的角色中擁有特定權限，以便它可以存取 Google Cloud BigQuery 服務。查看以下權限，如果需要修改策略，請依照下列步驟操作。

步驟

1. 在 "[Google 雲端控制台](#)"，轉到*角色*頁面。
2. 使用頁面頂部的下拉列表，選擇包含要編輯的角色的項目或組織。
3. 選擇自訂角色。
4. 選擇*編輯角色*來更新角色的權限。
5. 選擇*新增權限*為角色新增下列新權限。

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. 選擇*更新*以儲存編輯的角色。

驗證許可證要求

- 在為叢集啟動NetApp Backup and Recovery之前，您需要訂閱 Google 提供的即用即付 (PAYGO) 主機市場，或從NetApp購買並啟用NetApp Backup and Recovery BYOL 授權。這些許可證適用於您的帳戶，可以在

多個系統中使用。

- 對於NetApp Backup and Recovery PAYGO 許可，您需要訂閱 ["Google Marketplace 提供的NetApp Console"](#)。NetApp Backup and Recovery的計費透過此訂閱完成。
- 對於NetApp Backup and Recovery BYOL 許可，您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用該服務。["了解如何管理您的 BYOL 許可證"](#)。
- 您需要向 Google 訂閱用於儲存備份的物件儲存空間。

支援地區

您可以從本機系統建立備份到所有地區的 Google Cloud Storage。您在設定服務時指定儲存備份的區域。

準備ONTAP集群

準備來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統。

準備ONTAP集群涉及以下步驟：

- 在NetApp Console中發現您的ONTAP系統
- 驗證ONTAP系統要求
- 驗證ONTAP網路要求以將資料備份到對象存儲
- 驗證ONTAP複製卷的網路要求

在NetApp Console中發現您的ONTAP系統

您的來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統都必須在NetApp Console*系統* 頁面上可用。

您需要知道叢集管理 IP 位址和管理員使用者帳戶的密碼才能新增叢集。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>[\["了解如何發現集群"\]](#)。

驗證ONTAP系統要求

確保您的ONTAP系統符合以下要求：

- 最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。
- SnapMirror許可證（包含在高級捆綁包或資料保護捆綁包中）。

*注意：*使用NetApp Backup and Recovery時不需要「混合雲端捆綁包」。

了解如何 ["管理您的叢集許可證"](#)。

- 時間和時區設定正確。了解如何 ["配置叢集時間"](#)。
- 如果您複製數據，請檢查來源系統和目標系統是否要執行相容的ONTAP版本。

["查看與SnapMirror關係相容的ONTAP版本"](#)。

驗證ONTAP網路要求以將資料備份到對象存儲

您必須在連接到物件儲存的系統上配置以下要求。

- 對於扇出備份架構，請在主系統上配置以下設定。
- 對於級聯備份架構，請在_輔助_系統上設定下列設定。

需滿足以下ONTAP集群網路需求：

- ONTAP叢集透過連接埠 443 啟動從叢集間 LIF 到 Google Cloud Storage 的 HTTPS 連接，以進行備份和還原作業。

ONTAP從物件儲存讀取和寫入資料。物件儲存從不啟動，它只是響應。

- ONTAP需要從控制台代理到叢集管理 LIF 的入站連線。控制台代理可以駐留在 Google Cloud Platform VPC 中。
- 每個託管要備份的磁碟區的ONTAP節點上都需要一個叢集間 LIF。LIF 必須與ONTAP用於連接物件儲存的 *IPspace* 相關聯。["了解有關 IP 空間的更多信息"](#)。

當您設定NetApp Backup and Recovery時，系統會提示您輸入要使用的 IP 空間。您應該選擇與每個 LIF 關聯的 IP 空間。這可能是「預設」IP 空間或您建立的自訂 IP 空間。

- 節點的叢集間 LIF 能夠存取物件儲存。
- 已為磁碟區所在的儲存虛擬機器設定 DNS 伺服器。了解如何 ["為 SVM 配置 DNS 服務"](#)。

如果您使用的是 Private Google Access 或 Private Service Connect，請確保您的 DNS 伺服器已設定為指向 `storage.googleapis.com` 到正確的內部（私有）IP 位址。

- 請注意，如果您使用的 IP 空間與預設 IP 空間不同，則可能需要建立靜態路由才能存取物件儲存。
- 如有必要，請更新防火牆規則，以允許NetApp Backup and Recovery透過連接埠 443 從ONTAP連接到物件存儲，並透過連接埠 53（TCP/UDP）從儲存虛擬機器到 DNS 伺服器的名稱解析流量。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。
- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。["查看ONTAP文件中的叢集對等前提條件"](#)。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。

準備 Google Cloud Storage 作為備份目標

準備 Google Cloud Storage 作為備份目標涉及以下步驟：

- 設定權限。
- (可選) 創建您自己的儲存桶。(如果您願意，該服務將為您建立儲存桶。)
- (可選) 設定客戶管理的金鑰以進行資料加密

設定權限

您需要使用自訂角色為具有特定權限的服務帳戶提供儲存存取金鑰。服務帳戶使NetApp Backup and Recovery能夠驗證和存取用於儲存備份的 Cloud Storage 儲存桶。需要金鑰，以便 Google Cloud Storage 知道誰在發出請求。

步驟

1. 在 ["Google 雲端控制台"](#)，轉到*角色*頁面。
2. ["創建新角色"](#)具有以下權限：

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. 在 Google Cloud 控制台中，["前往服務帳戶頁面"](#)。
4. 選擇您的雲端項目。
5. 選擇*建立服務帳戶*並提供所需資訊：
 - a. 服務帳戶詳細資料：輸入名稱和描述。
 - b. 授予此服務帳戶存取項目的權限：選擇您剛剛建立的自訂角色。
 - c. 選擇*完成*。
6. 前往 ["GCP 儲存設定"](#)並為服務帳戶建立存取金鑰：
 - a. 選擇一個項目，然後選擇*互通性*。如果您還沒有這樣做，請選擇*啟用互通性存取*。
 - b. 在*服務帳戶的存取金鑰*下，選擇*為服務帳戶建立金鑰*，選擇剛剛建立的服務帳戶，然後按一下*建立金鑰*。

稍後設定備份服務時，您需要在NetApp Backup and Recovery中輸入金鑰。

建立您自己的儲存桶

預設情況下，該服務會為您建立儲存桶。或者，如果您想使用自己的儲存桶，您可以在啟動備份啟動精靈之前建立它們，然後在精靈中選擇這些儲存桶。

["了解有關創建您自己的存儲桶的更多信息"](#)。

設定客戶管理的加密金鑰 (CMEK) 以進行資料加密

您可以使用自己的客戶管理金鑰進行資料加密，而不是使用預設的 Google 管理加密金鑰。跨區域和跨項目密鑰均受支持，因此您可以為儲存桶選擇與 CMEK 密鑰的項目不同的項目。

如果您打算使用自己的客戶管理金鑰：

- 您需要有密鑰環和密鑰名稱，以便可以在啟動精靈中新增此資訊。 ["了解有關客戶管理加密金鑰的更多信息"](#)。
- 您需要驗證控制台代理程式的角色是否包含這些必要的權限：

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 您需要驗證您的專案中是否啟用了 Google 「雲端金鑰管理服務 (KMS)」 API。查看 ["Google Cloud 文件：啟用 API"](#) 了解詳情。

CMEK 注意事項：

- 支援 HSM（硬體支援）和軟體產生的金鑰。
- 支援新建立或匯入的 Cloud KMS 金鑰。
- 僅支援區域密鑰，不支援全域密鑰。
- 目前僅支援“對稱加密/解密”目的。
- NetApp Backup and Recovery 為與儲存帳戶關聯的服務代理程式指派了「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM 角色。

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- [\[選擇要備份的捲\]](#)
- [\[定義備份策略\]](#)

- [\[檢查您的選擇\]](#)

您還可以[顯示 API 命令](#)在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：

- 從控制台*系統*頁面中，選擇系統，然後選擇右側面板中備份和還原旁邊的*啟用>備份磁碟區*。

如果您的備份的 Google Cloud Storage 目標存在於控制台 系統 頁面上，則可以將ONTAP叢集拖曳到 Google Cloud 物件儲存上。

- 在備份和復原欄中選擇*卷*。從磁碟區選項卡中，選擇*操作*  圖示並選擇單一磁碟區（尚未啟用複製或備份到物件儲存）的*啟動備份*。

精靈的介紹頁面顯示保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您還沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何"[啟動系統中附加磁碟區的備份](#)"（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。

- 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
- 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區（FlexGroup磁碟區一次只能選擇一個）。若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
- 若要備份單一卷，請選取每個卷對應的複選框。

2. 選擇“下一步”。

定義備份策略

定義備份策略涉及設定以下選項：

- 您是否需要一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構
- 本機快照策略
- 複製目標和策略



如果您選擇的磁碟區具有與您在此步驟中選擇的策略不同的快照和複製策略，則現有策略將被覆寫。

- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：

- 本機快照：如果您正在執行複製或備份到物件存儲，則必須建立本機快照。
- 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
- 備份：將磁碟區備份到物件儲存。

2. 架構：如果您選擇複製和備份，請選擇下列資訊流之一：

- 級聯：資訊從主存儲流向輔助存儲，再從輔助存儲流向物件存儲。
- 扇出：資訊從主存儲流向輔助存儲，再從主存儲流向物件存儲。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。

3. 本機快照：選擇現有的快照原則或建立新的快照策略。



若要建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

4. 複製：設定以下選項：

- 複製目標：選擇目標系統和 SVM。或者，選擇將新增至複製磁碟區名稱的目標聚合或聚合以及前綴或後綴。
- 複製策略：選擇現有的複製策略或建立新的複製策略。



若要建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

5. 備份到物件：如果您選擇了*備份*，請設定以下選項：

- 提供者：選擇*Google Cloud*。
- 提供者設定：輸入提供者詳細資料和儲存備份的區域。

建立新儲存桶或選擇已建立的儲存桶。



如果您希望將較舊的備份檔案分層到 Google Cloud Archive 儲存空間以進一步優化成本，請確保儲存桶具有適當的生命週期規則。

輸入 Google Cloud 存取金鑰和金鑰。

- 加密金鑰：如果您建立了新的 Google Cloud 儲存帳戶，請輸入提供者提供給您的加密金鑰資訊。選擇是否使用預設的 Google Cloud 加密金鑰，或從您的 Google Cloud 帳戶中選擇您自己的客戶管理金鑰來管理您的資料加密。



如果您選擇了現有的 Google Cloud 儲存帳戶，加密資訊已經可用，因此您現在無需輸入。

如果您選擇使用自己的客戶管理金鑰，請輸入金鑰環和金鑰名稱。 ["了解有關客戶管理加密金鑰的更多信息"](#)。

- 網路：選擇 IP 空間。

您要備份的磁碟區所在的ONTAP叢集中的 IP 空間。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限。

- 備份策略：選擇現有的備份到物件儲存策略或建立新的策略。



若要建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。
- 將現有快照匯出至物件儲存作為備份副本：如果此系統中存在與您剛剛為此系統選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此方塊可將所有歷史快照複製到物件儲存作為備份文件，以確保對您的磁碟區進行最全面的保護。

6. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取核取方塊*自動將快照原則標籤與複製和備份策略標籤同步*。這將建立具有與複製和備份策略中的標籤相符的標籤的快照。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括主儲存系統資料的完整副本。後續傳輸包含快照中包含的主儲存系統資料的差異副本。

在目標群集中建立一個複製卷，該卷將與來源卷同步。

系統會在您輸入的 Google 存取金鑰和金鑰所指示的服務帳戶中自動建立 Google Cloud Storage 儲存桶，並將備份檔案儲存在那裡。顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用["作業監控頁面"](#)。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

使用NetApp Backup and Recovery將本機ONTAP資料備份到ONTAP S3

完成NetApp Backup and Recovery中的幾個步驟即可開始從主本機ONTAP系統備份磁碟區資料。您可以將備份傳送至輔助ONTAP儲存系統（複製磁碟區）或設定為 S3 伺服器的ONTAP系統上的儲存桶（備份檔案），或同時傳送至兩者。

主本地ONTAP系統可以是FAS、AFF或ONTAP Select系統。輔助ONTAP系統可以是本機ONTAP或Cloud Volumes ONTAP系統。物件儲存可以位於本機ONTAP系統或已啟用簡單儲存服務 (S3) 物件儲存伺服器的Cloud Volumes ONTAP系統上。



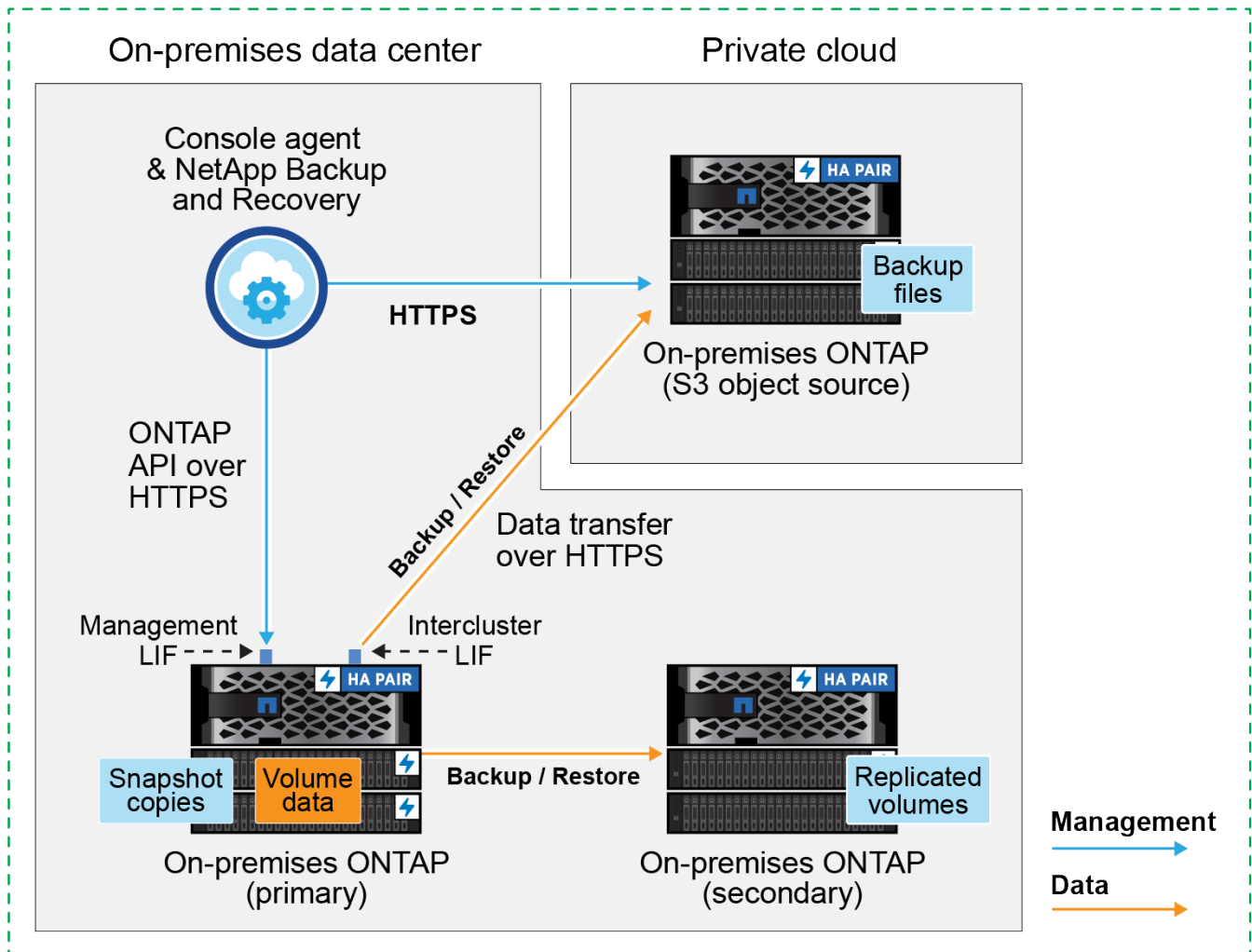
若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

識別連接方法

您可以使用多種配置在ONTAP系統上建立 S3 儲存桶的備份。下面顯示了兩種情況。

下圖顯示了將主本機ONTAP系統備份到為 S3 配置的本機ONTAP系統時的每個元件以及您需要在它們之間準備的連線。它還顯示了與同一本地位置的輔助ONTAP系統的連接以複製磁碟區。

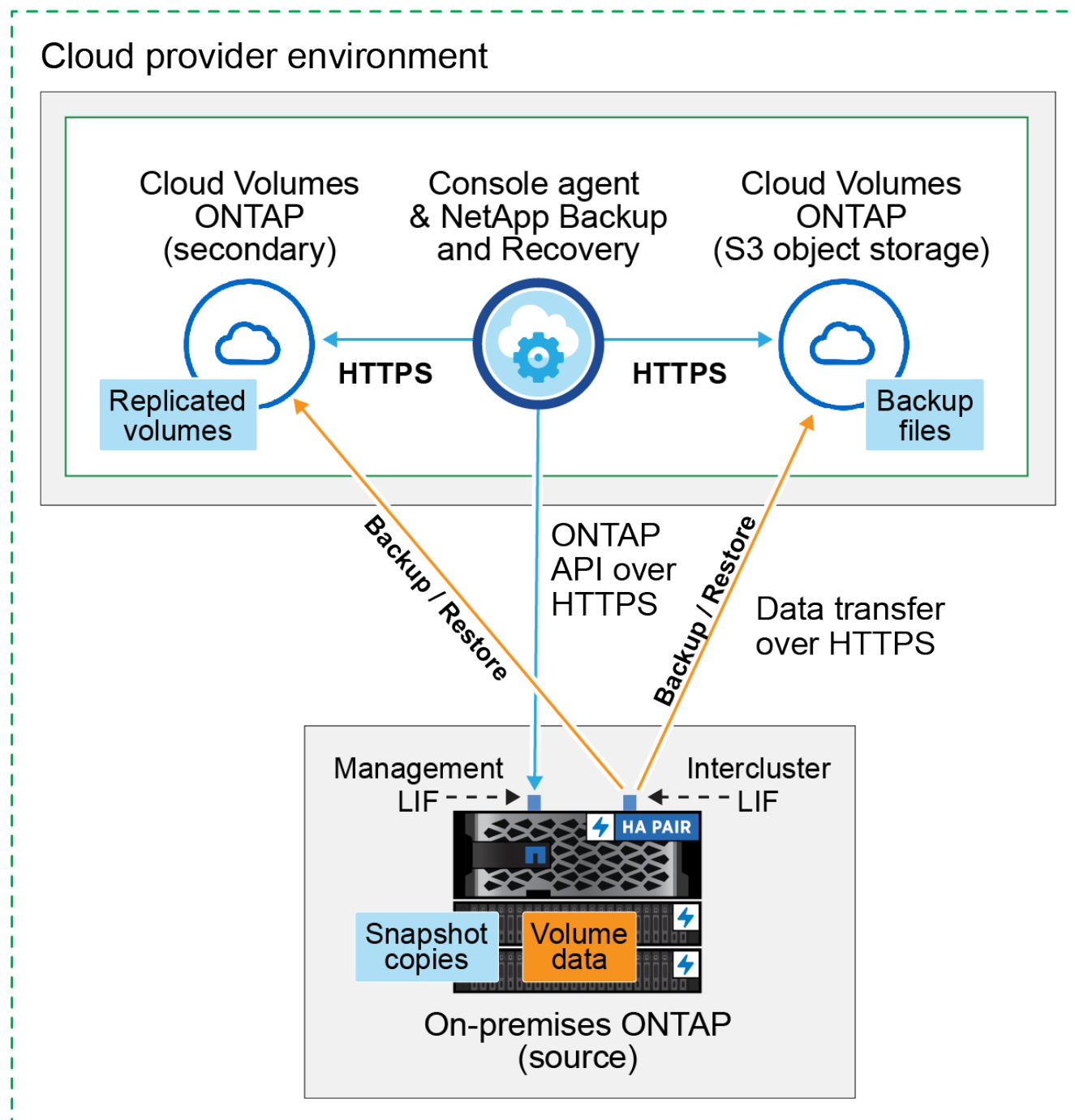
Console agent installed on premises (Public)



當控制台代理程式和主本機ONTAP系統安裝在沒有網際網路存取的本機位置（「私有」模式部署）時，ONTAP S3 系統必須位於同一個本機資料中心。

下圖顯示了將主本地ONTAP系統備份到為 S3 配置的Cloud Volumes ONTAP系統時的每個元件以及您需要在它們之間準備的連接。它還顯示了與同一雲端提供者環境中的輔助Cloud Volumes ONTAP系統的連接，以複製磁碟區。

Console agent deployed in cloud (Public)



在這種情況下，控制台代理應部署在部署Cloud Volumes ONTAP系統的相同雲端提供者環境中。

準備控制台代理

控制台代理程式是控制台功能的主要軟體。需要控制台代理程式來備份和還原您的ONTAP資料。

建立或切換控制台代理

當您將資料備份到ONTAP S3 時，您的本機或雲端中必須有控制台代理。您需要安裝新的控制台代理，或確保

目前選定的控制台代理位於其中一個位置。本機控制台代理程式可以安裝在有或沒有網路存取的網站中。

- ["了解控制台代理"](#)
- ["在您的雲端環境中安裝控制台代理"](#)
- ["在具有網際網路存取權限的 Linux 主機上安裝控制台代理"](#)
- ["在沒有網際網路存取的 Linux 主機上安裝控制台代理"](#)
- ["在控制台代理之間切換"](#)

準備控制台代理網路要求

確保安裝控制台代理程式的網路啟用以下連線：

- 透過連接埠 443 到ONTAP S3 伺服器的 HTTPS 連接
- 透過連接埠 443 建立到來源ONTAP叢集管理 LIF 的 HTTPS 連接
- 透過連接埠 443 到NetApp Backup and Recovery 的出站網路連線（當控制台代理安裝在「暗站」時不需要）

私人模式（暗站）注意事項

NetApp Backup and Recovery功能內建於控制台代理程式中。以私人模式安裝時，您需要定期更新控制台代理軟體才能存取新功能。檢查["NetApp Backup and Recovery新功能"](#)查看每個NetApp Backup and Recovery版本中的新功能。當您想要使用新功能時，請按照以下步驟操作 ["升級控制台代理軟體"](#)。

當您在標準 SaaS 環境中使用NetApp Backup and Recovery時， NetApp Backup and Recovery設定資料將會備份到雲端。當您在沒有網路存取的網站中使用NetApp Backup and Recovery時， NetApp Backup and Recovery設定資料將備份到儲存備份的ONTAP S3 儲存桶中。

驗證許可證要求

在為叢集啟動NetApp Backup and Recovery之前，您需要從NetApp購買並啟動NetApp Backup and Recovery BYOL 授權。此授權用於備份和還原物件儲存 - 建立快照或複製磁碟區不需要授權。此許可證適用於該帳戶，可跨多個系統使用。

您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用本服務。["了解如何管理您的 BYOL 許可證"](#)。



將檔案備份到ONTAP S3 時不支援 PAYGO 授權。

準備ONTAP集群

準備來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統。

準備ONTAP集群涉及以下步驟：

- 在NetApp Console中發現您的ONTAP系統
- 驗證ONTAP系統要求
- 驗證ONTAP網路要求以將資料備份到對象存儲

- 驗證ONTAP複製卷的網路要求

在NetApp Console中發現您的ONTAP系統

您的來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統都必須在NetApp Console*系統*頁面上可用。

您需要知道叢集管理 IP 位址和管理員使用者帳戶的密碼才能新增叢集。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["了解如何發現集群"^]。

驗證ONTAP系統要求

確保您的ONTAP系統符合以下要求：

- 最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。
- SnapMirror許可證（包含在高級捆綁包或資料保護捆綁包中）。

*注意：*使用NetApp Backup and Recovery時不需要「混合雲端捆綁包」。

了解如何 ["管理您的叢集許可證"](#)。

- 時間和時區設定正確。了解如何 ["配置叢集時間"](#)。
- 如果您複製數據，請檢查來源系統和目標系統是否要執行相容的ONTAP版本。

["查看與SnapMirror關係相容的ONTAP版本"](#)。

驗證ONTAP網路要求以將資料備份到對象存儲

您必須確保連接到物件儲存的系統符合以下要求。



- 當您使用扇出備份架構時，必須在主儲存系統上設定設定。
- 當您使用級聯備份架構時，必須在_輔助_儲存系統上設定設定。

["了解有關備份架構類型的更多信息"](#)。

需滿足以下ONTAP集群網路需求：

- ONTAP叢集透過使用者指定的連接埠從叢集間 LIF 啟動到ONTAP S3 伺服器的 HTTPS 連接，以執行備份和還原作業。此連接埠可在備份設定期間配置。

ONTAP從物件儲存讀取和寫入資料。物件儲存從不啟動，它只是響應。

- ONTAP需要從控制台代理到叢集管理 LIF 的入站連線。
- 每個託管要備份的磁碟區的ONTAP節點上都需要一個叢集間 LIF。LIF 必須與ONTAP用於連接物件儲存的 IPspace 相關聯。 ["了解有關 IP 空間的更多信息"](#)。

當您設定NetApp Backup and Recovery時，系統會提示您輸入要使用的 IP 空間。您應該選擇與每個 LIF 關聯的 IP 空間。這可能是「預設」 IP 空間或您建立的自訂 IP 空間。

- 節點的群集間 LIF 能夠存取物件儲存（當控制台代理安裝在「暗」站點時不需要）。
- 已為磁碟區所在的儲存虛擬機器設定 DNS 伺服器。了解如何 ["為 SVM 配置 DNS 服務"](#)。
- 如果您使用的 IP 空間與預設 IP 空間不同，則可能需要建立靜態路由才能存取物件儲存。
- 如有必要，請更新防火牆規則，以允許NetApp Backup and Recovery服務透過您指定的連接埠（通常為連接埠 443）從ONTAP連接到物件儲存，並透過連接埠 53（TCP/UDP）從儲存虛擬機器到 DNS 伺服器的名稱解析流量。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。
- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。 ["查看ONTAP文件中的叢集對等前提條件"](#)。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。

準備ONTAP S3 作為備份目標

您必須在計畫用於物件儲存備份的ONTAP叢集中啟用簡單儲存服務 (S3) 物件儲存伺服器。查看 ["ONTAP S3 文檔"](#)了解詳情。

*注意：*您可以將此叢集新增至控制台*系統*頁面，但它不會被識別為 S3 物件儲存伺服器，並且您無法將來源系統拖曳到此 S3 系統上以啟動備用啟動。

此ONTAP系統必須符合以下要求。

支援的 ONTAP 版本

本機ONTAP系統需要ONTAP 9.8 及更高版本。 Cloud Volumes ONTAP系統需要ONTAP 9.9.1 及更高版本。

S3 憑證

您必須建立 S3 使用者來控制對ONTAP S3 儲存的存取。 ["有關詳細信息，請參閱ONTAP S3 文檔"](#)。

當您設定備份到ONTAP S3 時，備份精靈會提示您輸入使用者帳戶的 S3 存取金鑰和金鑰。該用戶帳戶使NetApp Backup and Recovery能夠驗證和存取用於儲存備份的ONTAP S3 儲存桶。需要金鑰，以便ONTAP S3 知道誰在發出請求。

這些存取金鑰必須與具有以下權限的使用者相關聯：

```
"s3:ListAllMyBuckets",  
"s3:ListBucket",  
"s3:GetObject",  
"s3:PutObject",  
"s3:DeleteObject",  
"s3:CreateBucket",  
"s3:GetBucketLocation"
```

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- 選擇要備份的捲
- 定義備份策略和政策
- 檢查您的選擇

您還可以[顯示 API 命令](#)在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：

- 從控制台*系統*頁面中，選擇系統，然後選擇右側面板中備份和還原旁邊的*啟用>備份磁碟區*。
- 在備份和復原欄中選擇*卷*。從「磁碟區」標籤中，選擇「操作 (...)」選項，然後為單一磁碟區（尚未啟用複製或備份到物件儲存）選擇「啟動備份」。

精靈的簡介頁面顯示了保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何["啟動系統中附加磁碟區的備份"](#)（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

請注意，如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。
 - 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
 - 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區（FlexGroup磁碟區一次只能選擇一個）。若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
 - 若要備份單一卷，請選取每個卷對應的複選框。
2. 選擇“下一步”。

定義備份策略

定義備份策略涉及配置以下選項：

- 保護選項：您是否要實施一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構：您是否要使用扇出式或級聯備份架構
- 本機快照策略
- 複製目標和策略
- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：
 - 本機快照：建立本機快照。
 - 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
 - 備份：將磁碟區備份到為 S3 設定的ONTAP系統上的儲存桶。
2. 架構：如果您同時選擇了複製和備份，請選擇下列資訊流之一：
 - 級聯：備份資料從主系統流向輔助系統，然後從輔助系統流向物件儲存。
 - 扇出：備份資料從主系統流向輔助系統，並從主系統流向物件儲存。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。

3. 本機快照：選擇現有的快照原則或建立新的快照策略。



如果您想要在啟動快照之前建立自訂策略，則可以使用 System Manager 或ONTAP CLI ``snapmirror policy create`` 命令。參考。



若要使用備份和復原建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

4. 複製：如果選擇了*複製*，請設定以下選項：

- 複製目標：選擇目標系統和 SVM。或者，選擇目標聚合（或FlexGroup磁碟區的聚合）以及將新增至複製磁碟區名稱的前綴或後綴。
- 複製策略：選擇現有的複製策略或建立新的複製策略。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

5. 備份到物件：如果您選擇了*備份*，請設定以下選項：

- 提供者：選擇* ONTAP S3*。
- 提供者設定：輸入 S3 伺服器 FQDN 詳細資料、連接埠以及使用者的存取金鑰和金鑰。

存取金鑰和金鑰用於您建立的用戶，以授予ONTAP叢集對 S3 儲存桶的存取權限。

- 網路：選擇要備份的磁碟區所在的來源ONTAP叢集中的 IP 空間。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限（當控制台代理安裝在「暗站」時不需要）。



選擇正確的 IP 空間可確保NetApp Backup and Recovery可以建立從ONTAP到ONTAP S3 物件儲存的連線。

- 備份策略：選擇現有的備份策略或建立新的備份策略。



您可以使用 System Manager 或ONTAP CLI 建立政策。使用ONTAP CLI 建立自訂策略`snapmirror policy create`命令，請參閱。



若要使用備份和復原建立自訂策略，請參閱[“創建策略”](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 對於備份到物件策略，設定 DataLock 和 Ransomware Resilience 設定。有關 DataLock 和勒索軟體恢復的詳細信息，請參閱[“備份到對象策略設置”](#)。
- 選擇“創建”。
- 將現有快照匯出至物件儲存作為備份檔案：如果此系統中存在與您剛剛選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此方塊可將所有歷史快照複製到物件儲存作為備份文件，以確保對您的磁碟區進行最全面的保護。

6. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取核取方塊*自動將快照原則標籤與複製和備份策略標籤同步*。這將建立具有與複製和備份策略中的標籤相符的標籤的快照。如果策略不匹配，則不會建立備份。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括來源資料的完整副本。後續傳輸包含快照中包含的主儲存資料的差異副本。

在目標叢集中建立一個複製卷，該卷將與主儲存卷同步。

在您輸入的 S3 存取金鑰和金鑰指示的服務帳戶中建立一個 S3 儲存桶，並將備份檔案儲存在那裡。

顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用["作業監控頁面"](#)。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

使用NetApp Backup and Recovery將本機ONTAP資料備份到StorageGRID

完成NetApp Backup and Recovery中的幾個步驟，開始將磁碟區資料從本機主ONTAP系統備份到二級儲存系統以及NetApp StorageGRID系統中的物件儲存。



「本地ONTAP系統」包括FAS、AFF和ONTAP Select系統。

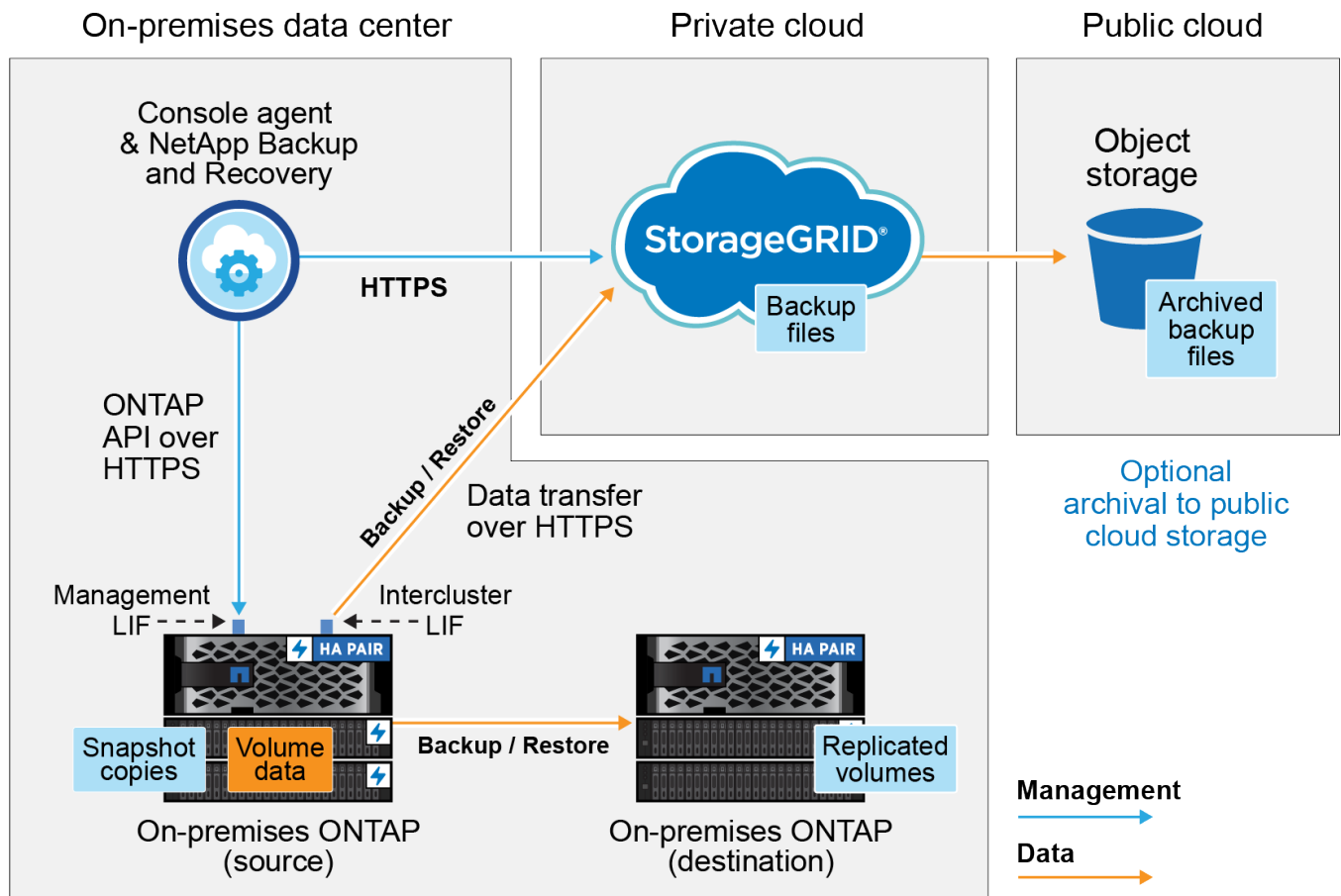


若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

識別連接方法

下圖顯示了將本機ONTAP系統備份到StorageGRID時的每個元件以及您需要在它們之間準備的連線。

或者，您可以連接到相同本機位置的輔助ONTAP系統來複製磁碟區。



當控制台代理程式和本機ONTAP系統安裝在沒有網際網路存取的本機位置（「暗站」）時，StorageGRID系統必須位於同一個本機資料中心。暗站配置不支援將舊備份檔案存檔到公有雲。

準備控制台代理

控制台代理程式是控制台功能的主要軟體。需要控制台代理程式來備份和還原您的ONTAP資料。

建立或切換控制台代理

當您將資料備份到StorageGRID時，您的場所必須有控制台代理。您需要安裝新的控制台代理程式或確保目前選定的控制台代理程式位於本機。控制台代理可以安裝在有或沒有網路存取的網站。

- ["了解控制台代理"](#)
- ["在具有網際網路存取權限的 Linux 主機上安裝控制台代理"](#)
- ["在沒有網際網路存取的 Linux 主機上安裝控制台代理"](#)
- ["在控制台代理之間切換"](#)

準備控制台代理網路要求

確保安裝控制台代理程式的網路啟用以下連線：

- 透過連接埠 443 到StorageGRID網關節點的 HTTPS 連接

- 透過連接埠 443 建立到ONTAP叢集管理 LIF 的 HTTPS 連接
- 透過連接埠 443 到NetApp Backup and Recovery 的出站網路連線（當控制台代理安裝在「暗站」時不需要）

私人模式（暗站）注意事項

- NetApp Backup and Recovery功能內建於控制台代理程式中。以私人模式安裝時，您需要定期更新控制台代理軟體才能存取新功能。檢查["NetApp Backup and Recovery新功能"](#)查看每個NetApp Backup and Recovery版本中的新功能。當您想要使用新功能時，請按照以下步驟操作 ["升級控制台代理軟體"](#)。

新版NetApp Backup and Recovery除了可以建立物件儲存備份外，還增加了規劃和建立快照及複製磁碟區的功能，但需要使用 3.9.31 或更高版本的控制台代理。因此建議您取得此最新版本來管理所有備份。

- 當您在 SaaS 環境中使用NetApp Backup and Recovery時，NetApp Backup and Recovery設定資料將會備份到雲端。當您在沒有網路存取的網站中使用NetApp Backup and Recovery時，NetApp Backup and Recovery設定資料將備份到儲存備份的StorageGRID桶中。

驗證許可證要求

在為叢集啟動NetApp Backup and Recovery之前，您需要從NetApp購買並啟動NetApp Backup and Recovery BYOL 授權。此許可證適用於該帳戶，可跨多個系統使用。

您需要NetApp提供的序號，以便您在許可證的有效期限和容量內使用本服務。["了解如何管理您的 BYOL 許可證"](#)。



將檔案備份到StorageGRID時不支援 PAYGO 授權。

準備ONTAP集群

準備來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統。

準備ONTAP集群涉及以下步驟：

- 在NetApp Console中發現您的ONTAP系統
- 驗證ONTAP系統要求
- 驗證ONTAP網路要求以將資料備份到對象存儲
- 驗證ONTAP複製卷的網路要求

在NetApp Console中發現您的ONTAP系統

您的來源本機ONTAP系統和任何輔助本機ONTAP或Cloud Volumes ONTAP系統都必須在NetApp Console*系統*頁面上可用。

您需要知道叢集管理 IP 位址和管理員使用者帳戶的密碼才能新增叢集。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>[["了解如何發現集群"](#)]。

驗證ONTAP系統要求

確保您的ONTAP系統符合以下要求：

- 最低版本為ONTAP 9.8；建議使用ONTAP 9.8P13 及更高版本。
- SnapMirror許可證（包含在高級捆綁包或資料保護捆綁包中）。

*注意：*使用NetApp Backup and Recovery時不需要「混合雲端捆綁包」。

了解如何 ["管理您的叢集許可證"](#)。

- 時間和時區設定正確。了解如何 ["配置叢集時間"](#)。
- 如果您複製數據，請檢查來源系統和目標系統是否要執行相容的ONTAP版本。

["查看與SnapMirror關係相容的ONTAP版本"](#)。

驗證ONTAP網路要求以將資料備份到對象存儲

您必須在連接到物件儲存的系統上配置以下要求。

- 當您使用扇出備份架構時，必須在主儲存系統上設定以下設定。
- 當您使用級聯備份架構時，必須在_輔助_儲存系統上設定下列設定。

需滿足以下ONTAP集群網路需求：

- ONTAP叢集透過使用者指定的連接埠從叢集間 LIF 啟動到StorageGRID網關節點的 HTTPS 連接，以執行備份和還原作業。此連接埠可在備份設定期間配置。

ONTAP從物件儲存讀取和寫入資料。物件儲存從不啟動，它只是響應。

- ONTAP需要從控制台代理到叢集管理 LIF 的入站連線。控制台代理必須位於您的場所。
- 每個託管要備份的磁碟區的ONTAP節點上都需要一個叢集間 LIF。LIF 必須與ONTAP用於連接物件儲存的 *IPspace* 相關聯。["了解有關 IP 空間的更多信息"](#)。

當您設定NetApp Backup and Recovery時，系統會提示您輸入要使用的 IP 空間。您應該選擇與每個 LIF 關聯的 IP 空間。這可能是「預設」IP 空間或您建立的自訂 IP 空間。

- 節點的群集間 LIF 能夠存取物件儲存（當控制台代理安裝在「暗」站點時不需要）。
- 已為磁碟區所在的儲存虛擬機器設定 DNS 伺服器。了解如何 ["為 SVM 配置 DNS 服務"](#)。
- 如果您使用的 IP 空間與預設 IP 空間不同，則可能需要建立靜態路由才能存取物件儲存。
- 如有必要，請更新防火牆規則，以允許NetApp Backup and Recovery服務透過您指定的連接埠（通常為連接埠 443）從ONTAP連接到物件存儲，並透過連接埠 53（TCP/UDP）從儲存虛擬機器到 DNS 伺服器的名稱解析流量。

驗證ONTAP複製卷的網路要求

如果您打算使用NetApp Backup and Recovery在輔助ONTAP系統上建立複製卷，請確保來源系統和目標系統符合下列網路需求。

本地ONTAP網路需求

- 如果叢集位於本機，則您應該從公司網路連接到雲端提供者中的虛擬網路。這通常是 VPN 連線。

- ONTAP叢集必須滿足額外的子網路、連接埠、防火牆和叢集要求。

由於您可以複製到Cloud Volumes ONTAP或本機系統，因此請查看本機ONTAP系統的對等需求。["查看ONTAP文件中的叢集對等前提條件"](#)。

Cloud Volumes ONTAP網路需求

- 實例的安全性群組必須包含所需的入站和出站規則：具體來說，ICMP 和連接埠 11104 和 11105 的規則。這些規則包含在預先定義的安全性群組中。

準備StorageGRID作為備份目標

StorageGRID必須符合以下要求。查看 ["StorageGRID文檔"](#) 了解更多。

有關StorageGRID的 DataLock 和勒索軟體復原要求的詳細信息，請參閱["備份到物件策略選項"](#)。

支援的StorageGRID版本

支援StorageGRID 10.3 及更高版本。

若要使用 DataLock 和 Ransomware Resilience 進行備份，您的StorageGRID系統必須執行 11.6.0.3 或更高版本。

要將舊備份分層到雲端檔案存儲，您的StorageGRID系統必須運行 11.3 或更高版本。此外，您的StorageGRID系統必須在控制台*系統*頁面上被發現。

對於使用者檔案存儲，需要管理節點 IP 存取。

始終需要網關 IP 存取。

S3 憑證

您必須建立 S3 租用戶帳戶來控制對StorageGRID儲存的存取。["有關詳細信息，請參閱StorageGRID文檔"](#)。

當您設定備份到StorageGRID時，備份精靈會提示您輸入租用戶帳戶的 S3 存取金鑰和金鑰。租用戶帳戶使NetApp Backup and Recovery能夠驗證並存取用於儲存備份的StorageGRID桶。需要金鑰，以便StorageGRID知道誰在發出請求。

這些存取金鑰必須與具有以下權限的使用者相關聯：

```
"s3:ListAllMyBuckets",  
"s3:ListBucket",  
"s3:GetObject",  
"s3:PutObject",  
"s3:DeleteObject",  
"s3:CreateBucket"
```

物件版本控制

您無法在物件儲存桶上手動啟用StorageGRID物件版本控制。

準備將較舊的備份文件存檔到公有雲存儲

將較舊的備份檔案分層到檔案儲存中可以節省資金，因為您可以使用較便宜的儲存類別來儲存您可能不需要的備份。StorageGRID是一種內部部署（私有雲）解決方案，不提供檔案存儲，但您可以將較舊的備份檔案移至公有雲檔案儲存。以這種方式使用時，分層到雲端儲存的資料或從雲端儲存恢復的資料會在StorageGRID和雲端儲存之間傳輸 - 控制台不參與此資料傳輸。

目前支援可讓您將備份存檔至 *AWS S3 Glacier/S3 Glacier Deep Archive* 或 *Azure Archive* 儲存體。

- ONTAP要求*
- 您的叢集必須使用ONTAP 9.12.1 或更高版本。
- StorageGRID要求*
- 您的StorageGRID必須使用 11.4 或更高版本。
- 您的StorageGRID必須 ["在控制台中發現並可用"](#)。

Amazon S3 要求

- 您需要註冊一個 Amazon S3 帳戶，用於儲存存檔備份所在的儲存空間。
- 您可以選擇將備份分層到 AWS S3 Glacier 或 S3 Glacier Deep Archive 儲存。["了解有關 AWS 存檔層的更多信息"](#)。
- StorageGRID應該對儲存桶具有完全控制存取權限(s3:*) ；但是，如果這不可能，則儲存桶策略必須向StorageGRID授予以下 S3 權限：
 - s3:AbortMultipartUpload
 - s3:DeleteObject
 - s3:GetObject
 - s3:ListBucket
 - s3:ListBucketMultipartUploads
 - s3:ListMultipartUploadParts
 - s3:PutObject
 - s3:RestoreObject

Azure Blob 需求

- 您需要註冊 Azure 訂閱，以取得存檔備份所在的儲存空間。
- 啟動精靈可讓您使用現有的資源群組來管理將儲存備份的 Blob 容器，或者您可以建立新的資源群組。

在為叢集的備份策略定義存檔設定時，您將輸入雲端提供者憑證並選擇要使用的儲存類別。當您啟動叢集備份時，NetApp Backup and Recovery會建立雲端儲存桶。AWS 和 Azure 檔案儲存所需的資訊如下所示。

AWS		Azure	
☒ Tier Backups to Archive		☒ Tier Backups to Archive	
Cloud Provider		Cloud Provider	
AWS		AZURE	
Account	Region	Azure Subscription	Region
Select Account	Select Region	Select Account	Select Region
AWS Access Key	AWS Secret Key	Resource Group Type	Resource Group
Enter AWS Access Key	Enter AWS Secret Key	Select an Existing Resource Group	Select Resource Group
Archive After (Days)	Storage Class	Archive After (Days)	Storage Class
(1-999)	S3 Glacier	(1-999)	Azure Archive

您選擇的歸檔策略設定將在StorageGRID中產生資訊生命週期管理 (ILM) 策略，並將設定新增為「規則」。

- 如果存在現有的活動 ILM 策略，則會將新規則新增至 ILM 策略以將資料移至存檔層。
- 如果存在處於「建議」狀態的現有 ILM 策略，則無法建立和啟動新的 ILM 策略。 [了解有關StorageGRID ILM 策略和規則的更多信息](#)。

啟動ONTAP磁碟區上的備份

隨時直接從您的本機系統啟動備份。

嚮導將引導您完成以下主要步驟：

- [\[選擇要備份的捲\]](#)
- [\[定義備份策略\]](#)
- [\[檢查您的選擇\]](#)

您還可以顯示 API 命令在審查步驟中，您可以複製程式碼來自動為未來的系統啟動備份。

啟動精靈

步驟

1. 使用以下方式之一存取啟動備份和復原精靈：

- 從控制台*系統*頁面中，選擇系統，然後選擇右側面板中備份和還原旁邊的*啟用>備份磁碟區*。

如果備份目標在控制台*系統*頁面上作為系統存在，則可以將ONTAP叢集拖曳到物件儲存上。

- 在備份和復原欄中選擇*卷*。從「磁碟區」標籤中，選擇「操作 (...)」選項，然後為單一磁碟區（尚未啟用複製或備份到物件儲存）選擇「啟動備份」。

精靈的介紹頁面顯示保護選項，包括本機快照、複製和備份。如果您在此步驟中選擇了第二個選項，則會出現「定義備份策略」頁面，其中選擇一個磁碟區。

2. 繼續以下選項：

- 如果您已經有控制台代理，那麼一切就緒了。只需選擇*下一步*。
- 如果您還沒有控制台代理，則會出現「新增控制台代理」選項。參考[\[準備控制台代理\]](#)。

選擇要備份的捲

選擇您想要保護的磁碟區。受保護的磁碟區是具有以下一項或多項的磁碟區：快照策略、複製策略、備份到物件策略。

您可以選擇保護FlexVol或FlexGroup磁碟區；但是，在啟動系統備份時不能選擇這些磁碟區的混合。了解如何[啟動系統中附加磁碟區的備份](#)（FlexVol或FlexGroup）在為初始磁碟區配置備份後。



- 您一次只能在單一FlexGroup磁碟區上啟動備份。
- 您選擇的捲必須具有相同的SnapLock設定。所有磁碟區都必須啟用SnapLock Enterprise或停用SnapLock。

步驟

如果您選擇的磁碟區已經套用了快照或複製策略，那麼您稍後選擇的策略將覆寫這些現有策略。

1. 在「選擇卷」頁面中，選擇要保護的一個或多個磁碟區。
 - 或者，過濾行以僅顯示具有特定卷類型、樣式等的捲，以便更輕鬆地進行選擇。
 - 選擇第一個磁碟區後，您可以選擇所有FlexVol磁碟區（FlexGroup磁碟區一次只能選擇一個）。若要備份所有現有的FlexVol卷，請先選取一個卷，然後選取標題行中的框。
 - 若要備份單一卷，請選取每個卷對應的複選框。
2. 選擇“下一步”。

定義備份策略

定義備份策略涉及設定以下選項：

- 您是否需要一個或所有備份選項：本機快照、複製和備份到物件存儲
- 架構
- 本機快照策略
- 複製目標和策略



如果您選擇的磁碟區具有與您在此步驟中選擇的策略不同的快照和複製策略，則現有策略將被覆寫。

- 備份到物件儲存資訊（提供者、加密、網路、備份策略和匯出選項）。

步驟

1. 在「定義備份策略」頁面中，選擇以下一項或全部。預設情況下，所有三個都被選中：
 - 本機快照：如果您正在執行複製或備份到物件存儲，則必須建立本機快照。
 - 複製：在另一個ONTAP儲存系統上建立複製磁碟區。
 - 備份：將磁碟區備份到物件儲存。
2. 架構：如果您同時選擇了複製和備份，請選擇下列資訊流之一：
 - 級聯：資訊從主存儲流向輔助存儲，然後從輔助存儲流向物件存儲。
 - 扇出：資訊從主存儲流向輔助存儲，再從主存儲流向物件存儲。

有關這些架構的詳細信息，請參閱["規劃您的保育之旅"](#)。

3. 本機快照：選擇現有的快照原則或建立新的快照策略。



若要建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

4. 複製：設定以下選項：

- 複製目標：選擇目標系統和 SVM。或者，選擇將新增至複製磁碟區名稱的目標聚合或聚合以及前綴或後綴。
- 複製策略：選擇現有的複製策略或建立一個。



若要建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 選擇“創建”。

5. 備份到物件：如果您選擇了*備份*，請設定以下選項：

- 提供者：選擇* StorageGRID*。
- 提供者設定：輸入提供者網關節點 FQDN 詳細資料、連接埠、存取金鑰和金鑰。

存取密鑰和密鑰適用於您建立的 IAM 用戶，用於授予ONTAP叢集對儲存桶的存取權限。

- 網路：選擇要備份的磁碟區所在的ONTAP叢集中的 IP 空間。此 IP 空間的群集間 LIF 必須具有出站網際網路存取權限（當控制台代理安裝在「暗站」時不需要）。



選擇正確的 IP 空間可確保NetApp Backup and Recovery可以建立從ONTAP到StorageGRID物件儲存的連線。

- 備份策略：選擇現有的備份到物件儲存策略或建立一個。



若要建立自訂策略，請參閱["創建策略"](#)。

若要建立策略，請選擇「建立新策略」並執行下列操作：

- 輸入策略的名稱。
- 選擇最多五個時間表，通常頻率不同。
- 對於備份到物件策略，設定 DataLock 和 Ransomware Resilience 設定。有關 DataLock 和勒索軟體

恢復的詳細信息，請參閱["備份到對象策略設置"](#)。

如果您的叢集使用的是ONTAP 9.11.1 或更高版本，您可以選擇透過設定「DataLock」和「Ransomware Resilience」來保護您的備份免遭刪除和勒索軟體攻擊。*DataLock* 保護您的備份檔案不被修改或刪除，而 *Ransomware Resilience* 會掃描您的備份檔案以查找備份檔案中勒索軟體攻擊的證據。

- 選擇“創建”。

如果您的叢集使用的是ONTAP 9.12.1 或更高版本，而您的StorageGRID系統使用的是 11.4 或更高版本，您可以選擇在一定天數後將舊備份分層到公有雲存檔層。目前支援 AWS S3 Glacier/S3 Glacier Deep Archive 或 Azure Archive 儲存層。[了解如何配置您的系統以實現此功能](#)。

- 分層備份到公有雲：選擇您想要分層備份的雲端提供者並輸入提供者詳細資料。

選擇或建立一個新的StorageGRID叢集。有關建立StorageGRID叢集以便控制台可以發現它的詳細信息，請參閱 ["StorageGRID文檔"](#)。

- 將現有快照匯出至物件儲存作為備份副本：如果此系統中存在與您剛剛為此系統選擇的備份計畫標籤（例如，每日、每週等）相符的磁碟區的本機快照，則會顯示此附加提示。選取此方塊可將所有歷史快照複製到物件儲存作為備份文件，以確保對您的磁碟區進行最全面的保護。

6. 選擇“下一步”。

檢查您的選擇

這是審查您的選擇並在必要時進行調整的機會。

步驟

1. 在「審核」頁面中，審核您的選擇。
2. （可選）選取核取方塊*自動將快照原則標籤與複製和備份策略標籤同步*。這將建立具有與複製和備份策略中的標籤相符的標籤的快照。
3. 選擇*啟動備份*。

結果

NetApp Backup and Recovery開始對您的磁碟區進行初始備份。複製捲和備份檔案的基線傳輸包括來源資料的完整副本。後續傳輸包含快照中包含的主儲存資料的差異副本。

在目標叢集中建立一個複製卷，該卷將與主儲存卷同步。

在您輸入的 S3 存取金鑰和金鑰指示的服務帳戶中建立一個 S3 儲存桶，並將備份檔案儲存在那裡。

顯示磁碟區備份儀表板，以便您可以監控備份的狀態。

您也可以使用["作業監控頁面"](#)。

顯示 API 命令

您可能想要顯示並選擇性地複製啟動備份和還原精靈中使用的 API 命令。您可能希望這樣做以便在未來的系統中自動啟動備份。

步驟

1. 從啟動備份和復原精靈中，選擇*查看 API 請求*。
2. 若要將指令複製到剪貼簿，請選擇*複製*圖示。

在NetApp Backup and Recovery中使用SnapMirror將磁碟區遷移到 Cloud Resync

NetApp Backup and Recovery中的SnapMirror到雲端重新同步功能簡化了NetApp環境中捲遷移期間的資料保護和連續性。當使用SnapMirror邏輯複製 (LRSE) 將磁碟區從一個本地NetApp部署遷移到另一個部署，或遷移到基於雲端的解決方案（例如Cloud Volumes ONTAP）時， SnapMirror到 Cloud Resync 可確保現有的雲端備份保持完整且可正常運作。

此功能無需重新建立基線，即可在遷移後繼續備份。此功能在工作負載遷移場景中很有價值，支援 FlexVols 和 FlexGroups，並且從ONTAP版本 9.16.1 開始可用。



此功能從 2025 年 5 月發布的NetApp Backup and Recovery版本 4.0.3 開始提供。

SnapMirror到 Cloud Resync 可跨環境保持備份連續性，因此更容易在混合雲和多雲環境中管理資料。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

開始之前

確保滿足以下先決條件：

- 目標ONTAP叢集必須執行ONTAP 9.16.1 或更高版本。
- 必須使用NetApp Backup and Recovery保護舊的來源ONTAP叢集。
- SnapMirror到雲端重新同步功能從 2025 年 5 月發布的NetApp Backup and Recovery版本 4.0.3 開始提供。
- 確保物件儲存中的最新備份是舊來源、新來源和物件儲存的通用快照。不要使用比備份到物件儲存的最新快照更舊的通用快照。
- 在開始重新同步操作之前，必須在新ONTAP叢集上建立舊ONTAP叢集上使用的快照策略和SnapMirror策略。如果在重新同步過程中使用任何策略，則也必須建立該策略。重新同步操作不會建立策略。
- 確保應用於遷移卷SnapMirror關係的SnapMirror策略包含雲端關係使用的相同標籤。為避免問題，請使用管理磁碟區和所有快照的精確鏡像的策略。



目前不支援使用 SVM-Migrate、SVM-DR 或 Head Swap 方法遷移後將SnapMirror重新同步到 Cloud。

NetApp Backup and Recovery SnapMirror到 Cloud Resync 的工作原理

如果您完成技術更新或將磁碟區從一個ONTAP叢集遷移到另一個 ONTAP 叢集，那麼確保備份繼續不間斷地運作非常重要。NetApp Backup and Recovery SnapMirror到 Cloud Resync 可協助您實現這一點，確保您的雲端備份即使在磁碟區移轉後也能保持一致。

以下是一個例子：

假設您有一個名為 Vol1a 的本機磁碟區。該卷有三個快照：S1、S2 和 S3。這些快照就是還原點。Vol1 使

用SnapMirror to Cloud (SM-C) 備份到雲端，但物件儲存中只有 S1 和 S2。

現在，您想要將 Vol1 遷移到另一個ONTAP叢集。為此，您需要建立與名為 Vol1b 的新雲端磁碟區的SnapMirror邏輯複製 (LRSE) 關係。這會將所有三個快照 (S1、S2 和 S3) 從 Vol1a 傳輸到 Vol1b。

遷移完成後，您將獲得以下設定：

- 刪除原有的SM-C關係式 (Vol1a→Object store)。
- LRSE 關係式 (Vol1a → Vol1b) 也被刪除。
- Vol1b 現在是您的活動卷。

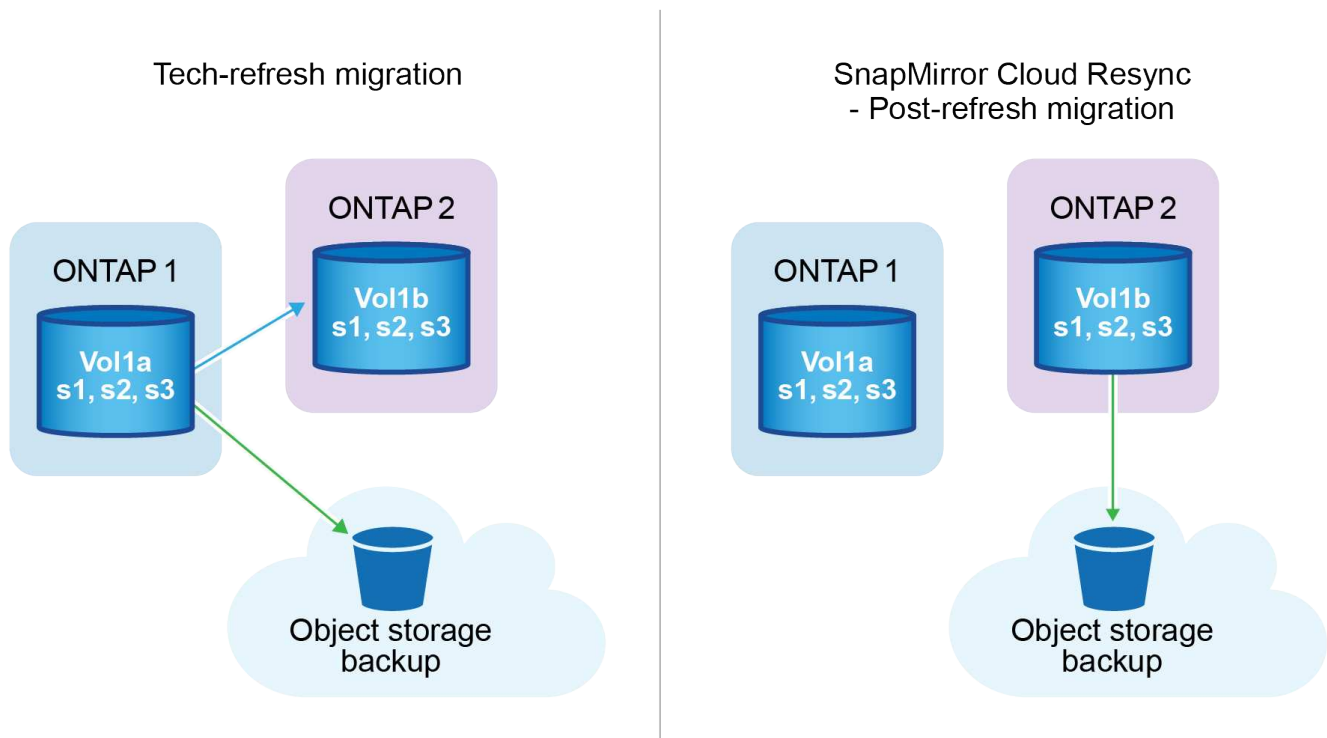
此時，您想要繼續將 Vol1b 備份到同一個雲端點。但是，您無需從頭開始進行完整備份（這會花費時間和資源），而是使用SnapMirror進行 Cloud Resync。

重新同步的工作原理如下：

- 系統檢查 Vol1a 和物件儲存之間的公共快照。在這種情況下，兩者都有 S2。
- 由於這個共享快照，系統只需要傳輸 S2 和 S3 之間的增量變化。

這意味著只有 S2 之後添加的新資料被發送到物件存儲，而不是整個磁碟區。

此過程可防止重複備份，節省頻寬，並在遷移後保持備份運作。



程式說明

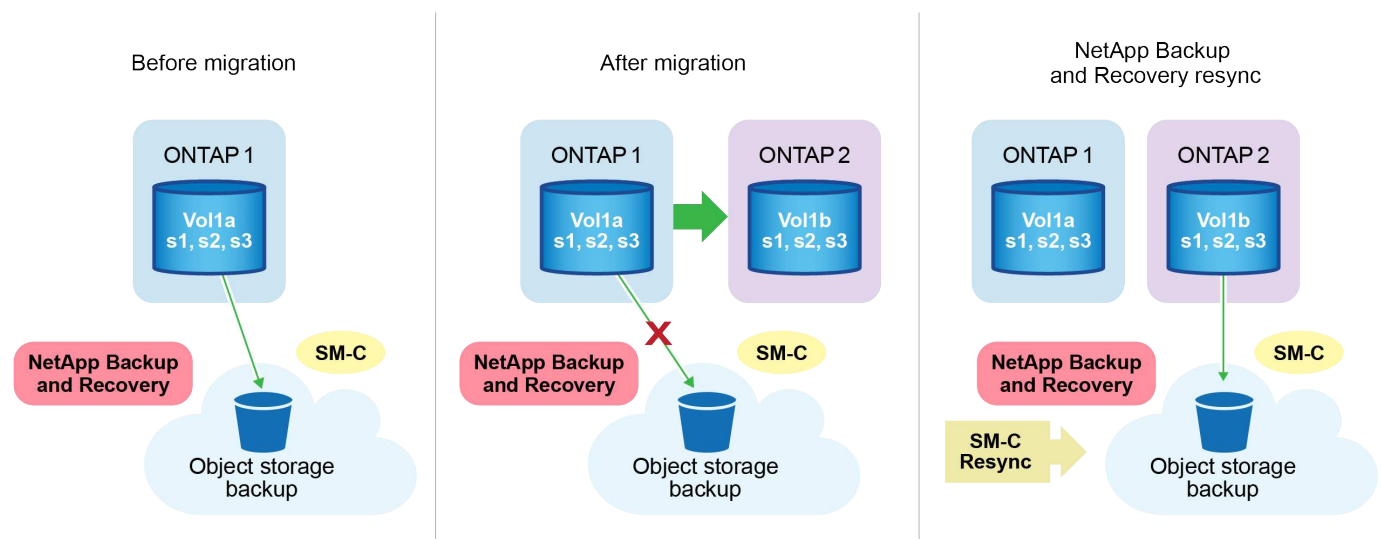
- 不使用NetApp Backup and Recovery執行遷移和技術更新。它們應該由專業服務團隊或合格的儲存管理員來執行。

- NetApp遷移團隊會在來源 ONTAP 叢集和目標ONTAP叢集之間建立SnapMirror關係，以協助遷移磁碟區。
- 確保技術更新期間的遷移是基於基於SnapMirror的遷移。

如何使用SnapMirror將磁碟區遷移到 Cloud Resync

使用SnapMirror到 Cloud Resync 遷移卷涉及以下主要步驟，以下將更詳細地描述每個步驟：

- 遵循遷移前檢查清單：在開始遷移之前， NetApp Tech Refresh 團隊會確保滿足以下先決條件，以避免資料遺失並確保遷移過程順利進行。
- 遵循遷移後檢查清單：遷移後， NetApp Tech Refresh 團隊確保完成以下步驟以建立保護並為重新同步做好準備。
- 執行**SnapMirror**到 **Cloud Resync**：遷移後， NetApp Tech Refresh 團隊執行SnapMirror到 Cloud Resync 作業，以從新遷移的磁碟區還原雲端備份。



遵循遷移前檢查清單

在遷移之前， NetApp技術更新團隊會檢查這些先決條件，以防止資料遺失並確保流程順利進行。

1. 確保所有要遷移的磁碟區都使用NetApp Backup and Recovery進行保護。
2. 記錄卷實例 UUID。在開始遷移之前，記下所有磁碟區的實例 UUID。這些標識符對於稍後的映射和重新同步操作至關重要。
3. 在刪除任何SnapMirror關係之前，對每個磁碟區進行最終快照以保留最新狀態。
4. 記錄SnapMirror策略。記錄目前附加到每個磁碟區關係的SnapMirror策略。稍後在SnapMirror到 Cloud Resync 過程中將需要此功能。
5. 刪除SnapMirror Cloud 與物件儲存的關係。
6. 與新的ONTAP叢集建立標準SnapMirror關係，以將磁碟區遷移到新的目標ONTAP叢集。

遵循遷移後檢查清單

遷移後， NetApp技術更新團隊將確保完成以下步驟以建立保護並為重新同步做好準備。

1. 記錄目標ONTAP叢集中所有遷移磁碟區的新磁碟區實例 UUID。
2. 確認舊ONTAP叢集中可用的所有必要SnapMirror策略均已在新ONTAP叢集中正確配置。
3. 在控制台*系統*頁面中將新的ONTAP叢集新增為系統。



應該使用磁碟區實例 UUID，而不是磁碟區 ID。磁碟區實例 UUID 是唯一標識符，在遷移過程中保持一致，而磁碟區 ID 可能會在遷移後發生變化。

執行SnapMirror到雲端重新同步

遷移後，NetApp Tech Refresh 團隊執行SnapMirror到 Cloud Resync 作業，以從新遷移的磁碟區還原雲端備份。

1. 在控制台*系統*頁面中將新的ONTAP叢集新增為系統。
2. 查看NetApp Backup and Recovery磁碟區頁面以確保舊來源系統詳細資訊可用。
3. 從NetApp Backup and Recovery卷頁頁面中，選擇*備份設定*。
 - 在備份設定頁面中，選擇*查看全部*。
 - 從新來源右側的操作...選單中，選擇*重新同步備份*。
4. 在重新同步系統頁面中，執行以下操作：
 - a. 新來源系統：進入已遷移磁碟區的新ONTAP叢集。
 - b. 現有目標物件儲存：選擇包含來自舊來源系統的備份的目標物件儲存。
5. 選擇「下載 CSV 範本」下載重新同步詳細資料 Excel 表。使用此表輸入要遷移的磁碟區的詳細資訊。在 CSV 檔案中，輸入以下詳細資訊：
 - 來源叢集中的舊磁碟區實例 UUID
 - 來自目標叢集的新磁碟區實例 UUID
 - 要應用於新關係的SnapMirror策略。
6. 選擇“上傳卷對映詳細資料”下的“上傳”，將完成的 CSV 表上傳到NetApp Backup and RecoveryUI。



應該使用磁碟區實例 UUID，而不是磁碟區 ID。磁碟區實例 UUID 是唯一標識符，在遷移過程中保持一致，而磁碟區 ID 可能會在遷移後發生變化。

7. 輸入重新同步操作所需的提供者和網路設定資訊。
8. 選擇*提交*開始驗證程序。

NetApp Backup and Recovery驗證選擇重新同步的每個磁碟區是否都是最新快照，並且至少有一個通用快照。這可確保磁碟區已準備好進行SnapMirror到 Cloud Resync 操作。

9. 查看驗證結果，包括新的來源磁碟區名稱和每個磁碟區的重新同步狀態。
10. 檢查容量是否合格。系統檢查磁碟區是否符合重新同步的條件。如果磁碟區不符合條件，則表示它不是最新的快照或未找到通用快照。



為了確保磁碟區仍然符合SnapMirror到 Cloud Resync 操作的條件，請在遷移前階段刪除任何SnapMirror關係之前，為每個磁碟區拍攝最終快照。這保留了資料的最新狀態。

11. 選擇*重新同步*以開始重新同步操作。系統使用最新且通用的快照僅傳輸增量更改，確保備份的連續性。

12. 在作業監視器頁面中監視重新同步過程。

在暗站中恢復NetApp Backup and Recovery配置數據

在沒有網際網路存取的網站（稱為_私有模式_）中使用NetApp Backup and Recovery時，NetApp Backup and Recovery設定資料將備份到儲存備份的StorageGRID或ONTAP S3 儲存桶中。如果控制台代理主機系統出現問題，您可以部署新的控制台代理並還原關鍵的NetApp Backup and Recovery資料。



此過程僅適用於ONTAP磁碟區資料。

當您在 SaaS 環境中使用NetApp Backup and Recovery，並在雲端供應商或您自己的網際網路連線主機上部署控制台代理程式時，系統會備份並保護雲端中所有重要的設定資料。如果您遇到控制台代理問題，請建立新的控制台代理並新增您的系統。備份詳細資訊將自動恢復。

備份的資料有兩種類型：

- NetApp Backup and Recovery資料庫 - 包含所有磁碟區、備份檔案、備份策略和設定資訊的清單。
- 索引目錄檔案 - 包含用於搜尋和復原功能的詳細索引，可讓您在尋找要復原的磁碟區資料時搜尋非常快速且有效。

這些資料每天午夜備份一次，每個檔案最多保留 7 份副本。如果控制台代理程式正在管理多個本機ONTAP系統，則NetApp Backup and Recovery檔案將儲存在首先啟動的系統的儲存桶中。



NetApp Backup and Recovery資料庫或索引目錄檔案中從未包含任何磁碟區資料。

將NetApp Backup and Recovery資料還原到新的控制台代理

如果您的內部控制台代理停止運作，您將需要安裝新的控制台代理，然後將NetApp Backup and Recovery資料還原到新的控制台代理。

您需要執行下列任務才能讓NetApp Backup and Recovery系統還原工作狀態：

- 安裝新的控制台代理
- 還原NetApp Backup and Recovery資料庫
- 恢復索引目錄文件
- 將所有本機ONTAP系統和StorageGRID系統重新發現到NetApp ConsoleUI

檢查系統正常運作後，建立新的備份檔案。

你需要什麼

您需要從儲存備份檔案的StorageGRID或ONTAP S3 儲存桶存取最新的資料庫和索引備份：

- NetApp Backup and RecoveryMySQL 資料庫文件

該檔案位於儲存桶中的以下位置 `netapp-backup-<GUID>/mysql_backup/`，它被命名為

CBS_DB_Backup_<day>_<month>_<year>.sql。

- 索引目錄備份 zip 文件

該檔案位於儲存桶中的以下位置 netapp-backup-<GUID>/catalog_backup/，它被命名為 Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip。

在新的本機 **Linux** 主機上安裝新的控制台代理

安裝新的控制台代理程式時，請下載與原始代理程式相同的軟體版本。NetApp Backup and Recovery 資料庫的變更可能會導致較新的軟體版本無法與舊的資料庫備份一起使用。你可以 ["恢復備份資料庫後，將控制台代理軟體升級至最新版本"](#)。

1. ["在新的本機 Linux 主機上安裝控制台代理"](#)
2. 使用您剛剛建立的管理員使用者憑證登入控制台。

還原 NetApp Backup and Recovery 資料庫

1. 將 MySQL 備份從備份位置複製到新的控制台代理主機。下面我們將使用範例檔案名稱「CBS_DB_Backup_23_05_2023.sql」。
2. 根據您使用的是 Docker 還是 Podman 容器，使用以下命令之一將備份複製到 MySQL docker 容器：

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. 根據您使用的是 Docker 還是 Podman 容器，使用以下命令之一進入 MySQL 容器 shell：

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. 在容器 shell 中，部署「env」。
5. 您將需要 MySQL DB 密碼，因此請複製鍵「MYSQL_ROOT_PASSWORD」的值。
6. 使用下列命令還原 NetApp Backup and Recovery MySQL DB：

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. 使用下列 SQL 指令驗證 NetApp Backup and Recovery MySQL DB 是否已正確還原：


```
mysql -u root -p cloud_backup
```

8. 輸入密碼。

```
mysql> show tables;  
mysql> select * from volume;
```

9. 請確保顯示的磁碟區與原始環境中的磁碟區相同。

恢復索引目錄文件

1. 將 Indexed Catalog 備份 zip 檔案（我們將使用範例檔案名稱「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」）從備份位置複製到「/opt/application/netapp/cbs」資料夾中的新控制台代理主機。
2. 使用下列命令解壓縮「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」檔案：

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. 執行 **ls** 命令以確保已建立資料夾“catalogdb1”，其下有子資料夾“changes”和“snapshots”。

發現您的ONTAP叢集和StorageGRID系統

1. "探索所有本地ONTAP系統"在您之前的環境中可用。這包括您用作 S3 伺服器的ONTAP系統。
2. "發現您的StorageGRID系統"。

設定StorageGRID環境詳細信息

添加與您的ONTAP系統關聯的StorageGRID系統的詳細信息，因為它們是在原始控制台代理設定上使用 **"NetApp ConsoleAPI"**。

以下資訊適用於從NetApp Console 3.9.xx 開始的私有模式安裝。對於舊版本，請使用以下步驟：["DarkSite 雲端備份：MySQL 和索引目錄備份和還原"](#)。

您需要對將資料備份到StorageGRID 的每個系統執行這些步驟。

1. 使用以下 oauth/token API 提取授權令牌。

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:  
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-  
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '  
{ "username": "admin@netapp.com", "password": "Netapp@123", "grant_type": "pas  
sword" }  
> '
```


雖然 IP 位址、使用者名稱和密碼是自訂值，但帳戶名稱不是。帳戶名稱始終為“account-DARKSITE1”。此外，使用者名稱必須使用電子郵件格式的名稱。

此 API 將傳回以下回應。您可以如下所示檢索授權令牌。

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiaXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW11IjoieWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWVpY29wZSI6Im9wZW5pZCBwcm9maWx1IiwiaWF0IjoxNjcyNzMDIzLCJleHAiOiE2NzI3NTc2MjMsImh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23PokyLglif67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-114v_pNDsPyNDyWqHaKizThdjJHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5ykODNDmrv5At_f9HHp0-xVMYHqywZ4nNFalMvAh4xESc5jfoKOZc-IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTURzB81-o-ipvrOqSolIwIeHXZJJV-Uswun9daNgIYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JfKf1-rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. 使用 tenancy/external/resource API 提取系統 ID 和 X-Agent-Id。

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiaXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW11IjoieWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWVpY29wZSI6Im9wZW5pZCBwcm9maWx1IiwiaWF0IjoxNjcyNzMDIzLCJleHAiOiE2NzI3NDQzMjMsImh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-yE0fH9gr4XgkdsWjWcNvw2rRkFzjHpWrETgfgAMkZcAukV4DHuxogHWh6-DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-sp81GaqMahPf0KcFVyjbBL4krOewgKHGfo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-KbZqmmBX9vDnYp7SSxC1hHJRdstcFgJLdJHtowweNH2829KsjEGBTtcBd08SvIDtctNH_GAxwSgMT3zUfwaOimPw'
```

此 API 將傳回以下回應。「resourceIdentifier」下的值表示 _WorkingEnvironment Id_，「agentId」下的值表示 _x-agent-id_。

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":{"\clusterUuid\":"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"},"workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. 使用與系統關聯的StorageGRID系統的詳細資訊更新NetApp Backup and Recovery資料庫。確保輸入StorageGRID的完全限定網域名稱以及存取金鑰和儲存金鑰，如下所示：

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwIiwiaXVkiIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWx1IiwiaWF0IjoxNjcyNzIyNzEzNDQzMjM5Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdsWjWcNvw2rRkFzjHpWrETgfgAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVYjbBL4krOewgKHGfO_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRdstcFgJLdJHtowweNH2829KsjEGBTtcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" } '
```

驗證NetApp Backup and Recovery設置

1. 選擇每個ONTAP系統，然後點擊右側面板中備份和還原服務旁邊的「檢視備份」。

您應該會看到為您的磁碟區建立的所有備份。

2. 在「恢復儀表板」的「搜尋與復原」部分下，按一下「索引設定」。

確保先前啟用了索引編目的系統仍然保持啟用狀態。

3. 在「搜尋和復原」頁面中，執行一些目錄搜尋以確認索引目錄復原已成功完成。

使用NetApp Backup and Recovery管理ONTAP系統的備份

透過NetApp Backup and Recovery，您可以透過變更備份計畫、啟用/停用磁碟區備份、暫停備份、刪除備份、強制刪除備份等方式管理Cloud Volumes ONTAP和本機ONTAP系統的備份。這包括所有類型的備份，包括快照、複製磁碟區和物件儲存中的備份檔案。您也可以取消註冊NetApp Backup and Recovery。



請勿直接在儲存系統或雲端提供者環境中管理或變更備份檔案。這可能會損壞檔案並導致不受支援的配置。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

查看系統中磁碟區的備份狀態

您可以在磁碟區備份儀表中查看目前正在備份的所有磁碟區的清單。這包括所有類型的備份，包括快照、複製磁碟區和物件儲存中的備份檔案。您也可以查看系統中目前未備份的磁碟區。

步驟

1. 從控制台選單中，選擇*保護>備份和還原*。
2. 選擇「磁碟區」選單以查看Cloud Volumes ONTAP和本機ONTAP系統的備份磁碟區清單。
3. 如果您正在尋找特定系統中的特定磁碟區，您可以按系統和磁碟區優化清單。您也可以使用搜尋過濾器，或者可以根據磁碟區樣式（FlexVol或FlexGroup）、磁碟區類型等對列進行排序。

若要顯示其他欄位（聚合、安全性樣式（Windows 或 UNIX）、快照原則、複製原則和備份策略），請選擇加號。

4. 查看「現有保護」欄位中保護選項的狀態。這 3 個圖示分別代表「本機快照」、「複製磁碟區」和「物件儲存中的備份」。

當此備份類型啟動時，對應的圖示會亮起；當該備份類型未啟動時，圖示會變為灰色。您可以將遊標停留在每個圖示上，查看正在使用的備份策略以及每種備份類型的其他相關資訊。

啟動系統中附加磁碟區的備份

如果您在首次啟用NetApp Backup and Recovery時僅在系統中的某些磁碟區上啟動了備份，則可以稍後在其他磁碟區上啟用備份。

步驟

1. 在「卷」標籤中，找到要啟動備份的捲，然後選擇「操作」選單。... 在行尾，選擇「啟動 3-2-1 保護」。
2. 在「定義備份策略」頁面中，選擇備份架構，然後定義本機快照、複製磁碟區和備份檔案的策略和其他詳細資訊。查看您在此系統中啟動的初始磁碟區的備份選項的詳細資訊。然後選擇“下一步”。
3. 檢查此卷的備份設置，然後選擇*啟動備份*。

更改分配給現有磁碟區的備份設置

您可以變更指派給已指派原則的現有磁碟區的備份策略。您可以變更本機快照、複製磁碟區和備份檔案的策略。

您想要套用於磁碟區的任何新快照、複製或備份策略都必須已經存在。

編輯單一磁碟區上的備份設置

步驟

1. 從「卷」選單中，找到要修改策略設定的捲，然後選擇「操作」選單。... 在行尾，選擇「編輯備份策略」。
2. 在「編輯備份策略」頁面中，對本機快照、複製磁碟區和備份檔案的現有備份策略進行更改，然後選擇「下一步」。

如果在為此叢集啟動NetApp Backup and Recovery時，在初始備份原則中為雲端備份啟用了 *DataLock* 和 *Ransomware Resilience*，您將只會看到已使用 DataLock 配置的其他策略。如果您在啟動NetApp Backup and Recovery時未啟用“DataLock 和 Ransomware Resilience”，您將只會看到未配置 DataLock 的其他雲端備份策略。

3. 檢查此卷的備份設置，然後選擇*啟動備份*。

編輯多個卷上的備份設置

如果您想在多個磁碟區上使用相同的備份設置，您可以同時在多個磁碟區上啟用或編輯備份設定。您可以選擇沒有備份設定、只有快照設定、只有備份到雲端設定等的捲，並使用不同的備份設定對所有這些磁碟區進行批次變更。

當使用多個磁碟區時，所有磁碟區必須具有以下共同特徵：

- 同一系統
- 相同樣式（FlexVol或FlexGroup磁碟區）
- 相同類型（讀寫或資料保護卷）

當啟用備份的磁碟區超過五個時， NetApp Backup and Recovery一次只會初始化五個磁碟區。當這些完成後，它會以 5 個為一組繼續進行，直到所有捲都初始化完畢。

步驟

1. 從「卷」標籤中，按磁碟區所在的系統進行篩選。
2. 選擇您想要管理備份設定的所有磁碟區。
3. 根據您要設定的備份作業類型，按一下批次作業選單中的按鈕：

備份作業...	選擇此按鈕...
管理快照備份設定	管理本機快照
管理複製備份設定	管理複製
管理備份到雲端備份設置	管理備份
管理多種類型的備份設定。此選項還使您能夠更改備份架構。	管理備份和復原

4. 在出現的備份頁面中，對本機快照、複製磁碟區或備份檔案的現有備份策略進行更改，然後選擇「儲存」。

如果在為此叢集啟動NetApp Backup and Recovery時，在初始備份原則中為雲端備份啟用了 *DataLock* 和 *Ransomware Resilience*，您將只會看到已使用 DataLock 配置的其他策略。如果您在啟動NetApp Backup and Recovery時未啟用“DataLock 和 Ransomware Resilience”，您將只會看到未配置 DataLock 的其他雲端

備份策略。

隨時建立手動卷備份

您可以隨時建立按需備份來擷取磁碟區的當前狀態。如果對磁碟區進行了非常重要的更改並且您不想等待下一次計劃的備份來保護該數據，這將非常有用。您也可以使用此功能為目前未備份且想要擷取其目前狀態的磁碟區建立備份。

您可以建立磁碟區的臨時快照或備份到物件儲存。您無法建立臨時複製磁碟區。

備份名稱包含時間戳，以便您可以從其他計畫備份中識別出您的按需備份。

如果在為此叢集啟動NetApp Backup and Recovery時啟用了“DataLock 和 Ransomware Resilience”，則按需備份也將配置 DataLock，保留期為 30 天。臨時備份不支援勒索軟體掃描。["了解有關 DataLock 和勒索軟體保護的更多信息"](#)。

當您建立臨時備份時，會在來源磁碟區上建立快照。由於此快照不是正常快照計劃的一部分，因此它不會旋轉。備份完成後，您可能會想要從來源磁碟區手動刪除此快照。這將允許釋放與此快照相關的區塊。快照名稱將以 cbs-snapshot-adhoc-。["了解如何使用ONTAP CLI 刪除快照"](#)。



資料保護卷不支援按需卷備份。

步驟

1. 從「卷」標籤中選擇...對於磁碟區並選擇*備份*>*建立臨時備份*。

此磁碟區的備份狀態列顯示“進行中”，直到備份建立完成。

查看每個卷的備份列表

您可以查看每個磁碟區的所有備份檔案的清單。此頁面顯示有關來源磁碟區、目標位置和備份詳細資訊（例如上次備份、目前備份策略、備份檔案大小等）。

步驟

1. 從「卷」標籤中選擇...對於來源磁碟區並選擇*查看磁碟區詳細資料*。

顯示磁碟區的詳細資訊和快照清單。

2. 選擇「快照」、「複製」或「備份」以查看每種備份類型的所有備份檔案清單。

對物件儲存中的磁碟區備份執行勒索軟體掃描

當建立目標檔案備份時以及還原備份檔案中的資料時，NetApp Backup and Recovery and Recovery會掃描您的備份檔案以尋找勒索軟體攻擊的證據。您也可以隨時執行按需掃描，以驗證物件儲存中特定備份檔案的可用性。如果您在特定磁碟區上遇到勒索軟體問題並且想要驗證該磁碟區的備份不受影響，這將很有用。

只有當磁碟區備份是從具有ONTAP 9.11.1 或更高版本的系統建立的，並且在備份到物件策略中啟用了_DataLock 和 Ransomware Resilience_ 時，此功能才可用。

步驟

1. 從「卷」標籤中選擇...對於來源磁碟區並選擇*查看磁碟區詳細資料*。

將顯示該卷的詳細資訊。

2. 選擇*備份*以查看物件儲存中的備份檔案清單。
3. 選擇...對於您想要掃描勒索軟體的捲備份文件，然後點擊*掃描勒索軟體*。

勒索軟體復原力列顯示掃描正在進行中。

管理與來源磁碟區的複製關係

在兩個系統之間設定資料複製後，您可以管理資料複製關係。

步驟

1. 從「卷」標籤中選擇...對於來源磁碟區並選擇*複製*選項。您可以看到所有可用的選項。
2. 選擇您想要執行的複製操作。

下表描述了可用的操作：

行動	描述
查看複製	顯示有關卷關係的詳細資訊：傳輸資訊、上次傳輸資訊、有關磁碟區的詳細資訊以及有關分配給該關係的保護策略的資訊。
更新複製	啟動增量傳輸來更新目標卷，使其與來源卷同步。
暫停複製	暫停快照的增量傳輸，以更新目標磁碟區。如果您想重新開始增量更新，可以稍後再恢復。
中斷複製	打破來源磁碟區和目標磁碟區之間的關係，並啟動目標磁碟區進行資料存取 - 使其可讀寫。當來源磁碟區因資料損壞、意外刪除或離線狀態等事件而無法提供資料時，通常會使用此選項。 https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html ["了解如何在ONTAP文件中配置目標磁碟區以進行資料存取並重新啟動來源磁碟區"]
中止複製	停用將此磁碟區備份到目標系統，並且也會停用還原磁碟區的功能。任何現有的備份都不會被刪除。這不會刪除來源磁碟區和目標磁碟區之間的資料保護關係。
反向重新同步	反轉來源磁碟區和目標磁碟區的角色。原始來源磁碟區的內容將被目標磁碟區的內容覆蓋。當您想要重新啟動離線的來源磁碟區時，這很有用。上次資料複製和來源磁碟區停用之間寫入原始來源磁碟區的任何資料都不會保留。
刪除關係	刪除來源磁碟區和目標磁碟區之間的資料保護關係，這表示磁碟區之間不再發生資料複製。此操作不會啟動目標磁碟區以進行資料存取 - 這表示它不會使其可讀寫。如果系統之間沒有其他資料保護關係，此操作也會刪除叢集對等關係和儲存虛擬機器 (SVM) 對等關係。

結果

選擇操作後，控制台將更新關係。

編輯現有的備份到雲端策略

您可以變更目前套用至系統中的磁碟區的備份策略的屬性。更改備份策略會影響所有使用該策略的現有磁碟區。



- 如果在為此叢集啟動NetApp Backup and Recovery時在初始原則中啟用了_DataLock 和 Ransomware Resilience_，則您編輯的任何策略都必須配置相同的 DataLock 設定（治理或合規性）。如果您在啟動NetApp Backup and Recovery時未啟用“DataLock 和 Ransomware Resilience”，則現在無法啟用 DataLock。

- 在 AWS 上建立備份時，如果您在啟動NetApp Backup and Recovery時在第一個備份策略中選擇了 *S3 Glacier* 或 *S3 Glacier Deep Archive*，則該層將是編輯備份策略時唯一可用的存檔層。如果您在第一個備份策略中未選擇存檔層，那麼在編輯策略時，*S3 Glacier* 將是您唯一的存檔選項。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 在「備份設定」頁面中，選擇...對於您想要變更策略設定的系統，然後選擇*管理策略*。
3. 在「管理策略」頁面中，選擇您想要在該系統中變更的備份策略的「編輯」。
4. 在「編輯策略」頁面中，選擇向下箭頭展開「標籤和保留」部分以變更計畫和/或備份保留，然後選擇「儲存」。

如果您的叢集運行的是ONTAP 9.10.1 或更高版本，您也可以選擇在一定天數後啟用或停用備份分層到檔案儲存。

["了解有關使用 AWS 檔案儲存的更多信息"](#)。"[了解有關使用 Azure 檔案儲存的詳細信息](#)"。"[詳細了解如何使用 Google 歸檔存儲](#)"。（需ONTAP 9.12.1。）

請注意，如果您停止將備份分層到歸檔存儲，則任何已分層到歸檔存儲的備份文件仍將保留在該層中 - 它們不會自動移回標準層。只有新建立的磁碟區備份才會位於標準圖層。

新增新的備份到雲端策略

當您為系統啟用NetApp Backup and Recovery時，您最初選擇的所有磁碟區都會使用您定義的預設備份策略進行備份。如果您想要為具有不同復原點目標 (RPO) 的某些磁碟區指派不同的備份策略，您可以為該叢集建立其他策略並將這些原則指派給其他磁碟區。

如果要將新的備份策略套用到系統中的某些卷，首先需要將備份策略新增到系統中。然後你可以[將策略應用於該系統中的捲](#)。



- 如果在為此叢集啟動NetApp Backup and Recovery時在初始原則中啟用了_DataLock 和 Ransomware Resilience_，則您建立的任何其他策略都必須使用相同的 DataLock 設定（治理或合規性）進行設定。如果您在啟動NetApp Backup and Recovery時未啟用“DataLock 和 Ransomware Resilience”，則無法建立使用 DataLock 的新政策。

- 在 AWS 上建立備份時，如果您在啟動NetApp Backup and Recovery時在第一個備份策略中選擇了 *S3 Glacier* 或 *S3 Glacier Deep Archive*，則該層將是該叢集未來備份策略可用的唯一存檔層。如果您在第一個備份策略中未選擇存檔層，那麼_S3 Glacier_ 將是您未來策略的唯一存檔選項。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 在「備份設定」頁面中，選擇...對於您想要新增策略的系統，然後選擇*管理策略*。
3. 從「管理策略」頁面中，選擇「新增策略」。

4. 在「新增政策」頁面中，選擇向下箭頭展開「標籤和保留」部分以定義計劃和備份保留，然後選擇「儲存」。

如果您的叢集運行的是ONTAP 9.10.1 或更高版本，您也可以選擇在一定天數後啟用或停用備份分層到檔案儲存。

["了解有關使用 AWS 檔案儲存的更多信息"](#)。"[了解有關使用 Azure 檔案儲存的詳細信息](#)"。"[詳細了解如何使用 Google 歸檔存儲](#)"。（需ONTAP 9.12.1。）

刪除備份

NetApp Backup and Recovery讓您能夠刪除單一備份檔案、刪除磁碟區的所有備份或刪除系統中所有磁碟區的所有備份。如果您不再需要備份，或者您刪除了來源磁碟區並想要刪除所有備份，則可能需要刪除所有備份。

您無法刪除使用 DataLock 和勒索軟體保護鎖定的備份檔案。如果您選擇了一個或多個鎖定的備份文件，則 UI 中的「刪除」選項將不可用。



如果您打算刪除具有備份的系統或集群，則必須在刪除系統之前刪除備份。當您刪除系統時，NetApp Backup and Recovery不會自動刪除備份，且 UI 中目前不支援在刪除系統後刪除備份。您將繼續為任何剩餘的備份支付對象儲存費用。

刪除系統的所有備份文件

刪除系統物件儲存上的所有備份並不會停用該系統中磁碟區的未來備份。如果要停止建立系統中所有磁碟區的備份，您可以停用備份[如這裡所述](#)。

請注意，此操作不會影響快照或複製磁碟區—這些類型的備份檔案不會被刪除。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 選擇...對於要刪除所有備份的系統，然後選擇*刪除所有備份*。
3. 在確認對話方塊中，輸入系統的名稱。
4. 選擇“進階設定”。
5. 強制刪除備份：指示是否要強制刪除所有備份。

在某些極端情況下，您可能會想要NetApp Backup and Recovery不再存取備份。例如，如果服務不再有權存取備份儲存桶或備份受到 DataLock 保護但您不再需要它們，則可能會發生這種情況。以前，您無法自行刪除這些內容，而需要致電NetApp支援。在此版本中，您可以使用選項強制刪除備份（在磁碟區和系統層級）。



請謹慎使用此選項，並且僅在極端清理需要時使用。即使這些備份未被從物件儲存中刪除，NetApp Backup and Recovery也將無法再存取它們。您需要前往雲端提供者並手動刪除備份。

6. 選擇*刪除*。

刪除卷的所有備份文件

刪除磁碟區的所有備份也會停用該磁碟區的未來備份。

步驟

1. 在「卷」標籤中，按一下...對於來源磁碟區並選擇*詳細資料和備份清單*。

顯示所有備份檔案的清單。

2. 選擇*動作* > 刪除所有備份。
3. 輸入卷名稱。
4. 選擇“進階設定”。
5. 強制刪除備份：指示是否要強制刪除所有備份。

在某些極端情況下，您可能會想要NetApp Backup and Recovery不再存取備份。例如，如果服務不再有權存取備份儲存桶或備份受到 DataLock 保護但您不再需要它們，則可能會發生這種情況。以前，您無法自行刪除這些內容，而需要致電NetApp支援。在此版本中，您可以使用選項強制刪除備份（在磁碟區和系統層級）。



請謹慎使用此選項，並且僅在極端清理需要時使用。即使這些備份未被從物件儲存中刪除，NetApp Backup and Recovery也將無法再存取它們。您需要前往雲端提供者並手動刪除備份。

6. 選擇*刪除*。

刪除卷的單一備份文件

如果您不再需要單一備份文件，可以將其刪除。這包括刪除磁碟區快照的單一備份或物件儲存中的備份。

您無法刪除複製的磁碟區（資料保護磁碟區）。

步驟

1. 從「卷」標籤中選擇...對於來源磁碟區並選擇*查看磁碟區詳細資料*。

顯示卷的詳細信息，您可以選擇*快照*、*複製*或*備份*來查看該卷的所有備份文件的列表。預設情況下，會顯示可用的快照。

2. 選擇「快照」或「備份」來查看要刪除的備份檔案類型。
3. 選擇...對於要刪除的磁碟區備份文件，然後選擇*刪除*。
4. 在確認對話方塊中，選擇*刪除*。

刪除卷備份關係

如果您想停止建立新的備份文件並刪除來源卷，但保留所有現有的備份文件，則刪除卷的備份關係為您提供了一種存檔機制。這樣，您就可以在將來需要時從備份檔案中還原卷，同時清除來源儲存系統中的空間。

您不一定需要刪除來源磁碟區。您可以刪除磁碟區的備份關係並保留來源磁碟區。在這種情況下，您可以稍後在磁碟區上「啟動」備份。在這種情況下，將繼續使用原始基線備份副本 - 不會建立新的基線備份副本並將其匯出到雲端。請注意，如果您重新啟動備份關係，則會為該磁碟區指派預設備份策略。

只有當您的系統運行ONTAP 9.12.1 或更高版本時，此功能才可用。

您無法從NetApp Backup and Recovery使用者介面刪除來源磁碟區。但是，您可以開啟控制台*系統*頁面上的

磁碟區詳細資料頁面，然後 ["從那裡刪除卷"](#)。



一旦關係被刪除，您就無法刪除單一磁碟區備份檔案。但是，您可以刪除該磁碟區的所有備份。

步驟

1. 從「卷」標籤中選擇...對於來源卷，然後選擇*備份*>*刪除關係*。

停用系統的NetApp Backup and Recovery

停用系統的NetApp Backup and Recovery會停用系統上每個磁碟區的備份，也會停用還原磁碟區的功能。任何現有的備份都不會被刪除。這不會從系統中取消註冊備份服務 - 它基本上允許您暫停所有備份和還原活動一段時間。

請注意，除非您[刪除備份](#)。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 從「備份設定」頁面中選擇...對於您想要停用備份的系統，然後選擇*停用備份*。
3. 在確認對話方塊中，選擇*停用*。



當備份被停用時，該系統會出現一個「啟動備份」按鈕。當您想要重新啟用該系統的備份功能時，可以選擇此按鈕。

取消註冊系統的NetApp Backup and Recovery

如果您不再想使用備份功能且不想再為該系統的備份付費，則可以取消NetApp Backup and Recovery and Recovery。通常，當您計劃刪除系統並想要取消備份服務時使用此功能。

如果您想更改儲存叢集備份的目標物件存儲，也可以使用此功能。取消註冊系統的NetApp Backup and Recovery後，您可以使用新的雲端供應商資訊為該叢集啟用NetApp Backup and Recovery。

在取消註冊NetApp Backup and Recovery之前，您必須依序執行以下步驟：

- 停用系統的NetApp Backup and Recovery
- 刪除該系統的所有備份

這兩個操作完成之前，取消註冊選項不可用。

步驟

1. 從*Volumes*選項卡中，選擇*Backup Settings*。
2. 從「備份設定」頁面中選擇...對於您想要取消註冊備份服務的系統，然後選擇*取消註冊*。
3. 在確認對話方塊中，選擇*取消註冊*。

從ONTAP備份還原

ONTAP磁碟區資料的備份以快照的形式儲存在複製磁碟區上，或儲存在物件儲存中。您可以從這些位置中的任何一個位置還原特定時間點的資料。使用NetApp Backup and Recovery，您可以根據需要還原整個磁碟區、資料夾或單一檔案。



若要切換至NetApp Backup and Recovery工作負載，請參閱["切換到不同的NetApp Backup and Recovery工作負載"](#)。

- 您可以將*磁碟區*（作為新磁碟區）還原到原始系統、使用相同雲端帳戶的其他系統或本機ONTAP系統。
- 您可以將*資料夾*還原到原始系統中的磁碟區、使用相同雲端帳戶的不同系統中的磁碟區或本機ONTAP系統上的磁碟區。
- 您可以將*檔案*還原到原始系統中的磁碟區、使用相同雲端帳戶的不同系統中的磁碟區或本機ONTAP系統上的磁碟區。

您需要有效的NetApp Backup and Recovery許可證才能將資料還原到生產系統。

總而言之，這些是可用於將磁碟區資料還原到ONTAP系統的有效流程：

- 備份檔案 → 還原卷
- 複製卷 → 恢復卷
- 快照 → 已恢復磁碟區



如果還原作業未完成，請等到作業監視器顯示「失敗」後再重試還原作業。



有關還原ONTAP資料的限制，請參閱["ONTAP磁碟區的備份和還原限制"](#)。

恢復儀表板

您可以使用還原儀表板執行磁碟區、資料夾和檔案還原作業。若要存取復原儀表板，請從控制台選單中選擇“備份和還原”，然後選擇“還原”標籤。您也可以選擇 ⓘ 從「服務」面板的「備份和復原服務」中查看「復原儀表板」。



NetApp Backup and Recovery必須已為至少一個系統激活，並且必須存在初始備份檔案。

復原儀表板提供了兩種從備份檔案還原資料的不同方法：瀏覽和還原*和*搜尋和還原。

比較“瀏覽和還原”與“搜尋和還原”

廣義上講，當您需要恢復上週或上個月的特定卷、資料夾或文件時，瀏覽和恢復通常更好——並且您知道文件的名稱和位置，以及它最後處於良好狀態的日期。當您需要恢復磁碟區、資料夾或文件，但不記得確切的名稱、它所在的磁碟區或它最後處於良好狀態的日期時，搜尋和復原通常會更好。

表格提供了兩種方法的功能比較。

瀏覽和恢復	搜尋和恢復
瀏覽資料夾樣式結構以尋找單一備份檔案中的磁碟區、資料夾或檔案。	透過部分或完整磁碟區名稱、部分或完整資料夾/檔案名稱、大小範圍和其他搜尋篩選器，在*所有備份檔案*中搜尋磁碟區、資料夾或檔案。
如果檔案已被刪除或重新命名，且使用者不知道原始檔案名，則不處理檔案復原	處理新建立/刪除/重新命名的目錄和新建立/刪除/重新命名的文件
支援快速恢復。	不支援快速恢復。

此表根據備份檔案所在的位置提供了有效還原作業的清單。

備份類型	瀏覽和恢復			搜尋和恢復		
	恢復音量	恢復檔案	恢復資料夾	恢復音量	恢復檔案	恢復資料夾
快照	是的	不	不	是的	是的	是的
複製卷	是的	不	不	是的	是的	是的
備份文件	是的	是的	是的	是的	是的	是的

在使用任何一種復原方法之前，請先配置您的環境以滿足資源需求。詳情請見以下章節。

請參閱要使用的還原操作類型的要求和還原步驟：

- ["使用「瀏覽和恢復」恢復卷"](#)
- ["使用「瀏覽和恢復」功能恢復資料夾和文件"](#)
- ["使用「搜尋和還原」功能還原磁碟區、資料夾和文件"](#)

使用搜尋和恢復功能從**ONTAP**備份中恢復

您可以使用搜尋和復原功能從ONTAP備份檔案中還原磁碟區、資料夾或檔案。搜尋和復原功能可讓您搜尋所有備份（包括本機快照、複製磁碟區和物件儲存），而無需提供確切的系統、磁碟區或檔案名稱。

從本機快照或複製磁碟區復原通常比從物件儲存復原更快、更便宜。

還原整個磁碟區時，NetApp Backup and Recovery會使用備份資料建立一個新磁碟區。您可以還原到原始系統、同一雲端帳戶內的另一個系統或本機ONTAP系統。資料夾和檔案可以恢復到其原始位置、同一系統中的不同磁碟區、同一雲端帳戶中的另一個系統或本機系統。

復原功能取決於您的ONTAP版本：

- 資料夾：使用ONTAP 9.13.0 或更高版本，您可以還原包含所有檔案和子資料夾的資料夾；使用早期版本，您只能還原資料夾中的檔案。
- *歸檔儲存：*從歸檔儲存復原（ONTAP 9.10.1 或更高版本可用）速度較慢，並且可能會產生額外費用。
- 目標群集需求：
 - 磁碟區恢復：ONTAP 9.10.1 或更高版本
 - 檔案復原：ONTAP 9.11.1 或更高版本

- Google Archive 和StorageGRID：ONTAP 9.12.1 或更高版本
- 資料夾恢復：ONTAP 9.13.1 或更高版本

"了解有關從 AWS 檔案儲存恢復的更多信息"。"了解有關從 Azure 檔案儲存還原的詳細信息"。"詳細了解如何從 Google 存檔儲存中恢復"。



- 如果物件儲存中的備份檔案已配置 DataLock 和勒索軟體保護，則僅當ONTAP版本為 9.13.1 或更高版本時才支援資料夾級還原。如果您使用的是早期版本的ONTAP，則可以從備份檔案還原整個卷，然後存取所需的資料夾和檔案。
- 如果物件儲存中的備份檔案駐留在檔案儲存中，則僅當ONTAP版本為 9.13.1 或更高版本時才支援資料夾層級還原。如果您使用的是早期版本的ONTAP，則可以從尚未存檔的較新備份檔案中還原資料夾，也可以從已存檔的備份中還原整個磁碟區，然後存取所需的資料夾和檔案。
- 將資料從 Azure 檔案儲存還原到StorageGRID系統時，不支援「高」還原優先權。
- 目前不支援從ONTAP S3 物件儲存中的磁碟區還原資料夾。

在開始之前，您應該對要還原的磁碟區或檔案的名稱或位置有所了解。

搜尋和恢復支援的系統和物件儲存提供者

您可以將ONTAP資料從位於二級系統（複製磁碟區）或物件儲存（備份檔案）中的備份檔案還原到下列系統。快照保存在來源系統上，並且只能還原到同一系統。

*注意：*您可以從任何類型的備份文件還原磁碟區和文件，但目前只能從物件儲存中的備份文件還原資料夾。

備份檔案位置		目的地系統
物件儲存（備份）	輔助系統（複製）	
亞馬遜 S3	AWS 本機ONTAP系統中的Cloud Volumes ONTAP	AWS 本機ONTAP系統中的Cloud Volumes ONTAP
Azure Blob	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP
Google 雲端儲存	Google 本機ONTAP系統中的Cloud Volumes ONTAP	Google 本機ONTAP系統中的Cloud Volumes ONTAP
NetAppStorageGRID	本機ONTAP系統Cloud Volumes ONTAP	本地ONTAP系統
ONTAP S3	本機ONTAP系統Cloud Volumes ONTAP	本地ONTAP系統

對於搜尋和還原，控制台代理可以安裝在以下位置：

- 對於 Amazon S3，控制台代理可以部署在 AWS 或您的場所
- 對於 Azure Blob，控制台代理程式可以部署在 Azure 中或您的本機
- 對於 Google Cloud Storage，控制台代理程式必須部署在您的 Google Cloud Platform VPC 中
- 對於StorageGRID，控制台代理必須部署在您的場所；無論是否有網路存取

- 對於ONTAP S3，控制台代理可以部署在您的場所（有或沒有網路存取）或雲端供應商環境中

請注意，「本地ONTAP系統」包括FAS、AFF和ONTAP Select系統。

搜尋與恢復的先決條件

在啟用搜尋和復原功能前，請確保您的環境符合以下要求：

- 集群要求：
 - ONTAP版本必須為 9.8 或更高版本。
 - 磁碟區所在的儲存虛擬機器 (SVM) 必須具有配置的資料 LIF。
 - 必須在磁碟區上啟用 NFS（支援 NFS 和 SMB/CIFS 磁碟區）。
 - 必須在 SVM 上啟動 SnapDiff RPC 伺服器。當您在系統上啟用索引時，控制台會自動執行此操作。（SnapDiff 是一種能夠快速識別快照之間檔案和目錄差異的技術。）
- NetApp建議在控制台代理上掛載單獨的捲，以提高搜尋和復原的彈性。有關說明，請參閱[掛載磁碟區以重新索引目錄](#)。

舊版搜尋與復原的先決條件（使用索引目錄 v1）

以下是使用傳統索引時搜尋和復原功能的要求：

- AWS 需求：

- 必須將特定的 Amazon Athena、AWS Glue 和 AWS S3 權限新增至為控制台提供權限的使用者角色。"確保所有權限均已正確配置"。

請注意，如果您已經使用過去設定的控制台代理程式來使用 NetApp Backup and Recovery，則現在需要將 Athena 和 Glue 權限新增至控制台使用者角色。它們是搜尋和恢復所必需的。

- Azure 需求：

- 您必須向您的訂閱註冊 Azure Synapse Analytics 資源提供者（稱為「Microsoft.Synapse」）。"[了解如何為您的訂閱註冊此資源提供程序](#)"。您必須是訂閱*擁有者*或*貢獻者*才能註冊資源提供者。
- 必須將特定的 Azure Synapse Workspace 和 Data Lake Storage 帳戶權限新增至為控制台提供權限的使用者角色。"確保所有權限均已正確配置"。

請注意，如果您已經使用 NetApp Backup and Recovery 以及過去配置的控制台代理，則現在需要將 Azure Synapse Workspace 和 Data Lake Storage 帳戶權限新增至控制台使用者角色。它們是搜尋和恢復所必需的。

- 控制台代理必須配置為*不帶*代理伺服器才能與網際網路進行 HTTP 通訊。如果您已為控制台代理程式設定了 HTTP 代理伺服器，則無法使用搜尋和還原功能。

- Google Cloud 需求：

- 必須將特定的 Google BigQuery 權限新增至為 NetApp Console 提供權限的使用者角色。"確保所有權限均已正確配置"。

如果您已經使用 NetApp Backup and Recovery 以及您過去設定的控制台代理，現在需要將 BigQuery 權限新增至控制台使用者角色。它們是搜尋和恢復所必需的。

- StorageGRID 和 ONTAP S3 需求：

根據您的配置，有兩種方法可以實現“搜尋和還原”：

- 如果您的帳戶中沒有雲端提供者憑證，則索引目錄資訊將儲存在控制台代理程式上。

有關索引目錄 v2 的信息，請參閱下面有關如何啟用索引目錄的部分。

- 如果您在私人（暗）網站中使用控制台代理，則索引目錄資訊將儲存在控制台代理上（需要控制台代理版本 3.9.25 或更高版本）。
- 如果你有 "AWS 憑證" 或者 "Azure 憑證" 在帳戶中，索引目錄儲存在雲端提供者處，就像在雲端部署控制台代理程式一樣。（如果您擁有這兩張憑證，則預設選擇 AWS。）

即使您使用的是本機控制台代理，也必須滿足控制台代理權限和雲端提供者資源的雲端提供者要求。使用此實作時，請參閱上面的 AWS 和 Azure 要求。

搜尋和恢復過程

這個過程如下：

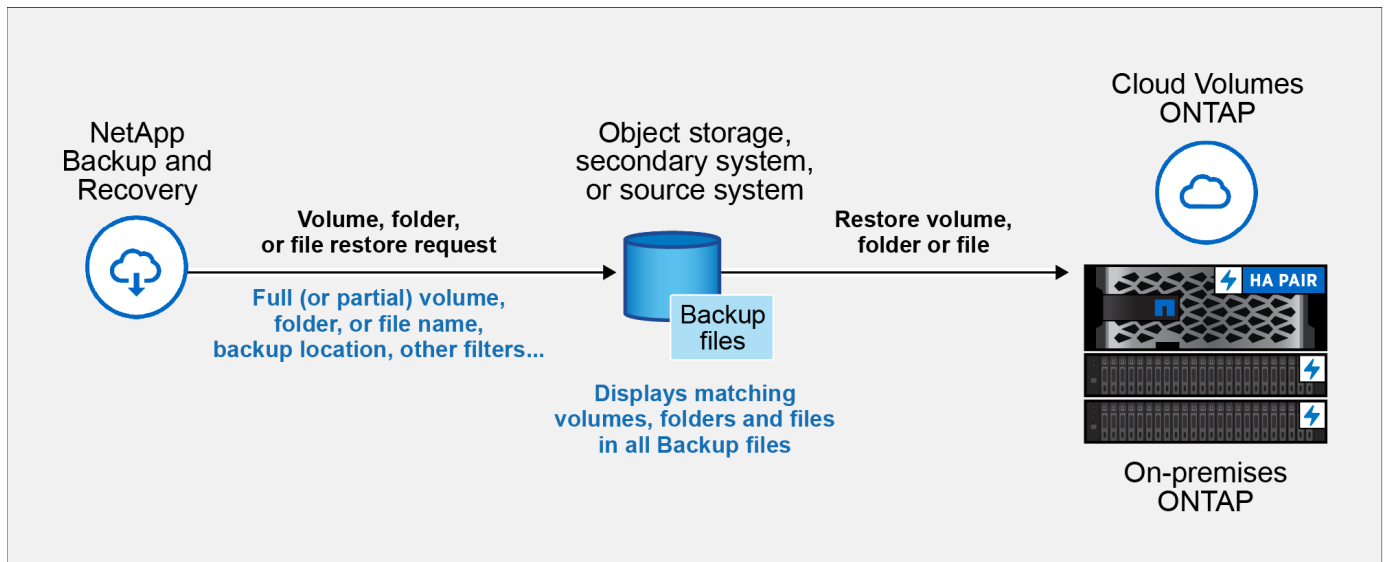
1. 在使用搜尋和還原之前，您需要在要從中還原磁碟區資料的每個來源系統上啟用「索引」。這使得索引目錄

可以追蹤每個卷的備份檔案。

2. 當您想要從磁碟區備份中還原磁碟區或檔案時，在「搜尋與還原」下選擇「搜尋和還原」。
3. 透過部分或完整磁碟區名稱、部分或完整檔案名稱、備份位置、大小範圍、建立日期範圍、其他搜尋篩選器輸入磁碟區、資料夾或檔案的搜尋條件，然後選擇*搜尋*。

搜尋結果頁面顯示具有符合搜尋條件的文件或磁碟區的所有位置。

4. 選擇要用於還原磁碟區或檔案的位置的“查看所有備份”，然後在要使用的實際備份檔案上選擇“還原”。
5. 選擇您想要復原磁碟區、資料夾或檔案的位置，然後選擇*復原*。
6. 磁碟區、資料夾或檔案已恢復。



您只需要知道部分名稱， NetApp Backup and Recovery就會搜尋所有與您的搜尋相符的備份檔案。

為每個系統啟用索引目錄

在使用搜尋和還原之前，您需要在計劃還原磁碟區或檔案的每個來源系統上啟用「索引」。這使得索引目錄可以追蹤每個捲和每個備份檔案 - 使您的搜尋非常快速和有效率。

索引目錄是一個資料庫，用於儲存系統中所有磁碟區和備份檔案的元資料。搜尋和復原功能使用它來快速找到包含要復原的資料的備份檔案。

索引目錄功能

使用索引目錄時， NetApp Backup and Recovery不會配置單獨的儲存桶。相反，對於儲存在 AWS、Azure、Google Cloud Platform、StorageGRID或ONTAP S3 中的備份，該服務會在控制台代理或雲端提供者環境上提供空間。

索引目錄支援以下功能：

- 3分鐘內即可實現全球搜尋效率
- 最多 50 億個文件
- 每個集群最多 5000 個卷
- 每個磁碟區最多 10 萬個快照

- 基線索引的最長時間少於 7 天。實際時間將根據您的環境而有所不同。

為系統啟用索引的步驟：

如果您的系統已啟用索引，請前往下一部分以還原您的資料。

您首先需要掛載一個單獨的磁碟區來存放目錄檔案。這樣可以防止因保存快照的檔案過大而導致資料遺失。並非每個叢集都需要這樣做；您可以從環境中的任何叢集掛載任何一個磁碟區。如果不這樣做，索引可能無法正常工作。

裝訂體積，請參考以下尺寸指南：

- 使用NetApp NFS 卷
- 建議使用磁碟吞吐量為 300 MB/s 的AFF儲存。吞吐量降低會影響搜尋和其他操作。
- 啟用NetApp快照功能，除了保護目錄備份 zip 檔案外，還可以保護目錄元資料。
- 每10億個檔案佔用50GB空間
- 目錄資料佔用 20 GB 空間，另有空間用於建立 zip 檔案和存放臨時檔案。

掛載磁碟區以重新索引目錄的步驟

1. 將卷掛載到 /opt/application/netapp/cbs 輸入以下命令，其中：

- volume name 這是在叢集上用於儲存目錄檔案的磁碟區。
- /opt/application/netapp/cbs 這是它安裝的路徑。

```
mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
```

範例：

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

啟用索引的步驟

1. 執行下列操作之一：

- 如果沒有系統被索引，請在「復原儀表板」的「搜尋與復原」下，選擇「啟用系統索引」。
- 如果至少有一個系統已被索引，請在「搜尋和復原」下的「復原儀表板」上選擇「索引設定」。

2. 為系統選擇*啟用索引*。

結果

在所有服務都配置完畢並且索引目錄啟動後，系統將顯示為「活動」狀態。

根據系統中捲的大小以及所有 3 個備份位置的備份檔案數量，初始索引過程可能需要長達一個小時。此後，它會每小時透明地更新，並進行增量更改以保持最新狀態。

使用「搜尋和還原」功能還原磁碟區、資料夾和文件

之後[為您的系統啟用索引](#)，您可以使用「搜尋和還原」還原磁碟區、資料夾和檔案。這使您可以使用廣泛的過濾器從所有備份檔案中找到要還原的確切檔案或磁碟區。

步驟

1. 從控制台選單中，選擇*保護>備份和還原*。
2. 選擇“恢復”選項卡，將顯示“恢復儀表板”。
3. 從“搜尋和恢復”部分，選擇“搜尋和恢復”。
4. 從“搜尋和恢復”部分，選擇“搜尋和恢復”。
5. 從「搜尋和還原」頁面：
 - a. 在「搜尋欄」中，輸入完整或部分磁碟區名稱、資料夾名稱或檔案名稱。
 - b. 選擇資源類型：磁碟區、檔案、資料夾*或*全部。
 - c. 在「過濾依據」區域中，選擇過濾條件。例如，您可以選擇資料所在的系統和檔案類型，例如 .JPEG 檔案。或者，如果您只想在物件儲存中的可用快照或備份檔案中搜尋結果，則可以選擇備份位置類型。
6. 選擇*搜尋*，搜尋結果區域將顯示所有具有與您的搜尋相符的文件、資料夾或磁碟區的資源。
7. 尋找包含您要復原的資料的資源，然後選擇「檢視所有備份」以顯示包含符合磁碟區、資料夾或檔案的所有備份檔案。
8. 找到您想要用於還原資料的備份檔案並選擇*復原*。

請注意，搜尋結果會識別包含您搜尋檔案的本機磁碟區快照和遠端複製磁碟區。您可以選擇從雲端備份檔案、快照或複製磁碟區中還原。

9. 選擇要還原磁碟區、資料夾或檔案的目標位置，然後選擇*復原*。
 - 對於卷，您可以選擇原始目標系統，也可以選擇備用系統。還原FlexGroup磁碟區時，您需要選擇多個聚合。
 - 對於資料夾，您可以還原到原始位置，也可以選擇備用位置；包括系統、磁碟區和資料夾。
 - 對於文件，您可以恢復到原始位置，也可以選擇備用位置；包括系統、磁碟區和資料夾。選擇原始位置時，您可以選擇覆蓋來源檔案或建立新檔案。

如果您選擇本機ONTAP系統，且尚未配置與物件儲存的叢集連接，系統將提示您輸入其他資訊：

- 從 Amazon S3 還原時，選擇ONTAP叢集中目標磁碟區所在的 IP 空間，輸入您建立的使用者的存取金鑰和金鑰，以授予ONTAP叢集對 S3 儲存桶的存取權限，並可選擇選擇私有 VPC 端點以進行安全資料傳輸。["查看有關這些要求的詳細信息"](#)。
- 從 Azure Blob 還原時，選擇目標磁碟區所在的ONTAP叢集中的 IP 空間，並透過選擇 VNet 和子網路來選擇用於安全資料傳輸的私有端點。["查看有關這些要求的詳細信息"](#)。
- 從 Google Cloud Storage 復原時，選擇目標磁碟區所在的ONTAP叢集中的 IP 空間，以及用於存取物件儲存的存取金鑰和金鑰。["查看有關這些要求的詳細信息"](#)。
- 從StorageGRID還原時，輸入StorageGRID伺服器的 FQDN 和ONTAP應用於與StorageGRID進行 HTTPS 通訊的端口，輸入存取物件儲存所需的存取金鑰和金鑰，以及目標磁碟區所在的ONTAP叢集中的 IP 空間。["查看有關這些要求的詳細信息"](#)。
- 從ONTAP S3 還原時，輸入ONTAP S3 伺服器的 FQDN 和ONTAP應用於與ONTAP S3 進行 HTTPS 通訊的端口，選擇存取物件儲存所需的存取金鑰和金鑰，以及目標磁碟區所在的ONTAP叢集中的 IP

空間。["查看有關這些要求的詳細信息"](#)。

結果

磁碟區、資料夾或檔案已恢復，您將返回恢復儀表板，以便您可以查看恢復操作的進度。您也可以選擇「作業監控」標籤來查看恢復進度。看["作業監控頁面"](#)。

使用“瀏覽和還原”功能還原**ONTAP**數據

使用NetApp Backup and Recovery and Recovery，透過瀏覽和復原功能恢復ONTAP資料。在復原之前，請記下來源磁碟區名稱、來源系統和 SVM 以及備份檔案日期。您可以從快照、複製磁碟區或儲存在物件儲存中的備份還原ONTAP資料。

復原功能取決於您的ONTAP版本：

- 資料夾：使用ONTAP 9.13.0 或更高版本，您可以還原包含所有檔案和子資料夾的資料夾；使用早期版本，您只能還原資料夾中的檔案。
- *歸檔儲存：*從歸檔儲存復原（ONTAP 9.10.1 或更高版本可用）速度較慢，並且可能會產生額外費用。
- 目標群集需求：
 - 磁碟區恢復：ONTAP 9.10.1 或更高版本
 - 檔案復原：ONTAP 9.11.1 或更高版本
 - Google Archive 和StorageGRID：ONTAP 9.12.1 或更高版本
 - 資料夾恢復：ONTAP 9.13.1 或更高版本

["了解有關從 AWS 檔案儲存恢復的更多信息"](#)。["了解有關從 Azure 檔案儲存還原的詳細信息"](#)。["詳細了解如何從 Google 存檔儲存中恢復"](#)。



將資料從 Azure 檔案儲存還原到StorageGRID系統時不支援高優先權。

瀏覽並恢復支援的系統和物件儲存提供者

您可以將ONTAP資料從位於二級系統（複製磁碟區）或物件儲存（備份檔案）中的備份檔案還原到下列系統。快照保存在來源系統上，並且只能還原到同一系統。

*注意：*您可以從任何類型的備份檔案還原卷，但目前只能從物件儲存中的備份檔案還原資料夾或單一檔案。

來自物件儲存（備份）	來自主（快照）	來自輔助系統（複製）	至目的地系統
亞馬遜 S3	AWS 本機ONTAP系統中的Cloud Volumes ONTAP	AWS 本機ONTAP系統中的Cloud Volumes ONTAP	Azure Blob
Azure 本地端ONTAP系統中的Cloud Volumes ONTAP	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP	Google 雲端儲存	Google 本機ONTAP系統中的Cloud Volumes ONTAP
Google 本機ONTAP系統中的Cloud Volumes ONTAP	NetAppStorageGRID	本地ONTAP系統	本機ONTAP系統Cloud Volumes ONTAP

來自物件儲存（備份）	來自主（快照）	來自輔助系統（複製）	至目的地系統
到本地ONTAP系統	ONTAP S3	本地ONTAP系統	本機ONTAP系統Cloud Volumes ONTAP

對於瀏覽和恢復，控制台代理可以安裝在以下位置：

- 對於 Amazon S3，控制台代理可以部署在 AWS 或您的場所
- 對於 Azure Blob，控制台代理程式可以部署在 Azure 中或您的本機
- 對於 Google Cloud Storage，控制台代理程式必須部署在您的 Google Cloud Platform VPC 中
- 對於StorageGRID，控制台代理必須部署在您的場所；無論是否有網路存取
- 對於ONTAP S3，控制台代理可以部署在您的場所（有或沒有網路存取）或雲端供應商環境中

請注意，「本地ONTAP系統」包括FAS、AFF和ONTAP Select系統。



如果您系統上的ONTAP版本低於 9.13.1，且備份檔案已配置 DataLock 和勒索軟體，則您無法還原資料夾或檔案。在這種情況下，您可以從備份檔案還原整個卷，然後存取所需的檔案。

使用「瀏覽和還原」還原卷

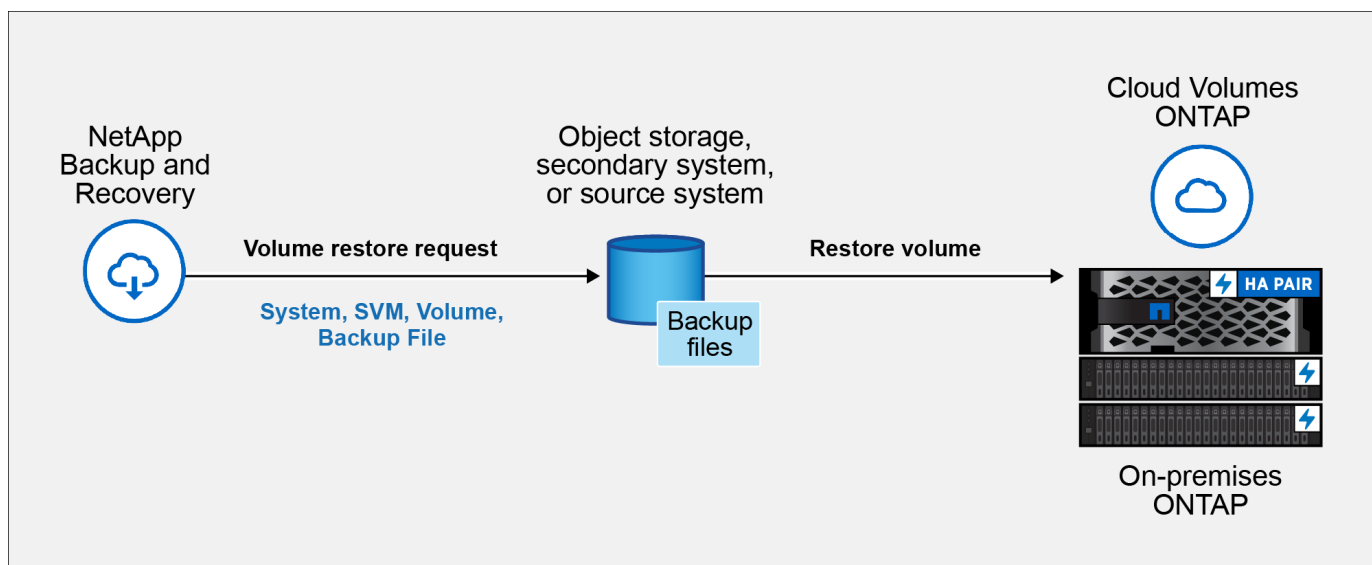
當您從備份檔案還原磁碟區時，NetApp Backup and Recovery會使用備份中的資料建立_新_磁碟區。使用物件儲存備份時，您可以將資料還原到原始系統中的磁碟區、與來源系統位於相同雲端帳戶的其他系統或本機ONTAP系統。

將雲端備份還原到使用ONTAP 9.13.0 或更高版本的Cloud Volumes ONTAP系統或執行ONTAP 9.14.1 的本機ONTAP系統時，您可以選擇執行_快速還原_操作。快速復原非常適合需要盡快提供對磁碟區的存取的災難復原情況。快速還原將備份檔案中的元資料還原到卷，而不是還原整個備份檔案。不建議對效能或延遲敏感的應用程式使用快速恢復，並且不支援歸檔儲存中的備份。



只有在建立雲端備份的來源系統執行ONTAP 9.12.1 或更高版本時，FlexGroup磁碟區才支援快速還原。並且僅當來源系統運行ONTAP 9.11.0 或更高版本時才支援SnapLock磁碟區。

從複製磁碟區還原時，您可以將磁碟區還原到原始系統或Cloud Volumes ONTAP或本機ONTAP系統。



若要還原卷，您需要來源系統名稱、儲存虛擬機器、磁碟區名稱和備份檔案日期。

步驟

1. 從控制台選單中，選擇*保護>備份和還原*。
2. 選擇“恢復”選項卡，將顯示“恢復儀表板”。
3. 從「瀏覽和復原」部分，選擇「恢復磁碟區」。
4. 在「選擇來源」頁面中，導覽至要還原的磁碟區的備份檔案。選擇具有要還原的日期/時間戳記的*系統*、*磁碟區*和*備份*檔案。

「位置」欄位顯示備份檔案（快照）是「本機」（來源系統上的快照）、「輔助」（輔助ONTAP系統上的複製磁碟區）或「物件儲存」（物件儲存中的備份檔案）。選擇您想要恢復的檔案。

5. 選擇“下一步”。

請注意，如果您選擇物件儲存中的備份文件，並且該備份的勒索軟體復原功能處於活動狀態（如果您在備份策略中啟用了 DataLock 和勒索軟體復原功能），則系統會提示您在復原資料之前對備份檔案執行額外的勒索軟體掃描。我們建議您掃描備份檔案以尋找勒索軟體。（您將需要向雲端提供者支付額外的出口費用才能存取備份檔案的內容。）

6. 在「選擇目標」頁面中，選擇要恢復磁碟區的*系統*。
7. 從物件儲存還原備份檔案時，如果您選擇本機ONTAP系統且尚未配置與物件儲存的叢集連接，系統將提示您輸入其他資訊：
 - 從 Amazon S3 還原時，選擇ONTAP叢集中目標磁碟區所在的 IP 空間，輸入您建立的使用者的存取金鑰和金鑰，以授予ONTAP叢集對 S3 儲存桶的存取權限，並可選擇選擇私有 VPC 端點以進行安全資料傳輸。
 - 從 Azure Blob 還原時，選擇目標磁碟區所在的ONTAP叢集中的 IP 空間，選擇用於存取物件儲存的 Azure 訂閱，並透過選擇 VNet 和子網路來選擇用於安全資料傳輸的私人端點。
 - 從 Google Cloud Storage 還原時，選擇 Google Cloud 專案以及存取金鑰和金鑰來存取物件儲存、儲存備份的區域以及目標磁碟區所在的ONTAP叢集中的 IP 空間。
 - 從StorageGRID還原時，輸入StorageGRID伺服器的 FQDN 和ONTAP應用於與StorageGRID進行 HTTPS 通訊的端口，選擇存取物件儲存所需的存取金鑰和金鑰，以及目標磁碟區所在的ONTAP叢集中的 IP 空間。
 - 從ONTAP S3 還原時，輸入ONTAP S3 伺服器的 FQDN 和ONTAP應用於與ONTAP S3 進行 HTTPS 通訊的端口，選擇存取物件儲存所需的存取金鑰和金鑰，以及目標磁碟區所在的ONTAP叢集中的 IP 空間。
8. 輸入要用於復原的磁碟區的名稱，然後選擇磁碟區所在的儲存虛擬機器和聚合。還原FlexGroup磁碟區時，您需要選擇多個聚合。預設情況下，<source_volume_name>_restore 用作磁碟區名。

當將備份從物件儲存還原到使用ONTAP 9.13.0 或更高版本的Cloud Volumes ONTAP系統或執行ONTAP 9.14.1 的本機ONTAP系統時，您可以選擇執行_快速還原_操作。

如果您要從位於歸檔儲存層（從ONTAP 9.10.1 開始可用）中的備份檔案還原卷，則可以選擇還原優先權。

["了解有關從 AWS 檔案儲存恢復的更多信息"](#)。"[了解有關從 Azure 檔案儲存還原的詳細信息](#)"。"[詳細了解如何從 Google 存檔儲存中恢復](#)"。Google Archive 儲存層中的備份檔案幾乎可以立即恢復，並且不需要恢復優先順序。

9. 選擇「下一步」來選擇是否執行正常還原或快速還原程序：

- 正常還原：在需要高效能的磁碟區上使用正常還原。還原過程完成之前，磁碟區將不可用。
- 快速恢復：恢復的捲和資料將立即可用。請勿在需要高效能的磁碟區上使用此功能，因為在快速復原過程中，存取資料的速度可能會比平常慢。

10. 選擇“恢復”，您將返回恢復儀表板，以便查看恢復操作的進度。

結果

NetApp Backup and Recovery根據您選擇的備份建立一個新磁碟區。

請注意，從駐留在檔案儲存中的備份檔案還原磁碟區可能需要幾分鐘或幾小時，具體取決於檔案層和復原優先權。您可以選擇「作業監控」標籤來查看恢復進度。

使用“瀏覽和還原”還原資料夾和文件

如果您只需要從ONTAP磁碟區備份中還原幾個文件，則可以選擇還原資料夾或單一文件，而不是還原整個磁碟區。您可以將資料夾和檔案還原到原始系統中的現有捲，或還原到使用相同雲端帳戶的其他系統。您也可以將資料夾和檔案還原到本機ONTAP系統上的磁碟區。



目前，您只能從物件儲存中的備份檔案還原資料夾或單一檔案。目前不支援從本機快照或位於輔助系統（複製磁碟區）中的備份檔案還原檔案和資料夾。

如果選擇多個文件，它們將還原到同一目標磁碟區。若要將檔案還原到不同的捲，請多次執行該過程。

使用ONTAP 9.13.0 或更高版本時，您可以還原資料夾以及其中的所有檔案和子資料夾。使用 9.13.0 之前的ONTAP版本時，僅還原該資料夾中的檔案 - 不會還原子資料夾或子資料夾中的檔案。

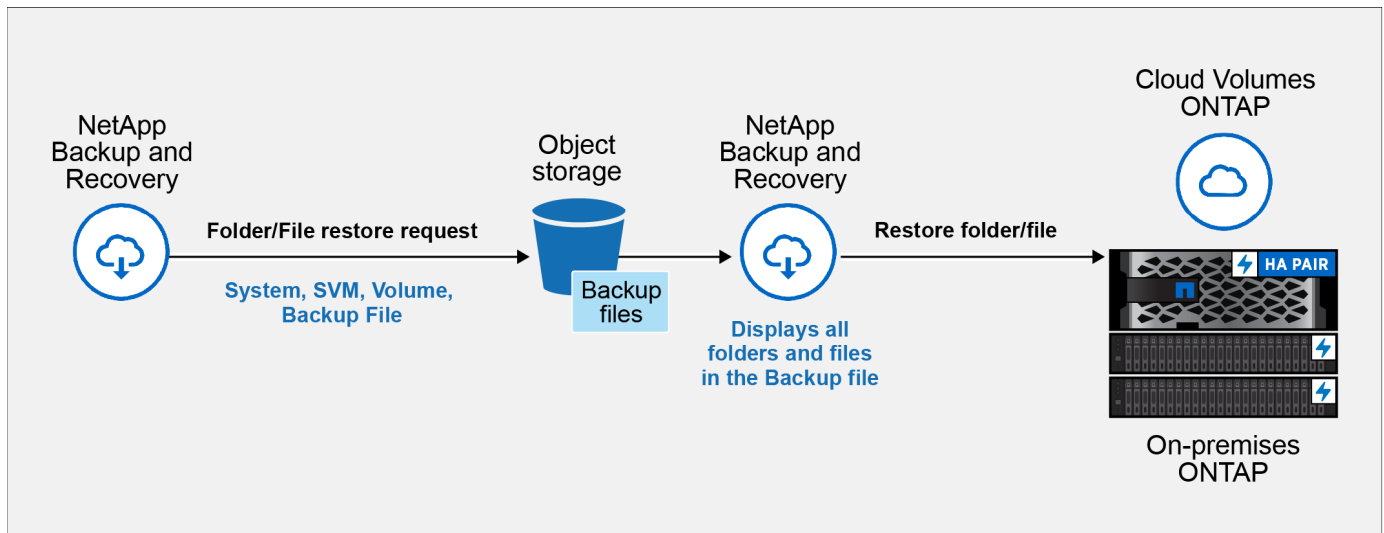


- 如果備份檔案已配置 DataLock 和勒索軟體保護，則僅當ONTAP版本為 9.13.1 或更高版本時才支援資料夾級還原。如果您使用的是早期版本的ONTAP，則可以從備份檔案還原整個卷，然後存取所需的資料夾和檔案。
- 如果備份檔案駐留在檔案儲存中，則僅當ONTAP版本為 9.13.1 或更高版本時才支援資料夾層級還原。如果您使用的是早期版本的ONTAP，則可以從尚未存檔的較新備份檔案中還原資料夾，也可以從已存檔的備份中還原整個磁碟區，然後存取所需的資料夾和檔案。
- 使用ONTAP 9.15.1，您可以使用「瀏覽和復原」選項還原FlexGroup資料夾。此功能處於技術預覽模式。

您可以使用 ["NetApp Backup and Recovery2024 年 7 月版本博客"](#)。

還原資料夾和文件

請依照下列步驟將資料夾或檔案從ONTAP磁碟區備份還原到磁碟區。您應該知道要用於還原資料夾或檔案的磁碟區的名稱和備份檔案的日期。此功能使用即時瀏覽，以便您可以查看每個備份檔案中的目錄和檔案清單。



開始之前

- ONTAP版本必須為 9.6 或更高版本才能執行_檔_復原操作。
- ONTAP版本必須為 9.11.1 或更高版本才能執行_資料夾_還原操作。如果資料位於檔案儲存中，或備份檔案使用 DataLock 和勒索軟體保護，則需要ONTAP版本 9.13.1。
- ONTAP版本必須為 9.15.1 p2 或更高版本才能使用瀏覽和還原選項還原FlexGroup目錄。

步驟

1. 從控制台選單中，選擇*保護>備份和還原*。
2. 選擇“恢復”選項卡，將顯示“恢復儀表板”。
3. 從「瀏覽和復原」部分，選擇「復原檔案或資料夾」。
4. 在「選擇來源」頁面中，導覽至包含要還原的資料夾或檔案的磁碟區的備份檔案。選擇具有要從中復原檔案的日期/時間戳記的*系統*、磁碟區*和*備份。
5. 選擇“下一步”，將顯示磁碟區備份中的資料夾和檔案清單。

如果您要從位於檔案儲存層的備份文件還原資料夾或文件，則可以選擇還原優先權。

["了解有關從 AWS 檔案儲存恢復的更多信息"](#)。"[了解有關從 Azure 檔案儲存還原的詳細信息](#)"。"[詳細了解如何從 Google 存檔儲存中恢復](#)"。Google Archive 儲存層中的備份檔案幾乎可以立即恢復，並且不需要恢復優先順序。

如果備份檔案的勒索軟體復原功能處於活動狀態（如果您在備份策略中啟用了 DataLock 和勒索軟體復原功能），則會提示您在復原資料之前對備份檔案執行額外的勒索軟體掃描。我們建議您掃描備份檔案以尋找勒索軟體。（您將需要向雲端提供者支付額外的出口費用才能存取備份檔案的內容。）

6. 在「選擇項目」頁面中，選擇要復原的資料夾或文件，然後選擇「繼續」。為了幫助您找到該物品：
 - 如果看到資料夾或檔案名，您可以選擇它。
 - 您可以選擇搜尋圖示並輸入資料夾或檔案的名稱以直接導航到該項目。
 - 您可以使用行尾的向下箭頭向下導航資料夾層級來尋找特定檔案。

當您選擇文件時，它們會被添加到頁面的左側，以便您可以看到已經選擇的文件。如果需要，您可以透過選擇檔案名稱旁邊的 **x** 從此清單中刪除檔案。

7. 在「選擇目標」頁面中，選擇要還原項目的*系統*。

如果您選擇本地集群，並且尚未配置與物件儲存的集群連接，系統將提示您輸入其他資訊：

- 從 Amazon S3 還原時，輸入目標磁碟區所在的ONTAP叢集中的 IP 空間，以及存取物件儲存所需的 AWS 存取金鑰和金鑰。您也可以選擇專用連結配置來連接到叢集。
- 從 Azure Blob 還原時，輸入目標磁碟區所在的ONTAP叢集中的 IP 空間。您也可以為與叢集的連線選擇私有端點配置。
- 從 Google Cloud Storage 復原時，輸入目標磁碟區所在的ONTAP叢集中的 IP 空間，以及存取物件儲存所需的存取金鑰和金鑰。
- 從StorageGRID還原時，輸入StorageGRID伺服器的 FQDN 和ONTAP應用於與StorageGRID進行 HTTPS 通訊的端口，輸入存取物件儲存所需的存取金鑰和金鑰，以及目標磁碟區所在的ONTAP叢集中的 IP 空間。

8. 然後選擇要還原資料夾或檔案的*磁碟區*和*資料夾*。

恢復資料夾和檔案時，您有幾個位置選項可供選擇。

- 當您選擇“選擇目標資料夾”時，如上所示：
 - 您可以選擇任意資料夾。
 - 您可以將滑鼠懸停在資料夾上，然後按一下行尾以深入查看子資料夾，然後選擇一個資料夾。
- 如果您選擇了與來源資料夾/檔案相同的目標系統和磁碟區，則可以選擇*維護來源資料夾路徑*將資料夾或檔案還原到來源結構中存在的相同資料夾。所有相同的資料夾和子資料夾必須已經存在；不會建立資料夾。將檔案還原到原始位置時，您可以選擇覆蓋來源檔案或建立新檔案。

9. 選擇“恢復”返回恢復儀表板並查看恢復操作的進度。

保護 Microsoft SQL Server 工作負載

使用NetApp Backup and Recovery保護 Microsoft SQL 工作負載概述

使用NetApp Backup and Recovery將 Microsoft SQL Server 應用程式資料從本機ONTAP系統備份到 AWS、Azure 或StorageGRID。系統會根據您的政策自動在您的雲端帳戶中建立並儲存備份。使用 3-2-1 策略：在兩個儲存系統上保留資料的三個副本，在雲端中保留一個副本。

3-2-1 方法的優點包括：

- 多個資料副本可防止內部和外部網路安全威脅。
- 如果一種媒體發生故障，使用不同類型的媒體可以幫助您恢復。
- 您可以從現場副本快速恢復，如果現場副本受到損害，則可以使用異地副本。

NetApp Backup and Recovery使用NetApp SnapMirror透過建立快照並將其傳輸到備份位置來同步備份。

您可以執行以下操作來保護您的資料：

- "如果從SnapCenter匯入，則配置其他項目"

- "發現 Microsoft SQL Server 工作負載並選擇性地匯入SnapCenter資源"
- "使用本機ONTAP主儲存上的本機快照備份工作負載"
- "將工作負載複製到ONTAP二級存儲"
- "將工作負載備份到物件儲存位置"
- "立即備份工作負載"
- "恢復工作負載"
- "克隆工作負載"
- "管理工作負載清單"
- "管理快照"

若要備份工作負載，您需要建立管理備份和復原作業的策略。看["創建策略"](#)了解更多。

支援的備份目標

NetApp Backup and Recovery可讓您將下列來源系統中的 Microsoft SQL Server 執行個體和資料庫備份到下列輔助系統以及公有雲和私有雲供應商中的物件儲存。快照保留在來源系統上。

來源系統	輔助系統（複製）	目標物件儲存（備份）
AWS 中的Cloud Volumes ONTAP	AWS 本機ONTAP系統中的Cloud Volumes ONTAP	亞馬遜 S3 ONTAP S3
Azure 中的Cloud Volumes ONTAP	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP	Azure Blob ONTAP S3
本地ONTAP系統	Cloud Volumes ONTAP本地ONTAP系統	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	不適用

支援的還原目標

您可以將 Microsoft SQL Server 執行個體和資料庫從駐留在主儲存或輔助系統（複製磁碟區）或物件儲存（備份檔案）中的備份還原到下列系統。快照保存在來源系統上，並且只能還原到同一系統。

從備份檔案位置	至目的地系統	
物件儲存（備份）	輔助系統（複製）	
亞馬遜 S3	AWS 本機ONTAP系統中的Cloud Volumes ONTAP	AWS 本機ONTAP系統ONTAP S3 中的雲端磁碟區
Azure Blob	Azure 本地端ONTAP系統中的Cloud Volumes ONTAP	Azure 中的Cloud Volumes ONTAP 本機ONTAP系統ONTAP S3
StorageGRID	Cloud Volumes ONTAP本地ONTAP系統	本地ONTAP系統ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	不適用



「本地ONTAP系統」包括FAS和AFF系統。

從外掛程式服務匯入NetApp Backup and Recovery 的先決條件

如果您要將資源從 Microsoft SQL Server 的SnapCenter外掛程式服務匯入NetApp Backup and Recovery，則需要設定更多項目。

首先在**NetApp Console**中建立系統

如果要從SnapCenter匯入資源，則應先將所有本機SnapCenter叢集儲存體新增至控制台 系統 頁面，然後再從SnapCenter匯入。這確保主機資源能夠被正確地發現和導入。

確保安裝**SnapCenter**插件的主機需求

若要從 Microsoft SQL Server 適用的SnapCenter外掛程式匯入資源，請確保符合安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式的主機需求。

專門檢查SnapCenter要求["NetApp Backup and Recovery前提條件"](#)。

停用使用者帳戶控制遠端限制

從SnapCenter匯入資源之前，請停用SnapCenter Windows 主機上的使用者帳戶控制 (UAC) 遠端限制。如果您使用本機管理帳戶遠端連線至SnapCenter Server 主機或 SQL 主機，請停用 UAC。

安全考慮

在停用 UAC 遠端限制之前，請考慮以下問題：

- 安全風險：停用令牌過濾可能會使您的系統面臨安全漏洞，尤其是在本機管理帳戶受到惡意行為者的攻擊時。
- 謹慎使用：
 - 僅當該設定對於您的管理任務至關重要時才修改它。
 - 確保採用強密碼和其他安全措施來保護管理帳戶。

替代解決方案

- 如果需要遠端管理訪問，請考慮使用具有適當權限的網域帳戶。
- 使用符合最佳安全實務的安全遠端管理工具來最大限度地降低風險。

停用使用者帳戶控制遠端限制的步驟

1. 修改 `LocalAccountTokenFilterPolicy` SnapCenter Windows 主機上的登錄項目。

使用以下方法之一執行此操作，並按照下面的說明進行操作：

- 方法 1：登錄編輯器
- 方法 2：PowerShell 腳本

方法 1：使用登錄編輯器停用使用者帳戶控制

這是可以用來停用使用者帳戶控制的方法之一。

步驟

1. 執行下列操作，在 SnapCenter Windows 主機上開啟登錄編輯程式：

- 按 `Windows+R` 開啟“運行”對話框。
- 類型 `regedit`` 並按 `Enter`。

2. 導航至策略密鑰：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

3. 建立或修改 `DWORD` 價值：

- 定位：`LocalAccountTokenFilterPolicy`
- 如果不存在，則建立一個新的 `DWORD`（32 位元）值命名 `LocalAccountTokenFilterPolicy`。

4. 支援以下值。對於這種情況，將值設為 1：

- 0（預設）：啟用 UAC 遠端限制。本機帳戶在遠端存取時已過濾令牌。
- 1：UAC 遠端限制已停用。本機帳戶繞過令牌過濾並在遠端存取時擁有完全的管理權限。

5. 按一下“確定”。

6. 關閉登錄編輯程式。

7. 重新啟動 SnapCenter Windows 主機。

註冊表修改範例

此範例將 `LocalAccountTokenFilterPolicy` 設為“1”，停用 UAC 遠端限制。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
```

```
"LocalAccountTokenFilterPolicy"=dword:00000001
```

方法 2：使用 **PowerShell** 腳本停用使用者帳號控制

這是您可以用來停用使用者帳戶控制的另一種方法。



以提升的權限執行 PowerShell 指令可能會影響系統設定。在運行命令之前，請確保您理解這些命令及其含義。

步驟

1. 在 SnapCenter Windows 主機上開啟具有管理權限的 PowerShell 視窗：

- 點選“開始”選單。
- 搜尋 **PowerShell 7** 或 **Windows Powershell**。
- 右鍵單擊該選項並選擇“以管理員身份執行”。

2. 確保您的系統上安裝了 PowerShell。安裝後，它應該會出現在“開始”選單中。



Windows 7 及更高版本預設包含 PowerShell。

- 若要停用 UAC 遠端限制，請透過執行下列命令將 LocalAccountTokenFilterPolicy 設定為「1」：

```
Set-ItemProperty -Path  
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
```

- 驗證目前值是否設定為「1」`LocalAccountTokenFilterPolicy`透過運行：

```
Get-ItemProperty -Path  
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"LocalAccountTokenFilterPolicy"
```

- 如果值為 1，則停用 UAC 遠端限制。
- 如果值為 0，則啟用 UAC 遠端限制。

- 若要套用更改，請重新啟動電腦。

停用 **UAC** 遠端限制的 **PowerShell 7** 命令範例：

此範例中的值設定為「1」，表示 UAC 遠端限制已停用。

```
# Disable UAC remote restrictions  
  
Set-ItemProperty -Path  
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord  
  
# Verify the change  
  
Get-ItemProperty -Path  
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"LocalAccountTokenFilterPolicy"  
  
# Output  
  
LocalAccountTokenFilterPolicy : 1
```

發現 **Microsoft SQL Server** 工作負載並可選擇從**NetApp Backup and Recovery**中的**SnapCenter**匯入

NetApp Backup and Recovery需要先發現 Microsoft SQL Server 工作負載，您才能使用該服務。如果您已經安裝了SnapCenter，則可以選擇從SnapCenter匯入備份資料和原則。

所需的**NetApp Console**角色 備份和還原超級管理員。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

發現 **Microsoft SQL Server** 工作負載並選擇性地匯入**SnapCenter**資源

在發現過程中， NetApp Backup and Recovery會分析組織內系統中的 Microsoft SQL Server 執行個體和資料庫。

NetApp Backup and Recovery評估 Microsoft SQL Server 應用程式。該服務評估現有保護級別，包括目前的備份保護策略、快照以及備份和還原選項。

發現以下列方式發生：

- 如果您已有SnapCenter，請使用NetApp Backup and Recovery and Recovery UI 將SnapCenter資源匯入NetApp Backup and Recovery and Recovery。



如果您已經擁有SnapCenter，請先檢查以確保在從SnapCenter匯入之前已滿足先決條件。例如，您應該先將本機SnapCenter叢集儲存系統新增至NetApp Console，然後再從SnapCenter匯入。看["從SnapCenter匯入資源的先決條件"](#)。

- 如果您還沒有SnapCenter，您仍然可以透過手動新增 vCenter 並執行發現來發現工作負載。

如果已安裝**SnapCenter**，請將**SnapCenter**資源匯入**NetApp Backup and Recovery**

如果您已安裝SnapCenter，請依照下列步驟將SnapCenter資源匯入NetApp Backup and Recovery。NetApp Console從SnapCenter發現資源、主機、憑證和計劃；您不必重新建立所有這些資訊。

您可以透過以下方式執行此操作：

- 在發現期間，選擇一個選項從SnapCenter匯入資源。
- 發現後，從「清單」頁面選擇一個選項來匯入SnapCenter資源。
- 發現後，從「設定」選單中選擇一個選項來匯入SnapCenter資源。有關詳細信息，請參閱["配置NetApp Backup and Recovery"](#)。

這是一個由兩個部分組成的過程：

- 匯入SnapCenter Server 應用程式和主機資源
- 管理選定的SnapCenter主機資源

匯入**SnapCenter Server** 應用程式和主機資源

第一步從SnapCenter匯入主機資源，並在NetApp Backup and Recovery清單頁面中顯示這些資源。此時，資源尚未由NetApp Backup and Recovery管理。



匯入SnapCenter主機資源後， NetApp Backup and Recovery不會自動接手保護管理。為此，您必須明確選擇在NetApp Backup and Recovery中管理匯入的資源。這可確保您已準備好透過NetApp Backup and Recovery備份這些資源。

步驟

1. 從NetApp Console左側導覽中，選擇 保護 > 備份和還原。

2. 選擇*庫存*。
3. 選擇*發現資源*。
4. 從NetApp Backup and Recovery Discover 工作負載資源頁面中，選擇 從**SnapCenter**匯入。
5. 輸入* SnapCenter應用程式憑證*：
 - a. * SnapCenter FQDN 或 IP 位址*：輸入SnapCenter應用程式本身的 FQDN 或 IP 位址。
 - b. 連接埠：輸入SnapCenter伺服器的連接埠號碼。
 - c. 使用者名稱*和*密碼：輸入SnapCenter伺服器的使用者名稱和密碼。
 - d. 控制台代理：選擇SnapCenter的控制台代理程式。
6. 輸入* SnapCenter伺服器主機憑證*：
 - a. 現有憑證：如果選擇此選項，則可以使用已新增的現有憑證。選擇憑證名稱。
 - b. 新增憑證：如果您沒有現有的SnapCenter主機憑證，則可以新增憑證。輸入憑證名稱、身份驗證模式、使用者名稱和密碼。
7. 選擇“導入”來驗證您的條目並註冊SnapCenter伺服器。



如果SnapCenter伺服器已註冊，您可以更新現有的註冊詳細資訊。

結果

清單頁面顯示匯入的SnapCenter資源，包括 MS SQL 主機、執行個體和資料庫。

若要查看匯入的SnapCenter資源的詳細信息，請從「操作」功能表中選擇「查看詳細資料」選項。

管理**SnapCenter**主機資源

匯入SnapCenter資源後，在NetApp Backup and Recovery中管理這些主機資源。選擇管理這些資源後，NetApp Backup and Recovery and Recovery能夠備份並還原您從SnapCenter匯入的資源。您不再在SnapCenter Server 中管理這些資源。

步驟

1. 匯入SnapCenter資源後，從備份和復原選單中選擇*Inventory*。
2. 從「清單」頁面中，選擇您希望從現在開始使用NetApp Backup and Recovery進行管理的匯入的SnapCenter主機。
3. 選擇“操作”圖標 > *查看詳情*顯示工作量詳情。
4. 在清單 > 工作負載頁面中，選擇操作圖標 > 管理 顯示管理主機頁面。
5. 選擇*管理*。
6. 在管理主機頁面中，選擇使用現有 vCenter 或新增新的 vCenter。
7. 選擇*管理*。

庫存頁面顯示新管理的SnapCenter資源。

您可以選擇從「操作」功能表中選擇「產生報表」選項來建立管理資源的報表。

從清單頁面發現後匯入**SnapCenter**資源

如果您已經發現資源，則可以從清單頁面匯入**SnapCenter**資源。

步驟

1. 從控制台左側導覽中，選擇*保護*>*備份和還原*。
2. 選擇*庫存*。
3. 從庫存頁面中，選擇*匯入**SnapCenter**資源*。
4. 請依照上面*匯入**SnapCenter**資源*部分中的步驟匯入**SnapCenter**資源。

如果您尚未安裝**SnapCenter**，請新增 **vCenter** 並發現資源

如果您尚未安裝**SnapCenter**，您可以新增 **vCenter** 資訊並讓**NetApp**備份和還原發現工作負載。在每個控制台代理程式中，選擇您想要發現工作負載的系統。

如果您有 **VMware** 環境，這是可選的。

步驟

1. 從控制台左側導覽中，選擇*保護*>*備份和還原*。

如果您是第一次登入備份和恢復，並且在控制台中有一個系統但沒有發現任何資源，則會顯示「歡迎使用新的**NetApp**備份和恢復」頁面，其中包含「發現資源」選項。

2. 選擇*發現資源*。
3. 輸入以下資訊：
 - a. 工作負載類型：對於此版本，僅 **Microsoft SQL Server** 可用。
 - b. **vCenter** 設定：選擇現有的 **vCenter** 或新增新的 **vCenter**。若要新增新的 **vCenter**，請輸入 **vCenter** FQDN 或 IP 位址、使用者名稱、密碼、連接埠和協定。



如果要輸入 **vCenter** 訊息，請輸入 **vCenter** 設定和主機註冊的資訊。如果您在這裡新增或輸入了 **vCenter** 訊息，接下來您還需要在進階設定中新增插件資訊。

- c. 主機註冊：選擇*新增憑證*並輸入包含您想要發現的工作負載的主機的資訊。



如果要新增獨立伺服器而不是 **vCenter** 伺服器，則僅輸入主機資訊。

4. 選擇*發現*。



此過程可能需要幾分鐘。

5. 繼續高級設定。

在發現期間設定進階設定選項並安裝插件

使用高級設置，您可以在所有註冊的伺服器上手動安裝插件代理。這使您能夠將所有**SnapCenter**工作負載匯入**NetApp Backup and Recovery**。**NetApp Backup and Recovery**顯示了安裝外掛程式所需的步驟。

步驟

1. 在「發現資源」頁面中，按一下右側的向下箭頭繼續進行「進階設定」。
2. 在發現工作負載資源頁面中，輸入以下資訊。
 - 輸入插件連接埠號碼：輸入插件使用的連接埠號碼。
 - 安裝路徑：輸入插件的安裝路徑。
3. 如果要手動安裝SnapCenter代理，請選取以下選項的核取方塊：
 - 使用手動安裝：勾選此方塊可手動安裝插件。
 - 新增叢集中的所有主機：選取此方塊可在發現期間將叢集中的所有主機新增至NetApp Backup and Recovery。
 - 跳過選購的預安裝檢查：勾選此方塊可跳過選購的預安裝檢查。例如，如果您知道記憶體或空間考慮因素將在不久的將來發生變化，並且您想立即安裝插件，那麼您可能想要這樣做。
4. 選擇*發現*。

繼續存取NetApp Backup and Recovery儀表板

1. 從NetApp Console選單中，選擇 保護 > 備份和還原。
2. 選擇一個工作負載圖塊（例如，Microsoft SQL Server）。
3. 從備份和還原選單中，選擇*儀表板*。
4. 檢討資料保護的健康狀況。處於危險中或受保護的工作負載的數量會根據新發現、受保護和備份的工作負載而增加。

["了解儀表板顯示的內容"](#)。

使用NetApp Backup and RecoveryMicrosoft SQL Server 工作負載

將 Microsoft SQL Server 應用程式資料從本機ONTAP系統備份到 Amazon Web Services、Microsoft Azure 或StorageGRID。系統會自動建立備份並將其儲存在您的雲端帳戶的物件儲存中以保護資料。

- 若要安排程備份工作負載，請建立管理備份和復原作業的策略。看["創建策略"](#)以取得說明。
- 在開始備份之前配置已發現主機的日誌目錄。
- 立即備份工作負載（立即建立按需備份）。

查看工作負載保護狀態

在開始備份之前，請先查看工作負載的保護狀態。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員、備份和還原復原管理員、備份和還原複製管理員或備份和還原檢視器角色。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。

2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 查看主機、保護群組、可用性群組、執行個體和資料庫標籤上的詳細資訊。

配置發現主機的日誌目錄

設定已發現主機的活動日誌路徑，以便在備份工作負載之前追蹤操作狀態。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員或備份和還原還原管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇主機。
5. 選擇“操作”圖標 ... > 配置日誌目錄。
6. 輸入主機路徑或瀏覽主機或節點清單以找到要儲存主機日誌的位置。
7. 選擇您想要儲存日誌的那些。



顯示的欄位會根據所選的部署模型而有所不同，例如故障轉移群集實例或獨立實例。

8. 選擇*儲存*。

建立保護組

建立保護組來管理多個工作負載的備份和還原作業。保護組是工作負載的邏輯分組。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇*建立保護組*。
6. 為保護組提供名稱。
7. 選擇要包含在保護組中的執行個體或資料庫。
8. 選擇“下一步”。
9. 選擇要套用於保護群組的*備份策略*。

如果要建立策略，請選擇*建立新策略*並依照指示建立策略。看"[創建策略](#)"了解更多。

10. 選擇“下一步”。
11. 檢查配置。
12. 選擇“建立”來建立保護組。

立即使用按需備份來備份工作負載

在對系統進行變更之前執行按需備份，以確保您的資料受到保護。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從選單中選擇*庫存*。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ...> 查看詳情。
4. 選擇「保護群組」、「實例」或「資料庫」標籤。
5. 選擇要備份的執行個體或資料庫。
6. 選擇“操作”圖標 ...> 立即備份。
7. 選擇要套用於備份的策略。
8. 選擇計劃層級。
9. 選擇*立即備份*。

暫停備份計劃

暫停計劃以在維護或故障排除期間暫時停止備份。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ...> 查看詳情。
4. 選擇「保護群組」、「實例」或「資料庫」標籤。
5. 選擇要暫停的保護群組、執行個體或資料庫。
6. 選擇“操作”圖標 ...> 暫停。

刪除保護群組

刪除保護群組會刪除該保護群組以及所有相關的備份計畫。如果不再需要某個保護群組，您可能需要將其刪除。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇“操作”圖標 ... > 刪除保護群組。

刪除工作負載的保護

如果您不再想要備份某个工作負載，或是想要停止在NetApp Backup and Recovery中管理該工作負載，則可以從該工作負載中移除保護。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇「保護群組」、「實例」或「資料庫」標籤。
5. 選擇保護群組、執行個體或資料庫。
6. 選擇“操作”圖標 ... > 移除保護。
7. 在「刪除保護」對話方塊中，選擇是否要保留備份和元資料或刪除它們。
8. 選擇*刪除*以確認操作。

使用NetApp Backup and RecoveryMicrosoft SQL Server 工作負載

使用NetApp Backup and Recovery還原 Microsoft SQL Server 工作負載。使用快照、複製到輔助儲存的備份或物件儲存中的備份。將工作負載還原到原始系統、具有相同雲端帳戶的不同系統或本機ONTAP系統。

從這些位置恢復

您可以從不同的起始位置恢復工作負載：

- 從主要位置還原
- 從複製的資源還原
- 從物件儲存備份還原

恢復到這些點

您可以將資料還原到最新快照或以下點：

- 從快照還原
- 如果您知道檔案名稱、位置 and 最後有效日期，則還原到特定時間點

- 還原到最新備份

從物件儲存中復原的注意事項

如果您在物件儲存中選擇了備份文件，並且該備份的勒索軟體復原功能處於活動狀態（如果您在備份策略中啟用了 DataLock 和勒索軟體復原功能），那麼系統會提示您在復原資料之前對備份檔案執行額外的完整性檢查。我們建議您執行掃描。

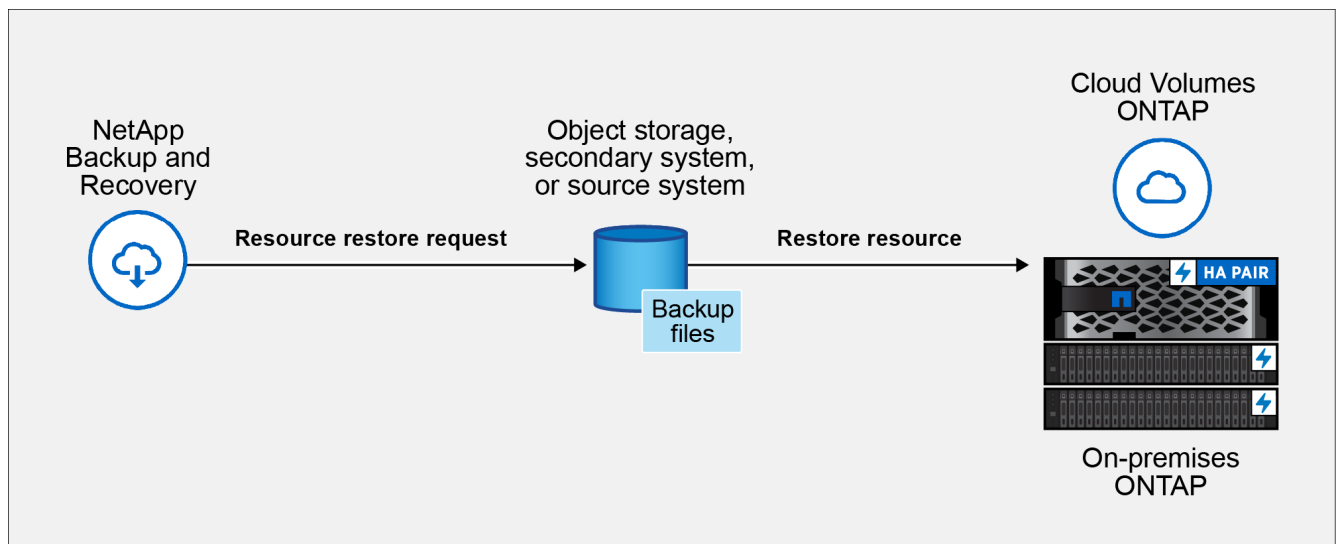


您需要向雲端提供者支付額外費用才能存取備份檔案。

恢復工作負載的工作原理

恢復工作負載時，會發生以下情況：

- 當您從備份檔案還原工作負載時，NetApp Backup and Recovery and Recovery會使用備份中的資料建立一個_新_資源。
- 從複製的工作負載復原時，您可以將工作負載還原到原始系統或本機ONTAP系統。



- 從物件儲存還原備份時，您可以將資料還原到原始系統或本機ONTAP系統。

恢復方法

使用下列方法之一恢復工作負載：

- 從恢復頁面：當您不知道資源的名稱、位置或最後有效日期時，使用此選項可恢復資源。使用過濾器搜尋快照。
- 從庫存頁面：當您知道特定資源的名稱、位置和最後有效日期時，使用此選項可恢復該資源。瀏覽清單以尋找資源。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

從“恢復”選項恢復工作負載數據

使用復原選項復原資料庫工作負載。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 復原。
2. 選擇要還原的資料庫。使用過濾器進行搜尋。
3. 選擇恢復選項：
 - 從快照還原
 - 如果您知道檔案名稱、位置 and 最後有效日期，則還原到特定時間點
 - 還原到最新備份

從快照恢復工作負載

1. 繼續從復原選項頁面，選擇*從快照復原*。

出現快照清單。

2. 選擇要復原的快照。
3. 選擇“下一步”。

接下來您將看到目的地選項。

4. 在目的地詳情頁面中，輸入以下資訊：
 - 目標設定：選擇是否將資料還原到原始位置還是其他位置。對於備用位置，選擇主機名稱和實例，輸入資料庫名稱，然後輸入要還原快照的目標路徑。
 - 預恢復選項：
 - 恢復時覆蓋同名資料庫：恢復時，保留原始資料庫名稱。
 - 保留 **SQL** 資料庫複製設定：恢復作業後保留 SQL 資料庫的複製設定。
 - 復原前建立交易日誌備份：在復原作業之前建立交易日誌備份。* 如果還原前的交易日誌備份失敗，則退出還原：如果交易日誌備份失敗，則停止還原作業。
 - **Prescript**：輸入應在復原作業之前執行的腳本的完整路徑、腳本所需的任何參數以及等待腳本完成的時間。
 - 恢復後選項：
 - 可操作，但無法還原其他交易日誌。套用交易日誌備份後，資料庫將恢復線上狀態。
 - 不可操作，但可用於還原額外的交易日誌。在還原交易日誌備份的同時，在還原作業後將資料庫維持在非作業狀態。此選項對於還原額外的交易日誌很有用。
 - 唯讀模式，可用來還原額外的交易日誌。以唯讀模式還原資料庫並套用交易日誌備份。
 - 後記：輸入恢復操作後應執行的腳本的完整路徑以及腳本所採用的任何參數。
5. 選擇*恢復*。

恢復到特定時間點

NetApp Backup and Recovery使用日誌和最新的快照來建立資料的時間點復原。

1. 繼續從「恢復選項」頁面，選擇「恢復到特定時間點」。

2. 選擇“下一步”。
3. 在「還原到特定時間點」頁面中，輸入以下資訊：
 - 資料復原的日期和時間：輸入您要復原的資料的確切日期和時間。此日期和時間來自 Microsoft SQL Server 資料庫主機。
4. 選擇*搜尋*。
5. 選擇要復原的快照。
6. 選擇“下一步”。
7. 在目的地詳情頁面中，輸入以下資訊：
 - 目標設定：選擇是否將資料還原到原始位置還是其他位置。對於備用位置，請選擇主機名稱和實例，輸入資料庫名稱，然後輸入目標路徑。
 - 預恢復選項：
 - 保留原始資料庫名稱：在復原過程中，保留原始資料庫名稱。
 - 保留 **SQL** 資料庫複製設定：恢復作業後保留 SQL 資料庫的複製設定。
 - **Prescript**：輸入應在復原作業之前執行的腳本的完整路徑、腳本所需的任何參數以及等待腳本完成的時間。
 - 恢復後選項：
 - 可操作，但無法還原其他交易日誌。套用交易日誌備份後，資料庫將恢復線上狀態。
 - 不可操作，但可用於還原額外的交易日誌。在還原交易日誌備份的同時，在還原作業後將資料庫維持在非作業狀態。此選項對於還原額外的交易日誌很有用。
 - 唯讀模式，可用來還原額外的交易日誌。以唯讀模式還原資料庫並套用交易日誌備份。
 - 後記：輸入恢復操作後應執行的腳本的完整路徑以及腳本所採用的任何參數。
8. 選擇*恢復*。

還原到最新備份

此選項使用最新的完整備份和日誌備份將資料恢復到最後的良好狀態。系統掃描從上次快照到現在的日誌。該過程追蹤變化和活動以恢復資料的最新和最準確的版本。

1. 繼續從復原選項頁面，選擇*還原到最新備份*。

NetApp Backup and Recovery 向您顯示可用於復原操作的快照。

2. 在還原到最新狀態頁面中，選擇本機、二級儲存或物件儲存的快照位置。
3. 選擇“下一步”。
4. 在目的地詳情頁面中，輸入以下資訊：
 - 目標設定：選擇是否將資料還原到原始位置還是其他位置。對於備用位置，請選擇主機名稱和實例，輸入資料庫名稱，然後輸入目標路徑。
 - 預恢復選項：
 - 恢復時覆蓋同名資料庫：恢復時，保留原始資料庫名稱。
 - 保留 **SQL** 資料庫複製設定：恢復作業後保留 SQL 資料庫的複製設定。

- 復原前建立交易日誌備份：在復原作業之前建立交易日誌備份。
- 如果還原前的交易日誌備份失敗，則退出還原：如果交易日誌備份失敗，則停止還原作業。
- **Prescript**：輸入應在復原作業之前執行的腳本的完整路徑、腳本所需的任何參數以及等待腳本完成的時間。
- 恢復後選項：
 - 可操作，但無法還原其他交易日誌。套用交易日誌備份後，資料庫將恢復線上狀態。
 - 不可操作，但可用於還原額外的交易日誌。在還原交易日誌備份的同時，在還原作業後將資料庫維持在非作業狀態。此選項對於還原額外的交易日誌很有用。
 - 唯讀模式，可用來還原額外的交易日誌。以唯讀模式還原資料庫並套用交易日誌備份。
 - 後記：輸入恢復操作後應執行的腳本的完整路徑以及腳本所採用的任何參數。

5. 選擇*恢復*。

從 **Inventory** 選項恢復工作負載數據

從庫存頁面還原資料庫工作負載。使用 **Inventory** 選項，您只能還原資料庫，而不能還原執行個體。

步驟

1. 從 **NetApp Backup and Recovery** 選單中，選擇 **Inventory**。
2. 選擇要復原的資源所在的主機。
3. 選擇*操作*  圖標，然後選擇*查看詳細資訊*。
4. 在 **Microsoft SQL Server** 頁面上，選擇「資料庫」標籤。
5. 在資料庫選單中，選擇具有「受保護」狀態的資料庫。
6. 選擇*操作*  圖標，然後選擇*恢復*。

與從「恢復」頁面恢復時出現的三個選項相同：

- 從快照還原
- 恢復到特定時間點
- 還原到最新備份

7. 繼續執行與「復原」頁面中的復原選項相同的步驟

使用 **NetApp Backup and Recovery** **Microsoft SQL Server** 工作負載

使用 **NetApp Backup and Recovery** 將 **Microsoft SQL Server** 應用程式資料複製到 VM 以進行開發、測試或保護。從 **SQL Server** 工作負載的即時或現有快照建立複製。

從以下克隆類型中進行選擇：

- 即時快照和複製：您可以從即時快照建立 **Microsoft SQL Server** 工作負載的克隆，即時快照是從備份建立的來源資料的時間點副本。克隆儲存在您的公有或私有雲帳戶的物件儲存中。如果資料遺失或損壞，您可以使用克隆來恢復您的工作負載。
- 從現有快照複製：您可以從可用於工作負載的快照清單中選擇現有快照。如果您想從特定時間點建立克隆，

此選項很有用。克隆到主存儲或輔助存儲。

您可以實現以下保護目標：

- 創建克隆
- 刷新克隆
- 分裂克隆
- 刪除克隆

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)" 。

創建克隆

您可以建立 Microsoft SQL Server 工作負載的複製。克隆是從備份建立的來源資料的副本。克隆儲存在您的公有或私有雲帳戶的物件儲存中。如果資料遺失或損壞，您可以使用克隆來恢復您的工作負載。

您可以從現有快照或即時快照建立複製。即時快照是根據備份建立的來源資料的時間點副本。如果資料遺失或損壞，您可以使用克隆來恢復您的工作負載。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 複製。
2. 選擇*建立新克隆*。
3. 選擇克隆類型：
 - 從現有快照克隆和刷新資料庫：選擇快照並配置克隆選項。
 - 即時快照和克隆：立即對來源資料進行快照並從該快照建立克隆。如果您想要從來源工作負載中的最新資料建立克隆，此選項很有用。
4. 完成*資料庫來源*部分：
 - 單一克隆或批次克隆：選擇建立單一克隆或多個克隆。如果您選擇*批次複製*，則可以使用已建立的保護群組一次建立多個克隆。如果您想為不同的工作負載建立多個克隆，此選項很有用。
 - 來源資料庫主機、執行個體和名稱：選擇複製的來源資料庫主機、執行個體和名稱。來源資料庫是將建立克隆的資料庫。
5. 完成*資料庫目標*部分：
 - 目標資料庫主機、執行個體和名稱：選擇複製的目標資料庫主機、執行個體和名稱。目標資料庫是將建立克隆的位置。

或者，從目標名稱下拉清單中選擇 **Suffix**，並為克隆的資料庫名稱加上後綴。如果不加入後綴，克隆的資料庫名稱與來源資料庫名稱相同。

 - **QoS**（最大吞吐量）：為複製選擇服務品質（QoS）最大吞吐量（MBps）。QoS 定義了克隆的效能特徵，例如最大吞吐量和 IOPS。
6. 完成*Mount*部分：
 - 自動分配掛載點：自動為物件儲存中的克隆分配掛載點。
 - 定義掛載點路徑：輸入複製的掛載點。掛載點是克隆將在物件儲存中掛載的位置。選擇磁碟機號，輸入資料檔路徑，輸入日誌檔案路徑。

7. 選擇“下一步”。
8. 選擇還原點：
 - 現有快照：從可用於工作負載的快照清單中選擇現有快照。如果您想從特定時間點建立克隆，此選項很有用。
 - 即時快照和克隆：從可用於工作負載的快照清單中選擇最新快照。如果您想要從來源工作負載中的最新資料建立克隆，此選項很有用。
9. 如果您選擇建立*即時快照和複製*，請選擇複製儲存位置：
 - 本機儲存：選擇此選項可在ONTAP系統的本機儲存中建立複製。本機儲存是直接連接到ONTAP系統的儲存。
 - 二級儲存：選擇此選項可在ONTAP系統的二級儲存中建立克隆。輔助儲存是用於備份和還原工作負載的儲存。
10. 選擇資料和日誌的目標位置。
11. 選擇“下一步”。
12. 完成*進階選項*部分。
13. 如果您選擇*即時快照和克隆*，請完成以下選項：
 - 克隆刷新計劃和到期時間：如果您選擇*即時複製*，請輸入開始刷新克隆的日期。克隆計劃定義了何時建立克隆。
 - 如果計劃到期則刪除克隆：如果您想在克隆到期日時刪除克隆。
 - 刷新克隆頻率：選擇克隆的刷新頻率。您可以選擇每小時、每天、每週、每月或每季刷新克隆。如果您希望克隆與來源工作負載保持同步，則此選項很有用。
 - 前言和後記：可選地，添加在克隆創建之前和之後運行的腳本。這些腳本可以執行額外的任務，例如設定複製或發送通知。
 - 通知：可選地，指定電子郵件地址以接收有關複製建立狀態以及作業報告的通知。您也可以指定一個webhook URL 來接收有關複製建立狀態的通知。您可以指定是否需要成功和失敗通知，或只需要其中一個。
 - 標籤：選擇標籤以協助您稍後搜尋資源組，然後選擇*應用程式*。例如，如果您將「HR」作為標籤新增至多個資源群組，則以後可以找到與「HR」標籤關聯的所有資源群組。
14. 選擇“創建”。
15. 當克隆創建完成後，您可以在*庫存*頁面中查看它。

刷新克隆

您可以刷新 Microsoft SQL Server 工作負載的克隆。刷新克隆會使用來源工作負載中的最新資料來更新克隆。如果您希望使克隆與來源工作負載保持同步，這將非常有用。

您可以選擇變更資料庫名稱、使用最新的即時快照或從現有生產快照刷新。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 複製。
2. 選擇要刷新的克隆。
3. 選擇“操作”圖標  > 刷新克隆。

4. 完成“進階設定”部分：

- 復原範圍：選擇是否要還原所有日誌備份或直到特定時間點的日誌備份。如果您想將克隆恢復到特定時間點，此選項很有用。
- 克隆刷新計劃和到期時間：如果您選擇*即時複製*，請輸入開始刷新克隆的日期。克隆計劃定義了何時建立克隆。
 - 如果計劃到期則刪除克隆：如果您想在克隆到期日時刪除克隆。
 - 刷新克隆頻率：選擇克隆的刷新頻率。您可以選擇每小時、每天、每週、每月或每季刷新克隆。如果您希望克隆與來源工作負載保持同步，則此選項很有用。
- **iGroup** 設定：選擇克隆的 iGroup。iGroup 是用於存取複製的啟動器的邏輯分組。您可以選擇現有的 iGroup 或建立一個新的 iGroup。從主或輔助 ONTAP 儲存系統中選擇 iGroup。
- 前言和後記：可選地，添加在克隆創建之前和之後運行的腳本。這些腳本可以執行額外的任務，例如設定複製或發送通知。
- 通知：可選地，指定電子郵件地址以接收有關複製建立狀態以及作業報告的通知。您也可以指定一個 webhook URL 來接收有關複製建立狀態的通知。您可以指定是否需要成功和失敗通知，或只需要其中一個。
- 標籤：輸入一個或多個標籤，以協助您稍後搜尋資源組。例如，如果您將「HR」作為標籤新增至多個資源群組，則以後可以找到與 HR 標籤關聯的所有資源群組。

5. 在刷新確認對話方塊中，若要繼續，請選擇*刷新*。

跳過克隆刷新

跳過克隆刷新以保持克隆不變。

步驟

1. 從 NetApp Backup and Recovery 選單中，選擇 複製。
2. 選擇您想要跳過刷新的克隆。
3. 選擇“操作”圖標  > 跳過刷新。
4. 在「跳過刷新確認」對話方塊中，執行以下操作：
 - a. 若要僅跳過下一個刷新計劃，請選擇*僅跳過下一個刷新計劃*。
 - b. 若要繼續，請選擇*跳過*。

分裂克隆

您可以拆分 Microsoft SQL Server 工作負載的複製。拆分克隆將從克隆中建立一個新的備份。新的備份可用於恢復工作負載。

您可以選擇將克隆拆分為獨立克隆或長期克隆。精靈會顯示 SVM 的聚合清單、其大小以及複製磁碟區的位置。NetApp Backup and Recovery 也會指示是否有足夠的空間來分割克隆。克隆分裂後，克隆成為一個獨立的資料庫進行保護。

克隆作業不會被刪除，並且可以再次用於其他克隆。

步驟

1. 從 NetApp Backup and Recovery 選單中，選擇 複製。

2. 選擇一個克隆。
3. 選擇“操作”圖標  > 分裂克隆。
4. 查看拆分克隆詳細資訊並選擇*拆分*。
5. 當分裂克隆創建完成後，您可以在*庫存*頁面中查看它。

刪除克隆

您可以刪除 Microsoft SQL Server 工作負載的複製。刪除克隆會從物件儲存中移除該複製並釋放儲存空間。

如果策略保護克隆，則克隆及其作業都會被刪除。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 複製。
2. 選擇一個克隆。
3. 選擇“操作”圖標  > 刪除克隆。
4. 在複製刪除確認對話方塊中，查看刪除詳細資訊。
 - a. 若要從SnapCenter中刪除克隆的資源，即使複製或其儲存不可訪問，也請選擇「強制刪除」。
 - b. 選擇*刪除*。
5. 當克隆被刪除時，它將從*庫存*頁面中刪除。

使用NetApp Backup and Recovery管理 Microsoft SQL Server 庫存

NetApp Backup and Recovery可協助您管理 Microsoft SQL Server 主機、資料庫和執行個體。您可以查看、變更或刪除庫存的保護設定。

您可以完成以下與管理庫存相關的任務：

- 管理主機資訊
 - 暫停時間表
 - 編輯或刪除主機
- 管理實例資訊
 - 將憑證與資源關聯
 - 立即啟動按需備份
 - 編輯保護設定
- 管理資料庫資訊
 - 保護資料庫
 - 還原資料庫
 - 編輯保護設定
 - 立即啟動按需備份
- 配置日誌目錄（從 清單 > 主機）。如果要在快照中備份資料庫主機的日誌，請先在NetApp Backup and

Recovery中設定日誌。有關詳細信息，請參閱["配置NetApp Backup and Recovery設置"](#)。

管理主機資訊

您可以管理主機資訊以確保正確的主機受到保護。您可以查看、編輯和刪除主機資訊。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員、備份和還原復原管理員或備份和還原複製管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

- 配置日誌目錄。有關詳細信息，請參閱["配置NetApp Backup and Recovery設置"](#)。
- 暫停時間表
- 編輯主機
- 刪除主機

管理主機

您可以管理系統中發現的主機。您可以單獨或作為一個群組來管理它們。



您可以在「主機」欄位中管理狀態為「未管理」的主機。NetApp Backup and Recovery已經管理具有「託管」狀態的主機。

在NetApp Backup and Recovery中管理主機後，SnapCenter不再管理這些主機上的資源。

所需的**NetApp Console**角色 儲存檢視器，或備份和還原超級管理員。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從選單中選擇*庫存*。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 > 查看詳情。
4. 選擇“主機”標籤。
5. 選擇一個或多個主機。如果您選擇多個主機，則會出現批次操作選項，您可以在其中選擇*管理（最多 5 個主機）*。
6. 選擇“操作”圖標 > 管理。
7. 查看主機依賴關係：
 - 如果未顯示 vCenter，請選擇鉛筆圖示以新增或編輯 vCenter 詳細資訊。
 - 如果您新增了 vCenter，您也必須透過選擇「註冊 vCenter」來註冊 vCenter。
8. 選擇*驗證設定*來測試您的設定。
9. 選擇*管理*來管理主機。

暫停時間表

暫停計劃以在主機維護期間停止備份和復原作業。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇要暫停計劃的主機。
3. 選擇*操作*  圖標，然後選擇*暫停計劃*。
4. 在確認對話方塊中，選擇*暫停*。

編輯主機

您可以變更 vCenter 伺服器資訊、主機註冊憑證和進階設定選項。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇要編輯的主機。
3. 選擇*操作*  圖標，然後選擇*編輯主機*。
4. 編輯主機資訊。
5. 選擇*完成*。

刪除主機

您可以刪除主機資訊以停止服務收費。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇要刪除的主機。
3. 選擇*操作*  圖標，然後選擇*刪除主機*。
4. 查看確認訊息並選擇*刪除*。

管理實例資訊

您可以透過以下方式管理實例訊息，分配適當的憑證來保護資源並備份資源：

- 保護實例
- 關聯憑證
- 取消關聯憑證
- 編輯保護
- 立即備份

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

保護資料庫實例

您可以使用管理資源保護計畫和保留的策略將政策指派給資料庫執行個體。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇您想要查看的工作負載並選擇*查看*。
3. 選擇“實例”標籤。
4. 選擇實例。
5. 選擇*操作*  圖標，然後選擇*保護*。
6. 選擇一個策略或建立一個新策略。

有關創建策略的詳細信息，請參閱["創建策略"](#)。

7. 提供有關您想要在備份之前和之後運行的腳本的資訊。
 - 預腳本：輸入您的腳本檔案名稱和位置，以便在觸發保護操作之前自動執行它。這有助於執行保護工作流程之前需要執行的額外任務或配置。
 - 後腳本：輸入您的腳本檔案名稱和位置，以便在保護操作完成後自動執行它。這有助於執行保護工作流程之後需要執行的附加任務或配置。
8. 提供有關如何驗證快照的資訊：
 - 儲存位置：選擇驗證快照的儲存位置。
 - 驗證資源：選擇要驗證的資源是在本機快照上還是在ONTAP二級儲存上。
 - 驗證計畫：選擇每小時、每天、每週、每月或每年的頻率。

將憑證與資源關聯

您可以將憑證與資源關聯起來，以便進行保護。

有關詳細信息，請參閱["配置NetApp Backup and Recovery設置，包括憑證"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇您想要查看的工作負載並選擇*查看*。
3. 選擇“實例”標籤。
4. 選擇實例。
5. 選擇*操作*  圖標，然後選擇*關聯憑證*。
6. 使用現有憑證或建立新憑證。

編輯保護設定

您可以變更策略、建立新策略、設定時間表和設定保留設定。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇您想要查看的工作負載並選擇*查看*。
3. 選擇“實例”標籤。
4. 選擇實例。

5. 選擇*操作*  圖標，然後選擇*編輯保護*。

有關創建策略的詳細信息，請參閱["創建策略"](#)。

立即備份

立即備份您的資料以立即保護它。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇您想要查看的工作負載並選擇*查看*。
3. 選擇“實例”標籤。
4. 選擇實例。
5. 選擇*操作*  圖標，然後選擇*立即備份*。
6. 選擇備份類型並設定計劃。

有關建立臨時備份的詳細信息，請參閱["創建策略"](#)。

管理資料庫資訊

您可以透過以下方式管理資料庫資訊：

- 保護資料庫
- 還原資料庫
- 查看保護詳細信息
- 編輯保護設定
- 立即備份

保護資料庫

您可以變更策略、建立新策略、設定時間表和設定保留設定。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇您想要查看的工作負載並選擇*查看*。
3. 選擇“資料庫”標籤。
4. 選擇資料庫。
5. 選擇*操作*  圖標，然後選擇*保護*。

有關創建策略的詳細信息，請參閱["創建策略"](#)。

還原資料庫

恢復資料庫以保護您的資料。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

1. 選擇“資料庫”標籤。
2. 選擇資料庫。
3. 選擇*操作*  圖標，然後選擇*恢復*。

有關恢復工作負載的信息，請參閱["恢復工作負載"](#)。

編輯保護設定

您可以變更策略、建立新策略、設定時間表和設定保留設定。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇您想要查看的工作負載並選擇*查看*。
3. 選擇“資料庫”標籤。
4. 選擇資料庫。
5. 選擇*操作*  圖標，然後選擇*編輯保護*。

有關創建策略的詳細信息，請參閱["創建策略"](#)。

立即備份

現在您可以備份您的 Microsoft SQL Server 執行個體和資料庫，以立即保護您的資料。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇您想要查看的工作負載並選擇*查看*。
3. 選擇“實例”或“資料庫”選項卡。
4. 選擇實例或資料庫。
5. 選擇*操作*  圖標，然後選擇*立即備份*。

使用NetApp Backup and Recovery管理 Microsoft SQL Server 快照

您可以透過從NetApp Backup and Recovery中刪除 Microsoft SQL Server 快照來管理它們。

刪除快照

您只能刪除本機快照。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)" 。

步驟

1. 在NetApp Backup and Recovery中，選擇 **Inventory** 。
2. 選擇工作負載並選擇*查看* 。
3. 選擇“資料庫”標籤。
4. 選擇要刪除快照的資料庫。
5. 從操作選單中，選擇*查看保護詳情* 。
6. 選擇要刪除的本機快照。



驗證該行*位置*列中的本機快照圖示是否顯示為藍色。

7. 選擇*操作*  圖標，然後選擇*刪除本機快照* 。
8. 在確認對話方塊中，選擇*刪除* 。

在NetApp Backup and Recovery中為 Microsoft SQL Server 工作負載建立報告

在NetApp Backup and Recovery中，建立 Microsoft SQL Server 工作負載的報告，以查看備份狀態和詳細信息，包括成功和失敗的備份計數、備份類型、儲存系統和時間戳記。

建立報告

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員、備份和還原復原管理員、備份和還原複製管理員。了解詳情"[備份和恢復角色和權限](#)"。 "[了解所有服務的NetApp Console存取角色](#)" 。

1. 從NetApp Backup and Recovery選單中，選擇 **報告** 選項。
2. 選擇*建立報告* 。
3. 輸入報告範圍詳細資料：
 - 報告名稱：輸入報告的唯一名稱。
 - 報表類型：選擇您想要按帳戶還是按工作量（Microsoft SQL Server）報表。
 - 選擇主機：如果您按工作負載選擇，請選擇要為其產生報告的主機。
 - 選擇內容：選擇報告是否包含所有備份的摘要或每個備份的詳細資訊。（如果您選擇“按帳戶”）

4. 輸入報告範圍：選擇您是否希望報告包含過去一天、過去 7 天、過去 30 天、上個季度或去年的資料。
5. 輸入報告發送詳情：如果您希望透過電子郵件發送報告，請選取*透過電子郵件發送報告*。輸入您想要接收報告的電子郵件地址。

在設定頁面配置電子郵件通知。有關配置電子郵件通知的詳細信息，請參閱["配置設定"](#)。

保護 VMware 工作負載（無需適用於 VMware 的 SnapCenter 外掛程式）

使用 NetApp Backup and Recovery 保護 VMware 工作負載概述

使用 NetApp Backup and Recovery 保護您的 VMware VM 和資料儲存。NetApp Backup and Recovery 提供快速、節省空間、崩潰一致和 VM 一致的備份和復原作業。您可以將 VMware 工作負載備份到 Amazon Web Services S3 或 StorageGRID，並將 VMware 工作負載還原至本機 VMware 主機。



此版本的 NetApp Backup and Recovery 僅支援 VMware vCenter，且無法發現 vVols 或 vVols 上的 VM。

使用 NetApp Backup and Recovery 實作 3-2-1 策略，即在 2 個不同的儲存系統上保留 3 個來源資料副本，並在雲端保留 1 個副本。3-2-1 方法的優點包括：

- 多個資料副本可防止內部和外部網路安全威脅。
- 如果一種媒體發生故障，使用不同類型的媒體可以幫助您恢復。
- 您可以從現場副本快速恢復，如果現場副本受到損害，則可以使用異地副本。



若要切換至 NetApp Backup and Recovery UI 版本或從 NetApp Backup and Recovery UI 版本切換，請參閱["切換到先前的 NetApp Backup and Recovery UI"](#)。

您可以使用 NetApp Backup and Recovery 執行與 VMware 工作負載相關的下列任務：

- ["發現 VMware 工作負載"](#)
- ["為 VMware 工作負載建立和管理保護群組"](#)
- ["備份 VMware 工作負載"](#)
- ["復原 VMware 工作負載"](#)

使用 NetApp Backup and Recovery 發現 VMware 工作負載

NetApp Backup and Recovery 服務需要先發現在 ONTAP 系統上執行的 VMware 資料儲存和虛擬機，以便您可以使用該服務。如果您已安裝 SnapCenter Plug-in for VMware vSphere 匯入備份資料和政策。

所需的控制台角色 備份和還原超級管理員。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的 NetApp Console 存取角色"](#)。

發現 VMware 工作負載並選擇性地匯入 SnapCenter 資源

在發現過程中，NetApp Backup and Recovery 會分析您組織內的 VMware 工作負載，並評估和匯入現有的保護策略、快照以及備份和復原選項。

您可以將 VMware NFS 和 VMFS 資料儲存庫和虛擬機器從其內部部署的 SnapCenter Plug-in for VMware vSphere NetApp Backup and Recovery 庫存。



此版本的 NetApp Backup and Recovery 僅支援 VMware vCenter，且無法發現 vVols 或 vVols 上的 VM。

在匯入過程中，NetApp Backup and Recovery 執行下列任務：

- 啟用對 vCenter 伺服器的安全 SSH 存取。
- 在 vCenter 伺服器中的所有資源群組上啟動維護模式。
- 準備 vCenter 的元資料並在 NetApp Console 中將其標記為不受管理。
- 配置資料庫存取。
- 發現 VMware vCenter、資料儲存區和虛擬機器。
- 從 SnapCenter Plug-in for VMware vSphere 匯入現有的保護策略、快照以及備份和復原選項。
- 顯示在 NetApp Backup and Recovery 清單頁面中發現的資源。

發現以下列方式發生：

- 如果您已經擁有 SnapCenter Plug-in for VMware vSphere，請使用 NetApp Backup and Recovery UI 將 SnapCenter 資源匯入 NetApp Backup and Recovery。



如果您已有 SnapCenter 插件，請確保在從 SnapCenter 匯入之前已滿足先決條件。例如，您應該先在 NetApp Console 中為所有本機 SnapCenter 叢集儲存體建立系統，然後再從 SnapCenter 匯入。看 ["從 SnapCenter 匯入資源的先決條件"](#)。

- 如果您還沒有 SnapCenter 插件，您仍然可以透過手動新增 vCenter 並執行發現來發現系統中的工作負載。

如果尚未安裝 SnapCenter 插件，請新增 vCenter 並發現資源

如果您尚未安裝適用於 VMware 的 SnapCenter 插件，請新增 vCenter 資訊並讓 NetApp Backup and Recovery 發現工作負載。在每個控制台代理程式中，選擇您想要發現工作負載的系統。

步驟

1. 從 NetApp Console 左側導覽中，選擇 保護 > 備份和還原。

如果您是第一次登入備份和恢復，並且在控制台中有一個系統但沒有發現任何資源，則會顯示「歡迎使用新的 NetApp 備份和恢復」頁面，其中包含「發現資源」選項。

2. 選擇*發現資源*。
3. 輸入以下資訊：
 - a. 工作負載類型：選擇*VMware*。
 - b. vCenter 設定：新增新的 vCenter。若要新增新的 vCenter，請輸入 vCenter FQDN 或 IP 位址、使用者

名稱、密碼、連接埠和協定。



如果要輸入 vCenter 訊息，請輸入 vCenter 設定和主機註冊的資訊。如果您在這裡新增或輸入了 vCenter 訊息，接下來您還需要在進階設定中新增插件資訊。

c. 主機註冊：VMware 不需要。

4. 選擇*發現*。



此過程可能需要幾分鐘。

5. 繼續高級設定。

如果已安裝**SnapCenter**插件，請將適用於 **VMware** 資源的**SnapCenter**插件匯入**NetApp Backup and Recovery**

如果您已安裝適用於 VMware 的 SnapCenter 插件，請依照下列步驟將 SnapCenter 插件資源匯入 NetApp Backup and Recovery。控制台發現 vCenter 中的 ESXi 主機、資料儲存區和虛擬機，並從插件中安排時間表；您不必重新建立所有這些資訊。

您可以透過以下方式執行此操作：

- 在發現期間，選擇一個選項從 SnapCenter 插件匯入資源。
- 發現後，從「清單」頁面中選擇一個選項來匯入 SnapCenter 插件資源。
- 發現後，從「設定」選單中選擇一個選項來匯入 SnapCenter 插件資源。有關詳細信息，請參閱["配置 NetApp Backup and Recovery"](#)。VMware 不支援此功能。

本節描述了一個由兩部分組成的過程：

1. 從 SnapCenter 插件匯入 vCenter 元資料。導入的 vCenter 資源尚未由 NetApp Backup and Recovery 管理。
2. 在 NetApp Backup and Recovery 中啟動選定 vCenter、VM 和資料儲存庫的管理。啟動管理後，NetApp Backup and Recovery 會在 Inventory 頁面上將 vCenter 標記為“Managed”，並且能夠備份並還原您匯入的資源。在 NetApp Backup and Recovery 中啟動管理後，您將不再在 SnapCenter 外掛程式中管理這些資源。

從**SnapCenter**插件匯入 **vCenter** 元數據

第一步是從 SnapCenter 插件匯入 vCenter 元資料。此時，資源尚未由 NetApp Backup and Recovery 管理。



從 SnapCenter 外掛程式匯入 vCenter 元資料後，NetApp Backup and Recovery 不會自動接手保護管理。為此，您必須明確選擇在 NetApp Backup and Recovery 中管理匯入的資源。這可確保您已準備好透過 NetApp Backup and Recovery 備份這些資源。

步驟

1. 從控制台左側導覽中，選擇*保護*>*備份和還原*。
2. 選擇*庫存*。
3. 從 NetApp Backup and Recovery Discover 工作負載資源頁面中，選擇 從**SnapCenter**匯入。
4. 在「匯入自」欄位中，選擇「* SnapCenter Plug-in for VMware*」。
5. 輸入*VMware vCenter 憑證*：

- a. **vCenter IP/主機名稱**：輸入要匯入NetApp Backup and Recovery 的vCenter 的 FQDN 或 IP 位址。
 - b. **vCenter 連接埠號碼**：輸入 vCenter 的連接埠號碼。
 - c. **vCenter 使用者名稱 和 密碼**：輸入 vCenter 的使用者名稱和密碼。
 - d. **連接器**：選擇 vCenter 的控制台代理程式。
6. 輸入 * SnapCenter插件主機憑證*：
- a. **現有憑證**：如果選擇此選項，則可以使用已新增的現有憑證。選擇憑證名稱。
 - b. **新增憑證**：如果您沒有現有的SnapCenter插件主機憑證，則可以新增憑證。輸入憑證名稱、身份驗證模式、使用者名稱和密碼。
7. 選擇“導入”來驗證您的條目並註冊SnapCenter插件。



如果SnapCenter插件已註冊，您可以更新現有的註冊詳細資訊。

結果

庫存頁面顯示 vCenter 在NetApp Backup and Recovery中處於未管理狀態，直到您明確選擇管理它。

管理從SnapCenter插件匯入的資源

從適用於 VMware 的SnapCenter外掛程式匯入 vCenter 元資料後，管理NetApp Backup and Recovery中的資源。在您選擇管理這些資源後， NetApp Backup and Recovery and Recovery能夠備份並還原您匯入的資源。在NetApp Backup and Recovery中啟動管理後，您將不再在SnapCenter外掛程式中管理這些資源。

選擇管理資源後，資源、虛擬機器和政策將從 VMware 的SnapCenter插件匯入。資源組、策略和快照從外掛程式遷移並在NetApp Backup and Recovery中進行管理。

步驟

1. 從SnapCenter外掛程式匯入 VMware 資源後，從「備份和復原」選單中選擇「Inventory」。
2. 從「庫存」頁面中，選擇您希望從現在開始由NetApp Backup and Recovery管理的匯入 vCenter。
3. 選擇“操作”圖標 ...> *查看詳情*顯示工作量詳情。
4. 在清單 > 工作負載頁面中，選擇操作圖標 ...> 管理 顯示管理 vCenter 頁面。
5. 選取「您想繼續遷移嗎？」複選框並選擇*遷移*。

結果

清單頁面顯示新管理的 vCenter 資源。

繼續存取NetApp Backup and Recovery儀表板

1. 若要顯示儀表板，請從「備份與還原」功能表中選擇「儀表板」。
2. 檢討資料保護的健康狀況。處於危險中或受保護的工作負載的數量會根據新發現、受保護和備份的工作負載而增加。

["了解儀表板顯示的內容"](#)。

使用NetApp Backup and Recovery為 VMware 工作負載建立和管理保護群組

建立保護組來管理一組工作負載的備份和還原作業。保護群組是您想要一起保護的資源（例如虛擬機器和資料儲存區）的邏輯分組。

您可以執行與保護群組相關的以下任務：

- 建立保護組。
- 查看保護詳情。
- 立即備份保護組。看["立即備份 VMware 工作負載"](#)。
- 暫停和恢復保護組的備份計畫。
- 刪除保護組。

建立保護組

將您想要保護的工作負載分組到保護群組中，以便一起備份和還原它們。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標  > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇*建立保護組*。
6. 為保護組提供名稱。
7. 選擇要包含在保護群組中的虛擬機器或資料庫。
8. 選擇“下一步”。
9. 選擇要套用於保護群組的*備份策略*。

如果要建立策略，請選擇*建立新策略*並依照指示建立策略。看["創建策略"](#)了解更多。

10. 選擇“下一步”。
11. 檢查配置。
12. 選擇“建立”來建立保護組。

暫停保護組的備份計畫

暫停保護組以暫停其計畫的備份。

當您暫停保護群組時，保護狀態將變更為「維護中」。您可以隨時還原備份計畫。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ...> 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇“操作”圖標 ...> 暫停保護組。
6. 查看確認訊息並選擇*暫停*。

恢復保護組的備份計劃

復原已暫停的保護群組將重新啟動該保護群組的計畫備份。

當您暫停保護群組時，保護狀態將從「維護中」變更為當您恢復保護群組時「受保護」。您可以隨時還原備份計畫。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ...> 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇“操作”圖標 ...> 恢復保護群組。
6. 查看確認訊息並選擇*恢復*。

結果

如果計畫有效，系統將驗證計畫，並將保護狀態變更為「已保護」。如果計畫無效，系統將顯示錯誤訊息並且不會恢復保護群組。

刪除保護群組

刪除保護群組時，也會刪除該群組以及該群組的所有備份計畫。如果不再需要某個保護群組，請將其刪除。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ...> 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇要刪除的保護組。
6. 選擇“操作”圖標 ...> 刪除。
7. 查看有關刪除相關備份的確認訊息並確認刪除。

使用NetApp Backup and RecoveryVMware 工作負載

將 VMware VM 和資料儲存區從本機ONTAP系統備份到 Amazon Web Services、Azure

NetApp Files或StorageGRID，以確保您的資料受到保護。備份會自動產生並儲存在您的公有或私有雲帳戶的物件儲存中。

- 若要安排程備份工作負載，請建立管理備份和還原作業的策略。看["創建策略"](#)以取得說明。
- 建立保護組來管理一組資源的備份和還原作業。看["使用NetApp Backup and Recovery為 VMware 工作負載建立和管理保護群組"](#)了解更多。
- 立即備份工作負載（立即建立按需備份）。

立即使用按需備份來備份工作負載

立即建立按需備份。如果您要對系統進行變更並希望確保在開始之前有備份，則可能需要執行按需備份。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員或備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從備份和還原選單中，選擇*庫存*。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標  > 查看詳情。
4. 選擇「保護群組」、「資料儲存」或「虛擬機器」標籤。
5. 選擇要備份的保護群組、資料儲存區或虛擬機器。
6. 選擇“操作”圖標  > 立即備份。



應用於備份的策略與指派給保護群組、資料儲存區或虛擬機器的策略相同。

7. 選擇計劃層級。
8. 選擇*立即備份*。

復原 VMware 工作負載

使用**NetApp Backup and Recovery**VMware 工作負載

使用NetApp Backup and Recovery從快照、複製到輔助儲存的工作負載備份或儲存在物件儲存中的備份還原 VMware 工作負載。

從這些位置恢復

您可以從不同的起始位置恢復工作負載：

- 從主位置還原（本地快照）
- 從二級儲存上的複製資源恢復
- 從物件儲存備份還原

恢復到這些點

您可以將資料還原到以下點：

- 恢復到原始位置：虛擬機器將恢復到原始位置，即相同的 vCenter 部署、ESXi 主機和資料儲存。虛擬機器及其所有資料均被覆蓋。
- 恢復到備用位置：您可以選擇不同的 vCenter、ESXi 主機或資料儲存作為虛擬機器的復原目標。這對於管理位於不同位置和狀態的相同虛擬機器的不同副本非常有用。

從物件儲存中復原的注意事項

如果為物件儲存中的備份檔案啟用了勒索軟體復原功能，則要求您在復原之前執行額外的檢查。我們建議進行掃描。

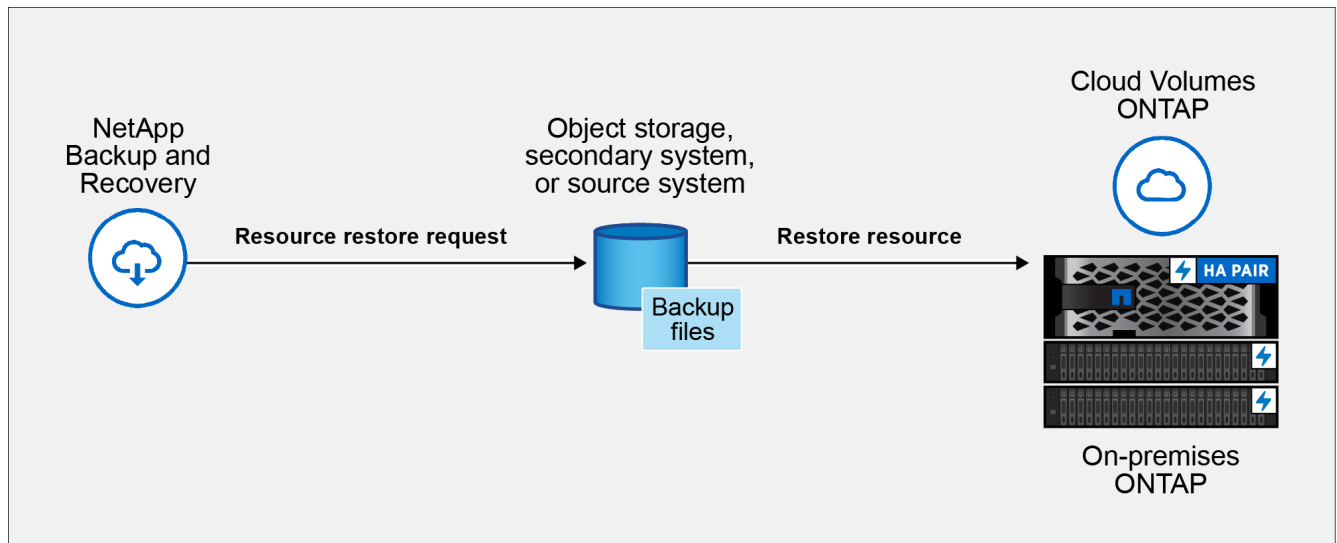


您可能需要向雲端提供者支付額外費用才能存取備份檔案。

恢復工作負載的工作原理

恢復工作負載時，會發生以下情況：

- 當您從本機快照或遠端備份還原工作負載時，如果您還原到原始位置，NetApp Backup and Recovery會覆寫原始虛擬機器；如果您還原到備用位置，則會建立新的資源。
- 從複製的工作負載復原時，您可以將工作負載還原到原始的本機ONTAP系統，也可以還原到不同的本機ONTAP系統。



- 從物件儲存還原備份時，您可以將資料還原到原始系統或本機ONTAP系統。

在「恢復」頁面（搜尋和恢復）中，您可以透過使用篩選器搜尋快照來恢復資源，即使您不記得其確切名稱、位置或最後已知日期。

從恢復選項恢復工作負載資料（搜尋和恢復）

使用復原選項還原 VMware 工作負載。您可以按名稱或使用篩選器來搜尋快照。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原復原管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 復原。

2. 從名稱搜尋欄位右側的下拉清單中，選擇 **VMware**。
3. 輸入要還原的資源的名稱，或篩選要還原的資源所在的 vCenter、資料中心或資料儲存。

將顯示符合您搜尋條件的虛擬機器清單。

4. 在清單中找到要從中復原的虛擬機，然後選擇該虛擬機的選項選單按鈕。
5. 在出現的選單中，選擇“恢復虛擬機器”。

顯示在該虛擬機器上建立的快照（還原點）清單。預設情況下，會顯示您在「時間範圍」下拉式選單中選擇的時間範圍內的最新快照。

對於每個快照，*位置*列中任何亮起的圖示都表示快照可用的儲存位置（主儲存、輔助儲存或物件儲存）。

6. 啟用要還原的快照對應的單選按鈕。
7. 選擇“下一步”。

顯示快照位置選項。

8. 選擇快照的還原目標位置：
 - 本地：從本機位置還原快照。
 - 輔助：從遠端儲存位置還原快照。
 - 物件儲存：從物件儲存恢復快照。

如果選擇輔助存儲，請從下拉清單中選擇目標位置。

9. 選擇“下一步”繼續。
10. 選擇恢復目標位置和設定：

目的地選擇

恢復到原始位置

還原到原始位置時，您無法變更目標 vCenter、ESXi 主機、資料儲存或虛擬機器的名稱。復原操作會覆蓋原始虛擬機器。

1. 選擇「原始位置」窗格。
2. 請從以下選項中選擇：
 - *恢復前選項*部分：
 - 預設腳本：啟用此選項可在復原作業開始前執行自訂腳本，以自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
 - *恢復後選項*部分：
 - 重新啟動虛擬機器：啟用此選項可在復原作業完成後以及套用復原後腳本後重新啟動虛擬機器。
 - 附註：啟用此選項可在復原完成後執行自訂腳本，從而自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
3. 選擇*恢復*。

恢復至備用位置

當您還原為備用位置時，您可以變更目標 vCenter、ESXi 主機、資料儲存和虛擬機器名稱，以便在不同的位置或使用不同的名稱建立虛擬機器的新副本。

1. 選擇「備用位置」窗格。
2. 輸入以下資訊：
 - *目的地設定*部分：
 - **vCenter FQDN 或 IP 位址**：選擇要還原快照的 vCenter 伺服器。
 - **ESXi 主機**：選擇要將快照還原到的主機。
 - **網路**：選擇要將快照還原到的網路。
 - **資料儲存**：從下拉清單中，選擇要將快照還原到的資料儲存體的名稱。
 - **虛擬機器名稱**：輸入要將快照還原到的虛擬機器的名稱。如果名稱與資料儲存中已存在的虛擬機器匹配，備份和復原功能會透過附加目前時間戳來使名稱唯一。
 - *恢復前選項*部分：
 - 預設腳本：啟用此選項可在復原作業開始前執行自訂腳本，以自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
 - *恢復後選項*部分：
 - 重新啟動虛擬機器：啟用此選項可在復原作業完成後以及套用復原後腳本後重新啟動虛擬機器。
 - 附註：啟用此選項可在復原完成後執行自訂腳本，從而自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
3. 選擇*恢復*。

您可以從傳統虛擬機器的主備份或輔助備份中還原現有的虛擬磁碟 (VMDK)，或已刪除或已分離的虛擬磁碟。這樣，您就可以只恢復特定的虛擬機器資料或應用程式，而無需在僅影響特定資料的情況下恢復整個虛擬機器及其所有關聯的虛擬磁碟。虛擬磁碟復原後，會附加到其原始虛擬機，即可使用。

您可以將虛擬機器上的一個或多個虛擬機器磁碟 (VMDK) 還原到相同資料儲存或不同的資料儲存體。



為了提高 NFS 環境中復原作業的效能，請啟用 VMware 應用程式 vStorage API for Array Integration (VAAI)。

開始之前

- 必須存在備份。
- VM 不得處於傳輸狀態。

您要復原的虛擬機器不能處於 vMotion 或 Storage vMotion 狀態。

關於此任務

- 如果 VMDK 被刪除或從 VM 中分離，則還原操作會將 VMDK 附加到 VM。
- 如果虛擬機器所在的FabricPool的儲存層不可用，則復原操作可能會失敗。
- 連接和恢復操作使用預設的 SCSI 控制器連接 VMDK。但是，當備份連接到具有 NVMe 磁碟的 VM 的 VMDK 時，連接和復原作業將使用 NVMe 控制器（如果可用）。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 復原。
2. 從名稱搜尋欄位右側的下拉清單中，選擇 **VMware**。
3. 輸入要還原的資源的名稱，或篩選要還原的資源所在的 vCenter、資料中心或資料儲存。

將顯示符合您搜尋條件的虛擬機器清單。

4. 在清單中找到要從中復原的虛擬機，然後選擇該虛擬機的選項選單按鈕。
5. 在出現的選單中，選擇「恢復虛擬磁碟」。

顯示在該虛擬機器上建立的快照（還原點）清單。預設情況下，會顯示您在「時間範圍」下拉式選單中選擇的時間範圍內的最新快照。

對於每個快照，*位置*列中任何亮起的圖示都表示快照可用的儲存位置（主儲存、輔助儲存或物件儲存）。

6. 啟用要還原的快照對應的單選按鈕。
7. 選擇“下一步”。

顯示快照位置選項。

8. 選擇快照的還原目標位置：
 - 本地：從本機位置還原快照。

- 輔助：從遠端儲存位置還原快照。
- 物件儲存：從物件儲存恢復快照。

如果選擇輔助存儲，請從下拉清單中選擇目標位置。

9. 選擇“下一步”繼續。
10. 選擇恢復目標位置和設定：

目的地選擇

恢復到原始位置

還原到原始位置時，您無法變更目標 vCenter、ESXi 主機、資料儲存或虛擬磁碟的名稱。原虛擬磁碟被覆蓋。

1. 選擇「原始位置」窗格。
2. 在「目標設定」部分，選取要還原的任何虛擬磁碟的核取方塊。
3. 請從以下選項中選擇：
 - *恢復前選項*部分：
 - 預設腳本：啟用此選項可在復原作業開始前執行自訂腳本，以自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
 - *恢復後選項*部分：
 - 附註：啟用此選項可在復原完成後執行自訂腳本，從而自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
4. 選擇*恢復*。

恢復至備用位置

當恢復到備用位置時，您可以變更目標資料儲存。無論您選擇哪個資料存儲，恢復作業後虛擬磁碟都會附加到原始虛擬機器。

1. 選擇「備用位置」窗格。
2. 在「目標設定」部分，選取要還原的任何虛擬磁碟的核取方塊。
3. 對於您選擇的任何虛擬磁碟：
 - a. 選擇「選擇資料儲存」可為虛擬磁碟選擇不同的資料儲存還原目標。
 - b. 選擇“選擇”以確認您的選擇並關閉選擇視窗。
4. 請從以下選項中選擇：
 - *恢復前選項*部分：
 - 預設腳本：啟用此選項可在復原作業開始前執行自訂腳本，以自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
 - *恢復後選項*部分：
 - 附註：啟用此選項可在復原完成後執行自訂腳本，從而自動執行其他任務。請輸入要執行的腳本的完整路徑以及腳本接受的所有參數。
5. 選擇*恢復*。

恢復訪客檔案和資料夾

恢復訪客文件和資料夾的要求和限制

您可以從 Windows 用戶作業系統上的虛擬機器磁碟 (VMDK) 還原檔案或資料夾。

來賓還原工作流程

客戶作業系統還原操作包含以下步驟：

1. 附

將虛擬磁碟附加到客戶虛擬機器並啟動客戶文件復原工作階段。

2. 等待

請等待附加操作完成，然後才能瀏覽和恢復。附加操作完成後，會自動建立訪客文件恢復工作階段。

3. 選擇檔案或資料夾

瀏覽 VMDK 文件，選擇一個或多個文件或資料夾進行還原。

4. 恢復

將選定的檔案或資料夾還原到指定位置。

恢復訪客文件和資料夾的先決條件

在 Windows 用戶作業系統上從 VMDK 還原檔案或資料夾之前，請檢查所有要求。

- 必須安裝並執行 VMware 工具。

NetApp Backup and Recovery 使用 VMware 工具的資訊來建立與 VMware 客戶作業系統的連線。

- Windows 客戶作業系統必須執行 Windows Server 2008 R2 或更高版本。

有關受支援版本的最新信息，請參閱 "[NetApp 互通性矩陣工具 \(IMT\)](#)"。

- 目標虛擬機器的憑證使用使用者名稱「Administrator」的內建網域或本機管理員帳號。在開始復原作業之前，請先設定要附加虛擬磁碟的虛擬機器的憑證。附加和恢復操作都需要憑證。工作群組使用者可以使用內建的本機管理員帳戶。



如果您必須使用非內建管理員帳戶但在 VM 內具有管理權限的帳戶，則必須在來賓 VM 上停用 UAC。

- 您必須知道要從中還原的備份快照和 VMDK。

NetApp Backup and Recovery 不支援搜尋檔案或資料夾進行還原。在開始之前，您必須知道快照中的檔案或資料夾以及對應的 VMDK 的位置。

- 要附加的虛擬磁碟必須位於 NetApp Backup and Recovery 備份中。

包含要還原的檔案或資料夾的虛擬磁碟必須位於使用 NetApp Backup and Recovery 執行的 VM 備份中。

- 對於名稱非英文字母的文件，您必須將它們恢復到目錄中，而不是單一文件。

您可以透過恢復文件所在的目錄來恢復具有非字母名稱的文件，例如日語漢字。

來賓檔案還原限制

在從客戶作業系統還原檔案或資料夾之前，您應該了解其功能限制。

- 您無法在來賓作業系統內還原動態磁碟類型。
- 如果還原加密的檔案或資料夾，則不會保留加密屬性。
- 您無法將檔案或資料夾還原到加密資料夾。
- 隱藏的文件和資料夾會顯示在文件瀏覽頁面中，但您無法對其進行篩選。
- 您無法從 Linux 客戶作業系統復原。

您無法從執行 Linux 客戶作業系統的 VM 還原檔案和資料夾。但是，您可以附加 VMDK，然後手動恢復檔案和資料夾。有關受支援的客戶作業系統的最新信息，請參閱 "[NetApp 互通性矩陣工具 \(IMT\)](#)"。

- 您無法從 NTFS 檔案系統還原到 FAT 檔案系統。

當您嘗試從 NTFS 格式還原為 FAT 格式時，不會複製 NTFS 安全性描述符，因為 FAT 檔案系統不支援 Windows 安全性屬性。

- 您無法從克隆的 VMDK 或未初始化的 VMDK 恢復客戶檔案。
- 您無法復原檔案的目錄結構。

從嵌套目錄恢復檔案時，系統只會恢復檔案本身，而不會恢復其目錄結構。若要復原整個目錄樹，請複製頂層目錄。

- 您無法將客戶檔案從 vVol VM 還原到備用主機。
- 您無法恢復加密的訪客檔案。

從 VMDK 還原客戶機檔案和資料夾

您可以從 Windows 用戶作業系統上的 VMDK 還原一個或多個檔案或資料夾。

開始之前

在從 NetApp Backup and Recovery 中還原檔案和資料夾之前，您需要為來賓虛擬機器建立憑證。NetApp Backup and Recovery 使用這些憑證在附加虛擬磁碟時對來賓虛擬機器進行驗證。

關於此任務

來賓檔案或資料夾恢復效能取決於兩個因素：正在復原的檔案或資料夾的大小；以及正在復原的檔案或資料夾的數量。如果要恢復的資料集大小相同，則恢復大量小檔案可能比恢復少量大檔案花費的時間比預期的要長。



一台虛擬機器上同時只能執行一個連線或還原操作。您無法在同一台虛擬機器上執行並行連線或復原操作。



透過訪客恢復功能，您可以查看和恢復系統文件和隱藏文件，以及查看加密文件。請勿覆蓋現有系統檔案或將加密檔案還原到加密資料夾。在復原作業期間，訪客檔案的隱藏屬性、系統屬性和加密屬性不會保留在復原的檔案中。查看或瀏覽保留分割區可能會導致錯誤。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇“虛擬機器”選單。
3. 從清單中選擇包含要復原的檔案的虛擬機器。
4. 選擇“操作”圖標  針對該虛擬機器。
5. 選擇“恢復檔案和資料夾”。
6. 選擇要從中復原的快照，然後選擇「下一步」。
7. 選擇要從中復原的快照位置。如果選擇輔助位置，請從清單中選擇輔助快照。
8. 選擇“下一步”。
9. 從清單中選擇要附加到虛擬機器的虛擬磁碟，然後選擇「下一步」。
10. 在「選擇虛擬機器憑證」頁面上，如果您尚未儲存客戶虛擬機器的憑證，請選擇「新增憑證」並執行下列操作：
 - a. 憑證名稱：輸入憑證的名稱。
 - b. 身份驗證模式：選擇 **Windows**。
 - c. 代理：從清單中選擇一個控制台代理，該代理將處理NetApp Backup and Recovery與此主機之間的通訊。
 - d. 網域和使用者名稱：輸入憑證的 NetBIOS 或網域 FQDN 和使用者名稱。
 - e. 密碼：請輸入憑證的密碼。
 - f. 選擇“新增”。
11. 選擇用於向客戶虛擬機器進行身份驗證的虛擬機器憑證。

NetApp Backup and Recovery將虛擬磁碟附加到虛擬機，並顯示所有檔案和資料夾，包括隱藏的檔案和資料夾。它會為每個分割區（包括系統保留分割區）分配一個磁碟機號碼。

您選擇的檔案和資料夾會列在螢幕右側窗格中。

12. 選擇“下一步”。
13. 輸入將復原所選檔案的來賓的 UNC 共用路徑。
 - IPv4 位址範例： \\10.60.136.65\c\$
 - IPv6位址範例： \\fd20-8b1e-b255-832e-61.ipv6-literal.net\C\restore

如果存在同名文件，您可以選擇覆蓋或跳過它們。

14. 選擇*恢復*。

您可以在「作業監控」頁面上查看恢復進度。

訪客文件恢復故障排除

嘗試恢復訪客文件時，您可能會遇到以下任一情況。

來賓文件恢復會話為空白

如果在建立用戶機檔案復原工作階段期間用戶機作業系統重啟，則會發生此問題。客戶作業系統中的 VMDK 可能處於離線狀態，因此客戶文件復原會話清單為空。

若要解決此問題，請在客戶作業系統中手動將 VMDK 重新置於連線狀態。當 VMDK 線上時，來賓文件恢復工作階段將顯示正確的內容。

來賓檔案恢復附加磁碟操作失敗

當您啟動用戶機檔案還原作業時會出現此問題，但即使 VMware 工具正在運作且用戶端作業系統憑證正確，連線磁碟操作也會失敗。如果發生這種情況，則會傳回下列錯誤：

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

若要解決此問題，請在用戶端作業系統上重新啟動 VMware Tools Windows 服務，然後重試用戶端檔案還原作業。

來賓檔案復原會話停止後，備份不會分離

當您從 VM 一致性備份執行來賓檔案還原作業時會發生此問題。當來賓檔案還原工作階段處於活動狀態時，將對相同 VM 執行另一個 VM 一致性備份。當客戶文件恢復會話斷開時（手動或 24 小時後自動斷開），該會話的備份不會被分離。

若要解決此問題，請手動分離從活動來賓檔案還原工作階段附加的 VMDK。

保護 KVM 工作負載（預覽版）

保護 KVM 工作負載概述

使用 NetApp Backup and Recovery 保護您的託管 KVM 虛擬機器和儲存池。NetApp Backup and Recovery 提供快速、節省空間、崩潰一致性和 VM 一致性的備份和復原作業。在使用備份和復原功能保護 KVM 主機和虛擬機器之前，必須先使用 Apache CloudStack 等管理平台來管理它們。

您可以將 KVM 工作負載備份到 Amazon Web Services S3、Azure NetApp Files 或 StorageGRID，並將 KVM 工作負載還原到本機 KVM 主機。

使用 NetApp Backup and Recovery 實作 3-2-1 保護策略，其中您在 2 個不同的儲存系統上擁有 3 個來源資料副本，並在雲端中擁有 1 個副本。3-2-1 方法的優點包括：

- 多個資料副本可防止內部和外部網路安全威脅。
- 如果一種媒體發生故障，使用不同類型的媒體可以幫助您恢復。
- 您可以從現場副本快速恢復，如果現場副本受到損害，則可以使用異地副本。



若要切換至NetApp Backup and Recovery UI 版本或從 NetApp Backup and Recovery UI 版本切換，請參閱["切換到先前的NetApp Backup and RecoveryUI"](#)。

您可以使用NetApp Backup and Recovery執行與 KVM 工作負載相關的下列任務：

- ["發現 KVM 工作負載"](#)
- ["為 KVM 工作負載建立和管理保護群組"](#)
- ["備份 KVM 工作負載"](#)
- ["恢復 KVM 工作負載"](#)

發現NetApp Backup and Recovery中的 KVM 工作負載

NetApp Backup and Recovery需要先發現 KVM 主機和虛擬機，然後才能對其進行保護。必須先使用 Apache CloudStack 等管理平台管理您的 KVM 主機和虛擬機，然後才能將其新增至備份和復原。

所需的控制台角色 備份和還原超級管理員。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

新增管理平台、KVM 主機並發現資源

新增管理平台和 KVM 主機訊息，讓NetApp Backup and Recovery發現工作負載。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 在“工作負載”下，選擇“KVM”磁貼。

如果您是第一次登入備份和恢復，並且在控制台中有一個系統但沒有發現任何資源，則會顯示「歡迎使用新的NetApp備份和恢復」頁面，其中包含「發現資源」選項。

3. 選擇*發現資源*。
4. 輸入以下資訊：
 - a. 工作負載類型：選擇*KVM*。
 - b. 如果您尚未將管理平台與備份和復原功能集成，請選擇「新增管理平台」。
 - i. 輸入以下資訊：
 - 管理平台 IP 位址或 FQDN：輸入管理平台的 IP 位址或完全限定網域名稱。
 - API金鑰：輸入用於驗證API請求的API金鑰。
 - 金鑰：輸入用於驗證 API 請求的金鑰。
 - 連接埠：輸入備份和還原與管理平台之間通訊所使用的連接埠。
 - 代理：選擇一個控制台代理，用於促進備份和還原與管理平台之間的通訊。
 - ii. 完成後，選擇“新增”。
 - c. KVM 設定：透過輸入下列資訊新增新的 KVM 主機：

- **KVM FQDN 或 IP 位址**：輸入主機的 FQDN 或 IP 位址。
- **憑證**：輸入 KVM 主機的使用者名稱和密碼。
- **控制台代理**：選擇用於備份和還原與 KVM 主機之間通訊的控制台代理程式。
- **連接埠號碼**：輸入備份和復原與 KVM 主機之間通訊所使用的連接埠。
- **管理平台**：如果 KVM 主機是受管理的，並且您已將管理平台新增至備份和復原中，請從清單中選擇管理平台。

5. 選擇*發現*。



此過程可能需要幾分鐘。

結果

KVM 工作負載顯示在「庫存」頁面的工作負載清單中。

繼續存取NetApp Backup and Recovery儀表板

步驟

1. 從NetApp Console選單中，選擇 保護 > 備份和還原。
2. 選擇一個工作負載圖塊（例如，Microsoft SQL Server）。
3. 從備份和還原選單中，選擇*儀表板*。
4. 檢討資料保護的健康狀況。處於危險中或受保護的工作負載的數量會根據新發現、受保護和備份的工作負載而增加。

使用NetApp Backup and Recovery為 KVM 工作負載建立和管理保護群組

建立保護組來管理一組 KVM 資源的備份作業。保護群組是您想要一起保護的資源（例如虛擬機器和儲存池）的邏輯分組。您需要建立一個保護群組來備份KVM虛擬機器或儲存池。

您可以執行與保護群組相關的以下任務：

- 建立保護組。
- 查看保護詳情。
- 立即備份保護組。看"[立即備份 KVM 工作負載](#)"。
- 刪除保護組。

建立保護組

將您想要保護的虛擬機器和儲存池分組到保護群組中。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇*建立保護組*。
6. 為保護組提供名稱。
7. 選擇要包含在保護群組中的虛擬機器或儲存池。
8. 選擇“下一步”。
9. 選擇要套用於保護群組的*備份策略*。

有關建立備份策略的更多信息，請參閱["建立和管理策略"](#)。

10. 選擇“下一步”。
11. 檢查配置。
12. 選擇“建立”來建立保護組。

刪除保護群組

刪除保護群組會刪除該保護群組以及所有相關的備份計畫。如果不再需要某個保護群組，您可能需要將其刪除。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇要刪除的保護組。
6. 選擇“操作”圖標 ... > 刪除。
7. 查看有關刪除相關備份的確認訊息並確認刪除。

使用NetApp Backup and Recovery KVM 工作負載

將 KVM 保護群組從本機ONTAP系統備份至 Amazon Web Services、Azure NetApp Files 或StorageGRID，以確保您的資料受到保護。備份保護群組時，NetApp Console會備份該保護群組中包含的虛擬機器和儲存池。備份會自動產生並儲存在您的公有或私有雲帳戶的物件儲存中。



若要安排程備份保護群組，請建立管理備份和還原作業的政策。看["創建策略"](#)以取得說明。

- 建立保護組來管理一組資源的備份和還原作業。看["使用NetApp Backup and Recovery為 KVM 工作負載建立和管理保護群組"](#)了解更多。

立即使用按需備份來備份保護群組

您可以立即執行按需備份。如果您要對系統進行更改並希望確保在開始之前有備份，這將很有幫助。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。"[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 在 KVM 圖塊中，選擇 發現和管理。
3. 選擇*庫存*。
4. 選擇一個工作負載來查看保護詳細資訊。
5. 選擇“操作”圖標  > 查看詳情。
6. 選擇「保護群組」、「資料儲存」或「虛擬機器」標籤。
7. 選擇要備份的保護組。
8. 選擇“操作”圖標  > 立即備份。



應用於備份的策略與指派給保護組的策略相同。

9. 選擇計劃層級。
10. 選擇*備份*。

使用NetApp Backup and Recovery和還原還原 KVM 虛擬機

使用NetApp Backup and Recovery從快照、複製到輔助儲存的保護群組備份或儲存在物件儲存中的備份還原 KVM 虛擬機器。

從這些位置恢復

您可以從不同的起始位置還原虛擬機器：

- 從主位置還原（本地快照）
- 從二級儲存上的複製資源恢復
- 從物件儲存備份還原

恢復到這些點

您可以將資料還原到以下點：

- 恢復到原始位置

從物件儲存中復原的注意事項

如果您選擇物件儲存中的備份文件，且該備份的勒索軟體保護處於活動狀態（如果您在備份策略中啟用了DataLock 和勒索軟體復原），系統會提示您在復原資料之前對備份檔案執行額外的完整性檢查。我們建議您執行掃描。



您將需要向雲端提供者支付額外的出口費用才能存取備份文件的內容。

虛擬機器復原的工作原理

還原虛擬機器時，會發生以下情況：

- 當您從本機備份檔案還原工作負載時，NetApp Backup and Recovery and Recovery會使用備份中的資料建立一個_新_資源。
- 從複製的虛擬機器還原時，您可以將其還原到原始系統或本機ONTAP系統。
- 從物件儲存還原備份時，您可以將資料還原到原始系統或本機ONTAP系統。

從「還原」頁面（也稱為「搜尋和還原」），您可以還原虛擬機，即使您不記得確切的名稱、虛擬機所在的位置或虛擬機上次處於良好狀態的日期。您可以使用過濾器搜尋快照。

從恢復選項恢復虛擬機器（搜尋和恢復）

使用復原選項還原 KVM 虛擬機器。您可以按名稱或使用篩選器來搜尋快照。

所需的控制台角色 備份和還原超級管理員或備份和還原復原管理員角色。"[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 從NetApp Backup and Recovery選單中，選擇 復原。
3. 從名稱搜尋欄位右側的下拉清單中，選擇 **KVM**。
4. 輸入要還原的 VM 的名稱或篩選要還原的資源所在的 VM 主機或儲存池。

出現符合您的搜尋條件的快照清單。

5. 選擇要還原的快照的“恢復”按鈕。

出現可能的還原點清單。

6. 選擇您想要使用的還原點。
7. 選擇快照來源位置。
8. 選擇“下一步”繼續。
9. 選擇恢復目標位置和設定：

目的地選擇

恢復到原始位置

1. 啟用快速復原：選擇此選項可執行快速復原作業。恢復的捲和資料將立即可用。請勿在需要高效能的磁碟區上使用此功能，因為在快速復原過程中，存取資料的速度可能會比平常慢。
2. 預先恢復選項：輸入應在復原作業之前執行的腳本的完整路徑以及該腳本所採用的任何參數。
3. 恢復後選項：
 - 重新啟動 **VM**：選擇此選項可在還原作業完成後以及套用還原後腳本後重新啟動 VM。
 - 後記：輸入恢復操作後應執行的腳本的完整路徑以及腳本所採用的任何參數。
4. *通知*部分：
 - 啟用電子郵件通知：選擇此選項可接收有關復原作業的電子郵件通知，並指示您想要接收的通知類型。
5. 選擇*恢復*。

恢復至備用位置

不適用於 KVM 工作負載預覽版。

保護 Hyper-V 工作負載

保護 Hyper-V 工作負載概述

使用 NetApp Backup and Recovery 保護您的 Hyper-V 虛擬機器。NetApp Backup and Recovery。您也可以保護由 System Center Virtual Machine Manager (SCVMM) 配置並託管在 CIFS 共用上的 Hyper-V 虛擬機器。

您可以將 Hyper-V 工作負載備份到 Amazon Web Services S3 或 StorageGRID，並將 Hyper-V 工作負載還原為本機 Hyper-V 主機。

使用 NetApp Backup and Recovery 實作 3-2-1 保護策略，其中您在 2 個不同的儲存系統上擁有 3 個來源資料副本，並在雲端中擁有 1 個副本。3-2-1 方法的優點包括：

- 多個資料副本可防止內部和外部網路安全威脅。
- 多種媒體類型可確保在一種媒體類型發生實體或邏輯故障時能夠進行故障轉移。
- 現場副本可幫助您快速恢復數據，如果現場副本受到損害，您可以使用異地副本。

當您新增 Hyper-V 主機並發現資源時，NetApp Backup and Recovery 會在 Hyper-V 主機上安裝 NetApp Hyper-V 插件和 NetApp SnapCenter Windows File System 插件，以協助管理和保護虛擬機器。



若要切換至 NetApp Backup and Recovery UI 版本或從 NetApp Backup and Recovery UI 版本切換，請參閱["切換到先前的 NetApp Backup and Recovery UI"](#)。

您可以使用 NetApp Backup and Recovery 執行與 Hyper-V 工作負載相關的下列任務：

- ["發現 Hyper-V 工作負載"](#)
- ["為 Hyper-V 工作負載建立和管理保護群組"](#)

- "備份 Hyper-V 工作負載"
- "復原 Hyper-V 工作負載"

在NetApp Backup and Recovery中發現 Hyper-V 工作負載

NetApp Backup and Recovery必須先發現 Hyper-V 虛擬機，然後您才能保護它們。

所需的控制台角色 備份和還原超級管理員。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

新增 Hyper-V 主機並發現資源

新增 Hyper-V 主機資訊並讓NetApp Backup and Recovery發現虛擬機器。在每個控制台代理程式中，選擇您想要發現資源的系統。



當您新增 Hyper-V 主機並發現資源時，NetApp Backup and Recovery會在 Hyper-V 主機上安裝NetApp Hyper-V 插件和NetApp SnapCenter Windows FileSystem 插件，以協助管理和保護虛擬機器。

步驟

1. 從NetApp Console選單中，選擇 保護 > 備份和還原。

如果這是您第一次登入NetApp Backup and Recovery，且控制台中已經有系統，但尚未發現任何資源，則會出現「歡迎使用新的NetApp Backup and Recovery」登入頁面並顯示「發現資源」選項。

2. 選擇*發現資源*。
3. 輸入以下資訊：
 - a. 工作負載類型：選擇*Hyper-V*。
 - b. 如果您尚未儲存此 Hyper-V 主機的憑證，請選擇「新增憑證」。
 - i. 選擇與該主機一起使用的控制台代理程式。
 - ii. 輸入此憑證的名稱。
 - iii. 輸入該帳戶的使用者名稱和密碼。
 - iv. 選擇*完成*。
 - c. 主機註冊：透過輸入主機的 FQDN 或 IP 位址、憑證、控制台代理程式和連接埠號碼來新增新的 Hyper-V 主機。如果控制台代理無法解析 FQDN，則改用 IP 位址。對於 FCI 集群，請輸入 FCI 集群管理 IP 位址。
4. 選擇*發現*。



此過程可能需要幾分鐘。

結果

NetApp Backup and Recovery發現資源後，「清單」頁面會在工作負載清單中顯示 Hyper-V 工作負載。

繼續存取NetApp Backup and Recovery儀表板

步驟

1. 從NetApp Console選單中，選擇 保護 > 備份和還原。
2. 選擇一個工作負載圖塊（例如，Microsoft SQL Server）。
3. 從備份和還原選單中，選擇*儀表板*。
4. 檢討資料保護的健康狀況。處於危險中或受保護的工作負載的數量會根據新發現、受保護和備份的工作負載而增加。

使用NetApp Backup and Recovery為 Hyper-V 工作負載建立和管理保護群組

建立保護群組來管理一組虛擬機器的備份作業。保護群組是您想要一起保護的資源（例如虛擬機器）的邏輯分組。

您可以執行與保護群組相關的以下任務：

- 建立保護組。
- 查看保護詳情。
- 立即備份保護組。看["立即備份 Hyper-V 工作負載"](#)。
- 刪除保護組。

建立保護組

將您想要保護的工作負載分組到一個保護群組。建立保護組來一起備份和還原工作負載。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 **...** > 查看詳情。
4. 選擇“保護組”選單。
5. 選擇*建立保護組*。
6. 為保護組提供名稱。
7. 選擇要包含在保護群組中的虛擬機器。
8. 選擇“下一步”。
9. 選擇要套用於保護群組的*備份策略*。
10. 選擇“下一步”。
11. 檢查配置。
12. 選擇“建立”來建立保護組。

編輯保護群組

編輯保護群組以變更其名稱或設定。如果保護群組中的資源發生了變化，您可能需要編輯該保護群組。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇要編輯的保護群組。
6. 選擇“操作”圖標 ... > 編輯。
7. 變更保護群組的任何設置，例如名稱或群組中的虛擬機器。
8. 選擇“下一步”。
9. 必要時更改保護策略。完成後，選擇“下一步”。
10. 檢查配置並選擇“提交”。

刪除保護群組

刪除保護群組會刪除該保護群組以及所有相關的備份計畫。如果不再需要某個保護群組，您可能需要將其刪除。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 ... > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇要刪除的保護組。
6. 選擇“操作”圖標 ... > 刪除。
7. 查看有關刪除相關備份的確認訊息並確認刪除。

使用NetApp Backup and RecoveryHyper-V 工作負載

將 Hyper-V VM 從本機ONTAP系統備份到 Amazon Web Services、Azure NetApp Files 或StorageGRID，以確保您的資料受到保護。備份會自動產生並儲存在您的公有或私有雲帳戶的物件儲存中。

- 若要安排程備份工作負載，請建立管理備份和還原作業的策略。看["創建策略"](#)以取得說明。
- 建立保護組來管理一組資源的備份和還原作業。看["使用NetApp Backup and Recovery為 Hyper-V 工作負載建立和管理保護群組"](#)了解更多。
- 立即備份工作負載（立即建立按需備份）。

立即使用按需備份來備份工作負載

使用按需備份，以便在進行系統變更之前保護您的資料。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。"[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從選單中選擇*庫存*。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標  > 查看詳情。
4. 選擇「保護群組」、「資料儲存」或「虛擬機器」標籤。
5. 選擇要備份的保護群組或虛擬機器。
6. 選擇“操作”圖標  > 立即備份。



備份使用指派給保護群組或虛擬機器的相同原則。

7. 選擇計劃層級。
8. 選擇*備份*。

使用NetApp Backup and Recovery復原 Hyper-V 工作負載

使用NetApp Backup and Recovery從快照、複製到輔助儲存的工作負載備份或儲存在物件儲存中的備份還原 Hyper-V 工作負載。

從這些位置恢復

您可以從不同的起始位置恢復工作負載：

- 從主位置還原（本地快照）
- 從二級儲存上的複製資源恢復
- 從物件儲存備份還原

恢復到這些點

您可以將資料還原到以下點：

- 恢復到原始位置
- 恢復到備用位置

從物件儲存中復原的注意事項

如果您選擇物件儲存中的備份文件，且該備份的勒索軟體保護處於活動狀態（如果您在備份策略中啟用了DataLock 和勒索軟體復原），系統會提示您在復原資料之前對備份檔案執行額外的完整性檢查。我們建議您執行掃描。



您將需要向雲端提供者支付額外的出口費用才能存取備份文件的內容。

恢復工作負載的工作原理

恢復工作負載時，會發生以下情況：

- 當您從本機備份檔案還原工作負載時，NetApp Backup and Recovery and Recovery會使用備份中的資料建立一個_新_資源。
- 從複製的工作負載復原時，您可以將工作負載還原到原始系統或本機ONTAP系統。

從「恢復」頁面（也稱為「搜尋和恢復」），您可以恢復資源，即使您不記得確切的名稱、它所在的位置或它最後處於良好狀態的日期。您可以使用過濾器搜尋快照。

從恢復選項恢復工作負載資料（搜尋和恢復）

使用復原選項恢復 Hyper-V 工作負載。您可以按名稱或使用篩選器來搜尋快照。

所需的控制台角色 備份和還原超級管理員或備份和還原復原管理員角色。"[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 復原。
2. 從名稱搜尋欄位右側的下拉清單中，選擇 **Hyper-V**。
3. 輸入要還原的資源的名稱，或篩選要還原的資源所在的 VM 名稱、VM 主機或儲存池。

出現符合您的搜尋條件的快照清單。

4. 選擇要還原的快照的“恢復”按鈕。

出現可能的還原點清單。

5. 選擇您想要使用的還原點。
6. 選擇快照來源位置。
7. 選擇“下一步”繼續。
8. 選擇恢復目標位置和設定：

目的地選擇

恢復到原始位置

恢復到原始位置後，您可以透過展開「目標設定」部分來查看目標設置，但您無法變更它們。

1. 在「恢復後選項」部分，請考慮以下選項：
 - 啟動虛擬機器：啟用此選項可在復原後啟動新的虛擬機器。
2. 選擇*恢復*。

恢復至備用位置

1. 在「目標設定」部分，輸入以下資訊：
 - **Hyper-V FQDN 或 IP 位址**：輸入目標 Hyper-V 主機的完全限定網域名稱或 IP 位址。
 - **網路**：選擇要將快照還原到的目標網路。
 - **虛擬機器名稱**：輸入要還原的虛擬機器的名稱。
 - **目標位置**：輸入應包含已復原資料的目標資料夾或 CIFS 共用。
2. 在「恢復前選項」部分，請考慮以下選項：
 - **快速復原**：啟用此選項可使復原的虛擬機器立即可用。僅從物件儲存中恢復運行虛擬機器所需的文件，而不是整個磁碟區。
3. 在「恢復後選項」部分，請考慮以下選項：
 - 啟動虛擬機器：啟用此選項可在復原後啟動新的虛擬機器。
4. 選擇*恢復*。

保護 Oracle Database 工作負載（預覽版）

保護 Oracle 資料庫工作負載概述

使用 NetApp Backup and Recovery 保護 Oracle 資料庫和日誌。取得快速、節省空間、崩潰一致性且資料庫一致的備份和還原。將 Oracle Database 工作負載備份到 AWS S3、NetApp StorageGRID、Azure Blob Storage 或 ONTAP S3。將備份還原到內部部署 Oracle 主機。

使用 NetApp Backup and Recovery 實作 3-2-1 保護策略，其中您在 2 個不同的儲存系統上擁有 3 個來源資料副本，並在雲端中擁有 1 個副本。3-2-1 方法的優點包括：

- 多個資料副本可防止內部和外部網路安全威脅。
- 如果一種媒體發生故障，使用不同類型的媒體可以幫助您恢復。
- 您可以從現場副本快速恢復，如果現場副本受到損害，則可以使用異地副本。



若要切換至 NetApp Backup and Recovery UI 版本或從 NetApp Backup and Recovery UI 版本切換，請參閱["切換到先前的 NetApp Backup and Recovery UI"](#)。

您可以使用 NetApp Backup and Recovery 來執行下列與 Oracle Database 工作負載相關的任務：

- ["探索 Oracle Database 工作負載"](#)
- ["建立和管理 Oracle Database 工作負載的保護群組"](#)
- ["備份 Oracle Database 工作負載"](#)
- ["還原 Oracle Database 工作負載"](#)

在 NetApp Backup and Recovery 中探索 Oracle Database 工作負載

NetApp Backup and Recovery 需要先發現您的 Oracle 資料庫，以便您可以保護它們。

所需的控制台角色 備份和還原超級管理員。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

新增 Oracle 主機並發現資源

新增 Oracle 主機資訊並讓NetApp Backup and Recovery發現工作負載。在每個控制台代理程式中，選擇您想要發現工作負載的系統。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 在“工作負載”下，選擇“Oracle”磁貼。

如果您是第一次登入備份和恢復，並且在控制台中有一個系統但沒有發現任何資源，則會顯示「歡迎使用新的NetApp備份和恢復」頁面，其中包含「發現資源」選項。

3. 選擇*發現資源*。
4. 輸入以下資訊：
 - a. 工作負載類型：選擇*Oracle*。
 - b. 如果您尚未儲存此 Oracle 主機的憑證，請選擇「新增憑證」。
 - i. 選擇與該主機一起使用的控制台代理程式。
 - ii. 輸入此憑證的名稱。
 - iii. 輸入該帳戶的使用者名稱和密碼。
 - iv. 選擇*完成*。
 - c. 主機註冊：新增的 Oracle 主機。輸入主機的 FQDN 或 IP 位址、憑證、控制台代理程式和連接埠號碼。
5. 選擇*發現*。



此過程可能需要幾分鐘。

結果

Oracle 工作負載顯示在清單頁面的工作負載清單中。

繼續存取NetApp Backup and Recovery儀表板

1. 從NetApp Console選單中，選擇 保護 > 備份和還原。

2. 選擇一個工作負載圖塊（例如，Microsoft SQL Server）。
3. 從備份和還原選單中，選擇*儀表板*。
4. 檢討資料保護的健康狀況。處於危險中或受保護的工作負載的數量會根據新發現、受保護和備份的工作負載而增加。

使用 **NetApp Backup and Recovery** 為 **Oracle Database** 工作負載建立及管理保護群組

建立保護群組來管理一組 Oracle 資料庫資源的備份作業。保護組是您想要一起保護的資源（例如資料庫）的邏輯分組。您需要建立一個保護群組來備份 Oracle 資料庫。

您可以執行與保護群組相關的以下任務：

- 建立保護組。
- 查看保護詳情。
- 立即備份保護群組。請參閱 ["立即備份 Oracle Database 工作負載"](#)。
- 刪除保護組。

建立保護組

將您想要保護的虛擬機器和儲存池分組到保護群組中。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標 **...** > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇*建立保護組*。
6. 為保護組提供名稱。
7. 選擇要包含在保護群組中的虛擬機器或儲存池。
8. 選擇“下一步”。
9. 選擇要套用於保護群組的*備份策略*。

如果要建立策略，請選擇*建立新策略*並依照指示建立策略。看["創建策略"](#)了解更多。

10. 選擇“下一步”。
11. 檢查配置。
12. 選擇“建立”來建立保護組。

刪除保護群組

刪除保護群組會刪除該保護群組以及所有相關的備份計畫。如果不再需要某個保護群組，您可能需要將其刪除。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇一個工作負載來查看保護詳細資訊。
3. 選擇“操作”圖標  > 查看詳情。
4. 選擇*保護群組*標籤。
5. 選擇要刪除的保護組。
6. 選擇“操作”圖標  > 移除保護。
7. 查看有關刪除相關備份的確認訊息並確認刪除。

使用 NetApp Backup and Recovery 備份 Oracle Database 工作負載

使用NetApp Backup and Recovery將 Oracle 資料庫保護群組或資料庫從本機ONTAP系統備份到雲端存儲，包括 Amazon S3、NetApp StorageGRID、Microsoft Azure Blob Storage 或ONTAP S3。NetApp Backup and Recovery每個保護群組中的資料庫和日誌資料。



若要安排備份保護群組或單一資料庫，請建立管理備份和還原作業的策略。看["創建策略"](#)以取得說明。

- 建立保護群組以管理一組資源的備份和還原作業。如需詳細資訊，請參閱 ["使用 NetApp Backup and Recovery 為 Oracle Database 工作負載建立及管理保護群組"](#)。
- 立即備份保護群組（立即建立按需備份）。
- 立即備份資料庫。

立即使用按需備份來備份保護群組

在進行系統變更之前執行按需備份以確保您的資料受到保護。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。 ["了解所有服務的NetApp Console存取角色"](#)。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 在“工作負載”下，選擇“Oracle”磁貼。
3. 選擇*庫存*。
4. 選擇一個工作負載來查看保護詳細資訊。
5. 選擇“操作”圖標  > 查看詳情。
6. 選擇「保護群組」、「資料儲存」或「虛擬機器」標籤。
7. 選擇要備份的保護組。

8. 選擇“操作”圖標 ...> 立即備份。



NetApp Backup and Recovery使用相同的策略。

9. 選擇計劃層級。
10. 選擇*備份*。

立即使用按需備份來備份資料庫

您可以執行單一資料庫的按需備份。

所需的控制台角色 備份和還原超級管理員或備份和還原備份管理員角色。 "[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 在“工作負載”下，選擇“Oracle”磁貼。
3. 選擇*庫存*。
4. 選擇一個工作負載來查看保護詳細資訊。
5. 選擇“操作”圖標 ...> 查看詳情。
6. 選擇“資料庫”標籤。
7. 選擇要備份的資料庫。
8. 選擇“操作”圖標 ...> 立即備份。
9. 選擇計劃層級。
10. 選擇*備份*。

使用NetApp Backup and RecoveryOracle 資料庫

使用NetApp Backup and Recovery從快照、複製到輔助儲存的備份或儲存在物件儲存中的備份還原 Oracle 資料庫。

從這些位置恢復

您可以從不同的起始位置還原資料庫：

- 從主位置還原（本地快照）
- 從二級儲存上的複製資源恢復
- 從物件儲存備份還原

恢復到這些點

您可以將資料恢復到原始位置；在此私人預覽版中不提供恢復到備用位置的功能。

- 恢復到原始位置

Oracle 資料庫復原的工作原理

還原 Oracle 資料庫時，會發生以下情況：

- 當您從本機快照還原資料庫時，NetApp Backup and Recovery會使用備份中的資料建立_新_資源。
- 從複製的儲存空間還原時，您可以將其恢復到原始位置。
- 從物件儲存還原備份時，您可以將資料還原到來源儲存或本機ONTAP系統，然後從那裡還原資料庫。

從「復原」頁面（也稱為「搜尋與復原」），您可以還原資料庫，即使您不記得確切的名稱、它所在的位置或它最後處於良好狀態的日期。您可以使用過濾器搜尋資料庫。

還原 Oracle 資料庫

根據您的需要，將 Oracle 資料庫還原到特定時間點、特定系統變更號碼 (SCN) 或最後的良好狀態。您也可以簡單地從快照還原資料庫並跳過自動復原程序。如果您想手動執行恢復，您可能想要跳過自動恢復程序。您可以使用資料庫名稱或特定篩選器來搜尋資料庫。

所需的控制台角色 備份和還原超級管理員或備份和還原復原管理員角色。"[了解所有服務的NetApp Console存取角色](#)"。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 從NetApp Backup and Recovery選單中，選擇 復原。
3. 從名稱搜尋欄位右側的下拉清單中，選擇 **Oracle**。
4. 輸入要還原的資料庫的名稱或篩選要還原的資料庫所在的資料庫主機。

出現符合您的搜尋條件的快照清單。

5. 選擇要還原的資料庫的“恢復”按鈕。
6. 選擇恢復選項：

恢復到特定時間點

- a. 選擇*恢復到特定時間點*。
- b. 選擇“下一步”。
- c. 從下拉式選單中選擇一個日期，然後選擇*搜尋*。

顯示指定日期的符合快照清單。

恢復到特定的系統變更號碼 (SCN)

- a. 選擇*恢復到特定的系統變更號碼 (SCN)*。
- b. 選擇“下一步”。
- c. 輸入要用作還原點的 SCN，然後選擇*搜尋*。

顯示指定 SCN 的符合快照清單。

恢復到最新備份（上次良好狀態）

- a. 選擇*恢復到最新備份*。
- b. 選擇“下一步”。

顯示最新的完整備份和日誌備份。

從快照還原，無需恢復

- a. 選擇*從沒有恢復的快照中恢復*。
- b. 選擇“下一步”。

顯示符合的快照。

7. 選擇快照來源位置。
8. 選擇“下一步”繼續。
9. 選擇恢復目標位置和設定：

目的地選擇

恢復到原始位置

1. 目的地設定：
 - 選擇還原整個資料庫或僅還原資料庫的表空間。
 - 控制檔案：可選地，啟用此選項也可以還原資料庫控制檔案。
2. 預恢復選項：
 - 或者，啟用此選項並輸入應在還原作業之前執行的腳本的完整路徑以及該腳本所採用的任何參數。
 - 為腳本選擇一個超時值。如果腳本未能在此時間段內執行，則復原仍將繼續。
3. 恢復後選項：
 - 後記：可選地，啟用此選項並輸入應在復原作業後執行的腳本的完整路徑以及該腳本所採用的任何參數。
 - 恢復後以 **READ-WRITE** 模式開啟資料庫或容器資料庫：復原作業完成後，備份和復原將為資料庫啟用 **READ-WRITE** 模式。
4. *通知*部分：
 - 啟用電子郵件通知：選擇此選項可接收有關復原作業的電子郵件通知，並指示您想要接收的通知類型。
5. 選擇*恢復*。

恢復至備用位置

不適用於 Oracle Database 工作負載預覽。

使用NetApp Backup and Recovery掛載和解除安裝 Oracle 資料庫復原點

如果您需要以受控狀態存取資料庫來執行復原操作，則可能需要安裝 Oracle 資料庫復原點。

安裝 Oracle 資料庫還原點

如果您將資料庫的保護策略配置為保留存檔日誌，則可以掛載復原點來查看資料庫變更歷史記錄。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 選擇 Oracle 圖塊。
3. 在備份和還原選單中，選擇*Inventory*。
4. 對於清單中的 Oracle 資料庫工作負載，選擇「檢視」。
5. 選擇*資料庫*選單。
6. 從清單中選擇一個資料庫並選擇“操作”圖標  > 查看保護詳情。

出現該資料庫的復原點清單。

7. 從清單中選擇一個復原點，然後選擇「動作」圖示  > 安裝。

8. 在出現的對話方塊中，執行以下操作：
 - a. 從清單中選擇應安裝恢復點的主機。
 - b. 選擇「備份和復原」應使用哪個位置來安裝復原點。對於預覽版本，不支援從物件儲存掛載。

顯示備份和復原應使用的安裝路徑。

9. 選擇*安裝*。

恢復點安裝在 Oracle 主機上。

解除安裝 Oracle 資料庫還原點

當您不再需要查看對該資料庫所做的變更時，請卸載復原點。

步驟

1. 從NetApp Console選單中，選擇「保護」>「備份和復原」。
2. 選擇 Oracle 圖塊。
3. 在備份和還原選單中，選擇*Inventory*。
4. 對於清單中的 Oracle 工作負載，選擇「檢視」。
5. 選擇*資料庫*選單。
6. 從清單中選擇一個資料庫並選擇“操作”圖標  > 查看保護詳情。

出現該資料庫的復原點清單。

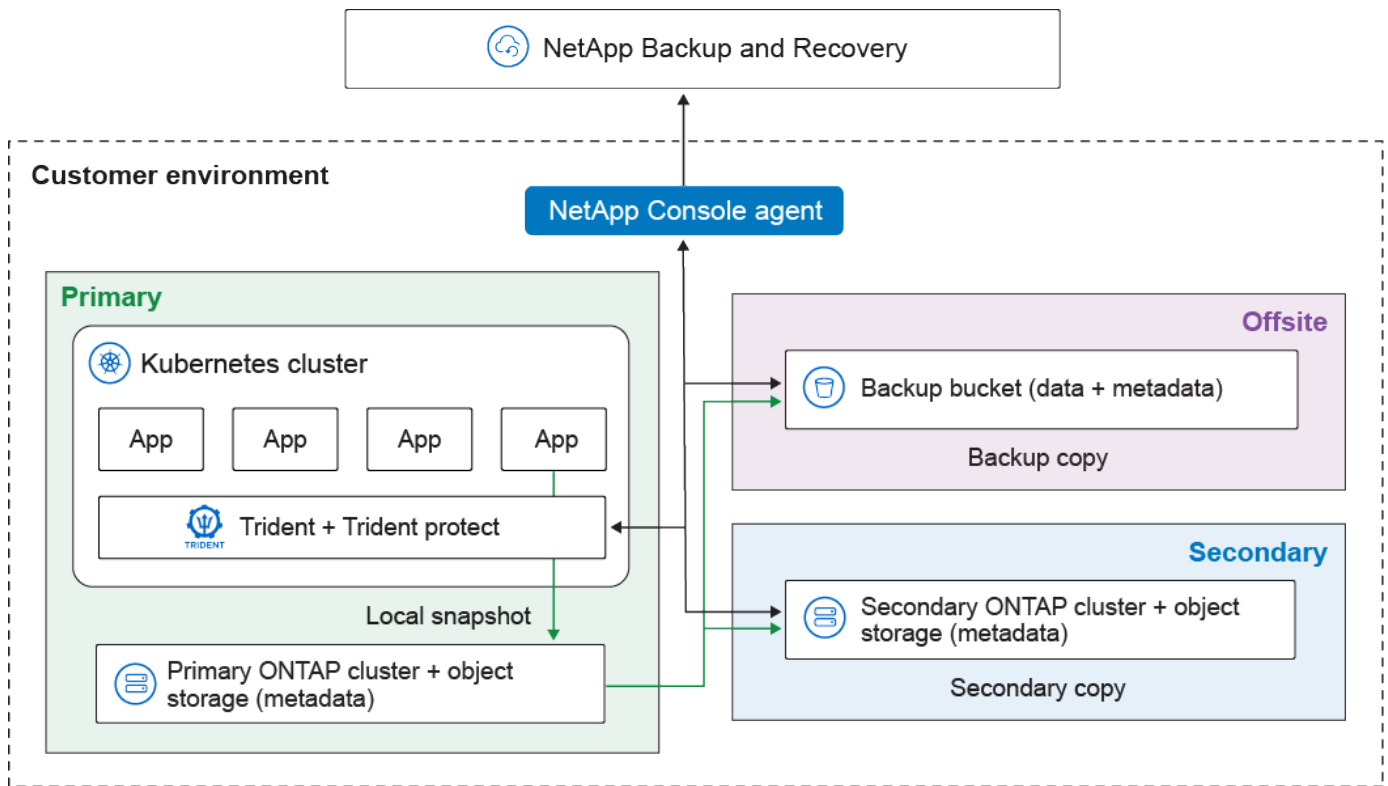
7. 從清單中選擇一個復原點，然後選擇「動作」圖示  > 卸載。
8. 選擇“卸載”確認操作。

保護 Kubernetes 工作負載（預覽版）

管理 Kubernetes 工作負載概覽

透過在NetApp Backup and Recovery中管理 Kubernetes 工作負載，您可以在一個地方發現、管理和保護您的 Kubernetes 叢集和應用程式。您可以管理託管在 Kubernetes 叢集上的資源和應用程式。您還可以建立保護策略並將其與 Kubernetes 工作負載關聯，所有這些都使用單一介面完成。

下圖展示了 Kubernetes 工作負載的備份和還原的元件和基本架構，以及如何將資料的不同副本儲存在不同位置：



NetApp Backup and Recovery為管理 Kubernetes 工作負載提供了以下優點：

- 單一控制平面，用於保護跨多個 Kubernetes 叢集運行的應用程式。這些應用程式可以包括在 Kubernetes 叢集上執行的容器或虛擬機器。
- 與NetApp SnapMirror本機集成，為所有備份和恢復工作流程提供儲存卸載功能。
- Kubernetes 應用程式的永久增量備份，轉換為更低的復原點目標 (RPO) 和復原時間目標 (RTO)。



本文檔作為技術預覽提供。在預覽期間，不建議將 Kubernetes 功能用於生產工作負載。對於此預覽版產品，NetApp保留在正式發布之前修改產品詳細資訊、內容和時間表的權利。

您可以完成與管理 Kubernetes 工作負載相關的下列任務：

- "發現 Kubernetes 工作負載"。
- "管理 Kubernetes 集群"。
- "新增和保護 Kubernetes 應用程式"。
- "管理 Kubernetes 應用程式"。
- "恢復 Kubernetes 應用程式"。

探索NetApp Backup and Recovery中的 Kubernetes 工作負載

NetApp Backup and Recovery需要在保護 Kubernetes 工作負載之前發現它們。

所需的**NetApp Console**角色 備份和還原超級管理員。了解詳情["備份和恢復角色和權限"](#)。"了解所有服務的NetApp Console存取角色"。

發現 Kubernetes 工作負載

在備份和復原清單中，發現您環境中的 Kubernetes 工作負載。新增工作負載會將 Kubernetes 叢集新增至 NetApp Backup and Recovery。然後，您可以新增應用程式並保護叢集資源。



當您發現目前受 Trident Protect 保護的叢集時，所有與 Trident Protect 一起使用的備份計畫都會在發現過程中停用（Trident Protect 備份計畫與 Backup and Recovery 不相容）。若要保護叢集中的應用程式，"[建立新的保護原則](#)"或將應用程式與現有原則建立關聯。之後，您可以視需要移除 Trident Protect 備份計畫。

步驟

1. 執行下列操作之一：

- 如果您是第一次發現 Kubernetes 工作負載，請在 NetApp Backup and Recovery 中，在「工作負載」下，選擇「Kubernetes」磁貼。
- 如果您已經發現 Kubernetes 工作負載，請在 NetApp Backup and Recovery 中選擇 **Inventory > Workloads**，然後選擇 **Discover resources**。

2. 選擇 **Kubernetes** 工作負載類型。

3. 輸入叢集名稱並選擇與叢集一起使用的連接器。

4. 按照出現的命令列說明進行操作：

- 建立 Trident Protect 命名空間
- 建立 Kubernetes 機密
- 新增 Helm 儲存庫
- 安裝或升級 Trident Protect 和 Trident Protect 連接器

這些步驟確保 NetApp Backup and Recovery 可以與叢集互動。

5. 完成這些步驟後，選擇*發現*。

該集群已新增至清單。

6. 在關聯的 Kubernetes 工作負載中選擇「檢視」以查看該工作負載的應用程式、叢集和命名空間清單。

繼續存取 NetApp Backup and Recovery 儀表板

請依照以下步驟查看 NetApp Backup and Recovery 儀表板。

1. 從 NetApp Console 選單中，選擇 保護 > 備份和還原。
2. 選擇一個工作負載圖塊（例如，Microsoft SQL Server）。
3. 從備份和還原選單中，選擇*儀表板*。
4. 檢討資料保護的健康狀況。處於危險中或受保護的工作負載的數量會根據新發現、受保護和備份的工作負載而增加。

["了解儀表板顯示的內容"](#)。

新增和保護 **Kubernetes** 應用程式

新增和保護 **Kubernetes** 應用程式

NetApp Backup and Recovery 讓您輕鬆發現 Kubernetes 集群，而無需產生和上傳 kubeconfig 檔案。您可以使用從 NetApp Console 使用者介面複製的簡單命令連接 Kubernetes 叢集並安裝所需的軟體。

所需的 **NetApp Console** 角色

組織管理員或 SnapCenter 管理員。"[了解 NetApp Backup and Recovery 存取角色](#)"。"[了解所有服務的 NetApp Console 存取角色](#)"。

新增並保護新的 **Kubernetes** 應用程式

保護 Kubernetes 應用程式的第一步是在 NetApp Backup and Recovery 中建立應用程式。建立應用程式時，您會讓控制台了解 Kubernetes 叢集上正在執行的應用程式。

開始之前

在新增和保護 Kubernetes 應用程式之前，您需要"[發現 Kubernetes 工作負載](#)"。

使用 Web UI 新增應用程式

步驟

1. 在NetApp Backup and Recovery中，選擇 **Inventory**。
2. 選擇一個 Kubernetes 實例，然後選擇「檢視」以查看與該實例關聯的資源。
3. 選擇“應用程式”標籤。
4. 選擇*建立應用程式*。
5. 輸入應用程式的名稱。
6. 或者，選擇以下任意欄位來搜尋您想要保護的資源：
 - 關聯集群
 - 關聯的命名空間
 - 資源類型
 - 標籤選擇器
7. （可選）選擇「叢集範圍資源」以選擇任何在叢集層級範圍限定的資源。如果包含這些資源，它們會在建立應用程式時新增到應用程式中。
8. 或者，選擇“搜尋”以根據您的搜尋條件尋找資源。



控制台不會儲存搜尋參數或結果；這些參數用於在選定的 Kubernetes 叢集中搜尋可包含在應用程式中的資源。

9. 控制台顯示符合您的搜尋條件的資源清單。
10. 如果清單包含您想要保護的資源，請選擇「下一步」。
11. （可選）在「策略」區域中，選擇現有保護策略來保護應用程序，或建立新策略。如果不選擇策略，則建立的應用程式將不帶保護策略。你可以["新增保護策略"](#)之後。
12. 在*Prescripts and postscripts*區域中，啟用並配置您想要在備份操作之前或之後執行的任何prescript或postscript執行掛鉤。若要啟用處方或附言，您必須至少已建立了一個["執行鉤子模板"](#)。
13. 選擇“創建”。

結果

應用程式已建立並出現在 Kubernetes 清單的 應用程式 標籤中的應用程式清單中。NetApp Console會根據您的設定啟用對應用程式的保護，並且您可以在備份和還原的*監控*區域中監控進度。

使用 CR 新增應用程式

步驟

1. 建立目的地應用程式 CR 檔案：
 - a. 建立自訂資源（CR）檔案並將其命名為（例如、`my-app-name.yaml`）。
 - b. 設定下列屬性：
 - **metadata.name**：（必填）應用程式自訂資源的名稱。請記住您選擇的名稱，因為保護作業所需的其他 CR 檔案會參照此值。
 - **spec.includedNamespaces**：（必要）使用命名空間和標籤選擇器來指定應用程式使用的命

名空間和資源。應用程式命名空間必須包含在此清單中。標籤選擇器是可選的，可用來篩選每個指定命名空間中的資源。

- **spec.includedClusterScopedResources**：（選用）使用此屬性指定要包含在應用程式定義中的叢集範圍資源。此屬性可讓您根據資源的群組、版本、類型和標籤來選擇這些資源。
 - **groupVersionKind**：（必要）指定叢集範圍資源的 API 群組、版本和類型。
 - **labelSelector**：（可選）依照標籤篩選叢集範圍的資源。

c. 如有需要，請設定下列註解：

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**：（可選）此註解僅適用於從虛擬機器定義的應用程式，例如在 KubeVirt 環境中，快照之前會發生檔案系統凍結。指定此應用程式在快照期間是否可以寫入檔案系統。如果設定為 `true`，則應用程式會忽略全域設定，並可在快照期間寫入檔案系統。如果設定為 `false`，則應用程式會忽略全域設定，且檔案系統會在快照期間凍結。如果已指定但應用程式定義中沒有虛擬機器，則會忽略該註解。如果未指定，則應用程式會遵循["全域檔案系統凍結設定"](#)。
- **protect.trident.netapp.io/protection-command**：（選用）使用此註釋指示 Backup and Recovery 保護或停止保護應用程式。可能的值為 `protect` 或 `unprotect`。
- **protect.trident.netapp.io/protection-policy-name**：（選用）使用此註解指定要用於保護此應用程式的 Backup and Recovery 保護原則名稱。此保護原則必須已存在於 Backup and Recovery 中。

如果需要在應用程式建立後套用此註解，可以使用以下命令：

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```


+
YAML 範例：

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (選用) 新增篩選條件，包含或排除標記有特定標籤的資源：

- **resourceFilter.resourceSelectionCriteria**：(篩選必需) 使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：
- **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，則它們之間按 OR 運算匹配，每個元素內的欄位 (group、kind、version) 之間按 AND 運算匹配。
 - **resourceMatchers[].group**：(可選) 要篩選的資源群組。
 - **resourceMatchers[].kind**：(可選) 要篩選的資源類型。
 - **resourceMatchers[].version**：(可選) 要篩選的資源版本。

- **resourceMatchers[].names** : (可選) 要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
- **resourceMatchers[].namespaces** : (可選) 要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
- **resourceMatchers[].labelSelectors** : (可選) 資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如：
"trident.netapp.io/os=linux"。



當兩者 resourceFilter 和 labelSelector 同時使用時，resourceFilter 首先運行，然後 labelSelector 將應用於生成的資源。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
  resourceMatchers:
    - group: my-resource-group-1
      kind: my-resource-kind-1
      version: my-resource-version-1
      names: ["my-resource-names"]
      namespaces: ["my-resource-namespaces"]
      labelSelectors: ["trident.netapp.io/os=linux"]
    - group: my-resource-group-2
      kind: my-resource-kind-2
      version: my-resource-version-2
      names: ["my-resource-names"]
      namespaces: ["my-resource-namespaces"]
      labelSelectors: ["trident.netapp.io/os=linux"]
```

2. 建立與您的環境相符的應用程式 CR 後、套用該 CR。例如：

```
kubectl apply -f my-app-name.yaml
```

現在即可使用 **Backup and Recovery Web UI** 備份 **Kubernetes** 應用程式

NetApp Backup and Recovery 可讓您使用 Web 介面手動備份 Kubernetes 應用程式。

所需的**NetApp Console**角色

組織管理員或SnapCenter管理員。["了解NetApp Backup and Recovery存取角色"](#)。["了解所有服務的NetApp Console存取角色"](#)。

現在即可使用 **Web UI** 備份 **Kubernetes** 應用程式

手動建立 Kubernetes 應用程式的備份，為未來的備份和快照建立基線，或確保最新資料受到保護。

步驟

1. 在 NetApp Backup and Recovery 中，選擇 **Inventory**。
2. 選擇一個 Kubernetes 實例，然後選擇「檢視」以查看與該實例關聯的資源。
3. 選擇“應用程式”標籤。
4. 在應用程式清單中，選擇要備份的應用程式並選擇相關的操作選單。
5. 選擇*立即備份*。
6. 確保選擇了正確的應用程式名稱。
7. 選擇*備份*。

結果

控制台建立應用程式的備份並在備份和還原的*監控*區域中顯示進度。此備份是根據與應用程式關聯的保護策略建立的。

現在可以使用 **Backup and Recovery** 中的自訂資源備份 **Kubernetes** 應用程式

NetApp Backup and Recovery 可讓您使用自訂資源（CR）手動備份 Kubernetes 應用程式。

立即使用自訂資源備份 **Kubernetes** 應用程式

手動建立 Kubernetes 應用程式的備份，為未來的備份和快照建立基線，或確保最新資料受到保護。



如果叢集範圍的資源在應用程式定義中被明確引用，或引用了任何應用程式命名空間，則這些資源將包含在備份、快照或複製中。

開始之前

請確保 AWS 會話令牌的有效期限足以應付任何長時間運行的 s3 備份作業。如果令牌在備份作業期間過期，則操作可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 文件"](#)。

使用自訂資源建立本機快照

若要為您的 Kubernetes 應用程式建立快照並將其儲存在本地，請使用具有特定屬性的 Snapshot 自訂資源。

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `local-snapshot-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.applicationRef**：要建立快照的應用程式的 Kubernetes 名稱。

- **spec.appVaultRef**：（必填）應儲存快照內容（元資料）的 AppVault 名稱。
- **spec.reclaimPolicy**：（選用）定義當快照 CR 刪除時，快照的 AppArchive 會發生什麼情況。這意味著即使設為 Retain，快照也會被刪除。有效選項：
 - Retain (預設)
 - Delete

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: local-snapshot-cr
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Retain
```

3. 在 local-snapshot-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f local-snapshot-cr.yaml
```

使用自訂資源將應用程式備份至物件儲存區

建立具有特定屬性的 Backup CR，以將應用程式備份到物件儲存區。

步驟

1. 建立自訂資源（CR）檔案並將其命名為 object-store-backup-cr.yaml。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.applicationRef**：（必需）要備份的應用程式的 Kubernetes 名稱。
 - **spec.appVaultRef**：（必需，與 *spec.appVaultTargetsRef* 互斥）如果您使用相同儲存桶來儲存快照和備份，則這是 AppVault 的名稱，備份內容應儲存在其中。
 - **spec.appVaultTargetsRef**：（必需，與 *spec.appVaultRef* 互斥）如果您使用不同的儲存貯體來儲存快照和備份，則此為應儲存備份內容的 AppVault 名稱。
 - **spec.dataMover**：（可選）字串，指示要用於備份作業的備份工具。該值區分大小寫，且必須為 CBS。
 - **spec.reclaimPolicy**：（選用）定義刪除 Backup CR 時備份內容（中繼資料/磁碟區資料）的處理方式。可能的值：
 - Delete
 - Retain (預設)
 - **spec.cleanupSnapshot**：（必需）確保備份 CR 建立的臨時快照在備份作業完成後不會被刪除。建議

值：false。

使用同一個儲存貯體儲存快照和備份時的範例 YAML：

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

使用不同儲存區分別儲存快照和備份時的 YAML 範例：

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. 在 object-store-backup-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f object-store-backup-cr.yaml
```

使用自訂資源建立 3-2-1 扇出備份

使用 3-2-1 扇出架構進行備份時，備份會同時複製到輔助儲存和物件儲存。若要建立 3-2-1 扇出備份，請建立具有特定屬性的 Backup CR。

步驟

1. 建立自訂資源（CR）檔案並將其命名為 3-2-1-fanout-backup-cr.yaml。
2. 在您建立的檔案中、設定以下屬性：

- **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
- **spec.applicationRef**：（必需）要備份的應用程式的 Kubernetes 名稱。
- **spec.appVaultTargetsRef**：（必填）應儲存備份內容的 AppVault 名稱。
- **spec.dataMover**：（可選）字串，指示要用於備份作業的備份工具。該值區分大小寫，且必須為 CBS。
- **spec.reclaimPolicy**：（選用）定義刪除 Backup CR 時備份內容（中繼資料/磁碟區資料）的處理方式。可能的值：
 - Delete
 - Retain (預設)
- **spec.cleanupSnapshot**：（必需）確保備份 CR 建立的臨時快照在備份作業完成後不會被刪除。建議值：false。
- **spec.replicateSnapshot**：（必要）指示 Backup and Recovery 將快照複製到次要儲存設備。必要值：true。
- **spec.replicateSnapshotReclaimPolicy**：（選用）定義刪除複製快照時的處理方式。可能的值：
 - Delete
 - Retain (預設)

YAML 範例：

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. 在 3-2-1-fanout-backup-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

支援的備份註釋

下表描述了建立備份 CR 時可以使用的註解。

註解	類型	描述	預設值
protect.trident.netapp.io/full-backup	字串	指定備份是否為非增量備份。設定為 `true` 可建立非增量備份。最佳實踐是定期執行完整備份，並在兩次完整備份之間執行增量備份，以最大程度地降低還原相關風險。	"false"
protect.trident.netapp.io/snapshots-hot-completion-timeout	字串	允許完成整個快照作業的最長時間。	"60 分鐘"
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	字串	磁碟區快照達到可用狀態所允許的最長時間。	"30 分鐘"
protect.trident.netapp.io/volume-snapshots-created-timeout	字串	建立磁碟區快照所允許的最長時間。	"5 分鐘"
protect.trident.netapp.io/pvc-bind-timeout-sec	字串	等待新建的任何 PersistentVolumeClaims (PVC) 到達該 Bound 階段的最大時間（以秒為單位），超過此時間操作將失敗。	"1200"（20 分鐘）

恢復 Kubernetes 應用程式

使用 Web UI 還原 Kubernetes 應用程式

NetApp Backup and Recovery 使您能夠恢復已透過保護策略保護的應用程式。要恢復應用程式，應用程式需要至少有一個可用的恢復點。復原點由本機快照或物件儲存備份（或兩者）組成。您可以使用本機、輔助或物件儲存存檔來還原應用程式。

開始之前

如果您要還原使用 Trident Protect 備份的應用程式，請確保來源叢集和目的地叢集上都安裝了 Trident Protect。

所需的 NetApp Console 角色

組織管理員或 SnapCenter 管理員。["了解 NetApp Backup and Recovery 存取角色"](#)。["了解所有服務的 NetApp Console 存取角色"](#)。

步驟

1. 在 NetApp Backup and Recovery 選單中，選取 還原。
2. 從清單中選擇一個 Kubernetes 應用程式，然後選擇該應用程式的 **View and Restore**。

出現還原點清單。

3. 選擇要使用的還原點的 **Restore** 按鈕。

常規設定

1. 選擇要從中還原的來源位置。
2. 從 *Cluster* 清單中選擇目標群集。



目前不支援將 Trident Protect 建立的本機快照還原到不同的叢集。

3. 選擇還原至原始命名空間或新命名空間。
4. 如果您選擇還原到新的命名空間、請輸入要使用的目標命名空間。
5. 選擇“下一步”。

資源選擇

1. 選擇是否要恢復與應用程式相關的所有資源，或使用篩選器選擇要復原的特定資源：

恢復所有資源

1. 選擇*恢復所有資源*。
2. 選擇“下一步”。

恢復特定資源

1. 選擇*選擇性資源*。
2. 選擇資源過濾器的行為。如果您選擇“包括”，則會恢復您選擇的資源。如果您選擇“排除”，則您選擇的資源將不會被恢復。
3. 選擇*新增規則*來新增定義選擇資源的篩選器的規則。您至少需要一條規則來過濾資源。

每個規則都可以根據資源命名空間、標籤、群組、版本和種類等標準進行過濾。

4. 選擇*儲存*來儲存每條規則。
5. 新增所有需要的規則後，選擇*搜尋*即可查看備份檔案中符合篩選條件的可用資源。



顯示的資源是叢集上目前存在的資源。

6. 對結果滿意後，選擇*下一步*。

目的地設定

1. 展開 **Destination settings** 部分，然後選擇還原至預設儲存類別、不同的儲存類別，或者如果您要還原至不同的叢集，則將儲存類別對應至目的地叢集。
2. 如果選擇還原到不同的儲存類別，請選擇與每個來源儲存類別相符的目標儲存類別。
3. 如果您要還原使用 Trident Protect 建立的備份或快照，則可以選擇查看用作還原作業儲存貯體的 AppVault 詳細資訊。如果您的環境或 AppVault 狀態發生變更，請選取 **Sync App Vault** 以重新整理詳細資訊。



如果您需要在 Kubernetes 叢集上建立 AppVault 以方便還原使用 Trident Protect 建立的備份或快照，請參閱 ["使用 Trident Protect AppVault 物件來管理儲存桶"](#)。

4. (可選) 展開 **Restore scripts** 部分，啟用 **Postscript** 選項，選擇將在復原作業完成後執行的執行鉤子範本。如有需要，輸入腳本所需的任何參數，並新增標籤選擇器，以便根據資源標籤篩選資源。
5. 選擇*恢復*。

您可以使用自訂資源從快照或備份還原應用程式。如果要將應用程式還原到同一個叢集，從現有快照還原速度會更快。



- 還原應用程式時，所有為該應用程式配置的執行鉤子都會隨應用程式一起還原。如果存在還原後執行鉤子，它會在還原操作過程中自動執行。
- qtree 磁碟區支援從備份還原到不同的命名空間或原始命名空間。但是，qtree 磁碟區不支援從快照還原到不同的命名空間或原始命名空間。
- 您可以使用進階設定來自訂還原操作。如需深入瞭解、請參閱 ["使用進階自訂資源還原設定"](#)。

將備份還原至不同的命名空間

當您使用 BackupRestore CR 將備份還原到不同的命名空間時，NetApp Backup and Recovery 會將應用程式還原到新的命名空間，並為還原的應用程式建立一個應用程式 CR。為了保護還原的應用程式，您可以建立隨需備份或快照，或製定保護排程。



- 將備份還原到具有現有資源的不同命名空間不會變更與備份中資源同名的任何資源。若要還原備份中的所有資源，請刪除並重新建立目標命名空間，或將備份還原到新的命名空間。
- 使用 CR 還原到新命名空間時，必須先手動建立目標命名空間，然後再套用 CR。NetApp Backup and Recovery 僅在使用 CLI 時才會自動建立命名空間。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期，則作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 文件"](#)。



當您使用 Kopia 作為資料移動工具還原備份時，您可以選擇在 CR 中指定註釋，以控制 Kopia 使用的暫存的行為。有關可配置選項的更多資訊，請參閱 ["Kopia 說明文件"](#)。

步驟

1. 建立自訂資源 (CR) 檔案並將其命名為 `trident-protect-backup-restore-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：(必填) 此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appArchivePath**：AppVault 內儲存備份內容的路徑。您可以使用以下命令尋找此路徑：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
```

- **spec.appVaultRef**：(必填) 儲存備份內容的 AppVault 名稱。
- **spec.namespaceMapping**：復原作業的來源命名空間到目標命名空間的對應。請將 ``my-source-`

namespace`和`my-destination-namespace`替換為您環境中的資訊。

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. (可選) 如果您只需要選擇應用程式中的某些資源進行還原，請新增篩選條件，以包含或排除帶有特定標籤的資源：



Trident Protect 會自動選擇一些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持久卷聲明資源，並且它關聯了一個 pod，Trident Protect 也會恢復該關聯 pod。

- **resourceFilter.resourceSelectionCriteria**：(篩選必需) 使用`Include`或`Exclude`來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：

- **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，則它們之間按 OR 運算匹配，每個元素內的欄位 (group、kind、version) 之間按 AND 運算匹配。
 - **resourceMatchers[].group**：(可選) 要篩選的資源群組。
 - **resourceMatchers[].kind**：(可選) 要篩選的資源類型。
 - **resourceMatchers[].version**：(可選) 要篩選的資源版本。
 - **resourceMatchers[].names**：(可選) 要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
 - **resourceMatchers[].namespaces**：(可選) 要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
 - **resourceMatchers[].labelSelectors**：(可選) 資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如："trident.netapp.io/os=linux"。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 `trident-protect-backup-restore-cr.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

將備份還原至原始命名空間

您可以隨時將備份還原至原始命名空間。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期，則作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 文件"](#)。



當您使用 Kopia 作為資料移動工具還原備份時，您可以選擇在 CR 中指定註釋，以控制 Kopia 使用的暫存的行為。有關可配置選項的更多資訊，請參閱 ["Kopia 說明文件"](#)。

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `trident-protect-backup-ipr-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appArchivePath**：AppVault 內儲存備份內容的路徑。您可以使用以下命令尋找此路徑：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath  
='{.status.appArchivePath}'
```

- **spec.appVaultRef**：（必填）儲存備份內容的 AppVault 名稱。

例如：

```
apiVersion: protect.trident.netapp.io/v1  
kind: BackupInplaceRestore  
metadata:  
  name: my-cr-name  
  namespace: my-app-namespace  
spec:  
  appArchivePath: my-backup-path  
  appVaultRef: appvault-name
```

3. （可選）如果您只需要選擇應用程式中的某些資源進行還原，請新增篩選條件，以包含或排除帶有特定標籤的資源：



Trident Protect 會自動選擇一些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持久卷聲明資源，並且它關聯了一個 pod，Trident Protect 也會恢復該關聯 pod。

- **resourceFilter.resourceSelectionCriteria**：（篩選必需）使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：
 - **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，則它們之間按 OR 運算匹配，每個元素內的欄位（group、kind、version）之間按 AND 運算匹配。
 - **resourceMatchers[].group**：（可選）要篩選的資源群組。
 - **resourceMatchers[].kind**：（可選）要篩選的資源類型。
 - **resourceMatchers[].version**：（可選）要篩選的資源版本。
 - **resourceMatchers[].names**：（可選）要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
 - **resourceMatchers[].namespaces**：（可選）要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
 - **resourceMatchers[].labelSelectors**：（可選）資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如："trident.netapp.io/os=linux"。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 `trident-protect-backup-ipr-cr.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

將備份還原至不同的叢集

如果原始叢集出現問題、您可以將備份還原至不同的叢集。



- 當您使用 Kopia 作為資料移動工具還原備份時，您可以選擇在 CR 中指定註釋，以控制 Kopia 使用的暫存的行為。有關可配置選項的更多資訊，請參閱 ["Kopia 說明文件"](#)。
- 使用 CR 還原到新命名空間時，必須先手動建立目的地命名空間，然後再套用 CR。

開始之前

請確保符合下列先決條件：

- 目標叢集已安裝 Trident Protect。
- 目標叢集可以存取與來源叢集相同的 AppVault 儲存桶路徑，備份檔案就儲存在該路徑中。
- 請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的還原作業。如果權杖在還原作業期間過期、作業可能會失敗。
 - 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 文件"](#)。
 - 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS 文件"](#)。

步驟

1. 使用 Trident Protect CLI 外掛程式檢查目標叢集上 AppVault CR 的可用性：

```
tridentctl-protect get appvault --context <destination_cluster_name>
```



確保用於應用程式還原的命名空間存在於目的地叢集上。

2. 從目的地叢集檢視可用 AppVault 的備份內容：

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

執行此命令將顯示 AppVault 中的可用備份，包括其來源叢集、相應的應用程式名稱、時間戳記和歸檔路徑。

範例輸出：

```
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| CLUSTER | APP | TYPE | NAME | TIMESTAMP |
| PATH |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| production1 | wordpress | backup | wordpress-bkup-1 | 2024-10-30
08:37:40 (UTC) | backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2 | 2024-10-30
08:37:40 (UTC) | backuppath2 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

3. 使用 AppVault 名稱和歸檔路徑將應用程式還原到目標叢集：

4. 建立自訂資源（CR）檔案並將其命名為 trident-protect-backup-restore-cr.yaml。

5. 在您建立的檔案中、設定以下屬性：

- **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
- **spec.appVaultRef**：（必填）儲存備份內容的 AppVault 名稱。
- **spec.appArchivePath**：AppVault 內儲存備份內容的路徑。您可以使用以下命令尋找此路徑：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```




如果 BackupRestore CR 不可用，您可以使用步驟 2 中提到的指令來查看備份內容。

- **spec.namespaceMapping**：復原作業的來源命名空間到目標命名空間的對應。請將 `my-source-namespace` 和 `my-destination-namespace` 替換為您環境中的資訊。

例如：

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
    "my-destination-namespace"}]
```

6. 在 trident-protect-backup-restore-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

將快照還原至不同的命名空間

您可以使用自訂資源 (CR) 檔案從快照還原資料到不同的命名空間或原始來源命名空間。當您使用 SnapshotRestore CR 將快照還原到不同的命名空間時，NetApp Backup and Recovery 會將應用程式還原到新的命名空間，並為還原的應用程式建立一個應用程式 CR。為了保護還原的應用程式，您可以建立隨需備份或快照，或製定保護排程。



- SnapshotRestore 支援 spec.storageClassMapping 屬性，但僅當來源儲存類別和目標儲存類別使用相同的儲存後端時才支援。如果嘗試還原到使用不同儲存後端的 StorageClass，則還原操作將會失敗。
- 使用 CR 還原到新命名空間時，必須先手動建立目的地命名空間，然後再套用 CR。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期，則作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 文件"](#)。

步驟

1. 建立自訂資源 (CR) 檔案並將其命名為 trident-protect-snapshot-restore-cr.yaml。
2. 在您建立的檔案中，設定以下屬性：

- **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
- **spec.appVaultRef**：（必填）儲存快照內容的 AppVault 名稱。
- **spec.appArchivePath**：AppVault 內儲存快照內容的路徑。您可以使用以下命令來尋找此路徑：

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.namespaceMapping**：復原作業的來源命名空間到目標命名空間的對應。請將 `my-source-namespace` 和 `my-destination-namespace` 替換為您環境中的資訊。

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. （可選）如果您只需要選擇應用程式中的某些資源進行還原，請新增篩選條件，以包含或排除帶有特定標籤的資源：



Trident Protect 會自動選擇一些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持久卷聲明資源，並且它關聯了一個 pod，Trident Protect 也會恢復該關聯 pod。

- **resourceFilter.resourceSelectionCriteria**：（篩選必需）使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：
 - **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，則它們之間按 OR 運算匹配，每個元素內的欄位（group、kind、version）之間按 AND 運算匹配。
 - **resourceMatchers[].group**：（可選）要篩選的資源群組。
 - **resourceMatchers[].kind**：（可選）要篩選的資源類型。
 - **resourceMatchers[].version**：（可選）要篩選的資源版本。
 - **resourceMatchers[].names**：（可選）要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
 - **resourceMatchers[].namespaces**：（可選）要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
 - **resourceMatchers[].labelSelectors**：（可選）資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如：`"trident.netapp.io/os=linux"`。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 trident-protect-snapshot-restore-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

將快照還原至原始命名空間

您可以隨時將快照還原至原始命名空間。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期，則作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 文件"](#)。

步驟

1. 建立自訂資源（CR）檔案並將其命名為 trident-protect-snapshot-ipr-cr.yaml。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appVaultRef**：（必填）儲存快照內容的 AppVault 名稱。
 - **spec.appArchivePath**：AppVault 內儲存快照內容的路徑。您可以使用以下命令來尋找此路徑：

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
jsonpath='{.status.appArchivePath}'
```

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
```

3. (可選) 如果您只需要選擇應用程式中的某些資源進行還原，請新增篩選條件，以包含或排除帶有特定標籤的資源：



Trident Protect 會自動選擇一些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持久卷聲明資源，並且它關聯了一個 pod，Trident Protect 也會恢復該關聯 pod。

- **resourceFilter.resourceSelectionCriteria**：(篩選必需) 使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：
 - **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，則它們之間按 OR 運算匹配，每個元素內的欄位 (group、kind、version) 之間按 AND 運算匹配。
 - **resourceMatchers[].group**：(可選) 要篩選的資源群組。
 - **resourceMatchers[].kind**：(可選) 要篩選的資源類型。
 - **resourceMatchers[].version**：(可選) 要篩選的資源版本。
 - **resourceMatchers[].names**：(可選) 要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
 - **resourceMatchers[].namespaces**：(可選) 要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
 - **resourceMatchers[].labelSelectors**：(可選) 資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如： "trident.netapp.io/os=linux"。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 `trident-protect-snapshot-ipr-cr.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

使用進階自訂資源還原設定

您可以利用註釋、命名空間設定和儲存選項等進階設定來自訂還原作業，以滿足您的特定需求。

還原和容錯移轉作業期間的命名空間註釋和標籤

在還原和容錯移轉作業期間，目的地命名空間中的標籤和註釋會與來源命名空間中的標籤和註釋相符。來源命名空間中存在但目的地命名空間中不存在的標籤或註釋會被新增，而任何已存在的標籤或註釋則會被覆寫以符合來源命名空間中的值。僅存在於目的地命名空間中的標籤或註釋則保持不變。



如果您使用 Red Hat OpenShift，請務必注意命名空間註解在 OpenShift 環境中的關鍵作用。命名空間註解可確保復原的 Pod 遵循 OpenShift 安全上下文約束（SCC）定義的相應權限和安全性配置，並能無權限問題地存取磁碟區。如需更多資訊，請參閱 ["OpenShift 安全上下文約束文檔"](#)。

您可以透過在執行復原或故障轉移操作之前設定 Kubernetes 環境變數

`RESTORE_SKIP_NAMESPACE_ANNOTATIONS`，來防止目標命名空間中的特定註解被覆寫。例如：

```
helm upgrade trident-protect -n trident-protect netapp-trident-protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_key_to_skip_2>}" \
  --reuse-values
```



執行還原或容錯移轉作業時，`restoreSkipNamespaceAnnotations` 和 `restoreSkipNamespaceLabels` 中指定的任何命名空間註釋和標籤都會從還原或容錯移轉作業中排除。請確保在初始 Helm 安裝期間配置這些設定。若要深入瞭解，請參閱 ["設定其他 Trident Protect Helm Chart 設定"](#)。

如果您使用 Helm 並帶有 `--create-namespace` 標誌安裝了來源應用程式，則會對 `name` 標籤鍵進行特殊處理。在還原或容錯移轉過程中，Trident Protect 會將此標籤複製到目的地命名空間，但如果來源的值與來源命名空間相符，則會將值更新為目的地命名空間值。如果此值與來源命名空間不相符，則會將其複製到目的地命名空間而不做任何變更。

範例

以下範例展示了來源命名空間和目標命名空間，它們各自具有不同的註解和標籤。您可以查看操作前後目標命名空間的狀態，以及註解和標籤在目標命名空間中是如何組合或覆蓋的。

在還原或容錯移轉作業之前

下表說明了復原或容錯移轉作業之前範例來源命名空間和目標命名空間的狀態：

命名空間	註解	標籤
命名空間 ns-1 (來源)	• <code>annotation.one/key</code>: 「updatedvalue」 • <code>annotation.two/key</code>: 「true」	• <code>environment=production</code> • 合規性=hipaa • 名稱=ns-1
命名空間 ns-2 (目標)	• <code>annotation.one/key</code>: 「true」 • <code>annotation.three/key</code>: 「false」	• 角色=資料庫

還原作業後

下表展示了復原或故障轉移作業後範例目標命名空間的狀態。一些鍵已被添加，一些鍵已被覆蓋，並且 `name` 標籤已更新以匹配目標命名空間：

命名空間	註解	標籤
命名空間 ns-2 (目標)	• annotation.one/key: 「updatedvalue」 • annotation.two/key: 「true」 • annotation.three/key: 「false」	• 名稱=ns-2 • 合規性=hipaa • environment=production • 角色=資料庫

支援的欄位

本節說明可用於還原作業的其他欄位。

儲存類別對應

此 `spec.storageClassMapping` 屬性定義了從來源應用程式中的儲存類別到目標叢集上新儲存類別的對應。在將應用程式遷移到具有不同儲存類別的叢集之間，或變更 BackupRestore 操作的儲存後端時，可以使用此屬性。

- 範例：*

```
storageClassMapping:
- destination: "destinationStorageClass1"
  source: "sourceStorageClass1"
- destination: "destinationStorageClass2"
  source: "sourceStorageClass2"
```

支援的註釋

本節列出系統中用於配置各種行為的支援註解。如果使用者未明確設定註解，系統將使用預設值。

註解	類型	描述	預設值
protect.trident.netapp.io/data-mover-timeout-sec	字串	資料移動器操作允許停止的最長時間（以秒為單位）。	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	字串	Kopia 內容快取的大小上限（以 MB 為單位）。	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	字串	等待所有新建立的 PersistentVolumeClaims (PVC) 達到 `Bound` 階段的最長時間（以秒為單位），超過此時間操作將會失敗。適用於所有還原 CR 類型（BackupRestore、BackupInplaceRestore、SnapshotRestore、SnapshotInplaceRestore）。如果您的儲存後端或叢集通常需要更多時間，請使用更高的值。	"1200" (20 分鐘)

管理 Kubernetes 集群

NetApp Backup and Recovery使您能夠發現和管理 Kubernetes 集群，以便保護集群託管的資源。

所需的NetApp Console角色

組織管理員或SnapCenter管理員。["了解NetApp Backup and Recovery存取角色"](#)。["了解所有服務的NetApp Console存取角色"](#)。



要發現 Kubernetes 集群，請參閱["發現 Kubernetes 工作負載"](#)。

編輯 Kubernetes 叢集訊息

如果需要變更叢集名稱，您可以編輯叢集。

步驟

1. 在NetApp Backup and Recovery中，選擇 **Inventory > Clusters**。
2. 在群集清單中，選擇要編輯的群集並選擇相關的操作選單。
3. 選擇*編輯群集*。
4. 對叢集名稱進行任何必要的更改。叢集名稱需要與您在發現過程中使用 Helm 命令的名稱相符。
5. 選擇*完成*。

刪除 Kubernetes 集群

若要停止保護 Kubernetes 集群，請停用保護並刪除相關應用程序，然後從NetApp Backup and Recovery中刪除該集群。NetApp Backup and Recovery不會刪除叢集或其資源；它只會從NetApp Console清單中刪除叢集。

步驟

1. 在NetApp Backup and Recovery中，選擇 **Inventory > Clusters**。
2. 在群集清單中，選擇要編輯的群集並選擇相關的操作選單。
3. 選擇*刪除群集*。
4. 查看確認對話方塊中的信息，然後選擇*刪除*。

管理 Kubernetes 應用程式

NetApp Backup and Recovery讓您能夠取消保護並刪除 Kubernetes 應用程式及相關資源。

所需的NetApp Console角色

組織管理員或SnapCenter管理員。["了解NetApp Backup and Recovery存取角色"](#)。["了解所有服務的NetApp Console存取角色"](#)。

取消保護 Kubernetes 應用程式

如果您不再需要保護某個應用程序，可以取消保護。當您取消保護應用程式時，NetApp Backup and Recovery會停止保護該應用程序，但保留所有相關的備份和快照。



在應用程式的保護操作仍在進行時，您無法取消其保護。您可以等待操作完成，或作為變通方法，[刪除還原點](#)正在執行的保護操作正在使用。然後您就可以取消應用程式的保護。

步驟

1. 在NetApp Backup and Recovery中，選擇 **Inventory**。
2. 選擇一個 Kubernetes 實例，然後選擇「檢視」以查看與該實例關聯的資源。
3. 選擇“應用程式”標籤。
4. 在應用程式清單中，選擇要取消保護的應用程式並選擇相關的操作選單。
5. 選擇*取消保護*。
6. 閱讀通知，準備好後，選擇*取消保護*。

刪除 Kubernetes 應用程式

刪除不再需要的應用程式。NetApp Backup and Recovery停止保護並刪除已刪除應用程式的所有備份和快照。

步驟

1. 在NetApp Backup and Recovery中，選擇 **Inventory**。
2. 選擇一個 Kubernetes 實例，然後選擇「檢視」以查看與該實例關聯的資源。
3. 選擇“應用程式”標籤。
4. 在應用程式清單中，選擇要刪除的應用程式並選擇相關的操作選單。
5. 選擇*刪除*。
6. 啟用*刪除快照和備份*以刪除應用程式的所有快照和備份。



您將無法再使用這些快照和備份還原應用程式。

7. 確認操作並選擇*刪除*。

刪除 Kubernetes 應用程式的還原點

如果您需要取消應用程式的保護，並且目前正在執行保護操作，則可能需要刪除該應用程式的還原點。

步驟

1. 在 NetApp Backup and Recovery 選單中，選取 **還原**。
2. 從清單中選擇一個 Kubernetes 應用程式，然後選擇該應用程式的 **View and Restore**。

出現還原點清單。

3. 選擇您需要刪除的復原點，然後選取 Actions 圖示  > **Delete recovery point** 將其刪除。

管理適用於 Kubernetes 工作負載的NetApp Backup and Recovery執行掛鉤模板

執行鉤子是一種自訂操作，它與託管 Kubernetes 應用程式中的資料保護操作一起運行。例如，透過使用執行掛鉤在快照之前暫停資料庫事務並在之後恢復它們來建立應用程式一

致的快照。建立執行鉤子模板時，指定鉤子類型、要執行的腳本以及目標容器的過濾器。使用模板將執行掛鉤連結到您的應用程式。



NetApp Backup and Recovery 會在資料保護期間，為像 KubeVirt 這樣的應用程式凍結和解除凍結檔案系統。您可以透過 Trident Protect 文件，全域或針對特定應用程式停用此行為：

- 若要為所有應用程式停用此行為，請參閱 ["使用 KubeVirt 虛擬機器保護數據"](#)。
- 若要針對特定應用程式停用此行為，請參閱 ["定義應用程式"](#)。

所需的NetApp Console角色

組織管理員或SnapCenter管理員。["了解NetApp Backup and Recovery存取角色"](#)。["了解所有服務的NetApp Console存取角色"](#)。

執行鉤子的類型

NetApp Backup and Recovery根據運行時間支援以下類型的執行掛鉤：

- 預快照
- 快照後
- 預備份
- 備份後
- 恢復後

執行順序

當執行資料保護操作時，執行掛鉤事件會依照下列順序發生：

1. 任何適用的自訂預操作執行掛鉤都在適當的容器上運行。您可以建立多個自訂預操作掛鉤，但它們的執行順序無法保證或配置。
2. 如果適用，則會發生檔案系統凍結。
3. 執行資料保護操作。
4. 如果適用，凍結的檔案系統將被解凍。
5. NetApp Backup and Recovery在適當的容器上執行任何適用的自訂操作前執行掛鉤。您可以建立多個自訂後操作掛鉤，但它們的執行順序無法保證或配置。

如果建立多個相同類型的鉤子，則無法保證它們的執行順序。不同類型的鉤子總是按照指定的順序運行。例如，以下是具有所有不同類型鉤子的配置的執行順序：

1. 快照前鉤子執行
2. 快照後鉤子執行
3. 執行備份前掛鉤
4. 執行備份後鉤子



在生產中啟用執行掛鉤腳本之前對其進行測試。使用“`kubectl exec`”測試腳本，然後透過將應用程式複製到臨時命名空間並還原來驗證快照和備份。



如果快照前執行鉤子新增、變更或刪除 Kubernetes 資源，則這些變更將包含在快照或備份以及任何後續復原作業中。

關於自訂執行鉤子的重要說明

在為您的應用程式規劃執行掛鉤時，請考慮以下事項。

- 執行鉤子必須使用腳本來執行操作。許多執行鉤子可以引用同一個腳本。
- 執行鉤子需要以可執行shell腳本的格式編寫。
- 腳本大小限制為 96KB。
- 執行掛鉤設定和任何符合條件用於確定哪些掛鉤適用於快照、備份或還原操作。



執行掛鉤可以減少或停用應用程式功能。讓您的自訂鉤子盡快運行。如果您啟動具有相關執行掛鉤的備份或快照操作，但隨後取消它，則如果備份或快照操作已經開始，則仍允許掛鉤運行。這意味著備份後執行掛鉤中使用的邏輯不能假定備份已完成。

執行鉤子過濾器

當您為應用程式新增或編輯執行掛鉤時，您可以向執行掛鉤添加過濾器來管理該掛鉤將匹配哪些容器。過濾器對於在所有容器上使用相同容器鏡像但可能將每個鏡像用於不同目的的應用程式（例如 Elasticsearch）很有用。過濾器可讓您建立執行掛鉤在某些（但不一定是所有）相同的容器上運行的場景。如果為單一執行掛鉤建立多個篩選器，它們將透過邏輯 AND 運算子組合在一起。每個執行掛鉤最多可以有 10 個活動過濾器。

新增到執行掛鉤的每個過濾器都使用正規表示式來匹配叢集中的容器。當鉤子與容器匹配時，鉤子將在該容器上運行其關聯的腳本。過濾器的正規表示式使用正規表示式 2 (RE2) 語法，該語法不支援建立從符合清單中排除容器的過濾器。有關NetApp Backup and Recovery在執行鉤子過濾器中支援的正規表示式的語法的信息，請參見 "[正規表示式 2 \(RE2\) 語法支持](#)"。



如果將命名空間過濾器新增至在復原或複製作業後執行的執行掛鉤，且復原或複製來源和目標位於不同的命名空間中，則命名空間篩選器僅適用於目標命名空間。

執行鉤子範例

訪問 "[NetApp Verda GitHub 項目](#)"下載流行應用程式（如 Apache Cassandra 和 Elasticsearch）的真實執行掛鉤。您還可以查看範例並獲得建立自己的自訂執行掛鉤的想法。

建立執行鉤子模板

您可以建立自訂執行掛鉤模板，用於在應用程式上執行資料保護操作之前或之後執行操作。



您在此處建立的範本僅可用於保護 Kubernetes 工作負載。

步驟

1. 在控制台中，前往*保護*>*備份和還原*。

2. 選擇“設定”標籤。
3. 展開*執行鉤子模板*部分。
4. 選擇*建立執行鉤子模板*。
5. 輸入執行掛鉤的名稱。
6. （可選）選擇一種鉤子類型。例如，還原後鉤子會在還原作業完成後執行。
7. 在 **Script** 文字方塊中，輸入要作為執行掛鉤範本的一部分執行的可執行 shell 腳本。或者，您可以選擇“上傳腳本”來上傳腳本檔案。
8. 選擇“創建”。

建立模板後，它將出現在*執行掛鉤模板*部分的模板清單中。

監控NetApp Backup and Recovery中的作業

使用NetApp Backup and Recovery作業。追蹤您啟動的恢復作業。查看已完成、正在進行或失敗的作業以協助診斷問題。在NetApp Console通知中心啟用電子郵件通知，以便在未登入時隨時了解系統活動。使用控制台時間軸查看從 UI 或 API 啟動的所有操作的詳細資訊。

NetApp Backup and Recovery會將作業資訊保留 15 天，然後刪除作業資訊並將其從作業監視器移除。

所需的**NetApp Console**角色 儲存檢視器、備份和還原超級管理員、備份和還原備份管理員、備份和還原復原管理員、備份和還原複製管理員或備份和還原檢視器角色。了解詳情["備份和恢復角色和權限"](#)。 ["了解所有服務的NetApp Console存取角色"](#)。

在作業監視器上查看作業狀態

您可以在「作業監控」標籤中查看所有快照、複製、備份到物件儲存和復原作業的清單及其目前狀態。這包括來自您的Cloud Volumes ONTAP、本地ONTAP、應用程式和虛擬機器的操作。每個操作或作業都有唯一的 ID 和狀態。

狀態可以是：

- 成功
- 進行中
- 排隊
- 警告
- 失敗的

您從NetApp Backup and RecoveryUI 和 API 啟動的快照、複製、物件儲存備份和還原作業均可在「作業監控」標籤中找到。



如果您已將ONTAP系統升級至 9.13.x，但在作業監視器中沒有看到正在進行的排程備份作業，請重新啟動NetApp Backup and Recovery。 ["了解如何重新啟動NetApp Backup and Recovery"](#)。

1. 從NetApp Backup and Recovery選單中，選擇 監控。
2. 若要顯示其他欄位（系統、SVM、使用者名稱、工作負載、政策名稱、快照標籤），請選擇加號。

搜尋並過濾職位列表

您可以使用多個篩選器在「作業監控」頁面上篩選操作，例如政策、快照標籤、操作類型（保護、復原、保留或其他）和保護類型（本機快照、複製或備份到雲端）。

預設情況下，「作業監控」頁面顯示過去 24 小時的保護和復原作業。您可以使用時間範圍篩選器變更時間範圍。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 監控。
2. 若要對結果進行不同的排序，請選擇每個列標題以按狀態、開始時間、資源名稱等進行排序。
3. 如果您正在尋找特定的工作，請選擇「進階搜尋和過濾」區域以開啟「搜尋」面板。

使用此面板可以輸入任何資源的自由文字搜尋；例如“卷 1”或“應用程式 3”。您也可以根據下拉式選單中的項目過濾作業清單。

大多數的過濾器都是不言自明。透過「工作量」篩選器，您可以查看以下類別的作業：

- ONTAP磁碟區（Cloud Volumes ONTAP和本機ONTAP磁碟區）
- 微軟 SQL 伺服器
- 虛擬機
- Kubernetes



- 只有當您先選擇了一個系統後，您才可以在特定的「SVM」中搜尋資料。
- 只有當您選擇了「保護」的「類型」時，您才可以使用「保護類型」過濾器進行搜尋。

4. 若要立即更新頁面，請選擇  按鈕。否則，此頁面每 15 分鐘刷新一次，以便您始終看到最新的工作狀態結果。

查看職位詳情

您可以查看與特定已完成作業相對應的詳細資訊。您可以以 JSON 格式匯出特定作業的詳細資訊。

您可以查看作業類型（計劃或按需）、SnapMirror備份類型（初始或定期）、開始和結束時間、持續時間、從系統到物件儲存的傳輸資料量、平均傳輸速率、政策名稱、啟用的保留鎖、執行的勒索軟體掃描、保護來源詳細資訊和保護目標詳細資訊等詳細資訊。

復原作業顯示詳細信息，例如備份目標提供者（Amazon Web Services、Microsoft Azure、Google Cloud、本機）、S3 儲存桶名稱、SVM 名稱、來源磁碟區名稱、目標磁碟區、快照標籤、還原的物件數、檔案名稱、檔案大小、上次修改日期和完整檔案路徑。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 監控。
2. 選擇作業的名稱。

3. 選擇“操作”選單...並選擇“查看詳細資料”。

4. 展開每個部分以查看詳細資訊。

下載作業監控結果報告

您可以在篩選或排序結果後將主作業監控頁面的內容下載為報表。NetApp Backup and Recovery會產生並下載一個 .CSV 文件，您可以根據需要查看該文件並傳送給其他群組。 .CSV 檔案包含最多 10,000 行資料。

從作業監控詳細資訊中，您可以下載包含單一作業詳細資訊的 JSON 檔案。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 監控。
2. 若要下載所有作業的 CSV 文件，請選擇「下載」按鈕並在下載目錄中找到該文件。
3. 若要下載單一作業的 JSON 文件，請選擇「操作」選單...對於該作業，選擇*下載 JSON 檔案*，然後在下載目錄中找到該檔案。

檢討保留（備份生命週期）作業

監控保留（備份生命週期）流程以檢查備份、確保其安全並支援稽核。確定備份副本何時過期以追蹤生命週期。

備份生命週期作業追蹤所有已刪除或正在排隊等待刪除的快照。從ONTAP 9.13 開始，您可以在「作業監控」頁面上查看所有名為「保留」的作業類型。

「保留」作業類型會擷取在受NetApp Backup and Recovery保護的磁碟區上啟動的所有快照刪除作業。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 監控。
2. 選擇“進階搜尋和過濾”區域以開啟搜尋面板。
3. 選擇“保留”作為工作類型。

在NetApp Console通知中心查看備份和還原警報

NetApp Console通知中心追蹤您啟動的備份和復原作業的進度，以便您可以驗證作業是否成功。

您可以在通知中心查看警報，並配置控制台以發送重要系統活動的電子郵件警報，即使您未登入。 ["了解有關通知中心以及如何發送備份和恢復作業警報電子郵件的更多信息"](#)。

通知中心會顯示大量的快照、複製、雲端備份和復原事件，但只有某些事件會觸發電子郵件警報：

操作類型	事件	已產生警報	電子郵件已發送
啟用設定	系統備份和恢復啟動失敗	是的	是的
啟用設定	系統備份和恢復編輯失敗	是的	是的
啟用設定	磁碟區現在與快照策略關聯	是的	是的
啟用設定	磁碟區備份或狀態已修改	是的	是的
啟用設定	系統備份和恢復啟動成功	是的	是的

操作類型	事件	已產生警報	電子郵件已發送
啟用設定	臨時磁碟區備份失敗	是的	是的
啟用設定	臨時卷備份成功	是的	不
啟用設定	多磁碟區備份失敗	是的	是的
定時任務	檢查是否缺少快照標籤	是的	是的
定時任務	未能向ONTAP發送此系統的安全令牌	是的	是的
酒吧/訂閱活動	連線失敗	是的	不
酒吧/訂閱活動	刪除計劃快照失敗	是的	不
酒吧/訂閱活動	卷的計劃備份失敗	是的	不
酒吧/訂閱活動	卷恢復成功。	是的	不
酒吧/訂閱活動	磁碟區恢復失敗	是的	不
勒索軟體	備份副本上發現潛在勒索軟體攻擊	是的	是的
勒索軟體	該系統的備份副本上偵測到潛在的勒索軟體攻擊	是的	是的
本地快照	NetApp Backup and Recovery快照建立作業失敗	是的	是的
複製	修改複製關係以克服容量故障	是的	是的
複製	NetApp Backup and Recovery暫時複製作業失敗	是的	是的
複製	NetApp Backup and Recovery與復原複製暫停作業失敗	是的	不
複製	NetApp Backup and Recovery複製中斷作業失敗	是的	不
複製	NetApp Backup and Recovery重新同步作業失敗	是的	不
複製	NetApp Backup and Recovery與復原複製停止作業失敗	是的	不
複製	NetApp Backup and Recovery反向重新同步作業失敗	是的	是的
複製	NetApp Backup and Recovery複製刪除作業失敗	是的	是的
目標行動	恢復到本機或雲端目標故障	是的	是的
目標行動	按需恢復失敗	是的	是的
系統操作	臨時磁碟區快照建立失敗	是的	是的



從ONTAP 9.13.0 開始，所有警報都會出現在Cloud Volumes ONTAP和本地ONTAP系統中。對於具有Cloud Volumes ONTAP 9.13.0 和本機ONTAP 的系統，僅出現與「復原作業已完成，但有警告」相關的警報。

預設情況下，NetApp Console組織和帳戶管理員會收到所有「嚴重」和「建議」警報的電子郵件。預設情況下，系統不會設定其他使用者和收件者接收通知郵件。為NetApp雲端帳戶中的任何控制台使用者或需要了解備份和復原活動的其他收件者配置電子郵件警報。

若要接收NetApp Backup and Recovery電子郵件警報，您需要在通知設定頁面中選擇通知嚴重性類型「嚴重」、「警告」和「錯誤」。

["了解如何傳送備份和復原作業的警報電子郵件"](#)。

步驟

1. 從控制台選單中，選擇  。
2. 查看通知。

在控制台時間軸中查看操作活動

您可以在控制台時間軸中查看備份和復原作業的詳細資訊以進行進一步調查。控制台時間軸提供每個事件的詳細信息，無論是用戶發起的還是系統發起的，並顯示在 UI 中或透過 API 發起的操作。

["了解時間軸和通知中心之間的區別"](#)。

重新啟動NetApp Backup and Recovery

在某些情況下，您可能需要重新啟動NetApp Backup and Recovery。

控制台代理程式包括NetApp Backup and Recovery功能。

步驟

1. 連接到控制台代理正在運行的 Linux 系統。

控制台代理位置	程式
雲端部署	按照說明進行操作 "連接到控制台代理 Linux 虛擬機" 取決於您使用的雲端提供者。
手動安裝	登入Linux系統。

2. 輸入命令重啟服務。

控制台代理位置	Docker 指令	Podman 指令
雲端部署	<code>docker restart cloudmanager_cbs</code>	<code>podman restart cloudmanager_cbs</code>
手動安裝（需連網）	<code>docker restart cloudmanager_cbs</code>	<code>podman restart cloudmanager_cbs</code>
無需互聯網訪問即可手動安裝	<code>docker restart ds_cloudmanager_cbs_1</code>	<code>podman restart ds_cloudmanager_cbs_1</code>

版權資訊

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

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

NetApp 保留隨時變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。