为 VMware vSphere 配置 ONTAP 工具

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

目录

为 VMware vSphere 配置 ONTAP 工具

添加vCenter Server实例

将vCenter Server实例添加到适用于VMware vSphere的ONTAP工具中、以配置、管理和保护vCenter Server环境中的虚拟数据存储库。添加多个 vCenter Server 实例时，需要自定义 CA 证书才能在 ONTAP 工具和每个 vCenter Server 之间进行安全通信。

- 关于此任务 *

通过与vCenter集成、ONTAP工具使您能够直接从vSphere客户端执行配置、快照和数据保护等存储任务、而无需切换到单独的存储管理控制台。

步骤

1. 打开Web浏览器并导航到URL： `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用您在部署期间提供的适用于VMware vSphere的ONTAP工具管理员凭据登录。
3. 选择* vCenter *>*添加*以载入vCenter Server实例。请提供您的vCenter IP地址或主机名、用户名、密码和端口详细信息。

> 您不需要管理员帐户即可将vCenter实例添加到ONTAP工具。您可以创建自定义角色、而无需具有有限权限的管理员帐户。有关详细信息、请参见 "将vCenter Server RBAC与适用于VMware vSphere 10的ONTAP工具结合使用" 。

将vCenter Server实例添加到ONTAP工具会自动触发以下操作：

- vCenter客户端插件已注册为远程插件。
- 此插件和API的自定义Privileges将应用于vCenter Server实例。
- 创建自定义角色以管理用户。
- 此插件会在vSphere用户界面上显示为快捷方式。

向vCenter Server实例注册VASA Provider

您可以使用适用于VMware vSphere的ONTAP工具向vCenter Server实例注册VASA Provider。VASA Provider设置部分显示选定vCenter Server的VASA Provider注册状态。在多 vCenter 部署中，确保每个 vCenter Server 实例都有自定义 CA 证书。

步骤

1. 登录到vSphere Client
2. 选择插件部分下的*快捷方式*>* NetApp ONTAP tools*。
3. 选择*Settings*>*VASA Provider settings *。VASA Provider注册状态将显示为未注册。
4. 选择*注册*按钮以注册VASA Provider。
5. 输入VASA Provider的名称并为VMware vSphere应用程序提供ONTAP工具用户凭据、然后选择*注册*。

6. 成功注册并刷新页面后、将显示已注册的VASA Provider的状态、名称和版本。注册后、取消注册操作将被激活。

    ◦ 完成后 *

验证已启用的VASA Provider是否列在vCenter Client的VASA Provider下：

步骤

1. 导航到vCenter Server实例。
2. 使用管理员凭据登录。
3. 选择*存储提供程序*>*配置*。验证是否已正确列出已启用的VASA Provider。

安装 NFS VAAI 插件

NFS vStorage API for Array Integration (NFS VAAI)插件是一个软件组件、用于集成VMware vSphere和NFS存储阵列。使用适用于VMware vSphere的ONTAP工具安装NFS VAAI插件、以利用NFS存储阵列的高级功能将某些与存储相关的操作从ESXi主机卸载到存储阵列本身。

开始之前

- 下载 "适用于 VMware VAAI 的 NetApp NFS 插件"安装包。
- 确保已安装ESXi主机和vSphere 7.0U3最新修补程序或更高版本以及9.14.1 9.14.1或更高版本。
- 挂载NFS数据存储库。

步骤

1. 登录到vSphere Client。
2. 选择插件部分下的*快捷方式*>* NetApp ONTAP tools*。
3. 选择*Settings*>*NFS VAAI Tools*。
4. 将VAAI插件上传到vCenter Server后、在*现有版本*部分中选择*更改*。如果VAAI插件未上传到vCenter Server、请选择*上传*按钮。
5. 浏览并选择 `.vib`文件，然后选择*Upload*将文件上传到ONTAP工具。
6. 选择*在ESXi主机上安装*、选择要安装NFS VAAI插件的ESXi主机、然后选择*安装*。

    仅显示符合此插件安装条件的ESXi主机。您可以在vSphere Web Client的近期任务部分中监控安装进度。

7. 安装后手动重新启动ESXi主机。

    当VMware管理员重新启动ESXi主机时、适用于VMware vSphere的ONTAP工具会自动检测并启用NFS VAAI插件。

下一步是什么?

安装NFS VAAI插件并重新启动ESXi主机后、您需要为VAAI副本卸载配置正确的NFS导出策略。在NFS环境中配置VAAI时、请根据以下要求配置导出策略规则：

- 相关ONTAP卷需要允许NFSv4调用。

- root用户应保持root身份、并且所有接合父卷都应允许使用NFSv4。
- 需要在相关NFS服务器上设置VAAI支持选项。

有关此过程的详细信息、请参阅 "为VAAI副本卸载配置正确的NFS导出策略"知识库文章。

相关信息

"支持基于 NFS 的 VMware vStorage"

"启用或禁用NFSv4.0"

"ONTAP支持NFSv4.2"

配置ESXi主机设置

配置ESXi服务器多路径和超时设置可在主路径发生故障时无缝切换到备份存储路径、从而确保高可用性和数据完整性。

配置ESXi服务器多路径和超时设置

适用于 VMware vSphere 的 ONTAP 工具可检查并设置最适合 NetApp 存储系统的 ESXi 主机多路径设置和 HBA 超时设置。

- 关于此任务 *

根据您的配置和系统负载、此过程可能需要很长时间。任务进度将显示在 " 近期任务 " 面板中。

步骤

1. 在VMware vSphere Web Client的主页页面中、选择*主机和群集*。
2. 右键单击某个主机并选择*Update NetApp ONTAP host data*。
3. 在VMware vSphere Web Client的快捷方式页面上，选择NetApp ONTAP插件部分下的*VMware tools*。
4. 转到适用于VMware vSphere的ONTAP工具插件概述(信息板)中的*ESXi主机兼容性*卡。
5. 选择*应用建议设置*链接。
6. 在*应用建议的主机设置*窗口中，选择要更新以符合NetApp建议的设置的主机，然后选择*下一步*。

   您可以展开ESXi主机以查看当前值。

7. 在设置页面中、根据需要选择建议值。
8. 在摘要窗格中，检查这些值并选择*Complet*。您可以在最近任务面板中跟踪进度。

设置ESXi主机值

使用适用于VMware vSphere的ONTAP工具、您可以在ESXi主机上设置超时值和其他值、以确保性能最佳并成功进行故障转移。适用于VMware vSphere的ONTAP工具设置的值基于内部NetApp测试。

您可以在 ESXi 主机上设置以下值：

HBA/CNA适配器设置

将以下参数设置为默认值：

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBA 超时
- QLogic FC HBA 超时

MPIO设置

MPIO设置定义NetApp存储系统的首选路径。它们可确定哪些可用路径已进行优化(与遍历互连缆线的非优化路径不同)、并将首选路径设置为其中一个路径。

在高性能环境中、或者在测试单个LUN数据存储库的性能时、请考虑将轮询(VMW_PSP_RR)路径选择策略(PSP)的负载平衡设置从默认IOPS设置1000更改为值1。

MPIO 设置不适用于 NVMe、NVMe/FC 和 NVMe/TCP 协议。

NFS 设置

参数	将此值设置为…
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128或更高
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

配置**ONTAP**用户角色和权限

您可以使用适用于VMware vSphere的ONTAP工具和ONTAP System Manager提供的JSON文件配置用于管理存储后端的新用户角色和特权。

开始之前

- 您应已使用以下<loadbalancerIP>命令从适用于VMware vSphere的ONTAP工具下载ONTAP特权文件：*\https：//VMware：8443/Virtualization：user-golites/User_roles.zip*。
- 您应该已使用从ONTAP工具下载ONTAP Privileges文件 `https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`。

您可以在集群级别或直接在Storage Virtual Machine (SVM)级别创建用户。您也可以在不使用user_roles.json文件的情况下创建用户、如果这样做、您需要在SVM级别具有一组最低权限。

- 您应已使用存储后端的管理员权限登录。

步骤

1. 提取下载的_\https：//https：<loadbalancerIP>：8443/Virtualization /用户权限/USER_Roles.zip_文件。
2. 使用集群的集群管理IP地址访问ONTAP系统管理器。
3. 使用管理Privileges登录到集群。要配置用户、请执行以下步骤：
   a. 要配置集群ONTAP工具用户，请选择*Cluster*>*Settings*>*Users and Roles*窗格。
   b. 要配置SVM ONTAP工具用户、请选择*存储SVM*>*设置*>*用户和角色*窗格。
   c. 在“用户”下选择*Add*。
   d. 在*添加用户*对话框中、选择*虚拟化产品*。
   e. *浏览*选择并上传ONTAP权限JSON文件。

      此时将自动填充"Product"字段。

   f. 从产品功能下拉菜单中选择所需的功能。

      系统将根据选定的产品功能自动填充“角色”字段。

   g. 输入所需的用户名和密码。
   h. 选择用户所需的Privileges (发现、创建存储、修改存储、销毁存储、NS/SAN角色)、然后选择*添加*。

此时将添加新角色和用户、您可以在已配置的角色下查看详细权限。

SVM聚合映射要求

要使用SVM用户凭据配置数据存储库、适用于VMware vSphere的内部ONTAP工具会在数据存储库发布API中指定的聚合上创建卷。ONTAP不允许使用SVM用户凭据在SVM上未映射的聚合上创建卷。要解决此问题、您需要使用ONTAP REST API或命令行界面将SVM映射到聚合、如下所述。

REST API：

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP命令行界面：

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State          Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

手动创建**ONTAP**用户和角色

按照本节中的说明手动创建用户和角色、而不使用JSON文件。

1. 使用集群的集群管理IP地址访问ONTAP系统管理器。
2. 使用管理Privileges登录到集群。
   a. 要配置集群ONTAP工具角色，请选择*Cluster*>*Settings*>*Users and Roles*窗格。
   b. 要配置集群SVM ONTAP工具角色、请选择*存储SVM*>*设置*>*用户和角色*窗格
3. 创建角色：
   a. 在*roles*表下选择*Add*。
   b. 输入*角色名称*和*角色属性*详细信息。

      从下拉列表中添加*REST API Path*和相应的访问权限。

   c. 添加所有所需的API并保存更改。
4. 创建用户：
   a. 在*USERS*表下选择*ADD*。
   b. 在*添加用户*对话框中，选择*系统管理器*。
   c. 输入*用户名*。
   d. 从上面的*Create Roles*步骤中创建的选项中选择*Role*。
   e. 输入要授予访问权限的应用程序和身份验证方法。ONTAPI和HTTP是必需的应用程序，并且身份验证类型为*Password*。
   f. 设置*用户密码*和*保存*用户。

非管理员全局范围集群用户所需的最低权限列表

本节列出了在不使用Users JSON文件的情况下创建的非管理员全局范围集群用户所需的最低权限。如果在本地范围添加了集群、建议使用JSON文件创建用户、因为适用于VMware vSphere的ONTAP工具不仅需要读取特权、还需要在ONTAP上进行配置。

使用API：

API	访问级别	用于
/API/cluster	只读	集群配置发现
/API/cluster-licensing /许可证	只读	协议专用许可证的许可证检查

/API/cluster-node	只读	平台类型发现
/api/安全性/帐户	只读	特权发现
/api/安全性/角色	只读	特权发现
/API/storage/Aggregates	只读	数据存储库/卷配置期间的聚合空间检查
/API/storage/cluster	只读	以获取集群级别空间和效率数据
/API/storage/disks	只读	以获取聚合中关联的磁盘
/API/storage/QoS/策略	读取/创建/修改	QoS和VM策略管理
/apI/SVM/SVM	只读	在本地添加集群的情况下获取SVM配置。
/API/network/IP/接口	只读	添加存储后端—要确定管理LIF的范围、请使用集群/SVM

为基于**VMware vSphere ONTAP API**的集群范围用户创建**ONTAP**工具

您需要发现、创建、修改和销毁Privileges、以便在数据存储库出现故障时执行修补操作和自动回滚。缺少所有这些Privileges会导致工作流中断和清理问题。

通过为基于VMware vSphere ONTAP API的用户创建ONTAP工具并执行发现、创建存储、修改存储、销毁存储Privileges、可以启动发现并管理ONTAP工具工作流。

要使用上述所有Privileges创建集群范围的用户、请运行以下命令：

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all
```

```
security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly
```

```
security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
```

```
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly
```

此外、对于ONTAP 9.16.0及更高版本、请运行以下命令：

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

为基于**VMware vSphere ONTAP API**的**SVM**范围的用户创建**ONTAP**工具

要使用所有Privileges创建SVM范围的用户、请运行以下命令：

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

此外、对于ONTAP 9.16.0及更高版本、请运行以下命令：

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

要使用上述基于API创建的角色创建基于API的新用户、请运行以下命令：

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

示例：

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

要解除帐户锁定、请运行以下命令以启用对管理界面的访问：

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

示例：

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

将适用于**VMware vSphere 10.1**用户的**ONTAP**工具升级到**10.3**用户

如果适用于VMware vSphere 10.1的ONTAP工具用户是使用json文件创建的集群范围用户、请使用admin用户在ONTAP命令行界面上运行以下命令、以升级到10.3版。

对于产品功能：

- VSC
- VSC和VASA Provider
- VSC和SRA

- VSC、VASA Provider和SRA。

集群Privileges：

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem show"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem host show"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem map show"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve sho-interface"-access read

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem host add"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem map add"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem delete"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem host remove"-access all

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem map remove"-access all

如果适用于VMware vSphere 10.1的ONTAP工具用户是使用json文件创建的SVM范围用户、请使用admin用户在ONTAP命令行界面上运行以下命令、以升级到10.3版。

SVM Privileges：

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve"-access all -vserver nve<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem show"-access all -vserver nv<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem host show"-access all -vserver nv<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem map show"-access all -vserver nv<vserver-name>

security login Role create -Role <existing-role-name>-cmddirname "vserver nve sho-interface"-access read -vserver nv<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem host add"-access all -vserver nv<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem map add"-access all -vserver nv<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve"-access all -vserver nve<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem delete"-access all -vserver nv<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem host remove"-access all -vserver nv<vserver-name>

security login Role create -Role <existing-role-name> nve -cmddirname "vserver nve subsystem map remove"-access all -vserver nv<vserver-name>

向现有角色添加命令_vserver nvexe命名空间show_和_vserver nvserver subsystem show_可添加以下命令。

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

添加存储后端

通过添加存储后端、您可以加入ONTAP集群。

- 关于此任务 *

如果在多租户设置中、vCenter充当关联SVM的租户、请使用ONTAP工具管理器添加集群。将存储后端与vCenter Server相关联、以便将其全局映射到已登录的vCenter Server实例。vCenter租户必须载入所需的Storage Virtual Machine (SVM)。这样、SVM用户便可配置Vvol数据存储库。您可以使用SVM在vCenter中添加存储。

使用ONTAP工具用户界面使用集群或SVM凭据添加本地存储后端。这些存储后端仅限于一个vCenter。在本地使用集群凭据时、关联的SVM会自动映射到vCenter以管理Vvol或VMFS。对于VMFS管理(包括SRA)、ONTAP工具支持SVM凭据、而不需要全局集群。

使用**ONTAP**工具管理器

在多租户设置中、您可以全局添加存储后端集群、并在本地添加SVM以使用SVM用户凭据。

步骤

1. 从Web浏览器启动ONTAP工具管理器：
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用您在部署期间提供的适用于VMware vSphere的ONTAP工具管理员凭据登录。
3. 从边栏中选择*存储后端*。
4. 添加存储后端并提供服务器IP地址或FQDN、用户名和密码详细信息。

   支持IPv4和IPv6地址管理生命周期。

使用**vSphere**客户端用户界面

通过vSphere客户端用户界面配置存储后端时、请务必注意、Vvol数据存储库不支持直接添加SVM用户。

1. 登录到vSphere Client。
2. 在快捷方式页面中，选择插件部分下的NetApp ONTAP tools*。
3. 从边栏中选择*存储后端*。
4. 添加存储后端并提供服务器IP地址、用户名、密码和端口详细信息。

   要直接添加SVM用户、您可以添加基于集群的凭据以及IPv4和IPv6地址管理LIF、或者通过SVM管理LIF提供基于SVM的凭据。

下一步是什么?

此时、此列表将刷新、您可以在此列表中看到新添加的存储后端。

将存储后端与**vCenter Server**实例相关联

将存储后端与vCenter Server相关联、以便在存储后端与全局已登录的vCenter Server实例之间创建映射。

步骤

1. 从Web浏览器启动ONTAP工具管理器： `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用您在部署期间提供的适用于VMware vSphere的ONTAP工具管理员凭据登录。
3. 从侧栏中选择vCenter。
4. 选择要与存储后端关联的vCenter Server实例旁边的垂直省略号。
5. 从下拉列表中选择存储后端、将vCenter Server实例与所需的存储后端关联起来。

配置网络访问

如果尚未配置网络访问、则从ESXi主机发现的所有IP地址都会默认添加到导出策略中。您可以对其进行配置、以便向导出策略中添加一些特定IP地址、并排除其余IP地址。但是、在排除的ESXi主机上执行挂载操作时、此操作将失败。

步骤

1. 登录到vSphere Client。
2. 在“插件”部分的“快捷方式”页面中选择NetApp ONTAP tools*。
3. 在ONTAP工具的左窗格中，导航到*Settings*>*Manage Network Access*>*Edit*。

   要添加多个IP地址、请使用逗号、范围、无类别域间路由(CIDR)或这三者的组合分隔列表。

4. 选择 * 保存 * 。

创建数据存储库

在主机集群级别创建数据存储库时、系统会创建数据存储库并将其挂载到目标的所有主机上、只有当前用户具有执行权限时、才会启用此操作。

创建一个卷数据存储库

从适用于VMware vSphere 10.3的ONTAP工具开始、您可以在ASA R2系统上创建空间效率为thin-vvol的vVol数据存储库。在创建VVOP数据存储库时、VASA Provider会创建一个容器和所需的协议端点。此容器不包含任何后备卷。

开始之前

- 确保根聚合未映射到SVM。
- 确保已向选定vCenter注册VASA Provider。
- 在ASA R2存储系统中、SVM应映射到SVM用户的聚合。

步骤

1. 登录到vSphere Client。
2. 右键单击主机系统、主机集群或数据中心，然后选择*Create NetApp ONTAP tools*>*Create DataSystem*。
3. 选择"vols 数据存储库类型"。
4. 输入*数据存储库名称*和*协议*信息。

   ASA R2系统支持对虚拟卷使用iSCSI和FC协议。

5. 选择要在其中创建数据存储库的Storage VM。
6. 在*高级选项*中为NFS协议选择自定义导出策略、或者为iSCSI和FC协议选择自定义启动程序组名称。

   在ASA R2存储系统类型SVM中、不会创建存储单元(LUN /命名空间)、因为数据存储库只是一个逻辑容器。

7. 在*存储属性*窗格中，您可以创建新卷或使用现有卷。但是、不能将这两种类型的卷组合在一起来创建一个卷数据存储库。

   创建新卷时、您可以在数据存储库上启用QoS。默认情况下、系统会为每个LUN创建的请求创建一个卷。此步骤不适用于使用ASA R2存储系统的虚拟卷数据存储库。

8. 在*摘要*窗格中查看您的选择，然后选择*完成*。

创建**NFS**数据存储库

VMware网络文件系统(NFS)数据存储库使用NFS协议通过网络将ESXi主机连接到共享存储设备。NFS数据存储库通常用于VMware vSphere环境、并具有多种优势、例如精简性和灵活性。

步骤

1. 登录到vSphere Client。
2. 右键单击主机系统、主机集群或数据中心，然后选择*Create NetApp ONTAP tools*>*Create dataC*。
3. 在*数据存储库类型*字段中选择NFS。
4. 在*名称和协议*窗格中输入数据存储库名称、大小和协议信息。在高级选项中选择*数据存储库集群*和*Kerberos身份验证*。

只有在选择了NFS 4.1协议时、才能使用Kerberos身份验证。

5. 在*存储*窗格中选择*平台*和*存储VM*。
6. 如有必要，在高级选项下选择*自定义导出策略*，但不建议这样做。如果使用了发现功能、请确保在vCenter中对所有对象运行发现。

   您不能使用SVM的默认/根卷策略创建NFS数据存储库。

   - 在高级选项中，只有在平台下拉列表中选择了性能或容量时，*非对称*切换按钮才可见。
   - 在平台下拉列表中选择*任何*选项后、无论平台或非对称标志如何、您都可以看到属于vCenter的SVM。
7. 在*存储属性*窗格中选择要创建卷的聚合。在高级选项中，根据需要选择*Space Reserve*和*Enable QoS*。
8. 查看*Summary (摘要)窗格中的选择，然后选择***Finish (**完成**)**。

此时将创建NFS数据存储库并将其挂载到所有主机上。

创建**VMFS**数据存储库

虚拟机文件系统(VMFS)是一种集群模式文件系统、用于在VMware vSphere环境中存储虚拟机文件。VMFS允许多个ESXi主机同时访问相同的虚拟机文件、从而实现vMotion和高可用性等功能。

在受保护集群上：

- 您只能创建VMFS数据存储库。将VMFS数据存储库添加到受保护集群时、该数据存储库将自动受到保护。
- 您不能在包含一个或多个受保护主机集群的数据中心上创建数据存储库。
- 如果父主机集群受"自动故障转移双工策略"类型的关系(统一/非统一配置)保护、则无法在ESXi主机上创建数据存储库。
- 您只能在受异步关系保护的ESXi主机上创建VMFS数据存储库。您不能在受"自动故障转移双工"策略保护的主机集群中的ESXi主机上创建和挂载数据存储库。

开始之前

- 在ONTAP存储端为每个协议启用服务和LUN。
- 为ASA R2存储系统中的SVM用户将SVM映射到聚合。
- 如果您使用的是NVMe/TCP协议、请配置ESXi主机：
  a. 查看 "VMware 兼容性指南"

     VMware vSphere 7.0 U3及更高版本支持NVMe/TCP协议。但是、建议使用VMware vSphere 8.0及更高版本。

  b. 验证网络接口卡(NIC)供应商是否支持采用NVMe/TCP协议的ESXi NIC。
  c. 根据NIC供应商规格为NVMe/TCP配置ESXi NIC。
  d. 使用VMware vSphere 7版本时、请按照VMware站点上的说明 "为基于TCP适配器的NVMe配置VMkernel绑定"配置NVMe/TCP端口绑定。使用VMware vSphere 8版本时，请按照 "在ESXi上配

置基于TCP的NVMe"配置NVMe/TCP端口绑定。

e. 对于VMware vSphere 7版本、请按照第页上的说明 "启用基于RDMA的NVMe或基于TCP的NVMe软件适配器"配置NVMe/TCP软件适配器。对于VMware vSphere 8版本、请按照 "添加基于RDMA的软件NVMe或基于TCP适配器的NVMe"配置NVMe/TCP软件适配器。

f. "发现存储系统和主机"在ESXi主机上运行操作。有关详细信息，请参阅 "如何使用vSphere 8.0 Update 1和VMfs.13.1为ONTAP 9数据存储库配置NVMe/TCP"。

- 如果您使用的是NVMe/FC协议、请执行以下步骤来配置ESXi主机：

a. 在ESXi主机上启用基于网络结构的NVMe (NVMe-oF)。

b. 完成SCSI分区。

c. 确保ESXi主机和ONTAP系统在物理层和逻辑层进行连接。

要为ONTAP SVM配置FC协议，请参见 "为 FC 配置 SVM"。

有关在VMware vSphere 8.0中使用NVMe/FC协议的详细信息，请参阅 "适用于采用ONTAP 的ESXi 8.x的NVMe-oF主机配置"。

有关在VMware vSphere 7.0中使用NVMe/FC的详细信息，请参阅 "《 ONTAP NVMe/FC 主机配置指南》" 和 "TR-4684"。

步骤

1. 登录到vSphere Client。
2. 右键单击主机系统、主机集群或数据中心，然后选择*Create NetApp ONTAP tools*>*Create DataSystem*。
3. 选择VMFS数据存储库类型。
4. 在*名称和协议*窗格中输入数据存储库名称、大小和协议信息。如果您选择将新数据存储库添加到现有VMFS数据存储库集群、请选择高级选项下的数据存储库集群选择器。
5. 在*存储*窗格中选择Storage VM。根据需要在*高级选项*部分中提供*自定义启动程序组名称*。您可以为此数据存储库选择一个现有igrop、也可以使用自定义名称创建一个新的igrop。

   如果选择NVMe/FC或NVMe/TCP协议、则会创建一个新的命名空间子系统、并使用该子系统进行命名空间映射。命名空间子系统会使用自动生成的名称来创建、该名称包含数据存储库名称。您可以在*Storage*窗格高级选项的*custom nam命名 空间子系统名称*字段中重命名命名命名命名空间子系统。

6. 从*storage attributes*窗格：

   a. 从下拉选项中选择*聚合*。

   > 对于ASA R2存储系统，由于ASA R2存储是离散式存储，因此不会显示*AGRELER*选项。选择ASA R2存储系统类型SVM时、存储属性页面将显示用于启用QoS的选项。

   b. 根据选定协议、系统会创建一个空间预留类型为精简的存储单元(LUN /命名空间)。

   c. 根据需要选择*使用现有卷*、*启用QoS*选项并提供详细信息。

在ASA R2存储类型中、卷创建或选择不适用于存储单元创建(LUN /命名空间)。因此、不会显示这些选项。

要使用NVMe/FC或NVMe/TCP协议创建VMFS数据存储库、您不能使用现有卷、应创建新卷。

7. 在*Summary (摘要)窗格中查看数据存储库详细信息，然后选择***Finish (完成)**。

如果您在受保护集群上创建数据存储库、则会看到一条只读消息："正在将数据存储库挂载到受保护集群上。"

结果

此时将创建VMFS数据存储库并将其挂载到所有主机上。