# 安全性與資料加密
## Cloud Volumes ONTAP

NetApp
June 27, 2024

# 目錄

# 安全性與資料加密

## 使用 NetApp 加密解決方案加密磁碟區

支援NetApp Volume Encryption（NVE）和NetApp Aggregate Encryption（NAE）Cloud Volumes ONTAP 。NVE和NAE是軟體型解決方案、可啟用FIPS 140-2標準的磁碟區閒置資料加密功能。 "深入瞭解這些加密解決方案"。

外部金鑰管理程式支援NVE和NAE。

## 使用 AWS 金鑰管理服務管理金鑰

您可以使用 "AWS 的金鑰管理服務（ KMS ）" 在ONTAP Google Cloud Platform部署的應用程式中保護您的不加密金鑰。

您可以使用 CLI 或 ONTAP REST API 來啟用 AWS KMS 的金鑰管理。

使用 KMS 時、請注意、根據預設、資料 SVM 的 LIF 會用於與雲端金鑰管理端點通訊。節點管理網路用於與 AWS 的驗證服務進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

開始之前

- Cloud Volumes ONTAP 必須執行 9.12.0 版或更新版本
- 您必須已安裝 Volume Encryption （ VE ）授權和
- 您必須已安裝多租戶加密金鑰管理（ MTEKM ）授權。
- 您必須是叢集或SVM管理員
- 您必須擁有有效的 AWS 訂閱

您只能設定資料 SVM 的金鑰。

### 組態

**AWS**

1. 您必須建立 "授予" 適用於管理加密的 IAM 角色所使用的 AWS KMS 金鑰。IAM 角色必須包含允許下列作業的原則：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
     若要建立授予、請參閱 "AWS 文件"。
2. "將原則新增至適當的 IAM 角色。" 原則應支援 `DescribeKey`、 `Encrypt`和 `Decrypt` 營運：

**Cloud Volumes ONTAP**

1. 切換至您的 Cloud Volumes ONTAP 環境。

2. 切換至進階權限層級：
   `set -privilege advanced`
3. 啟用 AWS 金鑰管理程式：
   `security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 出現提示時、請輸入秘密金鑰。
5. 確認 AWS KMS 已正確設定：
   `security key-manager external aws show -vserver svm_name`

# 使用Azure Key Vault管理金鑰

您可以使用 "Azure Key Vault（AKV）" 在ONTAP Azure部署的應用程式中保護您的不加密金鑰。

AKV可用於保護 "NetApp Volume Encryption（NVE）金鑰" 僅適用於資料SVM。

使用AKV的金鑰管理可透過CLI或ONTAP REST API來啟用。

使用AKV時、請注意、預設會使用資料SVM LIF與雲端金鑰管理端點進行通訊。節點管理網路用於與雲端供應商的驗證服務（login.microsoftonline.com）進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

開始之前

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權（NetApp Volume Encryption授權會自動安裝在Cloud Volumes ONTAP 向NetApp支援註冊的每個支援系統上）
- 您必須擁有多租戶加密金鑰管理（MT_EK-Mgmt）授權
- 您必須是叢集或SVM管理員
- 現用Azure訂閱

限制

- AKV只能在資料SVM上設定

## 組態程序

概述的步驟將說明如何向Cloud Volumes ONTAP Azure註冊您的「還原組態」、以及如何建立Azure Key Vault和金鑰。如果您已經完成這些步驟、請確定您擁有正確的組態設定、尤其是在中 建立Azure Key Vault，然後繼續 組態Cloud Volumes ONTAP。

- Azure應用程式註冊
- 建立Azure用戶端機密
- 建立Azure Key Vault
- 建立加密金鑰
- 建立Azure Active Directory端點（僅限HA）

- 組態Cloud Volumes ONTAP

**Azure**應用程式註冊

1. 您必須先在Azure訂閱中註冊您的應用程式Cloud Volumes ONTAP 、才能使用此功能來存取Azure Key Vault。在Azure入口網站中、選取「應用程式註冊」。
2. 選擇「**新登錄」。
3. 提供應用程式名稱、並選取支援的應用程式類型。Azure Key Vault使用預設的單一租戶即可滿足需求。選擇「註冊」。
4. 在Azure Overview（Azure總覽）視窗中、選取您已註冊的應用程式。將應用程式（用戶端）ID *和*目錄（租戶）ID *複製到安全位置。在稍後的註冊程序中、將會需要這些工具。

建立**Azure**用戶端機密

1. 在Azure入口網站中註冊Azure Key Vault應用程式、選取「**憑證與機密」窗格。
2. 選取「**新用戶端密碼」。輸入有意義的用戶端機密名稱。NetApp建議使用24個月到期日、不過您的特定雲端治理原則可能需要不同的設定。
3. 按一下「新增」以建立用戶端機密。複製「Value*」欄中所列的秘密字串、並將其儲存在安全的位置以供稍後使用 組態Cloud Volumes ONTAP。在您離開頁面後、不會再顯示機密值。

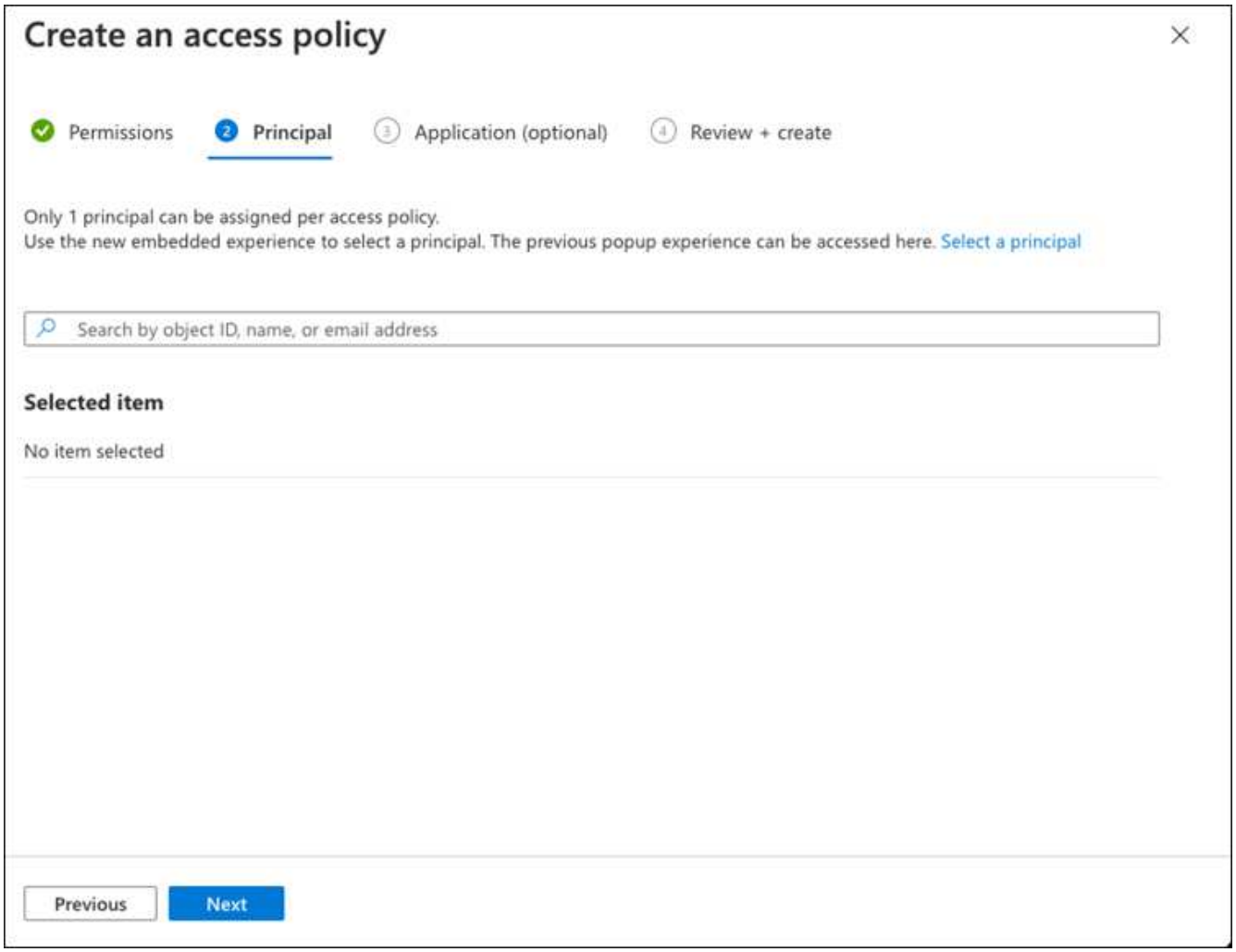
建立**Azure Key Vault**

1. 如果您有現有的Azure Key Vault、您可以將其連線至Cloud Volumes ONTAP 您的整套組態；不過、您必須根據此程序中的設定來調整存取原則。
2. 在Azure入口網站中、瀏覽至「**關鍵故障」區段。
3. 按一下「*+建立」、然後輸入所需資訊、包括資源群組、地區及價格層級。此外、請輸入保留刪除的保存庫的天數、然後在金鑰保存庫中選取「*啟用清除保護」。
4. 選擇「*下一步」以選擇存取原則。
5. 選取下列選項：
   a. 在「存取組態*」下、選取「資料庫存取原則*」。
   b. 在「資源存取*」下、選取「 Azure磁碟加密」以進行Volume加密*。
6. 選取「**+建立」以新增存取原則。
7. 在「從範本*設定」下、按一下下拉式功能表、然後選取「**金鑰、秘密及憑證管理」範本。
8. 選擇每個下拉式權限功能表（金鑰、秘密、憑證）、然後在功能表清單頂端選擇所有*、以選取所有可用的權限。您應該擁有：
   - 關鍵權限：已選取20項
   - **機密權限：選擇8項
   - 認證權限：16項已選取


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. 按一下「下一步」以選取您在其中建立的「*主要」* Azure註冊應用程式 Azure應用程式註冊。選擇「下一步」。

   每個原則只能指派一個主體。




10. 按兩次「下一步」、直到您抵達「審查並建立」為止。然後按一下「建立」。
11. 選擇「下一步」進入「*網路」*選項。
12. 選擇適當的網路存取方法、或選擇「所有網路」和「審查+建立」來建立金鑰保存庫。（網路存取方法可能由治理原則或您的企業雲端安全團隊規定。）
13. 記錄金鑰庫URI：在您建立的金鑰庫中、瀏覽至「總覽」功能表、然後從右側欄複製「** Vault URI」。您需要此功能、以便稍後進行。

建立加密金鑰

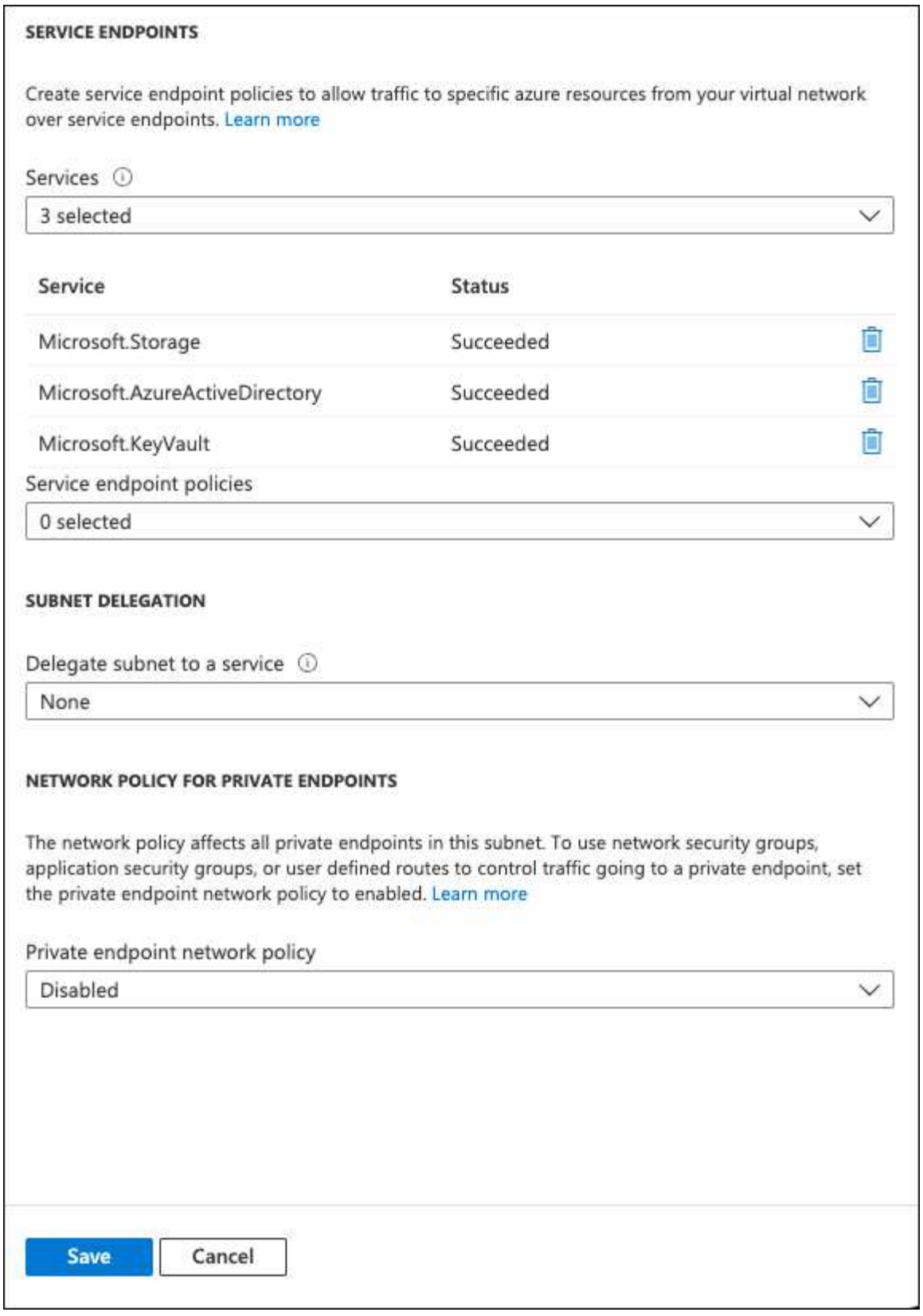
1. 在您為Cloud Volumes ONTAP 之建立的Key Vault功能表中、瀏覽至「** Keys」選項。
2. 選取「產生/匯入」以建立新的金鑰。
3. 將預設選項設為「**產生」。
4. 提供下列資訊：
   - 加密金鑰名稱

- 金鑰類型：RSA
- RSA金鑰大小：2048
- 已啟用：是

5. 選取「建立」以建立加密金鑰。
6. 返回「**按鍵」功能表、然後選取您剛建立的按鍵。
7. 在「目前版本」下方選取金鑰ID、即可檢視金鑰內容。
8. 找到「**金鑰識別碼」欄位。將URI複製到但不包括十六進位字串。

建立**Azure Active Directory**端點（僅限**HA**）

1. 只有在您將Azure Key Vault設定為HA Cloud Volumes ONTAP 功能環境時、才需要執行此程序。
2. 在Azure入口網站中、瀏覽至「**虛擬網路」。
3. 選取部署Cloud Volumes ONTAP 了整個功能區的虛擬網路、然後選取頁面左側的「**Subnets」（子網路）功能表。
4. 從Cloud Volumes ONTAP 清單中選取要部署的子網路名稱。
5. 瀏覽至「*服務端點」標題。在下拉式功能表中、選取下列項目：
   - **Microsoft.AzureActiveDirectory
   - **Microsoft.KeyVault**
   - ***Microsoft.Storage**（選用）




6. 選取「**儲存」以擷取您的設定。

組態**Cloud Volumes ONTAP**

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 進入進階權限模式ONTAP ：

```
set advanced -con off
```

3. 識別所需的資料 SVM 並驗證其 DNS 組態：
   `vserver services name-service dns show`

   a. 如果所需資料SVM的DNS項目存在、且其中包含Azure DNS項目、則不需要採取任何行動。如果沒有、請為資料SVM新增DNS伺服器項目、以指向Azure DNS、私有DNS或內部部署伺服器。 這應該符合叢集管理 SVM 的項目：
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. 確認已為資料 SVM 建立 DNS 服務：
      `vserver services name-service dns show`

4. 使用應用程式登錄後儲存的用戶端ID和租戶ID來啟用Azure Key Vault：
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_vault_name -key-id Azure_key_ID`

5. 檢查金鑰管理程式的狀態：
   `security key-manager external azure check`
   輸出內容如下：

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

   如果是 `service_reachability` 狀態不是 `OK`、SVM無法以所有必要的連線和權限來連線至Azure Key Vault服務。請確保您的Azure網路原則和路由不會封鎖您的私有vNet、使其無法到達Azure KeyVault Public端點。如果有、請考慮使用Azure私有端點、從vNet內存取金鑰庫。您可能還需要在SVM上新增靜態主機項目、以解析端點的私有IP位址。

   。 `kms_wrapped_key_status` 將會報告 `UNKNOWN` 初始組態時。其狀態將變更為 `OK` 加密第一個磁碟區之後。

6. 選用：建立測試Volume以驗證NVE的功能。

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

如果設定正確、Cloud Volumes ONTAP 則會自動建立Volume並啟用Volume加密。

7. 確認磁碟區已正確建立並加密。如果是、則是 `-is-encrypted` 參數會顯示為 `true`。
```
vol show -vserver SVM_name -fields is-encrypted
```

# 利用Google的雲端金鑰管理服務來管理金鑰

## 您可以使用 "Google Cloud Platform的金鑰管理服務（雲端KMS）" 在ONTAP Google Cloud Platform部署的應用程式中保護您的不加密金鑰。

雲端KMS的金鑰管理可透過CLI或ONTAP REST API啟用。

使用 Cloud KMS 時、請注意、根據預設、會使用 Data SVM 的 LIF 與雲端金鑰管理端點通訊。節點管理網路用於與雲端供應商的驗證服務（oauth2.googleapis.com）進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

開始之前

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權
- 安裝多租戶加密金鑰管理（MTEKM）授權、從Cloud Volumes ONTAP 版本號為E59.12.1 GA開始。
- 您必須是叢集或SVM管理員
- 現用Google Cloud Platform訂閱

限制

- 雲端KMS只能在資料SVM上設定

## 組態

**Google Cloud**

1. 在您的Google Cloud環境中、 "建立對稱的GCP金鑰環和金鑰"。
2. 為Cloud Volumes ONTAP 您的服務帳戶建立自訂角色。

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. 將自訂角色指派給 Cloud KMS 金鑰和 Cloud Volumes ONTAP 服務帳戶：
   `gcloud kms keys add-iam-policy-binding *key_name* --keyring *key_ring_name* --location *key_location* --member serviceAccount:_service_account_Name_ --role projects/*customer_project_id*/roles/kmsCustomRole`
4. 下載服務帳戶 JSON 金鑰：
   `gcloud iam service-accounts keys create key-file --iam-account=*sa-name*@*project-id*.iam.gserviceaccount.com`

**Cloud Volumes ONTAP**

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 切換至進階權限層級：
   `set -privilege advanced`
3. 為資料SVM建立DNS。
   `dns create -domains c.<*project*>.internal -name-servers *server_address* -vserver *SVM_name*`
4. 建立 CMEK 項目：
   `security key-manager external gcp enable -vserver *SVM_name* -project-id *project* -key-ring-name *key_ring_name* -key-ring-location *key_ring_location* -key-name *key_name*`
5. 出現提示時、請從GCP帳戶輸入服務帳戶Json金鑰。
6. 確認已啟用的程序成功：
   `security key-manager external gcp check -vserver *svm_name*`
7. 選用：建立磁碟區以測試加密 `vol create *volume_name* -aggregate *aggregate* -vserver *vserver_name* -size 10G`

## 疑難排解

如果您需要疑難排解、可以跳接上述最後兩個步驟中的原始REST API記錄：

1. `set d`
2. `systemshell -node *node* -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

# 改善防範勒索軟體的能力

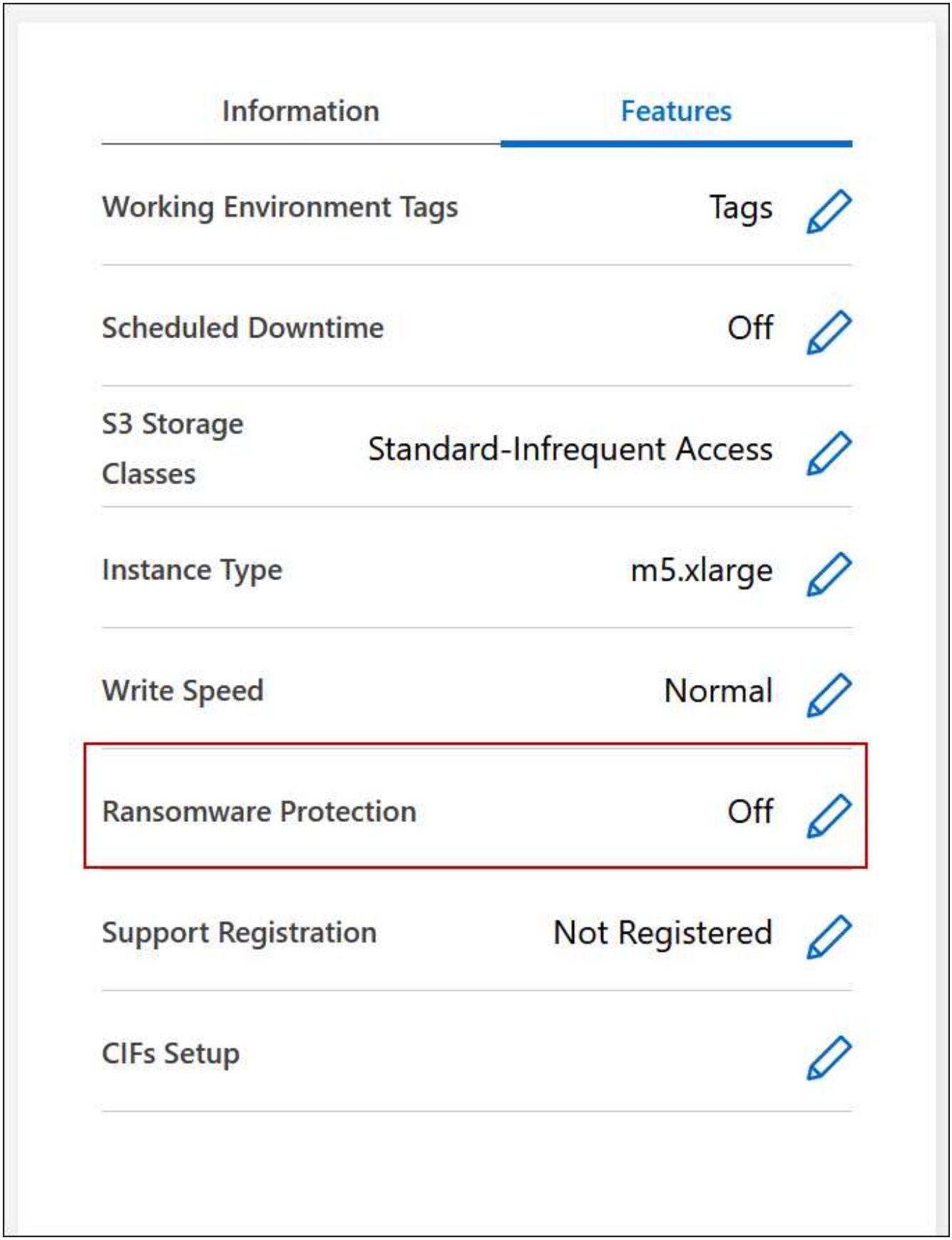
勒索軟體攻擊可能會耗費一定的時間、資源和商譽。BlueXP 可讓您針對勒索軟體實作兩種 NetApp 解決方案：防範常見的勒索軟體副檔名和自動勒索軟體保護（ ARP ）。這些解決方案可提供有效的工具、以利可見度、偵測和補救。

## 防止常見勒索軟體檔案副檔名

透過 BlueXP 、勒索軟體保護設定可讓您利用 ONTAP FPolicy 功能來防範常見的勒索軟體檔案副檔名類型。

步驟

1. 在 Canvas 頁面上、按兩下您設定為勒索軟體保護的系統名稱。
2. 在「概述」索引標籤上、按一下「功能」面板、然後按一下 * 勒索軟體保護 * 旁的鉛筆圖示。




3. 實作 NetApp 勒索軟體解決方案：

   a. 如果您的磁碟區未啟用 Snapshot 原則、請按一下「 * 啟動 Snapshot Policy* 」。

NetApp Snapshot 技術提供業界最佳的勒索軟體補救解決方案。成功還原的關鍵在於從未受感染的備份還原。Snapshot 複本為唯讀、可防止勒索軟體毀損。他們也能提供精細度、以建立單一檔案複本或完整災難恢復解決方案的映像。

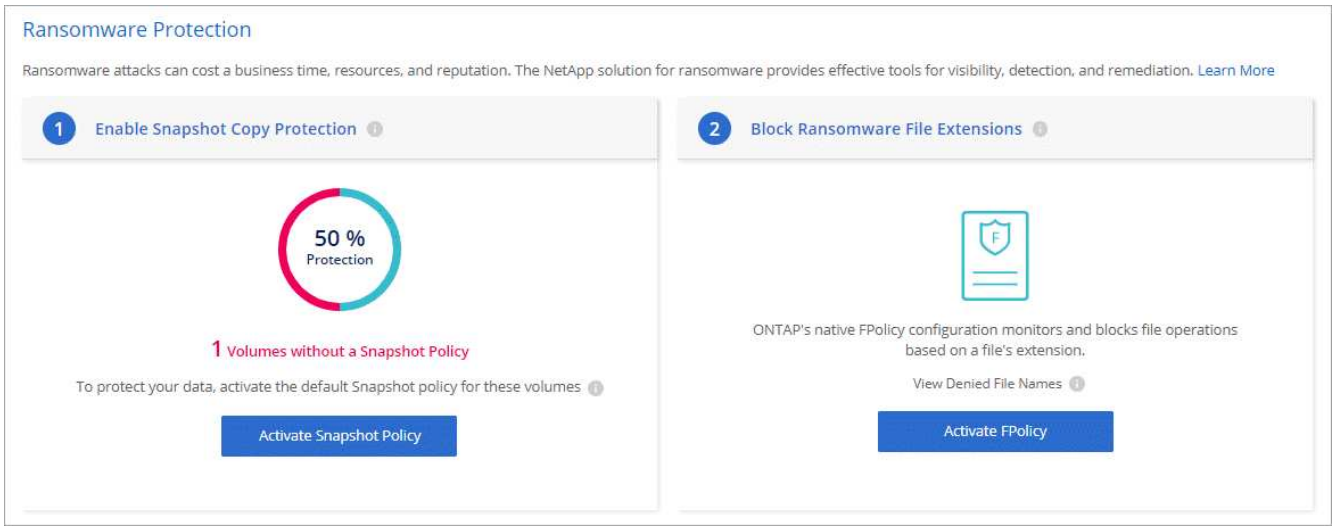
b. 按一下「 * 啟動 FPolicy* 」以啟用 ONTAP 的 FPolicy 解決方案、此解決方案可根據檔案副檔名來封鎖檔案作業。

這項預防解決方案可封鎖常見的勒索軟體檔案類型、藉此改善保護、避免勒索軟體攻擊。

預設FPolicy範圍會封鎖下列副檔名的檔案：

微、加密、鎖定、加密、加密、 crinf, r5a、XRNT, XDBL、R16M01D05、 Pzdc、好、好！、天哪！、RDM、 RRK、加密RS、crjoker、EnCipErEd、LeChiffre

當您啟動Cloud Volumes ONTAP 有關功能的FPolicy時、BlueXP就會建立這個範圍。此清單是根據常見的勒索軟體檔案類型。您可以使用Cloud Volumes ONTAP 來自於整個CLI的_vserver fpolicy scoon__命令來自訂封鎖的副檔名。




## 自主勒索軟體保護

Cloud Volumes ONTAP 支援「自動勒索軟體保護」（ARP ）功能、可對工作負載執行分析、主動偵測並警告可能表示勒索軟體攻擊的異常活動。

與透過提供的檔案副檔名保護分開 "勒索軟體保護設定"、 ARP 功能會使用工作負載分析、根據偵測到的「異常活動」來警示使用者可能遭受的攻擊。勒索軟體保護設定和 ARP 功能均可搭配使用、以提供全面的勒索軟體保護。

ARP 功能僅適用於節點型和容量型授權模式的 BYOL 授權（一、二及三年期限）。您必須聯絡您的 NetApp 銷售代表、以購買新的獨立附加授權、以搭配 Cloud Volumes ONTAP 中的 ARP 功能使用。

購買附加授權並將其新增至 Digital Wallet 後、您可以使用 Cloud Volumes ONTAP 以每個磁碟區為基礎來啟用 ARP 。磁碟區的 ARP 組態是透過 ONTAP 系統管理員和 ONTAP CLI 執行。

如需如何使用 ONTAP 系統管理員和 CLI 啟用 ARP 的詳細資訊、請參閱 "啟用自發勒索軟體保護"。

若未取得授權、則無法使用授權功能。