安全性和数据加密

Cloud Volumes ONTAP

NetApp
April 23, 2024

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 。

使用AWS密钥管理服务管理密钥

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ONTAP加密密钥。

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

使用KMS时、请注意、默认情况下、数据SVM的LIF用于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)许可证和
- 您必须已安装多租户加密密钥管理(MTEKM)许可证。
- 您必须是集群管理员或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。

Configuration

AWS

1. 您必须创建 "授予" 用于管理加密的IAM角色要使用的AWS KMS密钥。IAM角色必须包含一个允许执行以下操作的策略：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
     要创建授予、请参见 "AWS 文档"。
2. "将策略添加到相应的IAM角色。" 此策略应支持 `DescribeKey`， `Encrypt`，和 `Decrypt` 操作。

Cloud Volumes ONTAP

1. 切换到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、输入机密密钥。
5. 确认已正确配置AWS KMS：
   `security key-manager external aws show -vserver svm_name`

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。

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(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)
- 您必须具有多租户加密密钥管理(MT_EK_Mgmt)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
- NAE不能使用AKV。NAE需要外部支持的KMIP服务器。

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Azure密钥存储应用注册的Azure门户中、选择"*证书和密钥"窗格。
2. 选择"新建客户端密钥"。为您的客户端密钥输入一个有意义的名称。NetApp建议使用24个月的到期期限；但是、您的特定云监管策略可能需要其他设置。
3. 单击"添加"以创建客户端密钥。复制"value"列中列出的机密字符串、并将其存储在安全位置、以供稍后在中使用 Cloud Volumes ONTAP 配置。离开页面后、不会再显示此机密值。

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"*密钥存储"部分。
3. 单击"***+Create"(**创建**)**、然后输入所需信息、包括资源组、区域和定价层。此外、输入保留已删除存储的天数、然后在密钥存储上选择"*启用清除保护"。
4. 选择"*下一步"以选择访问策略。
5. 选择以下选项：
   a. 在"*访问配置"下、选择"*存储访问策略"。
   b. 在"*资源访问权限"下、选择"*用于卷加密的Azure磁盘加密"。
6. 选择"**+Create"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、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20个
   - "*机密权限"：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

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Cryptographic Operations

- [x] Select all
- [x] Decrypt
- [x] Encrypt
- [x] Unwrap Key
- [x] Wrap Key
- [x] Verify
- [x] Sign

Privileged Key Operations

- [x] Select all
- [x] Purge
- [x] Release

Rotation Policy Operations

- [x] Select all
- [x] Rotate
- [x] Get Rotation Policy
- [x] Set Rotation Policy

Secret permissions

Secret Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Set
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Privileged Secret Operations

- [x] Select all
- [x] Purge

Certificate permissions

Certificate Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore
- [x] Manage Contacts
- [x] Manage Certificate Authorities
- [x] Get Certificate Authorities
- [x] List Certificate Authorities
- [x] Set Certificate Authorities
- [x] Delete Certificate Authorities

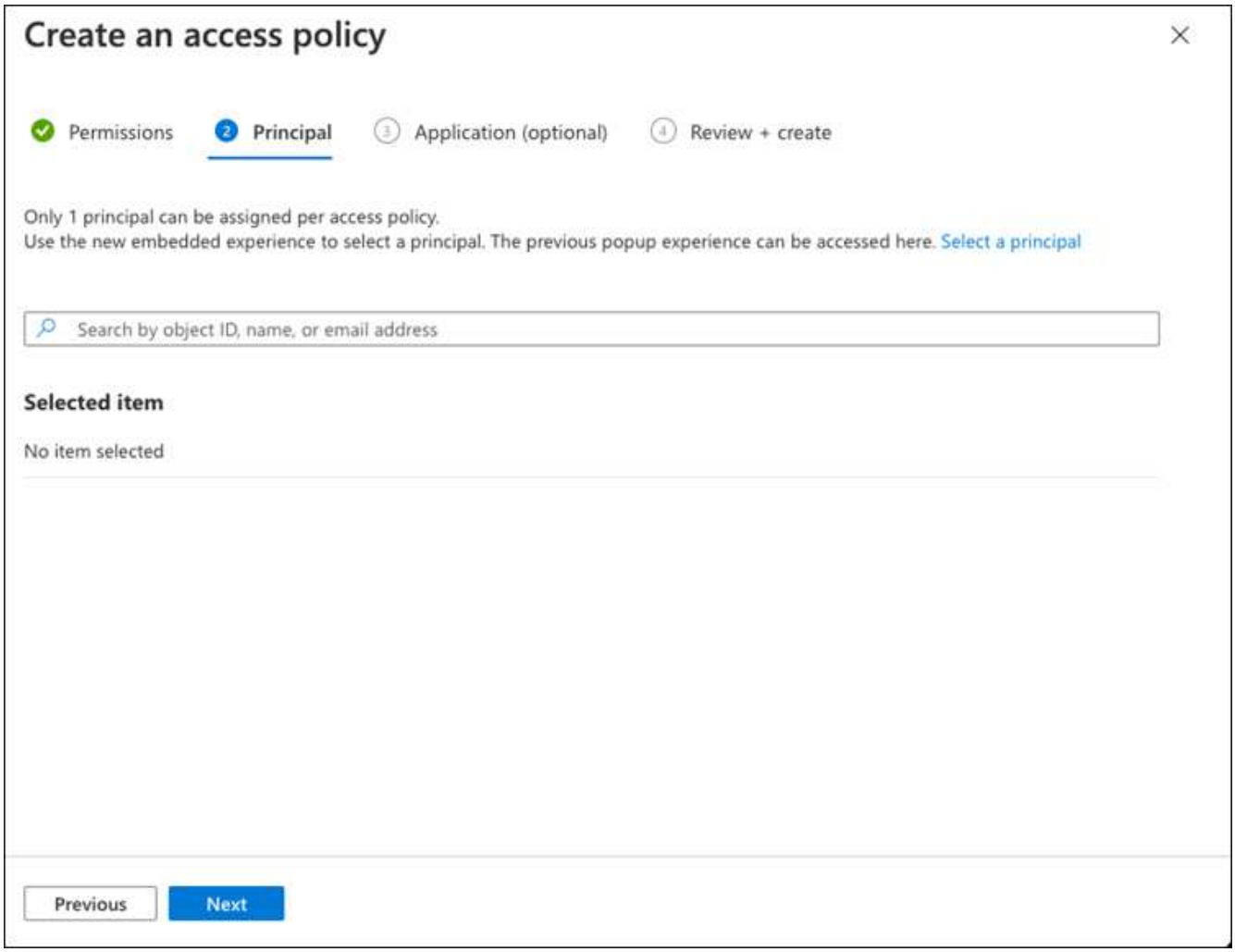
Privileged Certificate Operations

- [x] Select all
- [x] Purge

Previous Next

9. 单击"下一步"以选择您在中创建的"*主体"*已注册**Azure**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. 单击两次"下一步"、直到到达"查看并创建"。然后、单击"**创建"。
11. 选择"*下一步"*以进入"*网络连接"*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"*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。)
13. 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"。您需要在后续步骤中使用此功能。

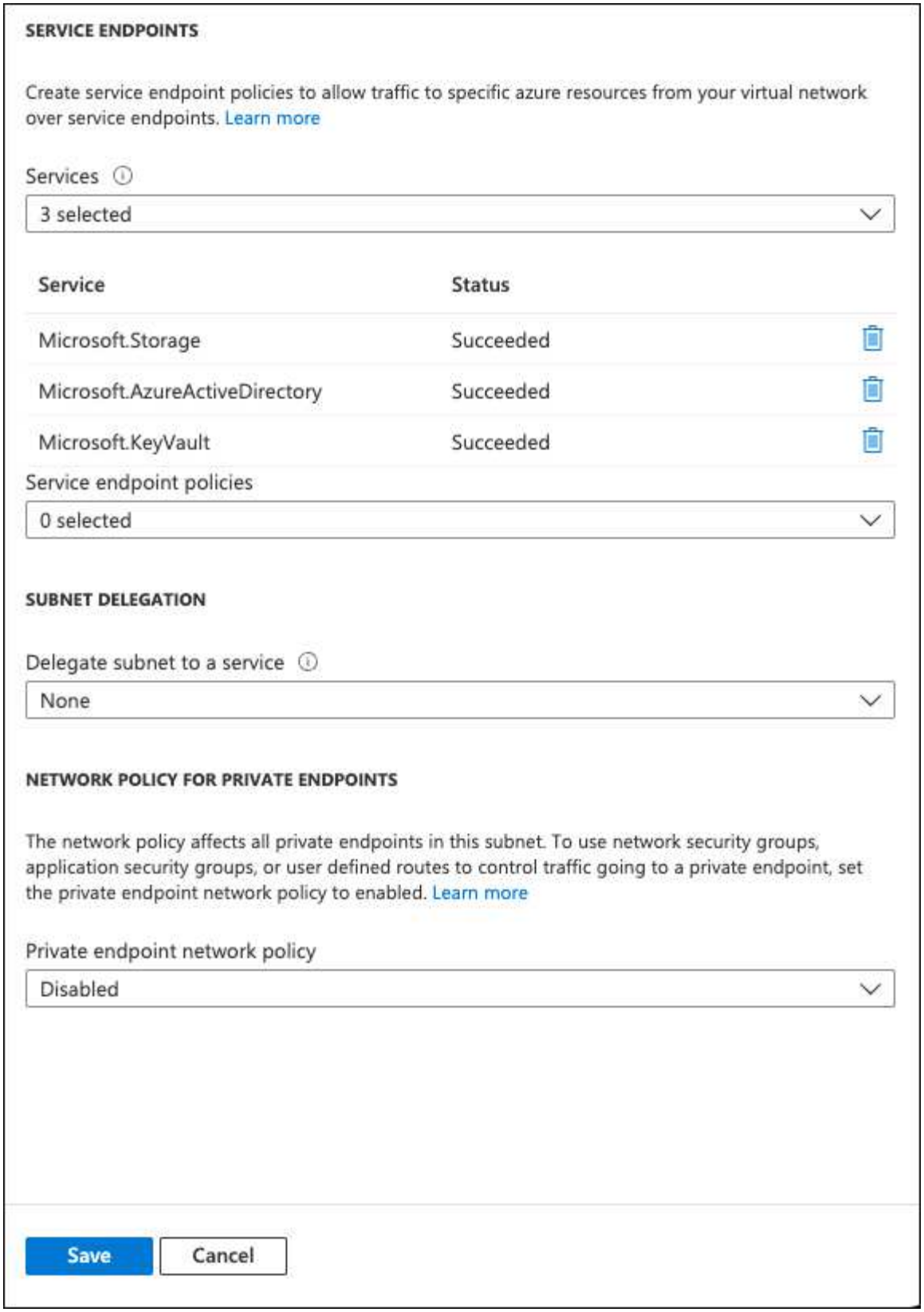
创建加密密钥

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、选择以下内容：
    - "10.microsoft.AzureActiveDirectory"
    - ***microsoft.KeyVaule**
    - "10.microsoft.Storage"*(可选)



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` *`key_vault_URI`* `-key-id` *`full_key_URI`*

   > 。 `_full_key_URI` 值必须使用 `<https:// <key vault host name>/keys/<key label>` 格式。

5. 成功启用Azure密钥存储后、输入 `client secret value` 出现提示时。

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 `service_reachability` 状态不是 `OK`、SVM无法使用所需的所有连接和权限访问Azure密钥存储服务。确保您的Azure网络策略和路由不会阻止您的专用vNet访问Azure KeyVault公共端点。如果有、请考虑使用Azure私有端点从vNet中访问密钥存储。您可能还需要在SVM上添加静态主机条目、以解析端点的专用IP地址。

   。 `kms_wrapped_key_status` 将报告 `UNKNOWN` 初始配置时。其状态将更改为 `OK` 对第一个卷进行加密后。

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的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。

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
- 安装了多租户加密密钥管理(MTEKM)许可证、从Cloud Volumes ONTAP 9.12.1 GA开始。
- 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

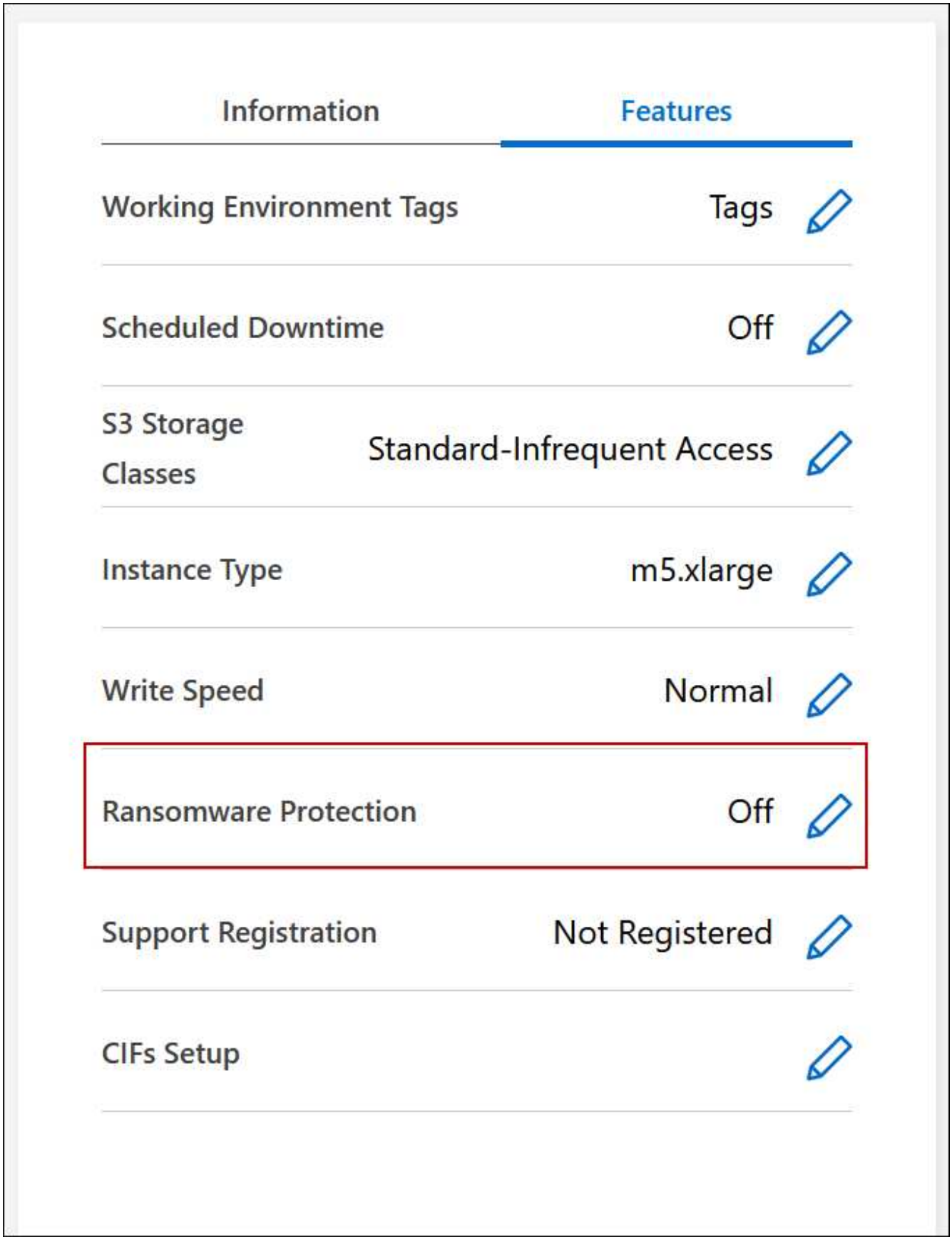
勒索软件攻击可能会耗费业务时间，资源和声誉。借助BlueXP、您可以实施两种NetApp勒索软件解决方案：防范常见勒索软件文件扩展名和自动勒索软件保护(ARP)。这些解决方案为可见性、检测和补救提供了有效的工具。

防止常见勒索软件文件扩展名

通过BlueXP、勒索软件保护设置允许您利用ONTAP FPolicy功能防范常见的勒索软件文件扩展名类型。

步骤

1. 在"画布"页面上、双击您配置为勒索软件保护的系统的名称。
2. 在概述选项卡上、单击功能面板、然后单击*勒索软件保护*旁边的铅笔图标。



3. 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。

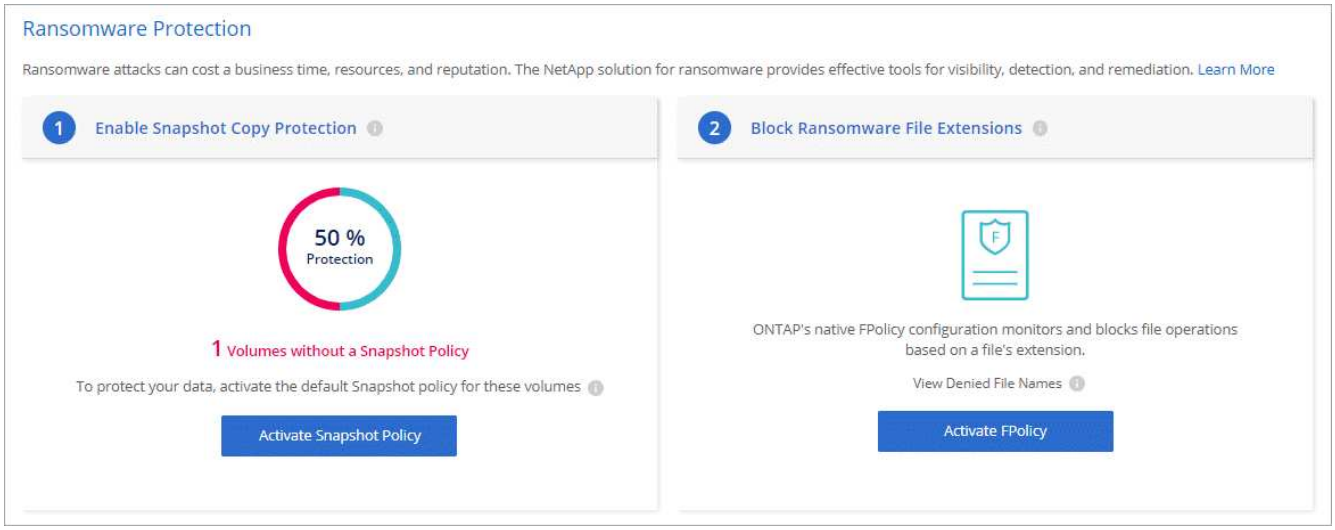
b. 单击 * 激活 FPolicy* 以启用 ONTAP 的 FPolicy 解决方案，它可以根据文件扩展名阻止文件操作。

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、BlueXP会创建此范围。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。



自主勒索软件保护

Cloud Volumes ONTAP支持自动勒索软件保护(ARP)功能、此功能可对工作负载执行分析、以主动检测可能指示勒索软件攻击的异常活动并发出警告。

与通过提供的文件扩展名保护分开 "勒索软件保护设置"，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。勒索软件保护设置和ARP功能均可结合使用来实现全面的勒索软件保护。

无论是基于节点的许可模式还是基于容量的许可模式、ARP功能都只能与BYOL许可证一起使用(期限为1到36个月)。要购买新的单独附加许可证、以便与Cloud Volumes ONTAP中的ARP功能结合使用、您必须与NetApp销售代表联系。

ARP许可证被视为"浮动"许可证、这意味着它不绑定到单个Cloud Volumes ONTAP实例、可应用于多个Cloud Volumes ONTAP环境。

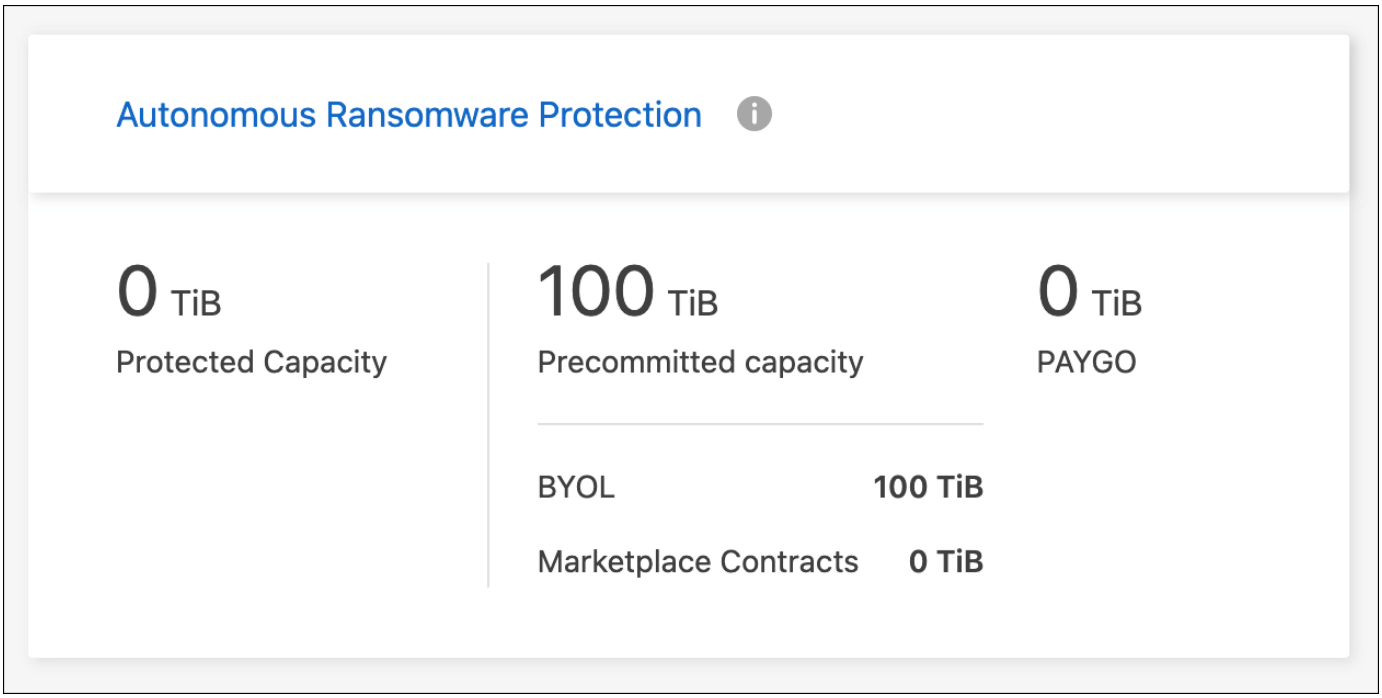
> 对基于节点的Cloud Volumes ONTAP许可证使用ARP功能的情况目前不会反映在数字钱包中。在未来的版本中、可以在"电子钱包"下查看基于节点的ARP使用情况。

购买附加许可证并将其添加到电子钱包后、您可以在Cloud Volumes ONTAP中按卷启用ARP。根据启用了ARP功能的卷的已配置总容量、在卷级别计量ARP收费。最低许可证容量为1 TB。但是、ARP功能没有最低容量充电要求。

启用了ARP的卷的指定状态为"学习模式"或"活动"。ARP状态为"Disabled (已禁用)"的任何卷均不会充电。例如、已配置容量为30 TiB的Cloud Volumes ONTAP环境可以选择仅配置一小部分15 TiB卷且启用了ARP。

可通过ONTAP系统管理器和ONTAP命令行界面为卷配置ARP。

有关如何使用ONTAP系统管理器和命令行界面启用ARP的详细信息、请参见 "启用自主勒索软件保护"。



如果没有许可证、则不支持使用已获得许可的功能。