安全性與資料加密
Cloud Volumes ONTAP

NetApp
June 15, 2022

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。

新的Aggregate在您設定外部金鑰管理程式之後、預設會啟用NAE。非 NAE Aggregate 一部分的新磁碟區預設會啟用 NVE （例如、如果在設定外部金鑰管理程式之前已建立現有的 Aggregate ）。

不支援內建金鑰管理。 Cloud Volumes ONTAP

您的支援系統應該已向 NetApp 註冊。 Cloud Volumes ONTAPNetApp Volume Encryption授權會自動安裝在Cloud Volumes ONTAP 每個註冊NetApp支援的支援系統上。

- "新增 NetApp 支援網站帳戶至 Cloud Manager"
- "註冊隨用隨付系統"

Cloud Manager 不會在中國地區的系統上安裝 NVE 授權。

步驟

1. 檢閱中支援的關鍵管理程式清單 "NetApp 互通性對照表工具"。

   搜尋 * 關鍵經理 * 解決方案。

2. "連線 Cloud Volumes ONTAP 至 CLI"。
3. 設定外部金鑰管理。
   - AWS ： "如ONTAP 需相關指示、請參閱《產品資訊》文件"
     - Azure ： "Azure Key Vault（AKV）"
     - Google Cloud： "Google Cloud金鑰管理服務"

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。

先決條件

- 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）
- 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
- 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Cloud Volumes ONTAP 中、選取「認證與機密」窗格。
2. 選取「**新用戶端機密」*輸入有意義的用戶端機密名稱。NetApp建議使用24個月的到期日、不過您的特定雲端治理原則可能需要不同的設定。
3. 選取「*新增」以儲存用戶端機密。立即複製機密的*值*、並將其儲存在安全的地方、以供未來設定使用。在您離開頁面後、不會顯示機密值。

建立**Azure Key Vault**

1. 如果您有現有的Azure Key Vault、您可以將其連線Cloud Volumes ONTAP 至您的功能表組態、不過您必須將存取原則調整為此程序中的設定。

2. 在Azure入口網站中、瀏覽至「**關鍵故障」區段。
3. 選擇「建立」。輸入所需資訊、包括資源群組、地區和價格層、並選擇保留刪除的保存資料室的天數、以及是否啟用清除保護。就本組態而言、預設值已足夠、不過您的特定雲端治理原則可能需要不同的設定。
4. 選擇「*下一步」以選擇存取原則。
5. 選擇「* Azure Disk Encryption*（* Azure磁碟加密）」作為磁碟區加密選項、選擇「* Vault存取原則*」作為權限模式。
6. 選取「**新增存取原則」。
7. 選取「自範本設定」（選用）字段旁邊的插入號。然後選擇「**金鑰、機密與認證管理」
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：19個已選取
    - **機密權限：選擇8項
    - 認證權限：16項已選取
9. 選取「*新增」以建立存取原則。
10. 選擇「下一步」進入「*網路」*選項。
11. 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。）
12. 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」。您稍後將需要此功能。

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、從清單中選取「Microsoft.AzureActiveDirectory」。
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 ：「et advanc進 階-con Off」（設定進階-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*-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：「安全金鑰管理程式外部azure enable -vserver *Svm_name*-client-id *Azure*用戶端_*ID*-租 戶ID *Azure*租戶_*ID*-name *Azure*金鑰名稱-key-id *Azure*金鑰_*ID*」
5. 驗證金鑰管理程式組態：「安全金鑰管理程式外部azure show」
6. 檢查金鑰管理程式的狀態：「安全金鑰管理程式外部azure檢查」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「連線能力」狀態不是「正常」、SVM將無法以所有必要的連線和權限來連線至Azure Key Vault服務。初始組態時、「kms」迴應鍵狀態會報告「unkNOWNKNOWNKY」。第一個磁碟區加密後、其狀態會變更為「OK（正常）」。

7. 選用：建立測試Volume以驗證NVE的功能。

「vol create -vserver *Svm_name*-volume *volVolume _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。

8. 確認磁碟區已正確建立並加密。如果是的話、「-is-Encrypted」參數會顯示為「true」。「vol show -vserver *svm_name*-Fields is加密」

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、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（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。

先決條件

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權
- 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
- 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金鑰與Cloud Volumes ONTAP 更新服務帳戶：「gCloud kms金鑰add-iam-policy-binding *key_name*-keyring *key_ring_name*-location *-member ServiceAccount*：*_service_Account_Name*-role專案/*customer_project _id*/ros/ros/kmsCustomrole」
4. 下載服務帳戶Json金鑰：「gCloud iam服務帳戶金鑰可建立金鑰檔案-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. 切換至進階權限等級：「et -priv榮幸 進階」
3. 為資料SVM建立DNS。「建立網域C_<project >_.internal -name-servers *server_address*-vserver *Svm_name*」
4. 建立CMEK項目：「安全金鑰管理程式外部GCP啟用-vserver *Svm_name*-project -id *project _-key-ring_name _key_ring_name*-key-ring_location *key_ring_stip*-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. 確認啟用的程序成功：「安全金鑰管理程式外部GCP檢查-vserver *svm_name*」
7. 選用：建立磁碟區以測試加密「volvol create *volvolvole_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. "以d為準"
2. "ystemShell -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。Cloud Manager 可讓您針對勒索軟體實作 NetApp 解決方案、提供有效的可見度、偵測及補救工具。

步驟

1. 在工作環境中、按一下 * 勒索軟體 * 圖示。

2. 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

      Cloud Manager會在Cloud Volumes ONTAP 啟用FPolicy on功能時建立此範圍。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。