安全性和数据加密
Cloud Volumes ONTAP

NetApp
June 14, 2022

目录

安全性和数据加密

使用 NetApp 加密解决方案对卷进行加密

Cloud Volumes ONTAP 支持 NetApp 卷加密（ NVE ）和 NetApp 聚合加密（ NAE ）。NVE和NAE是基于软件的解决方案、支持FIPS 140-2合规的卷空闲数据加密。 "详细了解这些加密解决方案"。

外部密钥管理器支持 NVE 和 NAE 。

在设置外部密钥管理器后，新聚合将默认启用 NAE 。默认情况下，不属于 NAE 聚合的新卷将启用 NVE （例如，如果您有在设置外部密钥管理器之前创建的现有聚合）。

Cloud Volumes ONTAP 不支持板载密钥管理。

您的 Cloud Volumes ONTAP 系统应向 NetApp 支持部门注册。向 NetApp 支持部门注册的每个 Cloud Volumes ONTAP 系统都会自动安装 NetApp 卷加密许可证。

- "将 NetApp 支持站点帐户添加到 Cloud Manager"
- "注册按需购买的系统"

Cloud Manager 不会在位于中国地区的系统上安装 NVE 许可证。

步骤

1. 查看中支持的密钥管理器列表 "NetApp 互操作性表工具"。

   搜索 * 密钥管理器 * 解决方案。

2. "连接到 Cloud Volumes ONTAP 命令行界面"。
3. 配置外部密钥管理。
   - Google Cloud "Google Cloud密钥管理服务"

使用Google的云密钥管理服务管理密钥

您可以使用 "Google Cloud Platform 的密钥管理服务（ Cloud KMS ）" 在部署了Google Cloud Platform的应用程序中保护ONTAP 加密密钥。

可以使用命令行界面或ONTAP REST API启用Cloud KMS的密钥管理。

使用Cloud KMS时、请注意、默认情况下、数据SVM LIF用于与云密钥管理端点进行通信。节点管理网络用于与云提供商的身份验证服务(oauth2.googleapis.com)进行通信。如果集群网络配置不正确，集群将无法正确利用密钥管理服务。

前提条件

- Cloud Volumes ONTAP 必须运行9.10.1或更高版本

- 已安装卷加密（ VE ）许可证
- 已安装多租户加密密钥管理（ MTEKM ）许可证
- 您必须是集群管理员或SVM管理员
- 有效的Google Cloud Platform订阅

限制

- 只能在数据SVM上配置Cloud KMS

Configuration

Google Cloud

1. 在Google Cloud环境中、 "创建对称GCP密钥环和密钥"。
2. 为Cloud Volumes ONTAP 服务帐户创建自定义角色。

```
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. 将自定义角色分配给云KMS密钥和Cloud Volumes ONTAP 服务帐户：`gcloud kms keys add-iam-policy-binding` *`key_name`*`-keyring` *`key_ring_name`*`-location` *`key_location`*`-member serviceAccount：` *`service_account_Name`*`-role projects_custom_id_/role/kmsRole`
4. 下载服务帐户JSON密钥：`gcloud iam service-accounts keys create key-file -iam -account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. 使用首选SSH客户端连接到集群管理LIF。
2. 切换到高级权限级别：`set -privilege advanced`
3. 为数据SVM创建DNS。`dns create -domains C.<`*`project`*`>.internal -name-servers` *`server_address`*`-vserver` *`svm_name`*
4. 创建CMEE条目：`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. 出现提示时、输入GCP帐户中的服务帐户JSON密钥。
6. 确认已启用的过程成功：`security key-manager external GCP check -vserver` *`svm_name`*
7. 可选：创建一个卷以测试加密`vol create *volume_name*-aggregate *aggregate*-vserver *vserver_name*-size

10G`

故障排除

如果您需要进行故障排除、可以在上述最后两个步骤中结束原始REST API日志：

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

提高防范勒索软件的能力

勒索软件攻击可能会耗费业务时间，资源和声誉。您可以通过 Cloud Manager 实施 NetApp 解决方案 for 勒索软件，它可以提供有效的工具来实现可见性，检测和补救。

步骤

1. 在工作环境中，单击 * 勒索软件 * 图标。

2. 实施 NetApp 解决方案 for 勒索软件：

   a. 如果卷未启用 Snapshot 策略，请单击 * 激活 Snapshot 策略 * 。

      NetApp Snapshot 技术可为勒索软件补救提供业内最佳的解决方案。成功恢复的关键在于从未受感染的备份中还原。Snapshot 副本为只读副本，可防止勒索软件损坏。它们还可以提供创建单个文件副本或完整灾难恢复解决方案映像的粒度。

   b. 单击 * 激活 FPolicy* 以启用 ONTAP 的 FPolicy 解决方案，它可以根据文件扩展名阻止文件操作。

      此预防性解决方案可通过阻止常见的勒索软件文件类型来增强抵御勒索软件攻击的能力。

      默认 FPolicy 范围会阻止具有以下扩展名的文件：

      微型，加密，锁定，加密，加密 crinf ， r5a ， rxNT ， XTbl ， R16M01D05 ， pzdc ，好， LOL ！ ， OMG ！ ， RDM ， RRK ， encryptedRS ， crjoker ， EnciPhErEd ， LeChiffre

当您在 Cloud Volumes ONTAP 上激活 FPolicy 时， Cloud Manager 将创建此范围。此列表基于常见的勒索软件文件类型。您可以使用 Cloud Volumes ONTAP 命令行界面中的 *vserver fpolicy policy scopes* 命令来自定义阻止的文件扩展名。