



安全性和数据加密 Cloud Volumes ONTAP

NetApp
June 01, 2022

目录

- 安全性和数据加密..... 1
 - 使用 NetApp 加密解决方案对卷进行加密..... 1
 - 提高防范勒索软件的能力..... 1
 - 使用Azure密钥存储管理密钥..... 3
 - 使用Google的云密钥管理服务管理密钥..... 4

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。

"[有关说明，请参见 ONTAP 文档](#)"。

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。

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。

可以使用 AKV 和 Cloud KMS 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
- Cloud Volumes ONTAP 集群的节点必须支持NVE
- 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
- Active Azure订阅

限制

- 对于NSE和NAE密钥、无法使用AKV
- MetroCluster 配置不支持AKV。
- 只能在数据SVM上配置AKV

配置过程

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`service_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_Wrapped_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AKV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、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启用密钥管理云KMS。要为Cloud Volumes ONTAP 配置Cloud KMS、必须首先

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 集群的节点必须支持NVE
- 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

限制

- Cloud Volumes ONTAP 必须运行9.10.1或更高版本
- Cloud KMS不适用于NSE和NAE。
- Cloud KMS不适用于MetroCluster 配置。
- 只能在数据SVM上配置Cloud KMS
- 有效的Google Cloud Platform订阅

-enable

1. 在Google Cloud环境中：

- 创建对称GCP密钥环和密钥：
- 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 -permission=cloudkms.CryptoKeyVersions.get、cloudkms.CryptoKeyVersions.list、cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.locations.get,cloudkms.locations.list,resourceManager.projects.get`
- 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/customid_custom_roles/kms_role_`
- 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`

2. 切换到Cloud Volumes ONTAP 环境：

- 切换到高级权限级别：`set -privilege advanced`
- 为数据SVM创建DNS。`dns create -domains c_[project]_.internal -name-servers server_address-vserver svm_name`
- 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`
- 出现提示时、输入GCP帐户中的服务帐户JSON密钥。
- 确认已启用的过程成功：`security key-manager external GCP check -vserver svm_name`
- 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

如果需要故障排除、可以在上述最后两个步骤中结束原始REST API日志：。`set d.systemshell -node node-command tail -f /mroot/etc/log/mlog/kmip2_client.log`

版权信息

版权所有©2022 NetApp、Inc.。保留所有权利。Printed in the U.S.版权所涵盖的本文档的任何部分不得以任何形式或任何手段复制、包括影印、录制、磁带或存储在电子检索系统中—未经版权所有者事先书面许可。

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

本软件由NetApp按"原样"提供、不含任何明示或默示担保、包括但不限于适销性和特定用途适用性的默示担保、特此声明不承担任何任何责任。IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

商标信息

NetApp、NetApp标识和中列出的标记 <http://www.netapp.com/TM> 是NetApp、Inc.的商标。其他公司和产品名称可能是其各自所有者的商标。