



開始

NetApp Backup and Recovery

NetApp
February 17, 2026

This PDF was generated from <https://docs.netapp.com/zh-tw/data-services-backup-recovery/concept-backup-to-cloud.html> on February 17, 2026. Always check docs.netapp.com for the latest.

目錄

開始	1
了解NetApp Backup and Recovery	1
NetApp Backup and Recovery	1
使用NetApp Backup and Recovery的優勢	2
成本	3
授權	4
支援的工作負載、系統和備份目標	4
NetApp Backup and Recovery的工作原理	5
可能對您使用NetApp Backup and Recovery有幫助的術語	6
NetApp Backup and Recovery前提條件	7
ONTAP 9.8 及更高版本的先決條件	7
備份到物件儲存的先決條件	7
保護 Microsoft SQL Server 工作負載的要求	7
保護 VMware 工作負載的要求	8
保護 KVM 工作負載的要求	8
保護 Oracle 資料庫工作負載的要求	9
保護 Kubernetes 應用程式的要求	9
保護 Hyper-V 工作負載的要求	10
在NetApp Console中	11
設定NetApp Backup and Recovery 的許可	11
30天免費試用	12
使用NetApp Backup and Recovery PAYGO 訂閱	12
使用年度合約	13
使用NetApp Backup and RecoveryBYOL 許可證	14
超出授權容量	14
在NetApp Backup and Recovery中為StorageGRID和ONTAP設定安全性證書	14
為StorageGRID建立安全性證書	14
為ONTAP建立安全性證書	18
為ONTAP和StorageGRID建立證書	21
在使用NetApp Backup and Recovery之前設定備份目標	22
準備備份目標	22
設定 S3 權限	23
登入NetApp Backup and Recovery	25
在NetApp Backup and Recovery中發現異地備份目標	25
發現備份目標	25
為備份目標新增儲存桶	27
更改備份目標的憑證	28
切換到不同的NetApp Backup and Recovery工作負載	28
切換到不同的工作負載	28

配置NetApp Backup and Recovery設置	29
為主機資源新增憑證	29
維護 VMware vCenter 設定	31
匯入並管理SnapCenter主機資源	31
新增 KVM 管理平台	33
在 Windows 主機的快照中設定日誌目錄	33
建立執行鉤子模板	33
在 NetApp Backup and Recovery 中設定基於角色的存取控制	34
相關資訊	35

開始

了解NetApp Backup and Recovery

NetApp Backup and Recovery是一種資料服務，可為您的所有ONTAP工作負載（包括磁碟區、資料庫、虛擬機器和 Kubernetes 工作負載）提供高效率、安全且經濟高效的資料保護。

所有ONTAP系統都已內建備份和復原的支持，因此無需額外的硬體、軟體授權或媒體網關。這使得備份操作變得簡單且經濟高效。NetApp Console簡化了任何備份策略的實施，包括所有 3-2-1 備份變體，而無需多個資源管理器或專業人員。



有關保護 VMware、KVM、Hyper-V 和 Kubernetes 工作負載的文件以技術預覽的形式提供。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。

NetApp Backup and Recovery

使用NetApp Backup and Recovery實現以下目標：

- *** ONTAP磁碟區工作負載***：
 - 建立本機快照，複製到二級存儲，並將ONTAP磁碟區從本機ONTAP或Cloud Volumes ONTAP系統備份到公有或私有雲帳戶中的物件儲存。
 - 建立區塊級、增量永久備份，並將其儲存在另一個ONTAP叢集和雲端中的物件儲存中。
 - 將NetApp Backup and Recovery與SnapCenter一起使用。
 - 參考["保護ONTAP卷"](#)。
- **Microsoft SQL Server 工作負載：**
 - 從本機ONTAP、Cloud Volumes ONTAP或Amazon FSx for NetApp ONTAP備份 Microsoft SQL Server 執行個體和資料庫。
 - 還原 Microsoft SQL Server 資料庫。
 - 克隆 Microsoft SQL Server 資料庫。
 - 不使用SnapCenter即可使用NetApp Backup and Recovery。
 - 參考["保護 Microsoft SQL Server 工作負載"](#)。
- **VMware 工作負載（使用新 UI 預覽，無需SnapCenter Plug-in for VMware vSphere）***：
 - 使用NetApp Backup and Recovery保護您的 VMware VM 和資料儲存。
 - 將 VMware 工作負載備份到 Amazon Web Services S3 或StorageGRID（預覽版）。
 - 將 VMware 資料從雲端還原到本機 vCenter。
 - 您可以將虛擬機器還原到與備份完全相同的位置或其他位置。
 - 使用NetApp Backup and Recovery，無需SnapCenter Plug-in for VMware vSphere。
 - 參考["保護 VMware 工作負載"](#)。
- **VMware 工作負載（使用SnapCenter Plug-in for VMware vSphere）**

- 將虛擬機器和資料儲存備份到 Amazon Web Services S3、Microsoft Azure Blob、Google Cloud Platform 和 StorageGRID，並將虛擬機器還原回 SnapCenter Plug-in for VMware vSphere。
- 使用 NetApp Backup and Recovery 將虛擬機器資料從雲端還原到本機 vCenter。您可以將虛擬機器還原到與備份完全相同的位置或其他位置。
- 將 NetApp Backup and Recovery 與適用於 SnapCenter Plug-in for VMware vSphere 一起使用。
- 參考 ["保護 VMware 工作負載"](#)。
- KVM 工作負載（預覽版）
 - 備份和還原虛擬機
 - 備份 KVM 儲存池
 - 使用保護組管理備份任務
 - 參考 ["保護 KVM 工作負載"](#)。
- Hyper-V 工作負載（預覽版）
 - 備份和還原虛擬機
 - 使用保護組管理備份任務
 - 參考 ["保護 Hyper-V 工作負載"](#)。
- **Oracle Database** 工作負載（預覽）：
 - 備份和還原資料庫和日誌
 - 使用保護組管理備份任務
 - 建立策略來管理資料庫和日誌備份
 - 使用 3-2-1 備份架構保護資料庫
 - 配置備份保留
 - 掛載和卸載 ARCHIVELOG 備份
 - 請參閱 ["保護 Oracle Database 工作負載"](#)。
- Kubernetes 工作負載（預覽版）
 - 在一個地方管理和保護您的 Kubernetes 應用程式和資源。
 - 使用保護策略來建立增量備份。
 - 將應用程式和資源恢復到相同或不同的叢集和命名空間。
 - 不使用 SnapCenter 即可使用 NetApp Backup and Recovery。
 - 參考 ["保護 Kubernetes 工作負載"](#)。

使用 NetApp Backup and Recovery 的優勢

NetApp Backup and Recovery 有以下優勢：

- 高效率：NetApp Backup and Recovery 執行區塊級、永久增量複製，從而顯著減少複製和儲存的資料量。這有助於最大限度地減少網路流量和儲存成本。
- 安全性：NetApp Backup and Recovery 對傳輸中和靜止的資料進行加密，並使用安全通訊協定來保護您的資料。

- 經濟高效：NetApp Backup and Recovery使用您的雲端帳戶中可用的成本最低的儲存層，有助於降低成本。
- 自動化：NetApp Backup and Recovery根據預先定義的計畫自動產生備份，這有助於確保您的資料受到保護。
- 靈活：NetApp Backup and Recovery使您能夠將資料恢復到相同或不同的系統，從而為資料恢復提供了靈活性。

成本

NetApp不會向您收取試用版的使用費用。但是，您需要承擔與您使用的雲端資源相關的費用，例如儲存和資料傳輸費用。

使用NetApp Backup and Recovery與ONTAP系統的備份到物件功能有兩種類型的成本：

- 資源費用
- 服務費

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

對於ONTAP磁碟區工作負載，您只需為受物件儲存保護的磁碟區付費。費用是根據來源ONTAP磁碟區在應用效率之前使用的邏輯容量計算的，也稱為前端 TB（FETB）。

對於 Kubernetes 工作負載，費用是根據所有持續磁碟區的總大小計算的。

對於所有其他工作負載，您需要為至少保護到一個輔助儲存目標或物件儲存目標的資源付費。費用是根據來源工作負載的邏輯大小計算的。對於資料庫而言，這意味著資料庫的大小；對於虛擬機器而言，這意味著虛擬機器的

大小。

備份和復原服務有三種付費方式：

- 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。
- 第二種選擇是購買年度合約。
- 第三種選擇是直接從NetApp購買授權。請參閱 [授權](#) 詳情請見相關章節。

授權

NetApp Backup and Recovery提供免費試用版，讓您在限定時間內無需許可證金鑰即可使用。

只有涉及物件儲存的備份和復原作業才需要備份許可證。建立快照和複製磁碟區不需要許可證。

您可以從三種授權選項中進行選擇：

- 自帶授權 (**BYOL**)：從NetApp購買基於期限（1 年、2 年或 3 年）和基於容量（以 1-TiB 為增量）的授權。在NetApp Console中輸入提供的序號進行啟動。該許可證涵蓋您組織中的所有來源系統。當期限或容量達到限制時，需要續約。
- 按需付費 (**PAYGO**)：透過雲端服務供應商的市場訂閱，並按備份資料的 GiB 數量付費，按月計費。無需預付任何費用。首次註冊即可享 30 天免費試用。更多信息，請參閱 "[使用NetApp Backup and Recovery按需付費訂閱](#)"。
- 年度合約：可透過 AWS 和 Azure Marketplace 購買，期限為 1 年、2 年或 3 年。現有兩份年度合約可供選擇：
 - 雲端備份：備份Cloud Volumes ONTAP和本地ONTAP資料。
 - **CVO** 專業版：捆綁了Cloud Volumes ONTAP和NetApp Backup and Recovery，Cloud Volumes ONTAP磁碟區可進行無限備份（備份容量不計入許可證）。
 - CVO 專業版方案包含兩種收費方式：
 - 資源費用：依儲存使用情況而定。更多信息，請參閱 "[Cloud Volumes ONTAP的許可](#)"。
 - 服務費用：NetApp Backup and Recovery費用。但是，如果來源磁碟區位於使用 CVO 專業方案的儲存系統中，則NetApp Backup and Recovery是免費提供的。

當您使用 Google Cloud Platform 時，請向NetApp申請私有報價，並在 Google Cloud Marketplace 啟用時選擇您的套餐。

["了解如何設定許可證"](#)。

支援的工作負載、系統和備份目標

支援的工作負載

NetApp Backup and Recovery可保護下列類型的工作負載：

- ONTAP卷
- 儲存在實體磁碟和 VMware 虛擬機器磁碟 (VMDK) 上的 Microsoft SQL Server 執行個體和資料庫，透過 VMFS 或 NFS 檔案系統進行儲存。
- VMware 虛擬機器與資料儲存區

- KVM 工作負載（預覽）
- Hyper-V 工作負載（預覽版）
- Oracle 資料庫工作負載（預覽版）
- Kubernetes 工作負載（預覽版）

支援的系統

- 本地部署的ONTAP SAN（iSCSI 協定）和 NAS（使用 NFS 和 CIFS 協定），ONTAP版本需為 9.8 或更高版本。
- 適用於 AWS 的Cloud Volumes ONTAP 9.8 或更高版本（使用 SAN 和 NAS）
- 適用於 Google Cloud Platform 的Cloud Volumes ONTAP 9.8 或更高版本（使用 NFS 和 CIFS 協定）
- 適用於 Microsoft Azure 的Cloud Volumes ONTAP 9.8 或更高版本（使用 SAN 和 NAS）
- Amazon FSx for NetApp ONTAP（僅限 Microsoft SQL Server 工作負載）

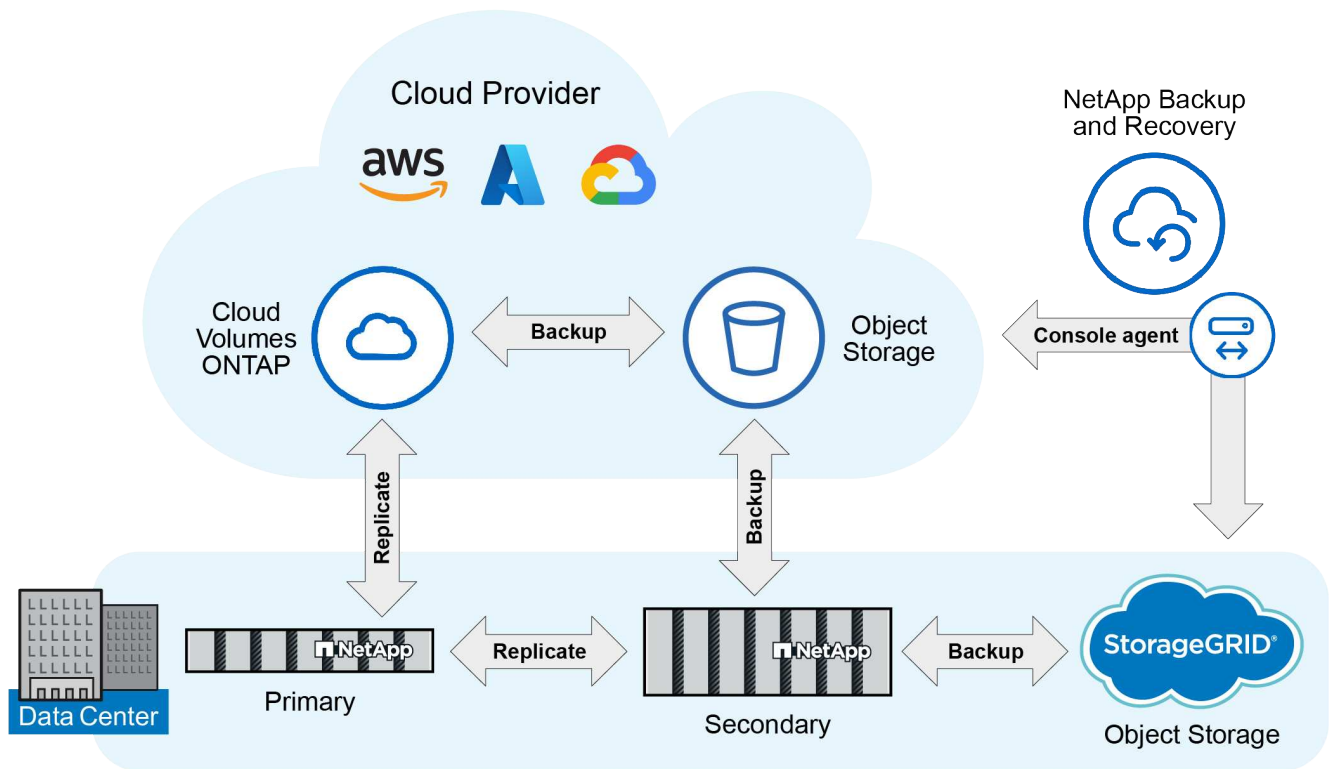
支援的備份目標

- 亞馬遜網路服務（AWS）S3
- Google 雲端儲存
- Microsoft Azure Blob（預覽版不適用於 VMware 工作負載）
- StorageGRID
- ONTAP S3（預覽版不適用於 VMware 工作負載）

NetApp Backup and Recovery的工作原理

當您啟用NetApp Backup and Recovery，本服務會為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備份。這使得網路流量保持最低限度。

下圖顯示了組件之間的關係。



還支援從主存儲到對象存儲，而不僅僅是從二級存儲到對象存儲。

備份在物件儲存位置的位置

備份副本儲存在NetApp Console在您的雲端帳戶中建立的物件儲存中。每個叢集或系統都有一個物件儲存，控制台以如下方式命名該物件儲存：`netapp-backup-clusteruuid`。請確保不要刪除此物件儲存。

- 在 AWS 中，NetApp Console可以實現以下功能：["Amazon S3 阻止公共存取功能"](#)在 S3 鏟斗上。
- 在 Azure 中，NetApp Console使用包含 Blob 容器儲存帳戶的新建或現有資源群組。["阻止公眾存取您的 Blob 數據"](#)預設情況下。
- 在StorageGRID中，控制台使用現有的儲存帳戶作為物件儲存桶。
- 在ONTAP S3 中，控制台使用 S3 儲存桶的現有使用者帳戶。

備份副本與您的NetApp Console組織相關聯

備份副本與控制台代理程式所在的NetApp Console組織相關聯。["了解NetApp Console身份和訪問"](#)。

如果同一個NetApp Console組織中有多個控制台代理，則每個控制台代理都會顯示相同的備份清單。

可能對您使用NetApp Backup and Recovery有幫助的術語

了解一些與保護相關的術語可能會對您有所幫助。

- **保護**：NetApp Backup and Recovery中的保護意味著確保使用保護策略定期將快照和不可變備份傳送到不同的安全域。

- 工作負載：NetApp Backup and Recovery中的工作負載可以包括ONTAP磁碟區、Microsoft SQL Server 執行個體和資料庫；VMware VM 和資料儲存區；或 Kubernetes 叢集和應用程式。

NetApp Backup and Recovery前提條件

透過驗證操作環境、NetApp Console代理程式和NetApp Console帳戶的準備情況，開始使用NetApp Backup and Recovery。要使用NetApp Backup and Recovery，您需要滿足這些先決條件。

ONTAP 9.8 及更高版本的先決條件

必須在本機ONTAP實例上啟用ONTAP One 授權。

備份到物件儲存的先決條件

若要使用物件儲存作為備份目標，您需要一個具有 AWS S3、Microsoft Azure Blob、StorageGRID或ONTAP 的帳戶並配置適當的存取權限。

- ["保護您的ONTAP卷數據"](#)

保護 Microsoft SQL Server 工作負載的要求

若要將NetApp Backup and Recovery用於 Microsoft SQL Server 工作負載，您需要滿足下列主機系統、空間和大小調整前提條件。

物品	要求
作業系統	Microsoft Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具" 。
Microsoft SQL Server 版本	VMware 虛擬機器檔案系統 (VMFS) 和 VMware 虛擬機器磁碟 (VMDK) NFS 支援 2012 及更高版本。
SnapCenter伺服器版本	如果要將現有資料從SnapCenter匯入NetApp Backup and Recovery，則需要SnapCenter Server 5.0 或更高版本。  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。看 "從SnapCenter匯入資源的先決條件"。
SQL Server 主機上插件的最小 RAM	1GB
SQL Server 主機上插件的最小安裝和日誌空間	5GB 分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於執行的備份次數和資料保護操作的頻率。如果沒有足夠的空間，則不會為操作建立日誌。

物品	要求
所需軟體包	• ASP.NET Core Runtime 8.0.23 Hosting Bundle（以及所有後續的 8.0.x 修補程式） • PowerShell 7.4.13 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

保護 VMware 工作負載的要求

您需要特定的要求來發現和保護您的 VMware 工作負載。

軟體支援

- 支援 NFS 和 VMFS 資料儲存。
- 支援的 NFS 版本：NFS 3 和 NFS 4.1
- 支援的 VMware ESXi Server 版本：7.0U1 以上
- 支援的 VMware vCenter vSphere 版本：7.0U1 及以上
- IP 位址：IPv4 和 IPv6
- VMware TLS：1.2、1.3
- 支援的連線儲存設備：ONTAP 9.13 或更新版本

保護 VMware 工作負載的連線和連接埠需求

連接埠類型	預配置連接埠
VMware ESXi 伺服器連接埠	443 (HTTPS)，雙向。來賓檔案復原功能使用此連接埠。
儲存叢集或儲存虛擬機器端口	443 (HTTPS)，雙向。80 (HTTP)，雙向。此連接埠用於虛擬設備與儲存虛擬機器或包含儲存虛擬機器的叢集之間的通訊。

保護 VMware 工作負載的基於角色的存取控制 (RBAC) 要求

vCenter 管理員帳號必須具有所需的 vCenter 權限。

有關所需 vCenter 權限的列表，請參閱 ["SnapCenter Plug-in for VMware vSphere vCenter 權限"](#)。

保護 KVM 工作負載的要求

您需要特定的要求來發現和保護 KVM 虛擬機器。

- 運行核心版本 5.14.0-503.22.1.el9_5.x86_64（長期）或更高版本的現代 Linux 發行版
- 您的 KVM 主機和虛擬機器必須由管理平台進行管理。NetApp Backup and Recovery 支援以下管理平台：
 - Apache CloudStack 4.22.0.0
- 確保允許從控制台代理到 KVM 主機的入站網路流量到達連接埠 22。

- QEMU Guest Agent 版本 9.0.0 或更高版本
- libvirt 版本 10.5.0 或更高版本



為確保 KVM 工作負載復原成功完成，請確保在用於 KVM 備份的保護策略中啟用「啟用 VM 一致性快照」設定。

若要啟用對非 root 使用者管理的 KVM 虛擬機器的保護，請依照下列步驟操作：

1. 將磁碟區掛載為 NFS3 類型，以避免使用 nobody 使用者和群組。
2. 使用以下命令將非root使用者新增至 qemu 在保留現有群體的同時，組成新的群體：

```
usermod -aG qemu <non-root-user>
```



3. 使用以下命令將掛載路徑的所有權授予... qemu 使用者和群組，並更改掛載路徑的權限：

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771  
<kvm_vm_mount_path>
```

4. 如果存在 NetApp_SnapCenter_Backups 目錄，請將其刪除。

保護 Oracle 資料庫工作負載的要求

確保您的環境符合發現和保護 Oracle 資源的特定要求。

- Oracle 資料庫：
 - Oracle 19C 和 21C 在獨立部署中支援。
 - Oracle 資料庫必須部署在主或輔助NetApp ONTAP儲存中。
 - 主機作業系統支援： Red Hat Enterprise Linux 8 和 9
- 對象存儲支援：
 - Azure 物件儲存
 - 亞馬遜 AWS
 - NetAppStorageGRID
 - ONTAP S3

保護 Kubernetes 應用程式的要求

您需要特定的要求來發現 Kubernetes 資源並保護您的 Kubernetes 應用程式。

有關NetApp Console要求，請參閱[在NetApp Console中](#)。

- 主ONTAP系統（ONTAP 9.16.1 或更高版本）

- Kubernetes 叢集 - 支援的 Kubernetes 發行版和版本包括：
 - Anthos On-Prem (VMware) 和 Anthos on Bare Metal 1.16
 - Kubernetes 1.27 - 1.33
 - OpenShift 4.10 - 4.18
 - Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1、v1.28.5+rke2r1
 - Suse Rancher
- NetApp Trident 24.10 或更高版本
- NetApp Trident Protect 25.07 或更新版本（在 Kubernetes 工作負載探索期間安裝）
- NetApp Trident Protect Connector 25.07 或更新版本（在 Kubernetes 工作負載探索期間安裝）
 - 確保 Kubernetes 叢集、Trident Protect Connector 和 Trident Protect Proxy 之間的出站方向 TCP 連接埠 443 未被過濾。

保護 Hyper-V 工作負載的要求

確保您的 Hyper-V 執行個體符合發現和保護虛擬機器的特定要求。

- Hyper-V Windows Server 主機的軟體需求：
 - Microsoft Hyper-V 2019、2022 及 2025 年版本
 - ASP.NET Core Runtime 8.0.23 Hosting Bundle（以及所有後續的 8.0.x 修補程式）
 - PowerShell 7.4.13 或更高版本
 - 如果非管理員網域使用者要保護 Hyper-V 虛擬機，請確保使用者擁有下列權限：
 - 請確保該使用者是本機管理員群組成員。
 - 確保使用者已加入「以服務身分登入」本機安全性原則。
 - 確保 Windows 防火牆設定中允許下列連接埠進行雙向 HTTPS 通訊：
 - 8144（適用於 Hyper-V 的 NetApp 插件）
 - 8145（適用於 Windows 的 NetApp 插件）
- Hyper-V 主機的硬體需求：
 - 支援獨立主機和 FCI 叢集主機
 - Hyper-V 主機上的 NetApp Hyper-V 插件至少需要 1GB RAM
 - Hyper-V 主機上插件的最低安裝和日誌空間為 5GB



確保在 Hyper-V 主機上為日誌資料夾分配足夠的磁碟空間並定期監控其使用情況。所需空間取決於備份和資料保護操作發生的頻率。如果空間不足，則不會產生日誌。

- NetApp ONTAP 設定需求：
 - 主 ONTAP 系統（ONTAP 9.14.1 或更高版本）
 - 對於使用 CIFS 共用儲存虛擬機器資料的 Hyper-V 部署，請確保在 ONTAP 系統上啟用了連續可用性共用屬性。請參閱 ["ONTAP 文檔"](#) 以取得說明。

在NetApp Console中

確保NetApp Console符合以下要求。

- 控制台使用者應具有對 Microsoft SQL Server 和 Kubernetes 工作負載執行操作所需的角色和權限。要發現資源，您必須具有NetApp Backup and Recovery超級管理員角色。看["NetApp Backup and Recovery基於角色的功能訪問"](#)有關在NetApp Backup and Recovery中執行操作所需的角色和權限的詳細資訊。
- 具有至少一個活動控制台代理的控制台組織，該代理連接到本地ONTAP叢集或Cloud Volumes ONTAP。
- 至少一個具有NetApp本地ONTAP或Cloud Volumes ONTAP叢集的控制台系統。
- 控制台代理

參考 ["了解如何配置控制台代理"](#)和 ["標準NetApp Console要求"](#)。

- 預覽版需要 Ubuntu 22.04 LTS 作業系統作為控制台代理。

設定NetApp Console

下一步是設定控制台和NetApp Backup and Recovery。

審查 ["標準NetApp Console要求"](#)。

建立控制台代理

您應該聯絡您的NetApp產品團隊來嘗試備份和復原。然後，當您使用控制台代理時，它將包含適合該服務的功能。

若要在使用服務之前在NetApp Console中建立控制台代理，請參閱描述 ["如何建立控制台代理"](#)。

控制台代理的安裝位置

若要完成還原操作，可以在下列位置安裝控制台代理程式：

- 對於 Amazon S3，控制台代理可以部署在您的場所。
- 對於 Azure Blob，可以在您的地方部署控制台代理程式。
- 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



「本地ONTAP系統」包括FAS和AFF系統。

設定NetApp Backup and Recovery 的許可

您可以透過從雲端供應商購買按使用量付費 (PAYGO) 或年度市場訂閱 * NetApp Intelligent Services* 來獲得NetApp Backup and Recovery許可，或透過從NetApp購買自帶許可 (BYOL)。需要有效的許可證才能在系統上啟動NetApp Backup and Recovery and Recovery、建立生產資料的備份以及將備份資料還原到生產系統。

在您繼續閱讀之前，請注意以下幾點：

- 如果您已經在雲端供應商的市場中訂閱了Cloud Volumes ONTAP系統的即用即付 (PAYGO) 服務，那麼您也會自動訂閱NetApp Backup and Recovery 。您無需再次訂閱。
- NetApp Backup and Recovery自帶許可證 (BYOL) 是一種浮動許可證，您可以在與NetApp Console組織或帳戶關聯的所有系統中使用它。因此，如果您現有的 BYOL 授權具有足夠的備份容量，則無需購買另一個 BYOL 授權。
- 如果您使用的是 BYOL 許可證，建議您也訂閱 PAYGO 訂閱。如果您備份的資料超出了 BYOL 許可證允許的範圍，或者許可證期限已過期，則備份將透過您的即用即付訂閱繼續進行 - 不會中斷服務。
- 將本機ONTAP資料備份到StorageGRID時，您需要 BYOL 許可證，但雲端提供者儲存空間無需付費。

["了解有關使用NetApp Backup and Recovery 的成本的更多資訊。"](#)

30天免費試用

如果您在雲端供應商的市場中註冊按使用量付費訂閱 * NetApp Intelligent Services*，則可以獲得NetApp Backup and Recovery 30 天免費試用。免費試用從您訂閱市場清單時開始。請注意，如果您在部署Cloud Volumes ONTAP系統時支付市場訂閱費用，然後在 10 天後開始NetApp Backup and Recovery免費試用，那麼您將有 20 天的剩餘時間來使用免費試用版。

免費試用結束後，您將自動切換至 PAYGO 訂閱，不會中斷。如果您決定不再繼續使用NetApp Backup and Recovery，只需["從系統取消註冊NetApp Backup and Recovery"](#)在試用期結束前，您將不會被收費。

結束免費試用

如果您想在免費試用結束後繼續使用NetApp Backup and Recovery，則必須設定付費訂閱。您可以從NetApp Console介面導覽至計費部分並選擇適合您需求的訂閱方案來執行此操作。如果您不想繼續使用NetApp Backup and Recovery，您可以結束免費試用。

當您結束免費試用而未訂閱付費方案時，您的資料將在免費試用結束後 60 天自動刪除。您可以選擇讓系統立即刪除您的資料。

步驟

1. 從NetApp Backup and Recovery登入頁面，選擇 查看免費試用版。
2. 選擇*結束免費試用*。
3. 選擇「免費試用結束後立即刪除資料」以立即刪除您的資料。
4. 在框框中輸入*結束試用*。
5. 選擇*結束*確認。

使用NetApp Backup and Recovery PAYGO 訂閱

對於即用即付，您將在單一訂閱中按小時向雲端供應商支付物件儲存成本和NetApp備份授權成本。即使您有免費試用版或自帶授權 (BYOL)，也應該在 Marketplace 中訂閱 * NetApp Intelligent Services*：

- 訂閱可確保免費試用結束後服務不會中斷。試用期結束後，我們將根據您備份的資料量按小時向您收費。
- 如果您備份的資料超出了 BYOL 授權允許的範圍，則資料備份和復原作業將透過即用即付訂閱繼續進行。例如，如果您擁有 10 TiB BYOL 許可證，則超過 10 TiB 的所有容量都將透過 PAYGO 訂閱收費。

在免費試用期間或未超出 BYOL 授權的情況下，您無需支付即用即付訂閱費用。

NetApp Backup and Recovery有幾種 PAYGO 計畫：

- 「雲端備份」套件可讓您備份Cloud Volumes ONTAP資料和本機ONTAP資料。
- “CVO Professional” 軟體包可讓您捆綁Cloud Volumes ONTAP和NetApp Backup and Recovery。這包括使用許可證對Cloud Volumes ONTAP系統進行無限制備份（備份容量不計入許可容量）。此選項不允許您備份本機ONTAP資料。

請注意，此選項還需要備份和還原 PAYGO 訂閱，但符合資格的Cloud Volumes ONTAP系統不會產生任何費用。

["了解有關這些基於容量的許可證包的更多信息"](#)。

使用這些連結從您的雲端供應商市場訂閱NetApp Backup and Recovery：

- AWS：["前往NetApp Intelligent Services市場了解定價詳情"](#)。
- Azure：["前往NetApp Intelligent Services市場了解定價詳情"](#)。
- Google Cloud：["前往NetApp Intelligent Services市場了解定價詳情"](#)。

使用年度合約

透過購買年度合約每年支付NetApp Backup and Recovery的費用。期限分為 1 年、2 年或 3 年。

如果您與市場簽訂了年度合同，則所有NetApp Backup and Recovery消費均根據該合約收費。您不能將年度市場合約與 BYOL 混合搭配。

當您使用 AWS 時，有兩種年度合約可供選擇 ["AWS Marketplace 頁面"](#)對於Cloud Volumes ONTAP和本機ONTAP系統：

- 「雲端備份」計畫可讓您備份Cloud Volumes ONTAP資料和本機ONTAP資料。

如果您想使用此選項，請從 Marketplace 頁面設定您的訂閱，然後 ["將訂閱與您的 AWS 憑證關聯"](#)。請注意，您還需要使用此年度合約訂閱來支付您的Cloud Volumes ONTAP系統的費用，因為您只能在控制台中為您的 AWS 憑證指派一個有效訂閱。

- 「CVO Professional」計畫可讓您捆綁Cloud Volumes ONTAP和NetApp Backup and Recovery。這包括使用許可證對Cloud Volumes ONTAP系統進行無限制備份（備份容量不計入許可容量）。此選項不允許您備份本機ONTAP資料。

查看 ["Cloud Volumes ONTAP授權主題"](#)了解有關此許可選項的更多資訊。

如果您想使用此選項，可以在建立Cloud Volumes ONTAP系統時設定年度合同，控制台會提示您訂閱 AWS Marketplace。

使用 Azure 時，有兩種年度合約可供選擇 ["Azure 市集頁面"](#)對於Cloud Volumes ONTAP和本機ONTAP系統：

- 「雲端備份」計畫可讓您備份Cloud Volumes ONTAP資料和本機ONTAP資料。

如果您想使用此選項，請從 Marketplace 頁面設定您的訂閱，然後 ["將訂閱與您的 Azure 憑證關聯"](#)。請注意，您還需要使用此年度合約訂閱來支付您的Cloud Volumes ONTAP系統的費用，因為您只能在控制台中為您的 Azure 憑證指派有效訂閱。

- 「CVO Professional」計畫可讓您捆綁Cloud Volumes ONTAP和NetApp Backup and Recovery。這包括使用許可證對Cloud Volumes ONTAP系統進行無限制備份（備份容量不計入許可容量）。此選項不允許您備份本機ONTAP資料。

查看 ["Cloud Volumes ONTAP授權主題"](#)了解有關此許可選項的更多資訊。

如果您想使用此選項，可以在建立Cloud Volumes ONTAP系統時設定年度合同，控制台會提示您訂閱 Azure Marketplace。

當您使用 GCP 時，請聯絡您的NetApp銷售代表購買年度合約。該合約在 Google Cloud Marketplace 中以私人優惠形式提供。

NetApp提供您專屬優惠後，您可以在啟動NetApp Backup and Recovery時透過 Google Cloud Marketplace 訂閱並選擇年度方案。

使用NetApp Backup and RecoveryBYOL 許可證

NetApp提供的自備授權的有效期限為 1 年、2 年或 3 年。您只需為您保護的資料付費，該費用根據正在備份的來源ONTAP磁碟區的邏輯使用容量（任何效率之前）計算。此容量也稱為前端兆位元組 (FETB)。

BYOL NetApp Backup and Recovery許可證是一種浮動許可證，其總容量在與您的NetApp Console組織或帳戶關聯的所有系統之間共用。對於ONTAP系統，您可以透過執行 CLI 命令來粗略估計所需的容量 ``volume show -fields logical-used-by-afs`` 對於您計劃備份的磁碟區。

如果您沒有NetApp Backup and Recovery BYOL 許可證，請點擊控制台右下角的聊天圖示購買。

或者，如果您擁有未指派的基於節點的Cloud Volumes ONTAP授權但不會使用，則可以將其轉換為具有相同美元等值和相同到期日的NetApp Backup and Recovery授權。 ["點此了解詳情"](#)。

您可以使用NetApp Console來管理 BYOL 授權。您可以從控制台新增許可證、更新現有許可證以及查看許可證狀態。

["了解如何新增許可證"](#)。

超出授權容量

超出許可容量將觸發 PAYGO 費率；如果沒有 PAYGO 訂閱，您將無法建立新的備份，但現有備份仍可恢復，只是服務不再有保障。請務必在許可證到期前續訂；過期的許可證將阻止建立新的備份並中斷服務。

在NetApp Backup and Recovery中為StorageGRID和ONTAP設定安全性證書

建立安全性憑證以啟用NetApp Backup and Recovery與StorageGRID或ONTAP之間的通訊。

為StorageGRID建立安全性證書

如果NetApp Backup and Recovery容器與StorageGRID之間的通訊應該驗證StorageGRID證書，則完成以下步驟。

產生的憑證應具有 CN 和主題備用名稱，作為啟動備份時NetApp Backup and Recovery中提供的名稱。

步驟

1. 請依照StorageGRID文件中的步驟建立StorageGRID憑證。

"有關配置證書的StorageGRID信息"

2. 如果您尚未更新StorageGRID，請使用憑證進行更新。
3. 以 root 使用者登入控制台代理程式。跑步：

```
sudo su
```

4. 取得NetApp Backup and Recovery (Cloud Backup Service) Docker 磁碟區。跑步：

```
docker volume ls | grep cbs
```

輸出範例：

```
local service-manager-2_cloudmanager_cbs_volume"
```



標準、私有和受限部署模式的磁碟區名稱不同。本範例使用標準模式。參考 ["NetApp Console部署模式"](#)。

5. 找到NetApp Backup and Recovery磁碟區的掛載點。跑步：

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep Mountpoint
```

輸出範例：

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data"
```



標準、私有和受限部署模式的掛載點有所不同。此範例展示了標準雲端部署。參考 ["NetApp Console部署模式"](#)。

6. 變更為 MountPoint 目錄。跑步：

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

7. 如果 StorageGRID 的憑證由根 CA 和中間 CA 簽名，則附加 `pem` 將兩個檔案合併到一個名為 `sgws.crt` 在目前位置。不要將舊證書新增至此文件。

cloudmanager_cbs 容器的步驟

您需要在 NetApp Backup and Recovery (Cloud Backup Service) 中啟用 StorageGRID 伺服器憑證驗證。

1. 將目錄更改為前面步驟中獲得的 Docker 磁碟區。

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

2. 將目錄變更為配置目錄。

```
cd cbs_config
```

3. 根據您的部署環境，建立並儲存如下所示的設定文件，並使用以下名稱之一：

- `production-customer.json` 用於標準模式和限制模式部署。
- `darksite-customer.json` 用於私人模式部署。

參考 ["NetApp Console 部署模式"](#)。

設定檔

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. 退出容器。跑步：

```
exit
```

5. 重啟 cloudmanager_cbs。跑步：

```
docker restart cloudmanager_cbs
```

cloudmanager_cbs_catalog 容器的步驟

接下來，您需要為編目服務啟用StorageGRID伺服器憑證驗證。

1. 將目錄更改為 Docker 磁碟區：

```
cd /var/lib/docker/volumes/service-manager-  
2_cloudmanager_cbs_volume/_data
```

2. 配置目錄。跑步：

```
cd cbs_catalog_config
```

3. 根據您的部署環境，使用以下名稱之一建立如下所示的設定檔：

- `production-customer.json` 用於標準模式和限制模式部署。
- `darksite-customer.json` 用於私人模式部署。

參考 ["NetApp Console部署模式"](#)。

目錄設定檔

```
{  
  "protocols": {  
    "sgws": {  
      "certificates": {  
        "reject-unauthorized": true,  
        "ca-bundle": "/config/sgws.crt"  
      }  
    }  
  }  
}
```

4. 重新啟動目錄。跑步：

```
docker restart cloudmanager_cbs_catalog
```

根據代理作業系統使用StorageGRID憑證更新控制台代理程式證書

Ubuntu

1. 將 SGWS 憑證複製到 /usr/local/share/ca-certificates。以下是一個例子：

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

在哪裡 `sgws.crt` 是根 CA 憑證。

2. 使用StorageGRID憑證更新主機憑證。跑步

```
sudo update-ca-certificates
```

紅帽企業 Linux

1. 將 SGWS 憑證複製到 /etc/pki/ca-trust/source/anchors/。

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

在哪裡 `sgws.crt` 是根 CA 憑證。

2. 使用StorageGRID憑證更新主機憑證。

```
update-ca-trust extract
```

3. 更新 ca-bundle.crt

```
cd /etc/pki/tls/certs/  
openssl x509 -in ca-bundle.crt -text -noout
```

4. 若要檢查憑證是否存在，請執行以下命令：

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |  
openssl pkcs7 -print_certs | grep subject | head
```

為ONTAP建立安全性證書

如果NetApp Backup and Recovery容器與ONTAP之間的通訊應驗證ONTAP證書，則完成以下步驟。

NetApp Backup and Recovery使用 Cluster Management IP 連接到ONTAP。在憑證的主題備用名稱中輸入叢集

的 IP 位址。使用系統管理員 UI 產生 CSR 時指定此步驟。

使用系統管理員文件為ONTAP建立新的 CA 憑證。

- ["使用系統管理員管理證書"](#)
- ["如何使用 System Manager 管理ONTAP SSL 憑證"](#)

步驟

1. 以 root 身分登入控制台代理程式。跑步：

```
sudo su
```

2. 取得NetApp Backup and RecoveryDocker 磁碟區。跑步：

```
docker volume ls | grep cbs
```

輸出範例：

```
local service-manager-2_cloudmanager_cbs_volume
```



標準、私有和受限部署模式的磁碟區名稱不同。此範例展示了標準雲端部署。參考 ["NetApp Console部署模式"](#)。

3. 取得卷的掛載。跑步：

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep Mountpoint
```

輸出範例：

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```



標準、私有和受限部署模式的掛載點有所不同。此範例展示了標準雲端部署。參考 ["NetApp Console部署模式"](#)。

4. 變更為掛載點目錄。跑步：

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

5. 完成以下步驟之一：

- 如果ONTAP憑證由根 CA 和中間 CA 簽名，則附加 `pem` 將兩個檔案合併到一個名為 `ontap.crt` 在目前位置。
- 如果ONTAP憑證由單一 CA 簽名，則重新命名 `pem` 文件為 `ontap.crt` 並將其複製到目前位置。不要將葉證書新增至此文件。

cloudmanager_cbs 容器的步驟

接下來，在NetApp Backup and Recovery Cloud Backup Service) 中啟用ONTAP伺服器憑證驗證。

1. 將目錄更改為前面步驟中獲得的 Docker 磁碟區。

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

2. 切換到配置目錄。跑步：

```
cd cbs_config
```

3. 根據您的部署環境，建立一個如下所示的設定文件，並使用以下名稱之一：

- `production-customer.json` 用於標準模式和限制模式部署。
- `darksite-customer.json` 用於私人模式部署。

參考 ["NetApp Console部署模式"](#)。

設定檔

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. 退出容器。跑步：

```
exit
```

5. 重新啟動NetApp Backup and Recovery。跑步：

```
docker restart cloudmanager_cbs
```

cloudmanager_cbs_catalog 容器的步驟

為編目服務啟用ONTAP伺服器憑證驗證。

1. 將目錄更改為 Docker 磁碟區。跑步：

```
cd /var/lib/docker/volumes/service-manager-  
2_cloudmanager_cbs_volume/_data
```

2. 跑步：

```
cd cbs_catalog_config
```

3. 根據您的部署環境，建立一個如下所示的設定文件，並使用以下名稱之一：

- `production-customer.json` 用於標準模式和限制模式部署。
- `darksite-customer.json` 用於私人模式部署。

參考 ["NetApp Console部署模式"](#)。

設定檔

```
{  
  "ontap": {  
    "certificates": {  
      "reject-unauthorized": true,  
      "ca-bundle": "/config/ontap.crt"  
    }  
  }  
}
```

4. 重新啟動NetApp Backup and Recovery。跑步：

```
docker restart cloudmanager_cbs_catalog
```

為ONTAP和StorageGRID建立證書

如果您需要為ONTAP和StorageGRID啟用證書，則設定檔如下所示：


```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

在使用NetApp Backup and Recovery之前設定備份目標

在使用NetApp Backup and Recovery之前，請執行幾個步驟來設定備份目標。

在開始之前，請查看[先決條件](#)以確保您的環境已準備就緒。

準備備份目標

準備以下一個或多個備份目標：

- NetAppStorageGRID。

參考 ["了解StorageGRID"](#)。

參考 ["StorageGRID文檔"](#)有關StorageGRID的詳細資訊。

- 亞馬遜網路服務。參考 ["Amazon S3 文檔"](#)。

執行下列操作以準備將 AWS 作為備份目標：

- 在 AWS 中設定一個帳戶。
- 在 AWS 中配置 S3 權限，列於下一節。
- 有關在控制台中管理 AWS 儲存的詳細信息，請參閱 ["管理您的 Amazon S3 儲存桶"](#)。

- 微軟 Azure。
 - 參考 ["Azure NetApp Files文檔"](#)。
 - 在 Azure 中設定一個帳戶。

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

在備份目標本身配置選項後，您稍後會將其配置為NetApp Backup and Recovery中的備份目標。有關如何在NetApp Backup and Recovery中配置備份目標的詳細信息，請參閱["發現備份目標"](#)。

設定 S3 權限

您需要設定兩組 AWS S3 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"
    }
  ]
}

```

登入NetApp Backup and Recovery

您可以使用NetApp Console登入NetApp Backup and Recovery。

NetApp Backup and Recovery使用身分和存取管理來控制每個使用者可以做什麼。

有關每個角色可以執行的操作的詳細信息，請參閱["NetApp Backup and Recovery使用者角色"](#)。

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

所需的**NetApp Console**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"](#)。

要新增控制台代理，您必須具有備份和還原超級管理員角色。

步驟

1. 開啟 Web 瀏覽器並前往 ["NetApp Console"](#)。

出現NetApp Console登入頁面。

2. 登入控制台。

3. 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，並且尚未將系統新增至「系統」頁面，則備份和恢復將顯示「歡迎使用新的NetApp Backup and Recovery」登入頁面，並提供新增系統的選項。有關向「系統」頁面添加系統的詳細信息，請參閱 ["NetApp Console標準模式入門"](#)。
- 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。

4. 如果您還沒有這樣做，請選擇*發現和管理*選項。

- 有關 Microsoft SQL Server 工作負載，請參閱["發現 Microsoft SQL Server 工作負載"](#)。
- 有關 VMware 工作負載，請參閱["發現 VMware 工作負載"](#)。
- 有關 KVM 工作負載，請參閱["發現 KVM 工作負載"](#)。
- 有關 Oracle Database 工作負載，請參閱 ["探索 Oracle Database 工作負載"](#)。
- 對於 Hyper-V 工作負載，請參閱["發現 Hyper-V 工作負載"](#)。
- 有關 Kubernetes 工作負載，請參閱["發現 Kubernetes 工作負載"](#)。

在NetApp Backup and Recovery中發現異地備份目標

完成幾個步驟即可在NetApp Backup and Recovery中發現或手動新增異地備份目標。

發現備份目標

在使用NetApp Backup and Recovery之前，請先設定您的備份目標（Amazon Web Services (AWS) S3、Microsoft Azure Blob Storage、Google Cloud Storage 或StorageGRID）。

您可以自動發現這些目標或手動新增它們。

提供存取儲存帳戶的憑證。NetApp Backup and Recovery使用這些憑證來發現您想要備份的工作負載。

開始之前

您需要先發現至少一個工作負載，然後才能新增異地備份目標。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇*異地備份目標*標籤。
3. 選擇*發現備份目標*。
4. 選擇下列備份目標類型之一：**Amazon Web Services (AWS) S3**、**Microsoft Azure Blob Storage**、***StorageGRID*** 或 ***ONTAP S3***。
5. 在「選擇憑證位置」部分中，選擇憑證所在的位置，然後選擇如何關聯憑證。
6. 選擇“下一步”。
7. 輸入憑證資訊。根據您選擇的備份目標類型和憑證位置，資訊會有所不同。
 - 對於 AWS：
 - 憑證名稱：輸入 AWS 憑證名稱。
 - 存取金鑰：輸入 AWS 金鑰。
 - 金鑰：輸入 AWS 金鑰。
 - 對於 Azure：
 - 憑證名稱：輸入 Azure Blob 儲存憑證名稱。
 - 客戶端金鑰：輸入 Azure Blob 儲存客戶端金鑰。
 - 應用程式（用戶端）ID：選擇 Azure Blob 儲存應用程式 ID。
 - 目錄租用戶 ID：輸入 Azure Blob 儲存租用戶 ID。
 - 對於StorageGRID：
 - 憑證名稱：輸入StorageGRID憑證名稱。
 - 網關節點 **FQDN**：輸入StorageGRID的 FQDN 名稱。
 - 連接埠：輸入StorageGRID的連接埠號碼。
 - 存取金鑰：輸入StorageGRID S3 存取金鑰。
 - 金鑰：輸入StorageGRID S3 金鑰。
 - 對於ONTAP S3：
 - 憑證名稱：輸入ONTAP S3 憑證名稱。
 - 網關節點 **FQDN**：輸入ONTAP S3 的 FQDN 名稱。
 - 連接埠：輸入ONTAP S3 的連接埠號碼。
 - 存取金鑰：輸入ONTAP S3 存取金鑰。
 - 金鑰：輸入ONTAP S3 金鑰。

8. 選擇*發現*。

為備份目標新增儲存桶

您可以手動將儲存桶新增至異地備份目標，而不是讓NetApp Backup and Recovery自動發現儲存桶。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇*異地備份目標*。
3. 選擇目標，然後在右側選擇“操作”  圖示並選擇*新增儲存桶*。
4. 輸入儲存桶資訊。根據您選擇的備份目標類型，資訊會有所不同。
 - 對於 AWS：
 - 儲存桶名稱：輸入 S3 儲存桶的名稱。「netapp-backup」前綴是必要的前綴，會自動加入您提供的名稱。
 - **AWS** 帳戶：輸入 AWS 帳戶名稱。
 - 儲存桶區域：輸入儲存桶的 AWS 區域。
 - 啟用 **S3** 物件鎖定：選擇此選項可為儲存桶啟用 S3 物件鎖定。S3 物件鎖定可防止在指定的保留期間內刪除或覆寫對象，從而提供額外的資料保護層。您只能在建立儲存桶時啟用此功能，並且以後無法將其關閉。
 - 治理模式：選擇此選項可為 S3 物件鎖定儲存桶啟用治理模式。治理模式使您能夠保護物件不被大多數使用者刪除或覆蓋，但允許某些使用者變更保留設定。
 - 合規模式：選擇此選項可為 S3 物件鎖定儲存桶啟用合規模式。合規模式可防止任何使用者（包括根使用者）在保留期到期之前變更保留設定或刪除物件。
 - 版本控制：選擇此選項可為 S3 儲存桶啟用版本控制。版本控制使您能夠在儲存桶中保留物件的多個版本，這對於備份和復原目的很有用。
 - 標籤：選擇 S3 儲存桶的標籤。標籤是可用於組織和管理 S3 資源的鍵值對。
 - 加密：選擇 S3 儲存桶的加密類型。選項是 AWS S3 管理金鑰或 AWS 金鑰管理服務金鑰。如果您選擇 AWS Key Management Service 金鑰，則必須提供金鑰 ID。
 - 對於 Azure：
 - 訂閱：選擇 Azure Blob 儲存容器的名稱。
 - 資源組：選擇 Azure 資源組的名稱。
 - 實例詳情：
 - 儲存帳戶名稱：輸入 Azure Blob 儲存容器的名稱。
 - **Azure** 區域：輸入容器的 Azure 區域。
 - 效能類型：為 Azure Blob 儲存容器選擇標準或進階效能類型，以指示所需的效能等級。
 - 加密：選擇 Azure Blob 儲存容器的加密類型。選項包括 Microsoft 管理的金鑰或客戶管理的金鑰。如果選擇客戶管理的金鑰，則必須提供金鑰保管庫名稱和金鑰名稱。
 - 對於StorageGRID：
 - 備份目標名稱：選擇StorageGRID桶的名稱。

- 儲存桶名稱：輸入StorageGRID桶的名稱。
 - 區域：輸入儲存桶的StorageGRID區域。
 - 啟用版本控制：選擇此選項可為StorageGRID桶啟用版本控制。版本控制使您能夠在儲存桶中保留物件的多個版本，這對於備份和復原目的很有用。
 - 物件鎖定：選擇此選項可為StorageGRID桶啟用物件鎖定。物件鎖定可防止物件在指定的保留期內被刪除或覆蓋，從而提供額外的資料保護層。您只能在建立儲存桶時啟用此功能，並且以後無法將其關閉。
 - 容量：輸入StorageGRID桶的容量。這是儲存桶中可以儲存的最大資料量。
- 對於ONTAP S3：
- 備份目標名稱：選擇ONTAP S3 儲存桶的名稱。
 - 儲存桶目標名稱：輸入ONTAP S3 儲存桶的名稱。
 - 容量：輸入ONTAP S3 儲存桶的容量。這是儲存桶中可以儲存的最大資料量。
 - 啟用版本控制：選擇此選項可為ONTAP S3 儲存桶啟用版本控制。版本控制使您能夠在儲存桶中保留物件的多個版本，這對於備份和復原目的很有用。
 - 物件鎖定：選擇此選項可為ONTAP S3 儲存桶啟用物件鎖定。物件鎖定可防止物件在指定的保留期內被刪除或覆蓋，從而提供額外的資料保護層。您只能在建立儲存桶時啟用此功能，並且以後無法將其關閉。

5. 選擇“新增”。

更改備份目標的憑證

輸入存取備份目標所需的憑證。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 選擇*異地備份目標*。
3. 選擇目標，然後在右側選擇“操作”  圖示並選擇*變更憑證*。
4. 輸入備份目標的新憑證。根據您選擇的備份目標類型，資訊會有所不同。
5. 選擇*完成*。

切換到不同的NetApp Backup and Recovery工作負載

您可以在不同的NetApp Backup and Recovery工作負載之間切換。

切換到不同的工作負載

您可以在NetApp Backup and RecoveryUI 中切換到不同的工作負載。

步驟

1. 從控制台左側導覽中，選擇*保護*>*備份和還原*。
2. 從頁面右上角，選擇*切換工作負載*下拉清單。

3. 選擇您想要切換到的工作負載。

頁面刷新並顯示所選的工作負載。

配置NetApp Backup and Recovery設置

設定NetApp Console後，配置備份和復原設定。新增主機資源的憑證、匯入SnapCenter資源、設定日誌目錄以及設定 VMware vCenter 設定。在備份或還原資料之前完成這些步驟。

- [\[為主機資源新增憑證\]](#) 適用於NetApp Backup and Recovery需要進行驗證的任何 Windows、Microsoft SQL Server、Oracle Database 或 Linux 主機。這包括恢復訪客檔案或資料夾時使用的 Windows 訪客作業系統憑證。
- [維護 VMware vCenter 設定](#)。
- [匯入並管理SnapCenter主機資源](#)。（僅限 Microsoft SQL Server 工作負載）
- [新增 KVM 管理平台](#)。（僅限 KVM 工作負載）
- [在 Windows 主機的快照中設定日誌目錄](#)。
- [\[建立執行鉤子模板\]](#)在備份作業前後執行腳本。（僅限 Kubernetes 工作負載）

所需的**NetApp Console**角色 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。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"](#)。

為主機資源新增憑證

新增主機資源憑證。NetApp Backup and Recovery使用這些憑證來發現工作負載並套用備份策略。

如果您沒有憑證，請建立具有存取和管理主機工作負載的權限的憑證。

您需要配置以下類型的憑證：

- Microsoft SQL Server 憑證
- SnapCenter Windows 主機憑證
- 復原用戶端檔案或資料夾時所使用的 Windows 用戶端作業系統憑證
- Oracle 資料庫憑證
- Linux 主機憑證

步驟

1. 從NetApp Backup and Recovery選單中，選擇 設定。
2. 選擇“憑證”的向下箭頭。
3. 選擇*新增憑證*。
4. 請輸入登入憑證資訊。根據您選擇的身份驗證模式，會顯示不同的欄位。將滑鼠懸停在資訊 i 圖示上，以查看有關欄位的更多資訊。
 - 憑證名稱：輸入憑證的名稱。

- 。驗證模式：選擇 **Windows**、**Microsoft SQL**、**Oracle Database** 或 **Linux**。



對於 Microsoft SQL Server 工作負載，您需要輸入 Windows 和 Microsoft SQL Server 的憑證，因此您需要新增兩組憑證。

視窗

i. 如果您選擇了 **Windows**：

- 代理：從清單中選擇一個控制台代理。
- 網域和使用者名稱：輸入憑證的 NetBIOS 或網域 FQDN 和使用者名稱。
- 密碼：輸入憑證的密碼。

微軟 SQL 伺服器

i. 如果您選擇了 **Microsoft SQL Server**：

- 網域和使用者名稱：輸入憑證的 NetBIOS 或網域 FQDN 和使用者名稱。
- 密碼：輸入憑證的密碼。
- 主機：選擇已發現的 SQL Server 主機位址。
- **SQL Server 執行個體**：選擇已發現的 SQL Server 執行個體。

Oracle 資料庫

i. 如果您選擇了*Oracle資料庫*：

- 代理：從清單中選擇一個控制台代理。
- 使用者名稱：請輸入用於登入憑證的使用者名稱。
- 密碼：輸入憑證的密碼。

Linux

i. 如果您選擇了 **Linux**：

- 代理：從清單中選擇一個控制台代理。
- 使用者名稱：請輸入用於登入憑證的使用者名稱。
- 密碼：輸入憑證的密碼。

5. 選擇“新增”。

編輯主機資源的憑證

您之後可以編輯您建立的任何憑證的密碼。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 設定。
2. 選擇向下箭頭以展開“**Credentials**”部分。
3. 選擇“操作”圖標  > 編輯憑證。

- 密碼：輸入憑證的密碼。

4. 選擇*儲存*。

維護 VMware vCenter 設定

提供 VMware vCenter 憑證來發現要備份的工作負載。如果您沒有憑證，請建立具有存取和管理 VMware vCenter Server 工作負載的權限的憑證。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 設定。
2. 選擇向下箭頭展開 **VMware vCenter** 部分。
3. 選擇“新增 vCenter”。
4. 輸入 VMware vCenter Server 資訊。
 - **vCenter FQDN 或 IP 位址**：輸入 VMware vCenter Server 的 FQDN 名稱或 IP 位址。
 - 使用者名稱*和*密碼：輸入 VMware vCenter Server 的使用者名稱和密碼。
 - 連接埠：輸入 VMware vCenter Server 的連接埠號碼。
 - 協定：選擇*HTTP*或*HTTPS*。
5. 選擇“新增”。

匯入並管理SnapCenter主機資源

如果您之前使用SnapCenter備份資源，則可以在NetApp Backup and Recovery中匯入和管理這些資源。此選項可讓您匯入SnapCenter伺服器資訊以註冊多個SnapCenter伺服器並發現資料庫工作負載。

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不會接手保護管理。為此，您必須明確選擇在NetApp Backup and Recovery中管理這些資源。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 設定。
2. 選擇向下箭頭以展開「從SnapCenter匯入」部分。
3. 選擇*從SnapCenter匯入*以匯入SnapCenter資源。
4. 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。
5. 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。輸入憑證名稱。
 - 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。
6. 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。

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。在您選擇管理這些匯入的資源後，NetApp Backup and Recovery可以備份並還原您從SnapCenter匯入的資源。您不再需要在SnapCenter Server 中管理這些資源。

步驟

1. 匯入SnapCenter資源後，在出現的「清單」頁面上，選擇您匯入的、希望從現在開始由NetApp Backup and Recovery管理的SnapCenter資源。
2. 選擇“操作”圖標 > 管理 管理資源。
3. 選擇“在NetApp Console中管理”*。

清單頁面在主機名稱下顯示 **Managed**，表示所選主機資源現在由NetApp Backup and Recovery管理。

編輯匯入的SnapCenter資源

您稍後可以重新匯入SnapCenter資源或編輯匯入的SnapCenter資源以更新註冊詳細資訊。

您只能變更SnapCenter伺服器的連接埠和密碼詳細資料。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 設定。
2. 選擇“從SnapCenter匯入”的向下箭頭。

從SnapCenter匯入頁面顯示所有先前的匯入。

3. 選擇“操作”圖標 > *編輯*以更新資源。
4. 根據需要更新SnapCenter密碼和連接埠詳細資訊。
5. 選擇*導入*。

新增 KVM 管理平台

如果您使用 Apache CloudStack 管理平台來管理 KVM 資源，則需要將其與NetApp Backup and Recovery集成，以便 Backup and Recovery 可以發現和保護受管 KVM 主機和虛擬機器。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 設定。
2. 選擇向下箭頭展開「管理平台」部分。
3. 選擇「新增管理平台憑證」。
4. 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。
5. 完成後，選擇“新增”。

在 Windows 主機的快照中設定日誌目錄

在為 Windows 主機建立原則之前，您應該為 Windows 主機設定快照中的日誌目錄。日誌目錄用於儲存備份過程中產生的日誌。

步驟

1. 從NetApp Backup and Recovery選單中，選擇 **Inventory**。
2. 在清單頁面中，選擇一個工作負載，然後選擇操作圖標  > *查看詳情*顯示工作量詳情。
3. 從顯示 Microsoft SQL Server 的庫存詳細資料頁面中，選擇「主機」標籤。
4. 在清單詳細資料頁面中，選擇一個主機並選擇操作圖標  > 配置日誌目錄。
5. 瀏覽或輸入日誌目錄的路徑。
6. 選擇*儲存*。

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。

在 NetApp Backup and Recovery 中設定基於角色的存取控制

為了提升安全性並控制資源存取，請為 NetApp Backup and Recovery 設定以角色為基礎的存取權限。NetApp Console 支援部分 Backup and Recovery 工作負載的角色型存取控制 (RBAC)。你可以針對這些工作負載指派管理員或檢視者角色。尚未支援角色型存取控制的其他工作負載，在支援專案層級關聯之前，仍可由所有具有 Backup and Recovery 角色的使用者存取。

請依照以下步驟控制對組織內資源的存取權限。在 NetApp Console 選單的「管理 > 身分和存取」頁面中進行變更。



這些步驟假設您在 Console 中被指派了組織管理員角色。

步驟

1. 建立身分和存取專案結構。

作為組織管理員，設定 Identity and access 資料夾以及工作負載將存放的專案結構。

2. 分配使用者角色。

- a. 主要選項：

將使用者新增至每個用於處理工作負載的專案中，並授予他們相應的角色。例如：

- 組織管理員*和 ***Backup and Recovery** 超級管理員：擁有這些角色的使用者可以查看所有組織中的所有資源，並發現 Backup and Recovery 工作負載，並將其分配給專案（例如，美國東部或美國西部）。
- 資料夾或專案管理員*和 ***Backup and Recovery** 超級管理員：擁有這些角色的使用者只能看到他們擁有權限的資料夾或專案中的資源，但可以發現 Backup and Recovery 工作負載並將其分配給該專案。

- b. 替代方案：

與其授予使用者完整的 Backup and Recovery 管理員權限，不如將自己指派為 Backup and Recovery 超級管理員角色，並直接探索工作負載。

3. 探索 Backup and Recovery 中的工作負載。

組織管理員、資料夾管理員或專案管理員可以發現可用的工作負載，並選擇相應的專案（例如 US East 或 US West）。每個工作負載都會自動關聯到所選專案。

4. 將使用者新增至專案。

組織管理員或資料夾/專案管理員可將 Console 使用者新增至包含工作負載的專案中。根據使用者的存取需求，為其指派組織查看者角色和 Backup and Recovery 角色。擁有相應 Backup and Recovery 角色的使用者將自動獲得對這些專案中新工作負載的存取權限。

相關資訊

- ["了解 NetApp Console 身分與存取管理"](#).
- ["NetApp Console 中的 NetApp Backup and Recovery 角色"](#).

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。