# 安全性和数据加密
## Cloud Volumes ONTAP

NetApp
July 19, 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。
   - AWS "有关说明，请参见 ONTAP 文档"
     - Azure 酒店 "Azure 密钥存储（ AKV ）"
     - Google Cloud "Google Cloud密钥管理服务"

## 使用Azure密钥存储管理密钥

您可以使用 "Azure 密钥存储（ AKV ）" 保护Azure部署应用程序中的ONTAP 加密密钥。

可使用AKV进行保护 "NetApp 卷加密（ NVE ）密钥" 仅适用于数据SVM。

可以使用命令行界面或ONTAP REST API启用使用AKV的密钥管理。

使用AKV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(login.microsoftonline.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(已向NetApp支持部门注册的每个Cloud Volumes ONTAP 系统会自动安装NetApp卷加密许可证)
- 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
- Active Azure订阅

限制

- 只能在数据SVM上配置AKV

## 配置过程

概述的步骤将介绍如何向Azure注册Cloud Volumes ONTAP 配置以及如何创建Azure密钥存储和密钥。如果您已完成这些步骤、请确保配置设置正确、尤其是在中 创建Azure密钥存储、然后继续 Cloud Volumes ONTAP 配置。

- Azure应用程序注册
- 创建Azure客户端密钥
- 创建Azure密钥存储
- 创建加密密钥
- 创建Azure Active Directory端点(仅限HA)
- Cloud Volumes ONTAP 配置

**Azure**应用程序注册

1. 您必须先在希望Cloud Volumes ONTAP 用于访问Azure密钥存储的Azure订阅中注册应用程序。在Azure门户中、选择"*应用注册"。
2. 选择"新建注册"。
3. 请为您的应用程序提供一个名称、然后选择支持的应用程序类型。默认的单个租户足以使用Azure密钥存储。选择"注册"。
4. 在Azure概述窗口中、选择已注册的应用程序。将**应用程序(客户端) ID*和*目录(租户) ID*复制到安全位置。注册过程稍后将需要这些许可证。

创建**Azure**客户端密钥

1. 在Cloud Volumes ONTAP 应用程序的Azure门户中、选择"证明 和机密"窗格。
2. 选择"*新客户端密钥"*输入一个有意义的客户端密钥名称。NetApp建议使用24个月的到期期限、但您的特定云监管策略可能需要其他设置。
3. 选择"*添加"以保存客户端密钥。立即复制该机密的"*值"、并将其存储在安全的位置、以供将来配置时使用。离开此页面后、不会显示此机密值。

创建**Azure**密钥存储

1. 如果您已有Azure密钥存储、则可以将其连接到Cloud Volumes ONTAP 配置、但您必须根据此过程中的设置调整访问策略。

2. 在Azure门户中、导航到"*密钥存储"部分。
3. 选择"创建"。输入所需信息、包括资源组、区域和定价层、并选择保留已删除存储的天数以及是否启用了清除保护。对于此配置、默认值足以满足要求、但您的特定云监管策略可能需要不同的设置。
4. 选择"*下一步"以选择访问策略。
5. 对于卷加密选项、请选择"* Azure磁盘加密"；对于权限模型、请选择"。存储访问策略"。
6. 选择"添加访问策略"。
7. 选择"**从模板配置(可选)"*字段旁边的插入项。然后、选择"*密钥"、"机密"和"认证管理"
8. 选择每个下拉权限菜单(密钥、密钥、证书)、然后选择菜单列表顶部的"**全选"*以选择所有可用权限。您应具备：
   - "关键权限"：已选择19个
   - "*机密权限"：已选择8个
   - "*证书权限"：已选择16个
9. 选择"*添加"以创建访问策略。
10. 选择"*下一步"*以进入"*网络连接"*选项。
11. 选择适当的网络访问方法或选择"**所有网络"*和"*查看+创建"*以创建密钥存储。(网络访问方法可能由监管策略或您的企业云安全团队规定。)
12. 记录密钥存储URI：在您创建的密钥存储中、导航到概述菜单并从右侧列复制"*存储URI"。您将在后续步骤中使用此功能。

创建加密密钥

1. 在为Cloud Volumes ONTAP 创建的密钥存储的菜单中、导航到"*密钥"选项。
2. 选择"*生成/导入"*以创建新密钥。
3. 将默认选项设置为"*生成"。
4. 请提供以下信息：
   - 加密密钥名称
   - 密钥类型：RSA
   - RSA密钥大小：2048
   - Enabled：是
5. 选择"**创建"以创建加密密钥。
6. 返回到"**密钥"菜单、然后选择刚刚创建的密钥。
7. 在"*当前版本"下选择密钥ID以查看密钥属性。
8. 找到"*密钥标识符"*字段。将此URI复制到、但不包括十六进制字符串。

创建**Azure Active Directory**端点(仅限**HA**)

1. 只有在为HA Cloud Volumes ONTAP 工作环境配置Azure密钥存储时、才需要执行此过程。
2. 在Azure门户中、导航到"**虚拟网络"。
3. 选择部署Cloud Volumes ONTAP 工作环境的虚拟网络、然后选择页面左侧的"*子网"*菜单。

4. 从列表中选择Cloud Volumes ONTAP 部署的子网名称。
5. 导航到"**服务端点"*标题。在下拉菜单中、从列表中选择"4.microsoft.AzureActiveDirectory"。
6. 选择"*保存"*以捕获设置。

**Cloud Volumes ONTAP** 配置

1. 使用首选SSH客户端连接到集群管理LIF。
2. 在ONTAP 中进入高级权限模式：`set advanced -con off`
3. 确定所需的数据SVM并验证其DNS配置：`vserver services name-service dns show`
   a. 如果所需数据SVM的DNS条目存在、并且其中包含Azure DNS的条目、则无需执行任何操作。如果不支持、请为指向Azure DNS、专用DNS或内部部署服务器的数据SVM添加DNS服务器条目。这应与集群管理SVM的条目匹配：`vserver services name-service dns create -vserver *svm_name* -domains *domain*-name-servers *ip_address*`
   b. 验证是否已为数据SVM创建DNS服务：`vserver services name-service dns show`
4. 使用应用程序注册后保存的客户端ID和租户ID启用Azure密钥存储：`security key-manager external azure enable -vserver *svm_name*-client-id *Azure_client_ID*-tenant-id *Azure_tenant_ID*-name *Azure_key_name*-key-id *Azure_key_ID*`
5. 验证密钥管理器配置：`security key-manager external azure show`
6. 检查密钥管理器的状态：`security key-manager external azure check` The output will look like：

```
::*> 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`sservice_reachability` status为not `OK`、则SVM无法使用所有必需的连接和权限访问Azure密钥存储服务。在初始配置时、`kms_Wraped_key_status`将报告`unknown`。对第一个卷加密后、其状态将更改为`OK`。

7. 可选：创建测试卷以验证NVE的功能。

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

如果配置正确、Cloud Volumes ONTAP 将自动创建卷并启用卷加密。

8. 确认卷已正确创建和加密。如果是、则` is-encrypted`参数将显示为`true`。`vol show -vserver svm_name-fields is-encrypted`

# 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。

使用此功能改进对勒索软件的保护可解决与不同的使用情形 "ONTAP 防勒索软件功能" 可通过System Manager或ONTAP 命令行界面启用。

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。