安全性與資料加密
Cloud Volumes ONTAP

NetApp
June 01, 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、可對磁碟區進行（ FIPS ） 140-2 相容的閒置資料加密。 "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。

   "如ONTAP 需相關指示、請參閱《產品資訊》文件"。

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。

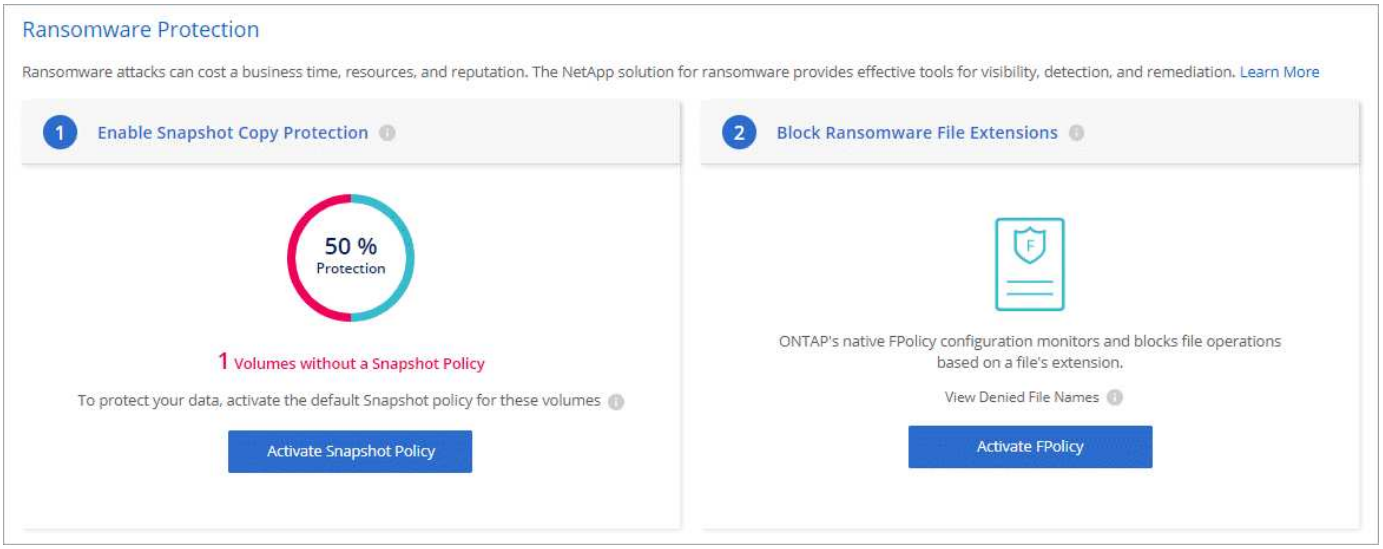
   b. 按一下「 * 啟動 FPolicy* 」以啟用 ONTAP 的 FPolicy 解決方案、此解決方案可根據檔案副檔名來封鎖檔案作業。

      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。



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和Cloud KMS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
- 這個支援NVE的叢集節點必須支援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Azure訂閱

限制

- NSE和NAE金鑰無法使用AKV
- AKV不適用於MetroCluster 不完整的組態。
- AKV只能在資料SVM上設定

組態程序

組態**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：建立測試磁碟區以驗證AKV的功能。「vol create -vserver *Svm_name*-volume *volVolume _name* -Aggregate *aggr _-size _size*-state online -policy預設值」如果設定正確、ONTAP 則會自動建立磁碟區並啟用磁碟區加密。
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。

金鑰管理雲端KMS可透過CLI或ONTAP REST API啟用。若要設定Cloud KMS Cloud Volumes ONTAP 以供使用、您必須先設定

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

- 這個支援NVE的叢集節點必須支援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

限制

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 雲端KMS不適用於NSE和NAE。
- 雲端KMS不適用於MetroCluster 不完整的組態。
- 雲端KMS只能在資料SVM上設定
- 現用Google Cloud Platform訂閱

啟用

1. 在Google Cloud環境中：
   a. 建立對稱的GCP金鑰環和金鑰：
   b. 為Cloud Volumes ONTAP 您的服務帳戶建立自訂角色：「gcloud iam角色可建立kmsCustom勞力 -project =*project _id*-TITLE=*kms_custom_roue_name*-description=*custom_rousion_description* -privations.cryptoKeyVerations.gms.list 、cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.locations.get,cloudkms.locations.list,resourcemanager.projects.get - ga-ga=bake /
   c. 將自訂角色指派Cloud Volumes ONTAP 給Cloud KMS金鑰與更新服務帳戶：「gCloud kms key add-iam-policy-bindusting $｛*key_name*｝-keyring $｛*key_ring_name*｝-location $｛*key_portation*｝ -member ServiceAccount：$｛*service_Account_Name*｝-role專案/客戶_專案/_<Customk_rooles_專案角色
   d. 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」
2. 切換Cloud Volumes ONTAP 到您的自然環境：
   a. 切換至進階權限等級：「et -priv榮幸 進階」
   b. 為資料SVM建立DNS。“建立網域C_[project]_.internal -name-servers *server_address*-vserver *Svm_name*`
   c. 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*」
   d. 出現提示時、請從GCP帳戶輸入服務帳戶Json金鑰。
   e. 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*」
   f. 選用：建立磁碟區以測試加密「volvol create *volvolvole_name*>-Aggregate *-vserver _vserver_name* -size 10G'

疑難排解

如果需要疑難排解、您可以跳接上述最後兩個步驟中的原始REST API記錄：。《設定》。"ystemShell -node_node_-command tail -f /mroot/etc/log/mlog/kmip2_client.log"