



## 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.....	1
使用 NetApp 加密解決方案加密磁碟區 .....	1
改善防範勒索軟體的能力 .....	1
使用Azure Key Vault管理金鑰 .....	3
利用Google的雲端金鑰管理服務來管理金鑰 .....	4

# 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：

- 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。

- 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 `_yscoper fpolicy soon__` 命令來自訂封鎖的副檔名。

### Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

#### 1 Enable Snapshot Copy Protection

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

# 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 *vol/Volume\_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\_rouision\_description*  
-privations.cryptoKeyVerations.gms.list  
、cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.useToEncrypt,cloudkms.cryp  
yptoKeys.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 vol/vol/*vole\_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"

## 版權資訊

Copyright©2022 NetApp、Inc.版權所有。美國印製本文件中版權所涵蓋的任何部分、不得以任何形式或任何方式（包括影印、錄製、在未事先取得版權擁有者書面許可的情況下、在電子擷取系統中進行錄音或儲存。

衍生自受版權保護之NetApp資料的軟體必須遵守下列授權與免責聲明：

本軟體係由NetApp「依現狀」提供、不含任何明示或暗示的保證、包括但不限於適售性及特定用途適用性的暗示保證、特此聲明。在任何情況下、NetApp均不對任何直接、間接、偶發、特殊、示範、或衍生性損害（包括但不限於採購替代商品或服務；使用損失、資料或利潤損失；或業務中斷）、無論是在合約、嚴格責任或侵權行為（包括疏忽或其他）中、無論是因使用本軟體而產生的任何責任理論（包括疏忽或其他）、即使已被告知可能造成此類損害。

NetApp保留隨時變更本文所述之任何產品的權利、恕不另行通知。除非NetApp以書面明確同意、否則NetApp不承擔因使用本文所述產品而產生的任何責任或責任。使用或購買本產品並不代表NetApp擁有任何專利權利、商標權利或任何其他智慧財產權。

本手冊所述產品可能受到一或多個美國國家/地區的保護專利、國外專利或申請中。

限制權利圖例：政府使用、複製或揭露受DFARS 252.277-7103（1988年10月）和FAR 52-227-19（1987年6月）技術資料與電腦軟體權利條款（c）（1）（ii）分段所述限制。

## 商標資訊

NetApp、NetApp標誌及所列的標章 <http://www.netapp.com/TM> 為NetApp、Inc.的商標。其他公司和產品名稱可能為其各自所有者的商標。