安全性和資料加密
Cloud Volumes ONTAP

NetApp
February 13, 2026

目錄

安全性和資料加密

使用NetApp加密解決方案加密Cloud Volumes ONTAP上的捲

Cloud Volumes ONTAP支援NetApp磁碟區加密 (NVE) 和NetApp聚合加密 (NAE)。 NVE 和 NAE 是基於軟體的解決方案，可實現符合 FIPS 140-2 標準的捲靜態資料加密。"了解有關這些加密解決方案的更多信息" 。

NVE 和 NAE 均由外部金鑰管理器支援。

如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果def::gcp[] endif::gcp[] 如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果你::gcp[] defendiffcp[]

使用 AWS 金鑰管理服務管理Cloud Volumes ONTAP加密金鑰

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

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

使用 KMS 時，請注意預設使用資料 SVM 的 LIF 與雲端金鑰管理端點進行通訊。節點管理網路用於與 AWS 的身份驗證服務進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服務。

開始之前

- Cloud Volumes ONTAP必須運作 9.12.0 或更高版本
- 您必須已安裝磁碟區加密 (VE) 許可證，並且
- 您必須已安裝多租用戶加密金鑰管理 (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

您只能為資料 SVM 配置金鑰。

配置

AWS

1. 您必須創建一個"授予"用於管理加密的 IAM 角色將使用的 AWS KMS 金鑰。 IAM 角色必須包含允許以下操作的策略：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`若要建立贈款，請參閱"AWS 文件"。
2. "為適當的 IAM 角色新增策略。"政策應該支持 `DescribeKey`， `Encrypt` ， 和 `Decrypt`營運.

Cloud Volumes ONTAP

1. 切換到您的Cloud Volumes ONTAP環境。
2. 切換到進階權限等級：
   `set -privilege advanced`
3. 啟用 AWS 金鑰管理員：
   `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，輸入金鑰。
5. 確認 AWS KMS 已正確配置：
   `security key-manager external aws show -vserver svm_name`

使用 Azure Key Vault 管理Cloud Volumes ONTAP加密金鑰

您可以使用 Azure Key Vault (AKV) 來保護 Azure 部署的應用程式中ONTAP加密金鑰。請參閱"Microsoft 文件"。

AKV 僅可用於保護資料 SVM 的NetApp磁碟區加密 (NVE) 金鑰。欲了解更多信息，請參閱"ONTAP文檔" 。

可以使用 CLI 或ONTAP REST API 啟用 AKV 金鑰管理。

使用 AKV 時，請注意預設使用資料 SVM LIF 與雲端金鑰管理端點通訊。節點管理網路用於與雲端提供者的身份驗證服務（login.microsoftonline.com）進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服務。

開始之前

- Cloud Volumes ONTAP必須運作 9.10.1 或更高版本
- 已安裝磁碟區加密 (VE) 授權（NetApp磁碟區加密許可證會自動安裝在每個在NetApp支援中註冊的Cloud Volumes ONTAP系統上）
- 您必須擁有多租戶加密金鑰管理 (MT_EK_MGMT) 許可證
- 您必須是叢集或 SVM 管理員
- 有效的 Azure 訂閱

限制

- AKV 只能在資料 SVM 上配置
- NAE 不能與 AKV 一起使用。 NAE 需要外部支援的 KMIP 伺服器。
- Cloud Volumes ONTAP節點每 15 分鐘輪詢一次 AKV，以確認可存取性和金鑰可用性。此輪詢週期是不可設定的，並且在輪詢嘗試連續四次失敗後（總共 1 小時），磁碟區將處於離線狀態。

配置過程

概述的步驟擷取如何向 Azure 註冊您的Cloud Volumes ONTAP配置以及如何建立 Azure Key Vault 和金鑰。如果您已經完成這些步驟，請確保您具有正確的配置設置，特別是在建立 Azure Key Vault，然後繼續Cloud Volumes ONTAP配置。

- 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）
- Cloud Volumes ONTAP配置

Azure 應用程式註冊

1. 您必須先在 Azure 訂閱中註冊您希望Cloud Volumes ONTAP用於存取 Azure Key Vault 的應用程式。在 Azure 入口網站中，選擇套用註冊。
2. 選擇新註冊。
3. 為您的應用程式提供名稱並選擇支援的應用程式類型。預設的單一租戶足以滿足 Azure Key Vault 的使用。選擇註冊。
4. 在 Azure 概覽視窗中，選擇已註冊的應用程式。將應用程式（客戶端）**ID**和目錄（租用戶）**ID**複製到安全位置。在稍後的註冊過程中將需要它們。

建立 **Azure** 用戶端機密

1. 在 Azure Key Vault 應用程式註冊的 Azure 入口網站中，選擇「憑證和機密」窗格。
2. 選擇新客戶端密鑰。為您的客戶端密鑰輸入一個有意義的名稱。 NetApp建議的有效期限為 24 個月；但是，您的特定雲端治理策略可能需要不同的設定。
3. 按一下新增以建立客戶端金鑰。複製值列中列出的秘密字串，並將其儲存在安全的位置，以便稍後使用Cloud Volumes ONTAP配置。當您離開該頁面後，秘密值將不再顯示。

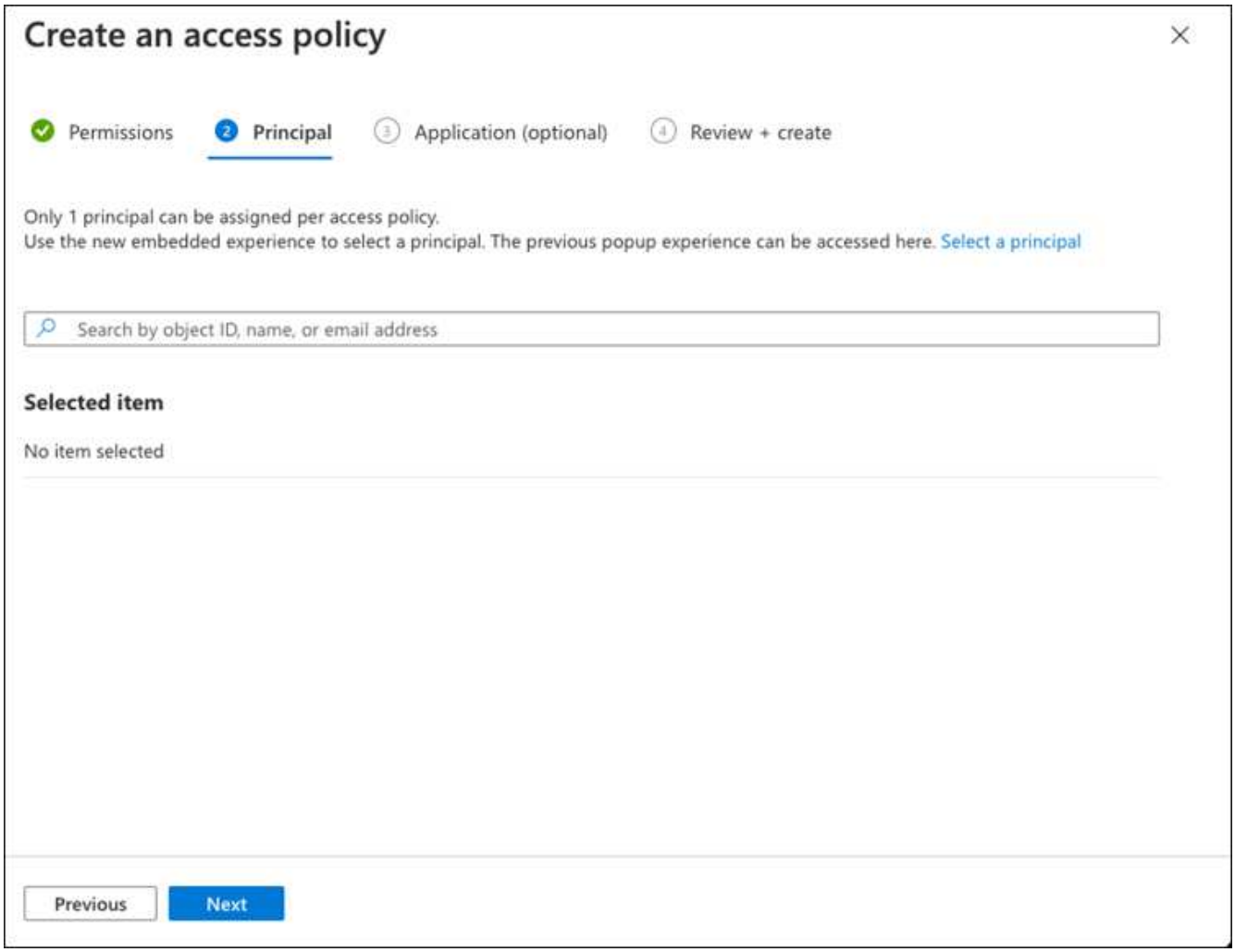
建立 **Azure Key Vault**

1. 如果您有現有的 Azure Key Vault，則可以將其連接到Cloud Volumes ONTAP配置；但是，您必須根據此過程中的設定調整存取原則。
2. 在 Azure 入口網站中，導覽至 **Key Vaults** 部分。
3. 點擊「+建立」並輸入所需信息，包括資源組、區域和定價層。此外，輸入保留已刪除保管庫的天數，並在金鑰保管庫上選擇啟用清除保護。
4. 選擇下一步來選擇存取策略。
5. 選擇以下選項：
   a. 在存取配置下，選擇**Vault** 訪問策略。
   b. 在資源存取下，選擇**Azure** 磁碟加密進行磁碟區加密。
6. 選擇“+建立”以新增存取策略。
7. 在從範本配置下，按一下下拉式選單，然後選擇金鑰、機密和憑證管理範本。
8. 選擇每個下拉權限選單（金鑰、秘密、憑證），然後在選單清單頂部選擇全選以選擇所有可用的權限。您應該：
   - 關鍵權限：已選擇 20 個
   - 秘密權限：已選擇 8 個
   - 憑證權限：已選擇 16 個


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，選擇您在 Azure 中建立的主體註冊應用程式Azure 應用程式註冊。選擇下一步。

   每個策略只能分配一個主體。



10. 按一下下一步兩次，直到到達審核並建立。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檢視 **+** 建立來建立金鑰保管庫。 （網路存取方法可能由治理策略或您的企業雲端安全團隊規定。）
13. 記錄金鑰保管庫 URI：在您建立的金鑰保管庫中，導覽至概覽功能表並從右側列複製**Vault URI**。您需要它來完成後面的步驟。

建立加密金鑰

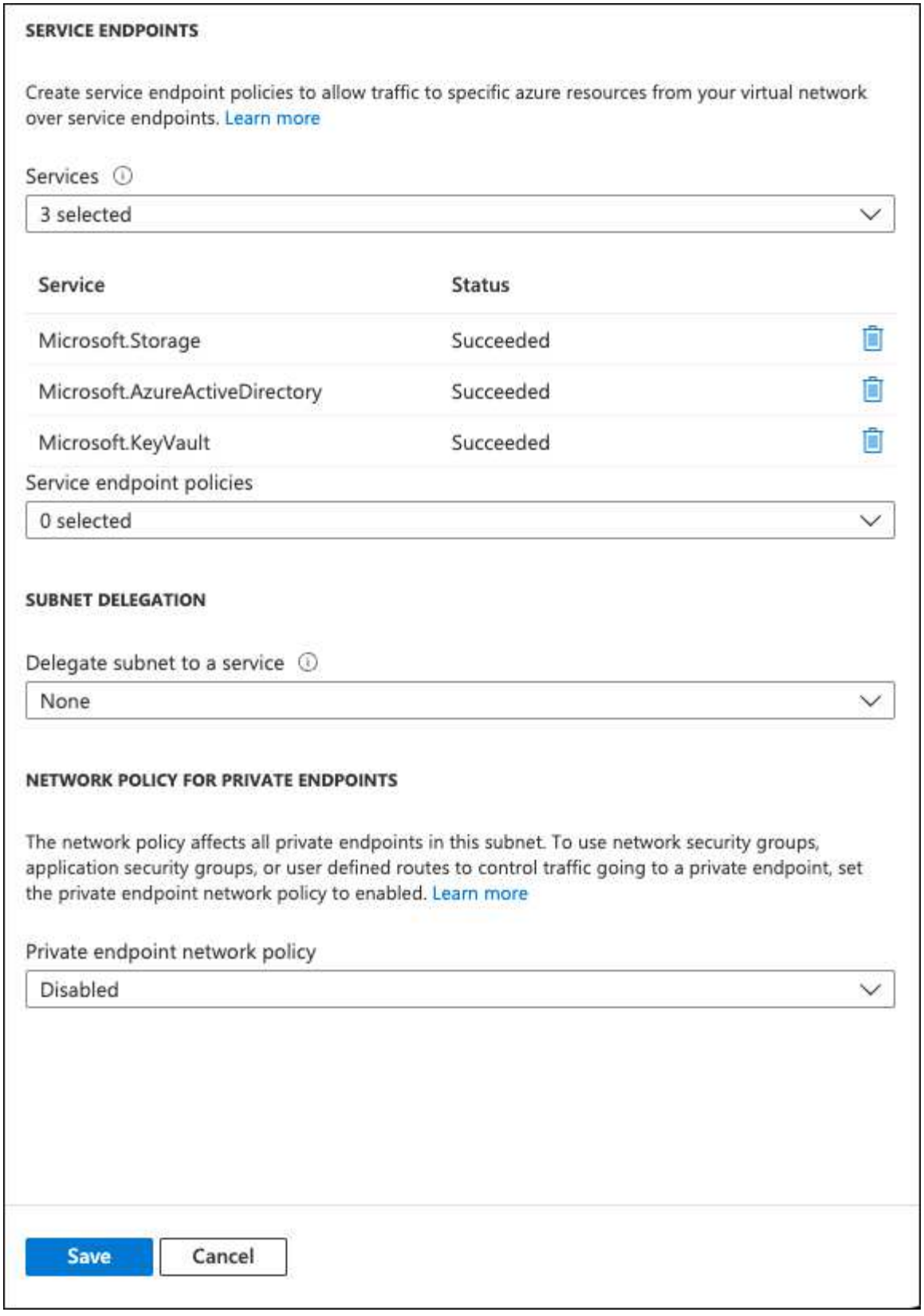
1. 在您為Cloud Volumes ONTAP建立的 Key Vault 選單中，導覽至 **Keys** 選項。
2. 選擇產生/導入來建立新金鑰。
3. 將預設選項設定為生成。
4. 提供以下資訊：
   - 加密金鑰名稱

- 金鑰類型：RSA
- RSA金鑰大小：2048
- 已啟用：是

5. 選擇建立來建立加密金鑰。
6. 返回**Keys**選單並選擇您剛剛建立的密鑰。
7. 選擇目前版本下的金鑰ID，查看金鑰屬性。
8. 找到密鑰標識符欄位。複製 URI，直到但不包括十六進位字串。

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

1. 僅當您為 HA Cloud Volumes ONTAP系統設定 Azure Key Vault 時才需要此程序。
2. 在 Azure 入口網站中導覽至虛擬網路。
3. 選擇部署Cloud Volumes ONTAP系統的虛擬網絡，然後選擇頁面左側的子網選單。
4. 從清單中選擇Cloud Volumes ONTAP部署的子網路名稱。
5. 導航至服務端點標題。在下拉式選單中，選擇以下內容：
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage**（可選）



6. 選擇儲存來捕獲您的設定。

Cloud Volumes ONTAP配置

1. 使用您首選的 SSH 用戶端連線到叢集管理 LIF。
2. 在ONTAP中進入進階權限模式：

```
set advanced -con off
```

3. 確定所需的資料 SVM 並驗證其 DNS 配置：
   `vserver services name-service dns show`

   a. 如果所需資料 SVM 的 DNS 項目存在且包含 Azure DNS 項目，則無需執行任何操作。如果沒有，請為資料 SVM 新增指向 Azure DNS、私人 DNS 或本機伺服器的 DNS 伺服器項目。這應該與叢集管理員 SVM 的條目相符：
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

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

4. 使用應用程式註冊後儲存的用戶端 ID 和租用戶 ID 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 key_vault_URI -key-id full_key_URI`

   這 `_full_key_URI`價值必須利用 `<https:// <key vault host name>/keys/<key label>`格式。

5. 成功啟用 Azure Key Vault 後，輸入 `client secret value`當出現提示時。

6. 檢查密鑰管理器的狀態：
   `security key-manager external azure check`輸出將如下所示：

```
::*> 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 `service_reachability`狀態不是 `OK`，SVM 無法透過所有必要的連線和權限存取 Azure Key Vault 服務。確保您的 Azure 網路策略和路由不會阻止您的私人 vNet 到達 Azure Key Vault 公共終端點。如果確實如此，請考慮使用 Azure Private 端點從 vNet 內部存取 Key Vault。您可能還需要在 SVM 上新增靜態主機條目來解析端點的私人 IP 位址。

這 `kms_wrapped_key_status`將會報告 `UNKNOWN`在初始配置時。其狀態將變為 `OK`第一卷加密後。

7. 可選：建立測試卷以驗證 NVE 的功能。

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

   如果配置正確， Cloud Volumes ONTAP將自動建立磁碟區並啟用磁碟區加密。

8. 確認卷已正確建立並加密。如果是的話， `-is-encrypted`參數將顯示為 `true`。
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```
9. 可選：如果要更新 Azure Key Vault 驗證憑證上的憑證，請使用下列命令：
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

相關連結

- "設定Cloud Volumes ONTAP以在 Azure 中使用客戶管理的金鑰"
- "Microsoft Azure 文件：關於 Azure Key Vault"
- "ONTAP指令參考指南"

使用 Google Cloud KMS 管理Cloud Volumes ONTAP加密金鑰

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

可以使用ONTAP CLI 或ONTAP REST API 啟用 Cloud KMS 的金鑰管理。

使用 Cloud KMS 時，請注意預設使用資料 SVM 的 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提供者的身份驗證服務（oauth2.googleapis.com）進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服務。

開始之前

- 您的系統應該執行Cloud Volumes ONTAP 9.10.1 或更高版本
- 您必須使用資料 SVM。 Cloud KMS 只能在資料 SVM 上配置。
- 您必須是叢集或 SVM 管理員
- 應在 SVM 上安裝磁碟區加密 (VE) 許可證
- 從Cloud Volumes ONTAP 9.12.1 GA 開始，也應安裝多租用戶加密金鑰管理 (MTEKM) 許可證
- 需要有效的 Google Cloud Platform 訂閱

配置

Google雲

1. 在您的 Google Cloud 環境中，"建立對稱 GCP 金鑰環和金鑰" 。
2. 為 Cloud KMS 金鑰和Cloud Volumes ONTAP服務帳戶指派自訂角色。
   a. 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.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

b. 指派您建立的自訂角色：
`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`

> 如果您使用的是Cloud Volumes ONTAP 9.13.0 或更高版本，則無需建立自訂角色。您可以指派預定義的[cloudkms.cryptoKeyEncrypterDecrypter^] 角色。

3. 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. 使用您首選的 SSH 用戶端連線到叢集管理 LIF。
2. 切換到進階權限等級：
`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 條目：
`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，請輸入您的 GCP 帳戶中的服務帳戶 JSON 金鑰。
6. 確認啟用流程成功：
`security key-manager external gcp check -vserver *svm_name*`
7. 可選：建立磁碟區來測試加密 `vol create *volume_name* -aggregate *aggregate* -vserver *vserver_name* -size 10G`

故障排除

如果需要進行故障排除，您可以在上面的最後兩個步驟中追蹤原始 REST API 日誌：

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

為Cloud Volumes ONTAP啟用NetApp勒索軟體防護解決方案

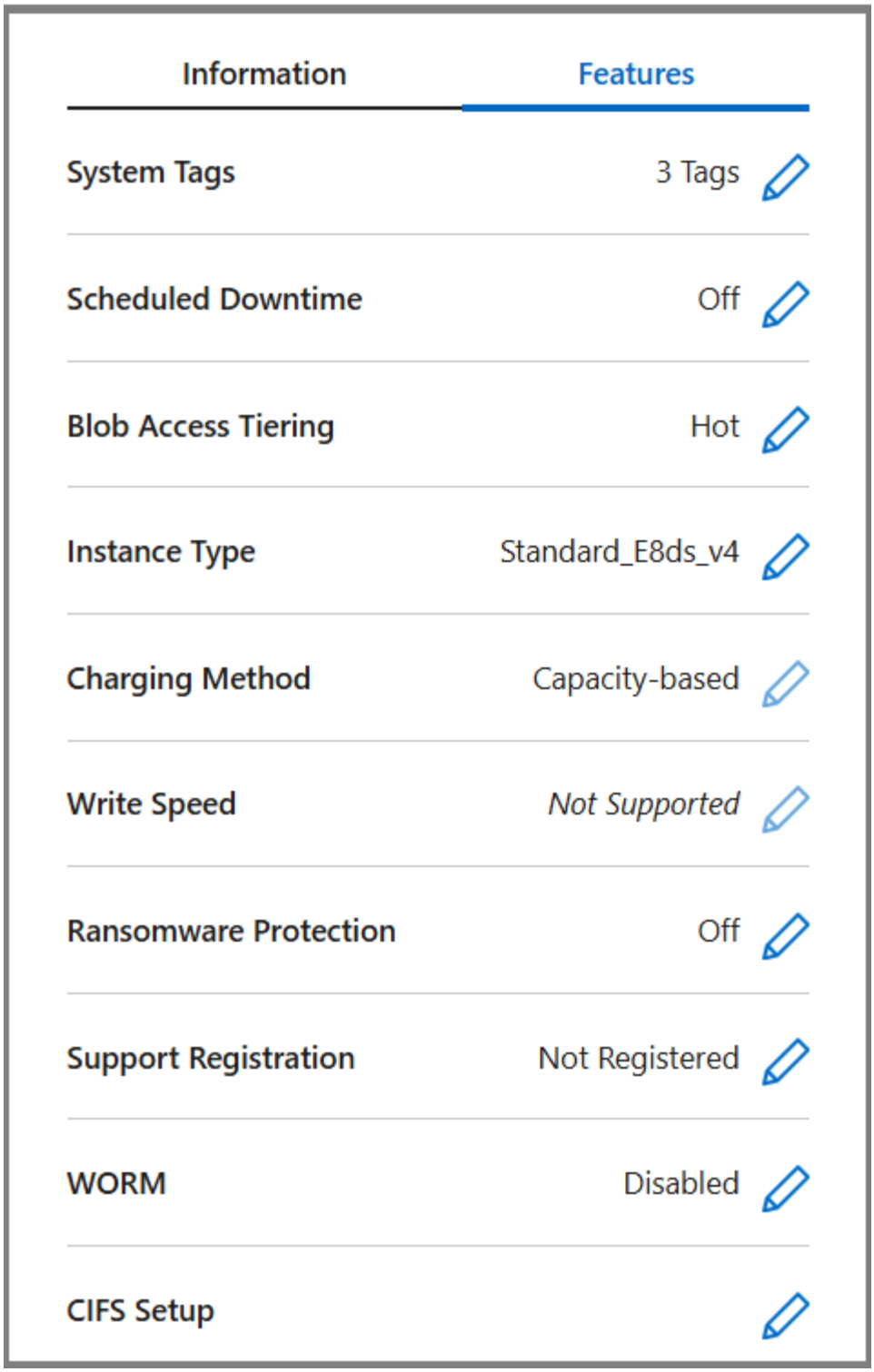
勒索軟體攻擊會浪費企業的時間、資源和聲譽。 NetApp Console可讓您實施兩種NetApp勒索軟體解決方案：針對共同勒索軟體檔案副檔名的防護和自主勒索軟體防護 (ARP)。這些解決方案為可見性、檢測和補救提供了有效的工具。

防禦常見勒索軟體檔案副檔名

控制台上的勒索軟體防護設定可讓您利用ONTAP FPolicy 功能來防禦常見的勒索軟體檔案擴充類型。

步驟

1. 在 **Systems** 頁面上，雙擊您配置為使用勒索軟體保護的Cloud Volumes ONTAP系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「勒索軟體防護」旁的鉛筆圖示。



3. 實施NetApp勒索軟體解決方案：

   a. 如果您的磁碟區未啟用快照策略，請按一下「啟動快照策略」。

      NetApp Snapshot 技術提供了業界最佳的勒索軟體補救解決方案。成功復原的關鍵是從未受感染的備份中復原。快照副本是唯讀的，可防止勒索軟體破壞。他們還可以提供創建單一文件副本或完整災難復原解決方案的圖像的粒度。

   b. 按一下「啟動 **FPolicy**」以啟用 ONTAP 的 FPolicy 解決方案，該解決方案可以根據檔案的副檔名阻止檔

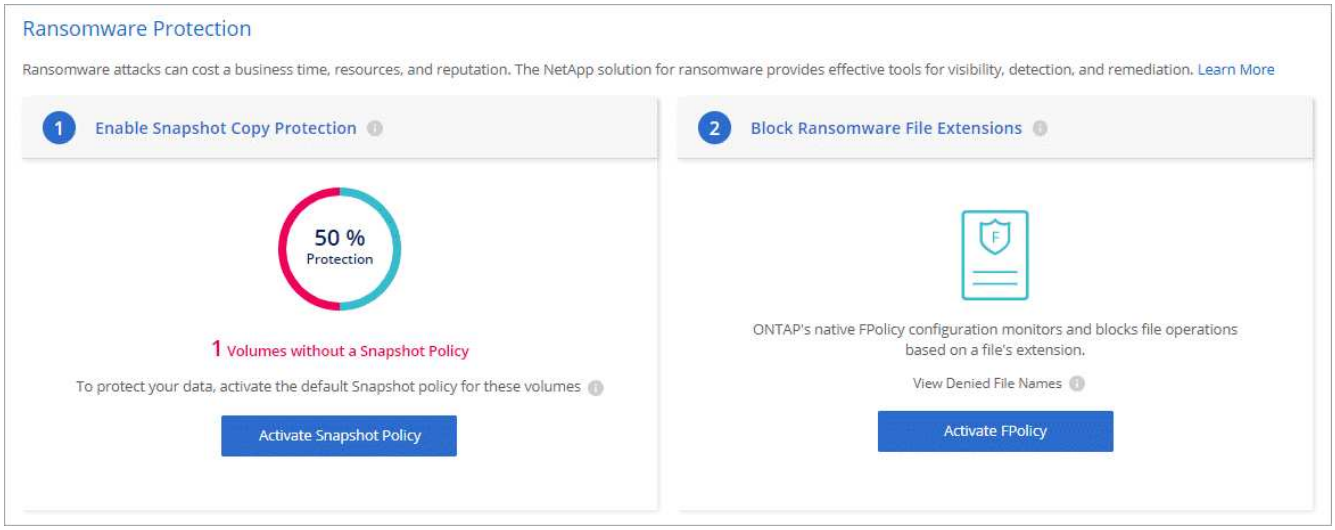
案操作。

此預防解決方案透過阻止常見的勒索軟體檔案類型來提高對勒索軟體攻擊的防護。

預設 FPolicy 範圍會封鎖具有下列副檔名的檔案：

micro、加密、鎖定、加密、crypt、crinf、r5a、XRNT、XTBL、R16M01D05、pzdc、好、哈哈！、OMG！ 、RDM、RRK、encryptedRS、crjoker、EnCiPhErEd、LeChiffre

當您在Cloud Volumes ONTAP上啟動 FPolicy 時，將會建立此範圍。此列表基於常見的勒索軟體檔案類型。您可以使用Cloud Volumes ONTAP CLI 中的 *vserver fpolicy policy scope* 指令自訂被封鎖的檔案副檔名。



自主勒索軟體防護

Cloud Volumes ONTAP支援自主勒索軟體防護 (ARP) 功能，可對工作負載進行分析，以主動偵測並警告可能表明勒索軟體攻擊的異常活動。

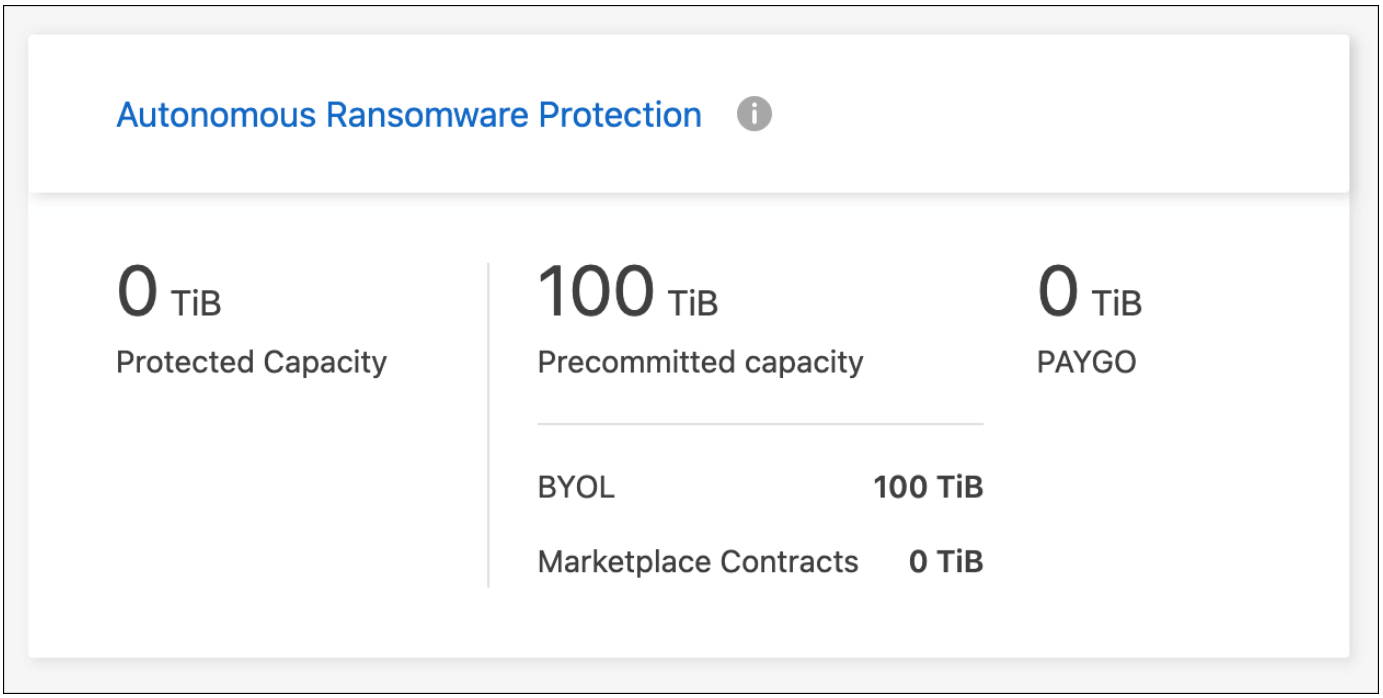
與透過以下方式提供的檔案副檔名保護分開 "勒索軟體防護設置"，ARP 功能使用工作負載分析根據偵測到的「異常活動」向使用者發出潛在攻擊警報。勒索軟體防護設定和 ARP 功能可以結合使用，以實現全面的勒索軟體防護。

ARP 功能可與自帶授權 (BYOL) 一起使用，且無需額外付費即可在市場訂閱您的授權。

啟用 ARP 的磁碟區具有指定狀態「學習模式」或「活動」 。

卷的 ARP 配置是透過ONTAP系統管理器和ONTAP CLI 執行的。

有關如何使用ONTAP System Manager 和ONTAP CLI 啟用 ARP 的更多信息，請參閱 "ONTAP文件：啟用自主勒索軟體防護"。



在Cloud Volumes ONTAP上建立 WORM 檔案的防篡改 Snapshot 副本

您可以在Cloud Volumes ONTAP系統上建立一次寫入、多次讀取 (WORM) 檔案的防篡改 Snapshot 副本，並在特定保留期內以未修改的形式保留快照。此功能由SnapLock技術提供支持，並提供了額外的資料保護和合規性層。

開始之前

確保用於建立 Snapshot 副本的磁碟區是SnapLock磁碟區。有關在卷上啟用SnapLock保護的信息，請參閱 "ONTAP文件：設定SnapLock"。

步驟

1. 從SnapLock磁碟區建立 Snapshot 副本。有關使用 CLI 或系統管理員建立 Snapshot 副本的信息，請參閱 "ONTAP文件：管理本機 Snapshot 副本概述"。

   Snapshot 副本繼承了磁碟區的 WORM 屬性，使其具有防篡改功能。底層的SnapLock技術可確保快照在指定的保留期結束之前受到保護，不會被編輯和刪除。

2. 如果需要編輯這些快照，您可以修改保留期。欲了解更多信息，請參閱 "ONTAP文檔：設定保留時間"。

即使 Snapshot 副本在特定保留期內受到保護，叢集管理員也可以刪除來源磁碟區，因為Cloud Volumes ONTAP中的 WORM 儲存在「可信任儲存管理員」模型下執行。此外，受信任的雲端管理員可以透過操作雲端儲存資源來刪除WORM資料。

相關連結

- 有關 WORM 的更多信息，請參閱"了解Cloud Volumes ONTAP上的 WORM 存儲"。
- 有關SnapLock卷的充電信息，請參閱"Cloud Volumes ONTAP中的授權和計費"。

版權資訊

商標資訊