安全和数据加密
Cloud Volumes ONTAP

NetApp
February 13, 2026

目录

安全和数据加密

使用NetApp加密解决方案加密Cloud Volumes ONTAP上的卷

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，可实现符合 FIPS 140-2 标准的卷静态数据加密。"了解有关这些加密解决方案的更多信息" 。

NVE 和 NAE 均由外部密钥管理器支持。

如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果def::gcp[] endif::gcp[] 如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果def::gcp[] endif::gcp[]

使用 AWS Key Management Service 管理Cloud Volumes ONTAP加密密钥

您可以使用"AWS 的密钥管理服务 (KMS)"在 AWS 部署的应用程序中保护您的ONTAP加密密钥。

可以使用 CLI 或ONTAP REST API 启用 AWS KMS 的密钥管理。

使用 KMS 时，请注意默认情况下使用数据 SVM 的 LIF 与云密钥管理端点进行通信。节点管理网络用于与 AWS 的身份验证服务进行通信。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。

开始之前

- Cloud Volumes ONTAP必须运行 9.12.0 或更高版本
- 您必须已安装卷加密 (VE) 许可证，并且
- 您必须已安装多租户加密密钥管理 (MTEKM) 许可证。
- 您必须是集群或 SVM 管理员
- 您必须拥有有效的 AWS 订阅

您只能为数据 SVM 配置密钥。

配置

AWS

1. 您必须创建一个"授予"用于管理加密的 IAM 角色将使用的 AWS KMS 密钥。 IAM 角色必须包含允许以下操作的策略：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`要创建赠款，请参阅"AWS 文档"。
2. "向适当的 IAM 角色添加策略。"政策应该支持 `DescribeKey`， `Encrypt` ， 和 `Decrypt`运营。

Cloud Volumes ONTAP

1. 切换到您的Cloud Volumes ONTAP环境。
2. 切换到高级权限级别：
   `set -privilege advanced`
3. 启用 AWS 密钥管理器：
   `security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 出现提示时，输入密钥。
5. 确认 AWS KMS 配置正确：
   `security key-manager external aws show -vserver svm_name`

使用 Azure Key Vault 管理Cloud Volumes ONTAP加密密钥

您可以使用 Azure Key Vault (AKV) 来保护 Azure 部署的应用程序中ONTAP加密密钥。请参阅"Microsoft 文档"。

AKV 仅可用于保护数据 SVM 的NetApp卷加密 (NVE) 密钥。欲了解更多信息，请参阅"ONTAP 文档" 。

可以使用 CLI 或ONTAP REST API 启用 AKV 密钥管理。

使用 AKV 时，请注意默认情况下使用数据 SVM LIF 与云密钥管理端点通信。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。

开始之前

- 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（NetApp卷加密许可证会自动安装在每个在NetApp支持中注册的Cloud Volumes ONTAP系统上）
- 您必须拥有多租户加密密钥管理 (MT_EK_MGMT) 许可证
- 您必须是集群或 SVM 管理员
- 有效的 Azure 订阅

限制

- AKV 只能在数据 SVM 上配置
- NAE 不能与 AKV 一起使用。 NAE 需要外部支持的 KMIP 服务器。
- Cloud Volumes ONTAP节点每 15 分钟轮询一次 AKV，以确认可访问性和密钥可用性。此轮询周期是不可配置的，并且在轮询尝试连续四次失败后（总共 1 小时），卷将处于脱机状态。

配置过程

概述的步骤捕获了如何向 Azure 注册您的Cloud Volumes ONTAP配置以及如何创建 Azure Key Vault 和密钥。如果您已经完成这些步骤，请确保您具有正确的配置设置，特别是在创建 Azure Key Vault，然后继续Cloud Volumes ONTAP配置。

- Azure 应用程序注册

- 创建 Azure 客户端机密
- 创建 Azure Key Vault
- 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. 您必须首先在 Azure 订阅中注册您希望Cloud Volumes ONTAP用于访问 Azure Key Vault 的应用程序。在 Azure 门户中，选择应用注册。
2. 选择新注册。
3. 为您的应用程序提供一个名称并选择支持的应用程序类型。默认的单个租户足以满足 Azure Key Vault 的使用。选择注册。
4. 在 Azure 概览窗口中，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。在稍后的注册过程中将需要它们。

创建 **Azure** 客户端机密

1. 在 Azure Key Vault 应用注册的 Azure 门户中，选择“证书和机密”窗格。
2. 选择新客户端密钥。为您的客户端密钥输入一个有意义的名称。 NetApp建议的有效期为 24 个月；但是，您的特定云治理策略可能需要不同的设置。
3. 单击添加以创建客户端密钥。复制值列中列出的秘密字符串，并将其存储在安全的位置，以便稍后使用Cloud Volumes ONTAP配置。离开该页面后，秘密值将不再显示。

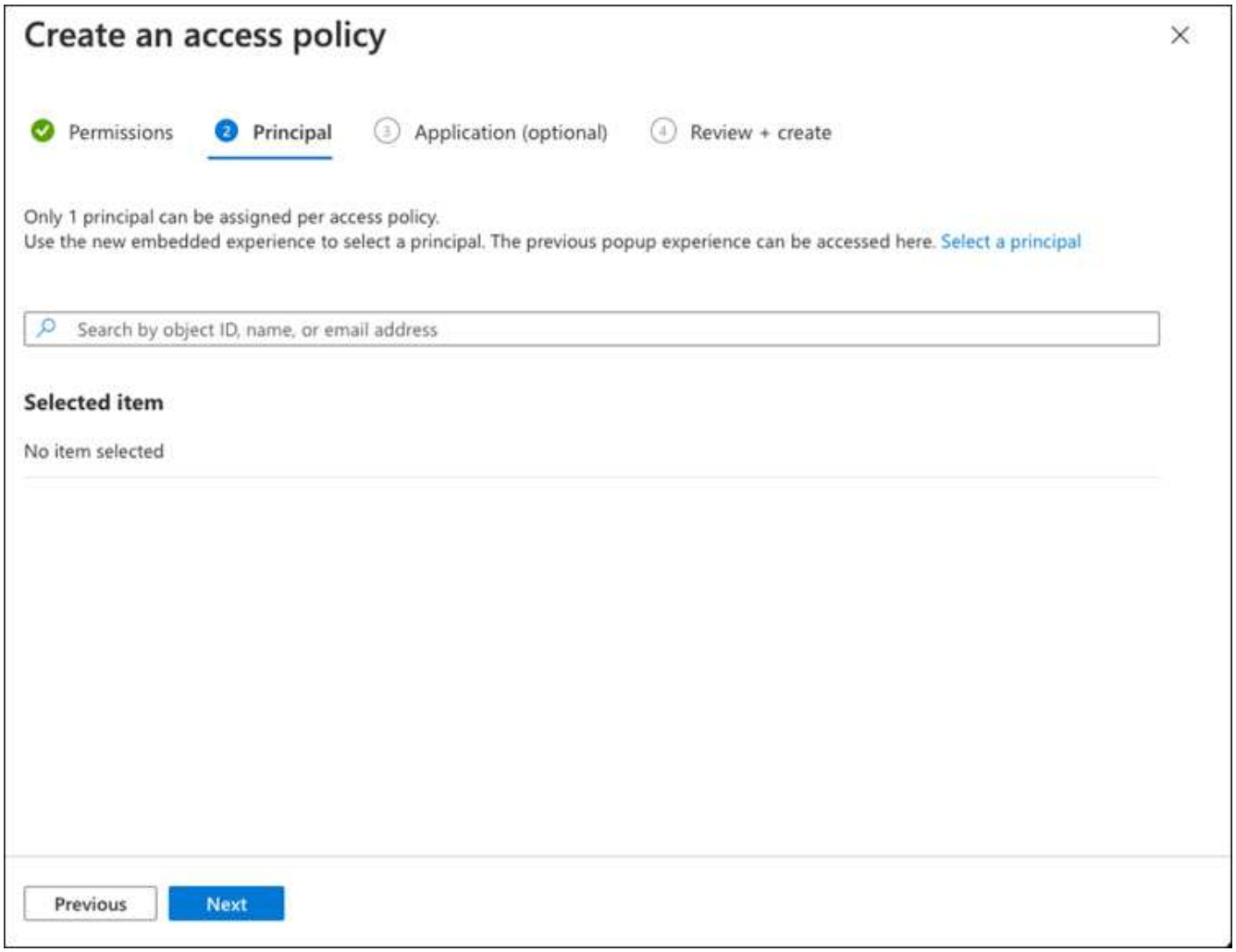
创建 **Azure Key Vault**

1. 如果您有现有的 Azure Key Vault，则可以将其连接到Cloud Volumes ONTAP配置；但是，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 **Key Vaults** 部分。
3. 单击“+创建”并输入所需信息，包括资源组、区域和定价层。此外，输入保留已删除保管库的天数，并在密钥保管库上选择启用清除保护。
4. 选择下一步来选择访问策略。
5. 选择以下选项：
   a. 在访问配置下，选择**Vault** 访问策略。
   b. 在资源访问下，选择**Azure** 磁盘加密进行卷加密。
6. 选择“+创建”以添加访问策略。
7. 在从模板配置下，单击下拉菜单，然后选择密钥、机密和证书管理模板。
8. 选择每个下拉权限菜单（密钥、秘密、证书），然后在菜单列表顶部选择全选以选择所有可用的权限。您应该：
   - 关键权限：已选择 20 个
   - 秘密权限：已选择 8 个
   - 证书权限：已选择 16 个


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. 单击下一步，选择您在 Azure 中创建的主体注册应用程序Azure 应用程序注册。选择下一步。

   每个策略只能分配一个主体。



10. 单击下一步两次，直到到达审核并创建。然后，单击创建。
11. 选择下一步进入网络选项。
12. 选择适当的网络访问方法或选择所有网络和查看 + 创建来创建密钥保管库。 （网络访问方法可能由治理策略或您的企业云安全团队规定。）
13. 记录密钥保管库 URI：在您创建的密钥保管库中，导航到概览菜单并从右侧列复制**Vault URI**。您需要它来完成后面的步骤。

创建加密密钥

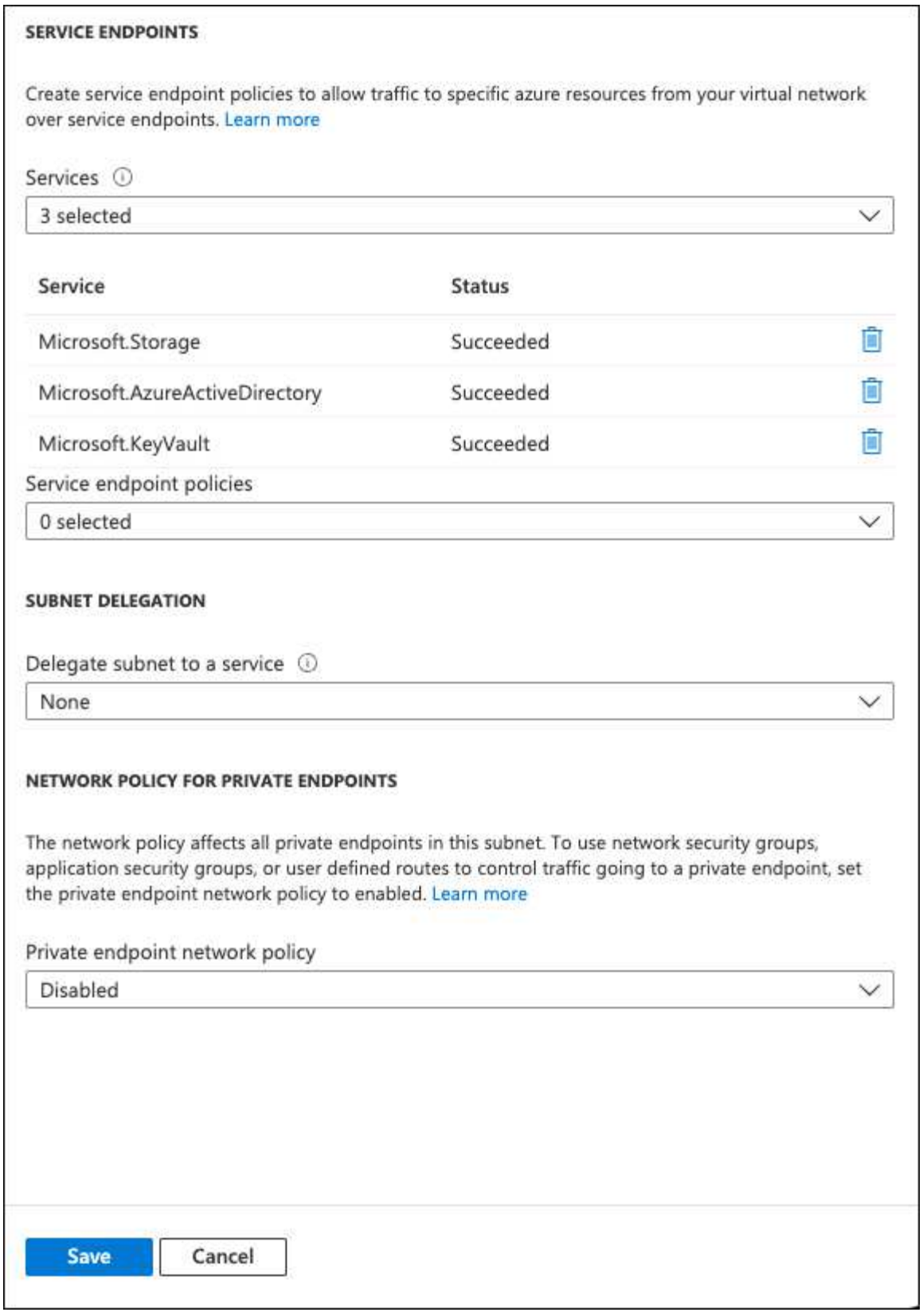
1. 在您为Cloud Volumes ONTAP创建的 Key Vault 菜单中，导航到 **Keys** 选项。
2. 选择生成/导入来创建新密钥。
3. 将默认选项设置为生成。
4. 提供以下信息：
   - 加密密钥名称

- 密钥类型：RSA
- RSA密钥大小：2048
- 已启用：是

5. 选择创建来创建加密密钥。
6. 返回**Keys**菜单并选择您刚刚创建的密钥。
7. 选择当前版本下的密钥ID，查看密钥属性。
8. 找到密钥标识符字段。复制 URI，直到但不包括十六进制字符串。

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

1. 仅当您为 HA Cloud Volumes ONTAP系统配置 Azure Key Vault 时才需要此过程。
2. 在 Azure 门户中导航到虚拟网络。
3. 选择部署Cloud Volumes ONTAP系统的虚拟网络，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，选择以下内容：
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage**（可选）



6. 选择保存来捕获您的设置。

Cloud Volumes ONTAP配置

1. 使用您首选的 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 条目存在并且包含 Azure DNS 条目，则无需执行任何操作。如果没有，请为数据 SVM 添加指向 Azure DNS、私有 DNS 或本地服务器的 DNS 服务器条目。这应该与集群管理员 SVM 的条目匹配：
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. 验证已为数据 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 Key Vault：
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   这 `_full_key_URI`价值必须利用 `<https:// <key vault host name>/keys/<key label>`格式。

5. 成功启用 Azure Key Vault 后，输入 `client secret value`当出现提示时。

6. 检查密钥管理器的状态：
   `security key-manager external azure check`输出将如下所示：

```
::*> 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 `service_reachability`状态不是 `OK`，SVM 无法通过所有必需的连接和权限访问 Azure Key Vault 服务。确保您的 Azure 网络策略和路由不会阻止您的私有 vNet 到达 Azure Key Vault 公共终结点。如果确实如此，请考虑使用 Azure Private 端点从 vNet 内部访问 Key Vault。您可能还需要在 SVM 上添加静态主机条目来解析端点的私有 IP 地址。

这 `kms_wrapped_key_status`将会报告 `UNKNOWN`在初始配置时。其状态将变为 `OK`第一卷加密后。

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. 确认卷已正确创建并加密。如果是的话， `-is-encrypted`参数将显示为 `true。
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```
9. 可选：如果要更新 Azure Key Vault 身份验证证书上的凭据，请使用以下命令：
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

相关链接

- "设置Cloud Volumes ONTAP以在 Azure 中使用客户管理的密钥"
- "Microsoft Azure 文档：关于 Azure Key Vault"
- "ONTAP命令参考指南"

使用 Google Cloud KMS 管理Cloud Volumes ONTAP加密密钥

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

可以使用ONTAP CLI 或ONTAP REST API 启用 Cloud KMS 的密钥管理。

使用 Cloud KMS 时，请注意默认情况下使用数据 SVM 的 LIF 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。

开始之前

- 您的系统应该运行Cloud Volumes ONTAP 9.10.1 或更高版本
- 您必须使用数据 SVM。 Cloud KMS 只能在数据 SVM 上配置。
- 您必须是集群或 SVM 管理员
- 应在 SVM 上安装卷加密 (VE) 许可证
- 从Cloud Volumes ONTAP 9.12.1 GA 开始，还应安装多租户加密密钥管理 (MTEKM) 许可证
- 需要有效的 Google Cloud Platform 订阅

配置

Google Cloud

1. 在您的 Google Cloud 环境中，"创建对称 GCP 密钥环和密钥" 。
2. 为 Cloud KMS 密钥和Cloud Volumes ONTAP服务帐户分配自定义角色。
   a. 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.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

b. 分配您创建的自定义角色：
`gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name --location key_location --member serviceAccount:_service_account_Name_ --role projects/customer_project_id/roles/kmsCustomRole`

> 如果您使用的是Cloud Volumes ONTAP 9.13.0 或更高版本，则无需创建自定义角色。您可以分配预定义的[cloudkms.cryptoKeyEncrypterDecrypter^] 角色。

3. 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. 使用您首选的 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 CMEK 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，请输入您的 GCP 帐户中的服务帐户 JSON 密钥。
6. 确认启用流程成功：
`security key-manager external gcp check -vserver svm_name`
7. 可选：创建卷来测试加密 `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

故障排除

如果需要进行故障排除，您可以在上面的最后两个步骤中跟踪原始 REST API 日志：

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

为Cloud Volumes ONTAP启用NetApp勒索软件防护解决方案

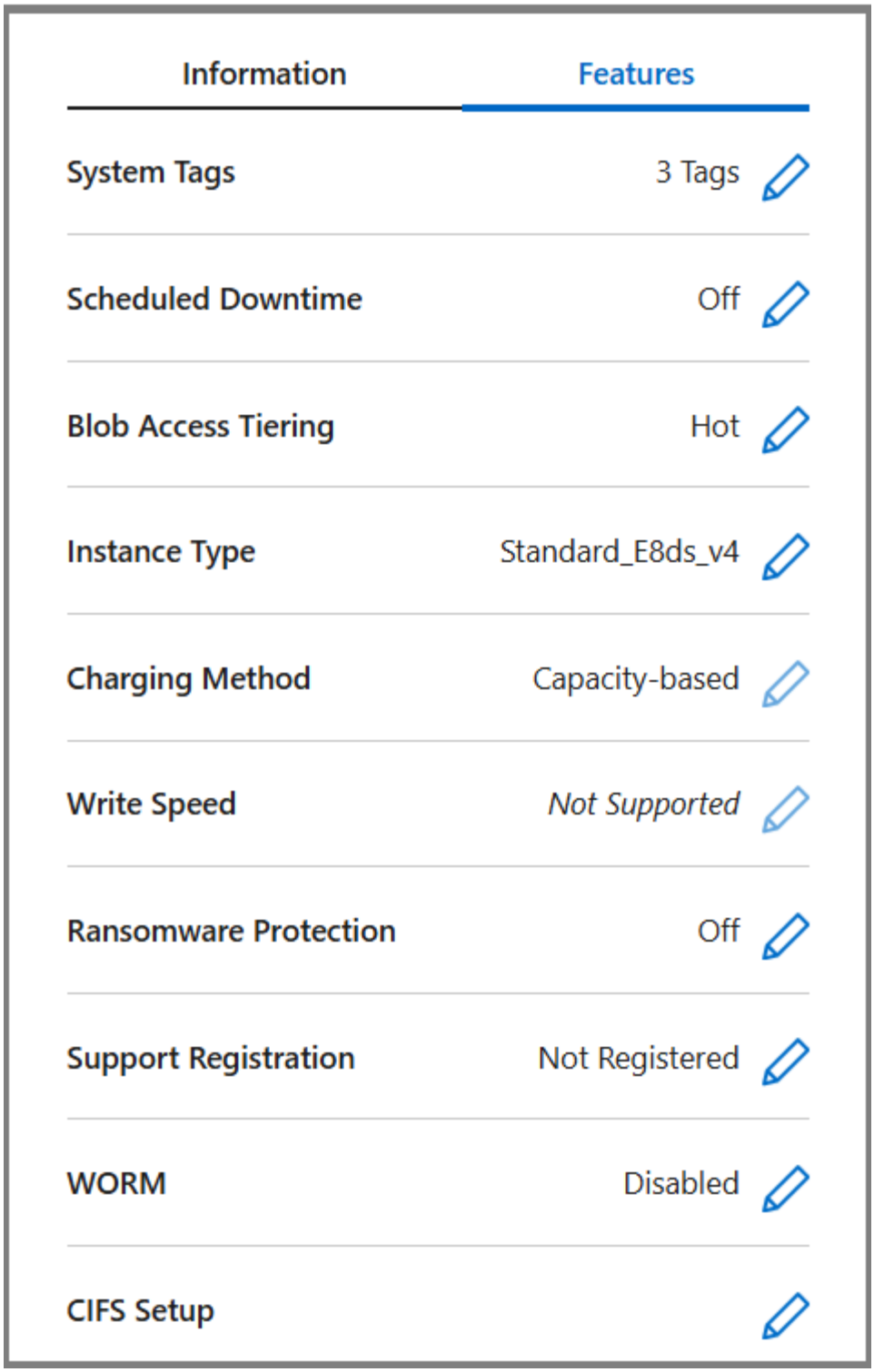
勒索软件攻击会浪费企业的时间、资源和声誉。 NetApp Console使您能够实施两种NetApp勒索软件解决方案：针对常见勒索软件文件扩展名的防护和自主勒索软件防护(ARP)。这些解决方案为可见性、检测和补救提供了有效的工具。

防御常见勒索软件文件扩展名

控制台上的勒索软件防护设置允许您利用ONTAP FPolicy 功能来防御常见的勒索软件文件扩展类型。

步骤

1. 在 **Systems** 页面上，双击您配置为使用勒索软件保护的Cloud Volumes ONTAP系统的名称。
2. 在“概述”选项卡上，单击“功能”面板，然后单击“勒索软件防护”旁边的铅笔图标。



3. 实施NetApp勒索软件解决方案：

   a. 如果您的卷未启用快照策略，请单击“激活快照策略”。

      NetApp Snapshot 技术提供了业界最佳的勒索软件补救解决方案。成功恢复的关键是从未受感染的备份中恢复。快照副本是只读的，可防止勒索软件破坏。他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的图像的粒度。

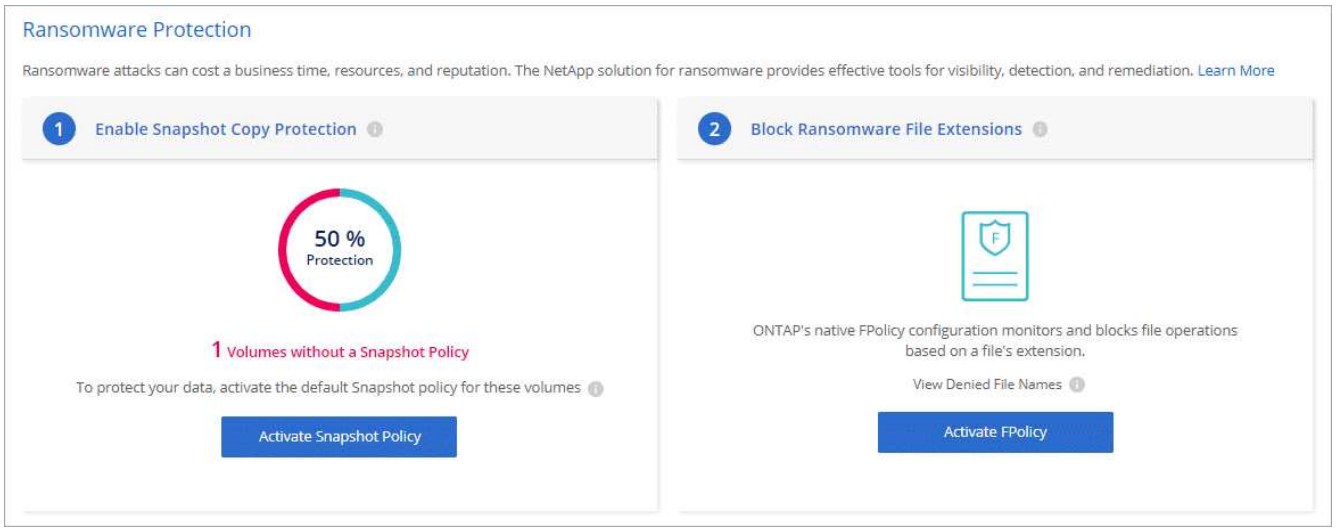
   b. 单击“激活 **FPolicy**”以启用 ONTAP 的 FPolicy 解决方案，该解决方案可以根据文件的扩展名阻止文件操作。

此预防解决方案通过阻止常见的勒索软件文件类型来提高对勒索软件攻击的防护。

默认 FPolicy 范围会阻止具有以下扩展名的文件：

micro、加密、锁定、加密、crypt、crinf、r5a、XRNT、XTBL、R16M01D05、pzdc、好、哈哈！、OMG！、RDM、RRK、encryptedRS、crjoker、EnCiPhErEd、LeChiffre

当您在Cloud Volumes ONTAP上激活 FPolicy 时，将创建此范围。该列表基于常见的勒索软件文件类型。您可以使用Cloud Volumes ONTAP CLI 中的 *vserver fpolicy policy scope* 命令自定义被阻止的文件扩展名。



自主勒索软件防护

Cloud Volumes ONTAP支持自主勒索软件防护 (ARP) 功能，该功能对工作负载进行分析，以主动检测并警告可能表明勒索软件攻击的异常活动。

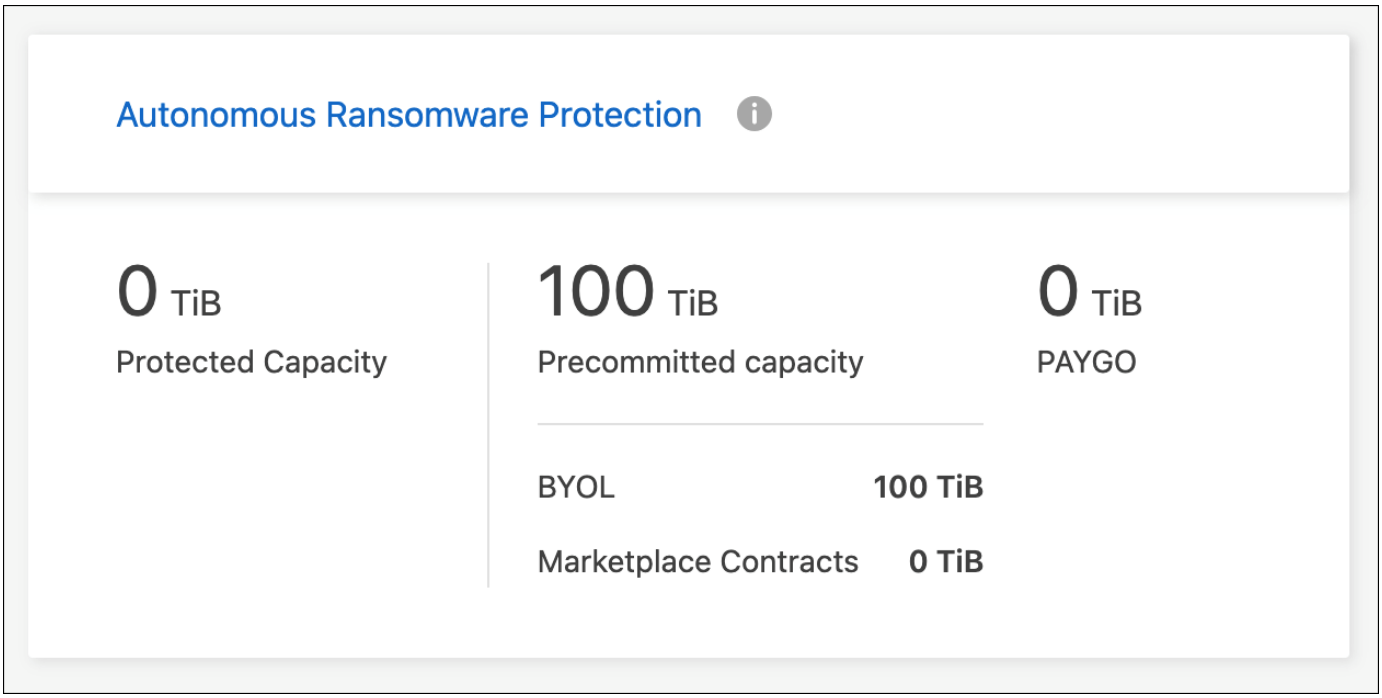
与通过以下方式提供的文件扩展名保护分开 "勒索软件防护设置"，ARP 功能使用工作负载分析根据检测到的“异常活动”向用户发出潜在攻击警报。勒索软件防护设置和 ARP 功能可以结合使用，以实现全面的勒索软件防护。

ARP 功能可与自带许可证 (BYOL) 一起使用，并且无需额外付费即可在市场订阅您的许可证。

启用 ARP 的卷具有指定状态“学习模式”或“活动”。

卷的 ARP 配置是通过ONTAP系统管理器和ONTAP CLI 执行的。

有关如何使用ONTAP System Manager 和ONTAP CLI 启用 ARP 的更多信息，请参阅 "ONTAP文档：启用自主勒索软件防护"。



在Cloud Volumes ONTAP上创建 WORM 文件的防篡改 Snapshot 副本

您可以在Cloud Volumes ONTAP系统上创建一次写入、多次读取 (WORM) 文件的防篡改 Snapshot 副本，并在特定保留期内以未修改的形式保留快照。此功能由SnapLock技术提供支持，并提供了额外的数据保护和合规性层。

开始之前

确保用于创建 Snapshot 副本的卷是SnapLock卷。有关在卷上启用SnapLock保护的信息，请参阅 "ONTAP文档：配置SnapLock"。

步骤

1. 从SnapLock卷创建 Snapshot 副本。有关使用 CLI 或系统管理器创建 Snapshot 副本的信息，请参阅 "ONTAP文档：管理本地 Snapshot 副本概述"。

   Snapshot 副本继承了卷的 WORM 属性，使其具有防篡改功能。底层的SnapLock技术可确保快照在指定的保留期结束之前受到保护，不会被编辑和删除。

2. 如果需要编辑这些快照，您可以修改保留期。欲了解更多信息，请参阅 "ONTAP文档：设置保留时间"。

即使 Snapshot 副本在特定保留期内受到保护，集群管理员也可以删除源卷，因为Cloud Volumes ONTAP中的 WORM 存储在“可信存储管理员”模型下运行。此外，受信任的云管理员可以通过操作云存储资源来删除WORM数据。

相关链接

- 有关 WORM 的更多信息，请参阅"了解Cloud Volumes ONTAP上的 WORM 存储"。
- 有关SnapLock卷的充电信息，请参阅"Cloud Volumes ONTAP中的许可和计费"。