



为 VMware vSphere 配置 ONTAP 工具

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

目录

为 VMware vSphere 配置 ONTAP 工具	1
将 vCenter Server 实例添加到 ONTAP 工具	1
在 ONTAP tools 中向 vCenter Server 实例注册 VASA Provider	2
使用 ONTAP 工具安装 NFS VAAI 插件	2
在 ONTAP tools 中配置 ESXi 主机设置	3
配置 ESXi 服务器多路径和超时设置	3
设置 ESXi 主机值	4
为 ONTAP tools 配置 ONTAP 用户角色和权限	5
SVM 聚合映射要求	6
手动创建 ONTAP 用户和角色	6
将适用于 VMware vSphere 10.1 用户的 ONTAP 工具升级到 10.3 用户	14
将适用于 VMware vSphere 10.3 用户的 ONTAP 工具升级到 10.4 用户	16
将存储后端添加到 ONTAP tools	16
在 ONTAP tools 中将存储后端与 vCenter Server 实例关联	19
在 ONTAP tools 中配置网络访问	19
在 ONTAP tools 中创建数据存储库	19

为 VMware vSphere 配置 ONTAP 工具

将 vCenter Server 实例添加到 ONTAP 工具

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

ONTAP 工具与 vCenter Server 集成，可直接从 vSphere 客户端执行配置、快照和数据保护等存储任务。

开始之前

- 确保 vCenter 服务器证书包含包含 DNS 和 IP 地址条目的有效使用者备用名称 (SAN) 扩展。例如：

```
X509v3 extensions:  
    X509v3 Subject Alternative Name:  
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

如果证书不包括 SAN 扩展，或者 SAN 扩展不包含正确的 DNS 或 IP 地址值，则 ONTAP tools 操作可能会由于证书验证错误而失败。

- SAN 详细信息中必须包含 vCenter Server 的主网络标识符 (PNID)。PNID 和 DNS 名称应相同且可在 DNS 中解析。
- 建议使用其完全限定的域名 (FQDN) 部署 vCenter Server，并确保证书中的 SAN 包括 DNS Name=machine_FQDN，以获得最佳兼容性和支持。
- 有关详细信息，请参见 VMware 文档：
 - ["不同解决方案路径的 vSphere 证书要求"](#)
 - ["替换 vCenter 计算机 SSL 证书自定义证书颁发机构签名的证书"](#)
 - ["错误：使用者备用名称 \(SAN\) 字段不包含 PNID。请提供有效证书"](#)



如果 FQDN 不可用，您可以将 PNID 设置为 IP 地址，并将 IP 地址包含在 SAN 中。但是，VMware 不建议这样做。

步骤

1. 打开 Web 浏览器并转到以下 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。
4. 在高级选项中，自动获取 vCenter Server 证书（授权）或手动上传。



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：

- ONTAP工具将 vCenter 客户端插件注册为远程插件。
- 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。

在 ONTAP tools 中向 vCenter Server 实例注册 VASA Provider

使用ONTAP tools for VMware vSphere将 VASA 提供程序注册到 vCenter Server 实例。这使得基于存储策略的管理、vVols支持以及与ONTAP系统上的 VMware Live Site Recovery 设备的集成成为可能。

VASA 提供程序设置显示所选 vCenter Server 的注册状态。

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“设置”>“VASA 提供程序设置”。ONTAP工具显示 VASA 提供程序注册状态为未注册。
4. 选择*注册*按钮以注册VASA Provider。
5. 输入 VASA 提供程序的名称和凭据。用户名只能包含字母、数字和下划线。将密码长度设置为 8 到 256 个字符之间。
6. 选择 * 注册 *。
7. 成功注册并刷新页面后，ONTAP工具将显示已注册的 VASA 提供程序的状态、名称和版本。

下一步行动

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

步骤

1. 转到 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。

使用ONTAP工具安装 NFS VAAI 插件

NFS vStorage API for Array Integration (NFS VAAI) 插件将 VMware vSphere 连接到 NFS 存储阵列。使用适用ONTAP tools for VMware vSphere安装 VAAI 插件。这允许 NFS 存储阵列代替 ESXi 主机处理某些存储操作。

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. 如果您已经将 VAAI 插件上传到 vCenter Server，请在 **现有版本** 中选择 **更改**。如果还没有，请选择 ***上传***。
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***。

vSphere Web Client 仅显示可以安装该插件的 ESXi 主机。您可以在“近期任务”部分监控安装进度。

7. 安装后手动重新启动 ESXi 主机。

重新启动 ESXi 主机后，ONTAP tools for VMware vSphere 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，配置 VAAI 副本卸载的 NFS 导出策略。确保出口策略规则满足以下要求：

- 相关的 ONTAP 卷允许 NFSv4 调用。
- 根用户仍为根用户，并且所有连接父卷中都允许使用 NFSv4。
- 在相关的 NFS 服务器上设置 VAAI 支持选项。

更多信息，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"](#)

在 ONTAP tools 中配置 ESXi 主机设置

配置 ESXi 服务器多路径和超时设置有助于维护数据可用性和完整性。如果主路径不可用，它可以自动故障转移到备份存储路径。

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

此过程可能需要一些时间，具体取决于您的设置和系统负载。您可以在“近期任务”面板中查看进度。

步骤

1. 在VMware vSphere Web Client的主页页面中、选择*主机和群集*。
2. 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*。
3. 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。
4. 选择*应用建议设置*链接。
5. 在“应用推荐的主机设置”窗口中，选择要更新以使用NetApp推荐设置的主机，然后选择“下一步”。



您可以展开ESXi主机以查看当前值。

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

设置ESXi主机值

使用ONTAP tools for VMware vSphere在 ESXi 主机上设置超时和其他值，以实现最佳性能和故障转移。它根据NetApp测试设置这些值。

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 设置为NetApp存储系统选择最佳路径。 MPIO 设置选择最佳路径并使用它。

对于高性能环境或使用单个 LUN 数据存储进行测试时，调整循环 (VMW_PSP_RR) 路径选择策略 (PSP) 的负载平衡设置以提高性能。将默认 IOPS 值从 1000 设置为 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

为 ONTAP tools 配置 ONTAP 用户角色和权限

使用此部分配置适用 ONTAP tools for VMware vSphere 和 ONTAP System Manager 的 ONTAP 工具的存储后端 ONTAP 用户角色和权限。您可以使用提供的 JSON 文件分配角色，手动创建用户和角色，并为非管理员帐户应用所需的最低权限。

开始之前

- 使用 https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip 从 ONTAP tools for VMware vSphere 下载 ONTAPPrivileges 文件。下载 zip 文件后，您会发现两个 JSON 文件。配置 ASA r2 系统时使用 ASA r2 特定的 JSON 文件。



您可以在集群级别或直接在存储虚拟机 (SVM) 级别创建用户。如果您不使用 user_roles.json 文件，请确保用户具有所需的最低 SVM 权限。

- 以存储后端的管理员权限登录。

步骤

1. 提取您下载的 https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_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. 使用管理员权限登录集群。要配置用户：
 - a. 要配置集群 ONTAP 工具用户，请选择 集群 > 设置 > *用户和角色* 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 ONTAPPrivilegesJSON 文件。对于非 ASA r2 系统，选择 users_roles.json 文件；对于 ASA r2 系统，选择 users_roles_ASAr2.json 文件。

ONTAP 工具会自动填充产品字段。

- f. 从下拉菜单中选择产品功能为 *VSC、VASA Provider 和 SRA*。

ONTAP 工具会根据您选择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. 选择用户需要的权限（发现、创建存储、修改存储、销毁存储、NAS/SAN 角色），然后选择*添加*。

ONTAP工具添加了新的角色和用户。您可以查看您配置的角色下的权限。

SVM聚合映射要求

使用 SVM 用户凭据配置数据存储库时，ONTAP tools for VMware vSphere在数据存储库 POST API 中指定的聚合上创建卷。ONTAP阻止 SVM 用户在未映射到 SVM 的聚合上创建卷。在创建卷之前，使用ONTAP REST API 或 CLI 将 SVM 映射到所需的聚合。

REST API:

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

ONTAP命令行界面:

```
still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State          Size Type      SnapLock
Type-----
-----svm_test      still15_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

手动创建ONTAP用户和角色

无需 JSON 文件即可手动创建用户和角色。

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 集群 > 设置 > 用户和角色。
 - 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。
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。

添加*REST API 路径*并从下拉列表中选择访问权限。
 - 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

本页列出了没有 JSON 文件的非管理员全局作用域集群用户所需的最低权限。如果集群处于本地范围内，请使用 JSON 文件创建用户，因为适用ONTAP tools for VMware vSphere需要的不仅仅是在ONTAP上进行配置的读取权限。

您可以使用 API 访问功能：

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	许可证检查协议特定的许可证
/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/卷配置期间的聚合空间检查
/API/storage/cluster	只读	获取集群级别空间和效率数据
/API/storage/disks	只读	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	在本地添加集群时获取 SVM 配置。
/API/network/IP/接口	只读	添加存储后端 - 确定管理 LIF 范围是集群/SVM
/API/storage/availability分区	只读	SAZ 发现。适用于ONTAP 9.16.1 及更高版本和ASA r2 系统。
/api/cluster/metrocluster	只读	获取MetroCluster状态和配置详细信息。

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



PATCH 操作和数据存储上的自动回滚需要发现、创建、修改和销毁权限。缺少权限可能会导致工作流程和清理问题。

具有发现、创建、修改和销毁权限的基于ONTAP API 的用户可以管理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

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -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
```

对于ASA ONTAP R2系统上的9.16.1及更高版本、运行以下命令：

```
security login rest-role create -role <role-name> -api  
/api/storage/availability-zones -access readonly
```

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

运行以下命令创建具有所有权限的 SVM 范围用户：

```
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 Cl_sti160-cluster_
```

运行以下命令解锁帐户并启用管理界面访问：

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

示例

```
security login unlock -username testvpsraall -vserver Cl_sti160-cluster
```

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

对于使用JSON文件创建了集群范围用户的适用于VMware vSphere 10.1的ONTAP工具用户、请对用户admin Privileges使用以下ONTAP命令行界面命令升级到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
```

对于使用json文件创建了SVM范围的用户适用于VMware vSphere 10.1的ONTAP工具用户、请对管理员用户Privileges使用ONTAP命令行界面命令升级到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>
```

要启用以下命令，请将命令 `vserver nvme namespace show` 和 `vserver nvme subset show` 添加到现有角色。

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

将适用于VMware vSphere 10.3用户的ONTAP工具升级到10.4用户

从ONTAP 9.16.1 开始，将ONTAP tools for VMware vSphere升级到 10.4 用户。

如果适用于VMware vSphere 10.3的ONTAP工具用户的集群范围用户是使用JSON文件和ONTAP 9.16.1或更高版本创建的、请对管理员用户Privileges使用ONTAP命令行界面命令升级到10.4版本。

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> -cmddirname "storage  
availability-zone show" -access all
```

将存储后端添加到 ONTAP tools

使用ONTAP tools for VMware vSphere，为您的 ESXi 主机添加和管理存储后端。您可以部署集群或 SVM，启用MetroCluster支持，并验证证书以确保安全连接。您可以使用ONTAP工具管理器或 vSphere 客户端配置存储后端，监控证书状态，并在集群更改后手动重新发现资源。

要在本地添加存储后端，请在ONTAP工具界面中使用集群或 SVM 凭据。本地存储后端仅对选定的 vCenter Server 可用。ONTAP工具将 SVM 映射到 vCenter Server 以进行vVols或 VMFS 数据存储库管理。对于 VMFS 数据存储和 SRA 工作流，您可以使用 SVM 凭据而无需全局映射集群。

要添加全局存储后端，请在ONTAP工具管理器中使用ONTAP集群凭据。全局存储后端支持发现工作流，以识别 vVol 管理所需的集群资源。在多租户环境中，您可以本地添加 SVM 用户来管理vVols数据存储。

如果ONTAP中启用了MetroCluster支持，则将源集群和目标集群都作为本地或全局存储后端加入。

开始之前

验证证书是否包含有效的主题备用名称 (SAN) 字段。ONTAP系统使用 SAN 字段来识别集群和 SVM 管理 LIF。

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。

5. 自动获取ONTAP集群证书并授权该证书，或者通过浏览到其位置手动上传。



如果需要，您可以从维护控制台禁用主题备用名称 (SAN) 验证。有关说明，请参阅["更改证书验证标志"](#)。

6. 如果您添加的存储后端是MetroCluster配置的一部分，ONTAP工具管理器会显示一条弹出消息以添加对等集群。选择“添加”并提供MetroCluster对等存储后端的详细信息。



ONTAP系统执行切换和切回后，手动运行ONTAP工具发现。

使用vSphere客户端用户界面



vVols数据存储不支持通过 vSphere Client 用户界面直接添加 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。



您可以使用基于集群的凭据以及 IPv4 或 IPv6 管理 LIF 添加存储后端。要直接添加 SVM 用户，请提供基于 SVM 的凭据以及 SVM 管理 LIF。如果集群已加入，则无法再次从该集群加入 SVM 用户。

5. 自动获取ONTAP集群证书并授权该证书，或者通过浏览到其位置手动上传。
6. 如果添加的存储后端是MetroCluster配置的一部分，ONTAP工具将显示 添加**MetroCluster**对等体 屏幕。选择*添加对等*以添加对等存储后端。



ONTAP系统执行切换和切回后，手动运行ONTAP工具发现。

下一步是什么？

ONTAP工具更新列表以显示新的存储后端。

ONTAP工具在 存储后端 页面上列出了新添加的存储后端。如果证书在 30 天或更短时间内过期，ONTAP工具会在证书过期日期列中显示警告。到期后，ONTAP工具会将存储后端标记为未知，因为它无法连接到存储系统。

相关信息

["将集群配置到 MetroCluster 配置中"](#)

在 ONTAP tools 中将存储后端与 vCenter Server 实例关联

将存储后端与 vCenter Server 实例关联，以启用所有 vCenter Server 实例的访问。对于MetroCluster配置，当关联存储后端集群时，请确保还将其对等集群与 vCenter Server 关联。

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. 选择要连接到存储后端的 vCenter Server 实例旁边的垂直省略号。
5. 从下拉菜单中，选择要与所选 vCenter Server 实例关联的存储后端。

在 ONTAP tools 中配置网络访问

默认情况下，除非配置网络访问，否则从 ESXi 主机发现的所有 IP 地址都会自动添加到导出策略中。您可以修改导出策略，仅允许特定 IP 地址访问。如果被排除的 ESXi 主机尝试执行挂载操作，则该操作会失败。

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工具的左侧窗格中，转到 设置 > 管理网络访问 > 编辑。

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 *。

在 ONTAP tools 中创建数据存储库

当您在主机集群级别创建数据存储库时，ONTAP工具会将其挂载到所有目标主机上，并且仅当您拥有所需的权限时才启用该操作。

本机数据存储与 vCenter Server 和 ONTAP 工具管理的数据存储之间的互操作性

从适用于ONTAP tools for VMware vSphere开始，ONTAP工具为数据存储区创建嵌套 igroup，其中父 igroup 特定于数据存储区，子 igroup 映射到主机。您可以从ONTAP系统管理器创建平面 igroup，并使用它们创建

VMFS 数据存储库，而无需使用ONTAP工具。参考 ["管理 SAN 启动器和 igroup"](#) 了解更多信息。

在您加入存储并运行数据存储发现后，ONTAP工具会将 VMFS 数据存储中的平面 igroup 更改为嵌套 igroup。您不能使用早期的平面 igroup 来创建新的数据存储。使用ONTAP工具界面或 REST API 来重用嵌套 igroup。

创建一个卷数据存储库

从适用于ONTAP tools for VMware vSphere开始，您可以在ASA r2 系统上创建具有与 thin.vVol 相同的空间效率的vVols数据存储。 VASA 提供程序在创建 vVol 数据存储时创建一个容器和所需的协议端点。 VASA 提供程序不会为该容器分配任何支持卷。

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 * NetApp ONTAP工具* > * 创建数据存储*。
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. 在高级选项下：
 - 如果您选择*自定义导出策略*，请确保在 vCenter 中对所有对象运行发现。建议您不要使用此选项。
 - 您可以为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创建一个卷数据存储库。

创建新卷时，您可以在数据存储上启用 QoS。默认情况下，每个 LUN 创建请求都会创建一个卷。对于ASA r2 存储系统上的vVols数据存储，请跳过此步骤。

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

NFS 数据存储使用 NFS 协议将 ESXi 主机连接到共享存储。它们简单、灵活，可用于 VMware vSphere 环境。

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 * NetApp ONTAP工具* > * 创建数据存储*。
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. 如果在高级选项下选择“自定义导出策略”，则在 vCenter 中对所有对象运行发现。建议您不要使用此选项。



您不能使用 SVM 的默认或根卷策略创建 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。
 - 当您在平台下拉菜单中选择“任何”选项时，您可以看到 vCenter 中的所有 SVM。平台和不对称旗帜不影响可见性。
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)*。

ONTAP工具创建 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

VMFS 是一个用于存储虚拟机文件的集群文件系统。多个 ESXi 主机可以同时访问相同的 VM 文件，以实现 vMotion 和高可用性功能。

在受保护集群上：

- 您只能创建 VMFS 数据存储区。将 VMFS 数据存储添加到受保护的集群会自动保护它。
- 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。
- 如果父主机群集受“自动故障转移双工策略”（统一或非统一配置）保护，则无法在 ESXi 主机上创建数据存储。
- 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. 检查网络接口卡 (NIC) 供应商是否支持采用 NVMe/TCP 协议的 ESXi NIC。
- c. 根据 NIC 供应商规范为 NVMe/TCP 设置 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 NVMe/FC 协议，请执行以下步骤来配置 ESXi 主机：

- a. 如果尚未启用、请在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 * NetApp ONTAP工具* > * 创建数据存储*。
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名称、大小和协议信息。要将新的数据存储区添加到现有的 VMFS 群集，请在高级选项中选择数据存储区群集。
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。

当选择NVMe/FC或NVMe/TCP协议时，会创建一个新的命名空间子系统，并用于命名空间映射。ONTAP工具使用包含数据存储名称的自动生成名称创建命名空间子系统。您可以在“存储”窗格的高级选项中的“自定义命名空间子系统名称”字段中重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，由于存储是分解的，因此不会显示 **Aggregate** 选项。当您选择ASA r2 存储系统类型的 SVM 时，存储属性页面会显示用于启用 QoS 的选项。

- b. ONTAP工具根据所选协议创建具有精简空间预留的存储单元（LUN/命名空间）。



从ONTAP 9.161开始、ASA R2存储系统支持每个集群最多12个节点。

- c. 为包含12个节点的异构集群SVM的ASA R2存储系统选择*性能服务级别*。如果选定SVM是同构集

群或使用SVM用户、则此选项不可用。

"any"是默认性能服务级别(PSL)值。此设置使用ONTAP平衡放置算法创建存储单元。但是、您可以根据需要选择性能或极高选项。

d. 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，这些选项不会显示。



您不能使用现有卷来创建具有 NVMe/FC 或 NVMe/TCP 协议的 VMFS 数据存储。为 VMFS 数据存储创建新卷。

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

ONTAP工具创建 VMFS 数据存储库并将其安装在所有主机上。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 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。