配置 ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目录

配置 ONTAP tools for VMware vSphere

将 vCenter Server 实例添加到 ONTAP tools

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

关于此任务

ONTAP tools 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。

将 vCenter Server 实例添加到 ONTAP tools 会自动触发以下操作：

- ONTAP tools 将 vCenter 客户端插件注册为远程插件。
- 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。
- 插件在 vSphere 用户界面上显示为快捷方式。

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，确保证书中的 SAN 包含 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 URL： `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. 使用部署期间提供的 ONTAP tools for VMware vSphere 管理员凭据登录。
3. 选择 **vCenters** > *添加*以载入 vCenter 服务器实例。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 服务器证书（授权）或手动上传。

> 您无需管理员账号即可将vCenter实例添加到 ONTAP tools。您可以创建不含管理员账号且权限受限的自定义角色。有关详细信息，请参阅"将 vCenter Server RBAC 与 ONTAP tools for VMware vSphere 10 结合使用"。

在 ONTAP tools 中向 vCenter Server 实例注册 VASA Provider

使用 ONTAP tools for VMware vSphere 向 vCenter Server 实例注册 VASA Provider。这样可以在 ONTAP 系统上启用基于存储策略的管理、vVols 支持以及与 VMware Live Site Recovery 设备的集成。

VASA Provider 设置显示选定 vCenter 服务器的注册状态。

步骤

1. 登录到 vSphere 客户端。
2. 在插件部分下选择*快捷方式* > **NetApp ONTAP tools**。
3. 选择 **Settings** > **VASA Provider settings**。ONTAP tools 将 VASA Provider 注册状态显示为未注册。
4. 选择*注册*按钮注册 VASA Provider。
5. 输入 VASA Provider 的名称和凭据。用户名只能包含字母、数字和下划线。密码必须介于 8 到 256 个字符之间。
6. 选择*注册*。
7. 成功注册和页面刷新后，ONTAP tools 将显示已注册的 VASA Provider 的状态、名称和版本。

下一步

验证已载入的 VASA Provider 是否已在 vCenter 客户端的 VASA Provider 下列出：

步骤

1. 转到 vCenter Server 实例。
2. 使用管理员凭据登录。
3. 选择*存储提供商* > 配置。确认已正确列出已启用的 VASA Provider。

使用 ONTAP tools 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 ONTAP tools for VMware vSphere 安装 VAAI 插件。这样，NFS 存储阵列便可处理某些存储操作，而无需由 ESXi 主机处理。

开始之前

- 下载 "适用于 VMware VAAI 的 NetApp NFS 插件" 安装包。
- 确保您的 ESXi 主机具有 vSphere 7.0 U3（最新补丁或更高版本）和 ONTAP 9.14.1 或更高版本。
- 挂载 NFS 数据存储库。

步骤

1. 登录到 vSphere 客户端。
2. 在插件部分下选择*快捷方式* > **NetApp ONTAP tools**。
3. 选择*设置* > **NFS VAAI** 工具。
4. 如果您已将 VAAI 插件上传到 vCenter Server，请在*现有版本*中选择*更改*。如果您还没有，请选择*上传*。
5. 浏览并选择 `.vib`文件，然后选择*上传*将文件上传到 ONTAP tools。
6. 选择 **Install on ESXi host**，选择要安装 NFS VAAI 插件的 ESXi 主机，然后选择 **Install**。

   vSphere Web 客户端仅显示可以安装此插件的 ESXi 主机。您可以在最近的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，为 VAAI 副本卸载配置 NFS 导出策略。确保导出策略规则满足以下要求：

- 相关的 ONTAP 卷允许 NFSv4 调用。
- root 用户仍为 root，并且在所有 junction 父卷中都允许使用 NFSv4。
- VAAI 支持选项在相关 NFS 服务器上设置。

有关详细信息，请参见 "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 对 NFSv4.2 的支持"

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，它会自动故障切换到备份存储路径。

配置 ESXi 服务器多路径和超时设置

ONTAP tools for VMware vSphere 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

此过程可能需要一段时间，具体取决于您的设置和系统负载。您可以在"最近的任务"面板中查看进度。

步骤

1. 从 VMware vSphere Web 客户端主页中，选择*主机和群集*。
2. 在 VMware vSphere Web 客户端的快捷方式页面上，在插件部分下选择 **NetApp ONTAP tools**。
3. 转到 ONTAP tools for VMware vSphere 插件概述（仪表板）中的 **ESXi Host compliance** 卡。
4. 选择*Apply Recommended Settings*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，根据需要选择推荐值。
7. 在摘要窗格中，检查值并选择*Finish*。您可以在"近期任务"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。

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 数据存储区进行测试时，请调整循环 (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

使用此部分可使用适用于 VMware vSphere 的 ONTAP tools 和 ONTAP System Manager 为存储后端配置 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 ONTAP Privileges 文件。下载 zip 文件后，您会找到两个 JSON 文件。配置 ASA r2 系统时，请使用特定于 ASA r2 的 JSON 文件。

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

- 使用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 System Manager。
3. 使用管理员权限登录到集群。要配置用户：
   a. 要配置集群 ONTAP tools 用户，请选择 集群 > 设置 > 用户和角色 窗格。
   b. 要配置 SVM ONTAP tools 用户，请选择 **Storage SVM** > **Settings** > **Users and Roles** 窗格。
   c. 在"用户"下选择*添加*。
   d. 在*添加用户*对话框中，选择*虚拟化产品*。
   e. *浏览*以选择并上传 ONTAP Privileges JSON 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 tools 会自动填充 Product 字段。

   f. 从下拉列表中选择产品功能为 **VSC, VASA Provider and SRA**。

      ONTAP tools 将根据您选择的产品功能自动填充*角色*字段。

   g. 请输入所需用户名和密码。

h. 选择用户需要的 Privileges（Discovery、Create Storage、Modify Storage、Destroy Storage 、NAS/SAN Role），然后选择*Add*。

ONTAP tools 添加新的角色和用户。您可以在配置的角色下查看 Privileges。

SVM聚合映射要求

使用 SVM 用户凭据配置数据存储时，ONTAP tools for VMware vSphere 会在数据存储 POST API 中指定的聚合上创建卷。ONTAP 会阻止 SVM 用户在未映射到 SVM 的聚合上创建卷。在创建卷之前，请使用 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 CLI：

```
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

在没有 JSON 文件的情况下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 System Manager。
2. 使用管理员权限登录到集群。
   a. 要配置集群 ONTAP tools 角色，请选择*集群* > 设置 > 用户和角色。
   b. 要配置集群 SVM ONTAP tools 角色，请选择 存储 **SVM** > 设置 > 用户和角色。
3. 创建角色：
   a. 选择*角色*表下的*添加*。
   b. 输入*角色名称*和*角色属性*详细信息。

      添加 **REST API Path** 并从下拉列表中选择访问权限。

   c. 添加所有必要的 API 并保存更改。
4. 创建用户：
   a. 在 用户 表下选择 添加。
   b. 在*添加用户*对话框中，选择*System Manager*。

c. 输入*用户名*。

d. 从上述*创建角色*步骤中创建的选项中选择*角色*。

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，身份验证类型为 **Password**。

f. 设置*此用户的密码*并*保存*此用户。

非管理员全局作用域集群用户所需的最低权限列表

此页面列出了没有 JSON 文件的非管理员全局范围集群用户所需的最低权限。如果集群在本地范围内，请使用 JSON 文件创建用户，因为 ONTAP tools for VMware vSphere 在 ONTAP 上进行配置时需要的不仅仅是读取权限。

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/licenses	只读	协议特定许可证的许可证检查
/api/cluster/nodes	只读	平台类型发现
/api/security/accounts	只读	权限发现
/api/security/roles	只读	权限发现
/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/policies	读取/创建/修改	QoS 和 VM 策略管理
/api/svm/svms	只读	在本地添加集群时获取 SVM 配置。
/api/network/ip/interfaces	只读	添加存储后端 - 识别管理 LIF 范围是集群/SVM
/api/storage/availability-zones	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 **VMware vSphere** 创建基于 **ONTAP API** 的集群范围用户的 **ONTAP tools**

PATCH 操作和数据存储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 tools 工作流。

要创建具有上述所有权限的集群范围的用户，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 版本 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 ONTAP 版本 9.16.1 及更高版本上的 ASA r2 系统，运行以下命令：

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

为 **VMware vSphere** 创建基于 **ONTAP API** 的 **SVM** 范围用户的 **ONTAP tools**

运行以下命令以创建具有所有权限的 SVM 范围的用户：

```
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 版本 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>
```

要使用以前创建的基于 API 的角色创建新的基于 API 的用户，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_
```

运行以下命令来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 C1_sti160-cluster
```

将 **ONTAP tools for VMware vSphere 10.1** 用户升级到 **10.3** 用户

对于使用 JSON 文件创建了集群范围用户的 ONTAP tools for VMware vSphere 10.1 用户，请使用具有用户管理员权限的以下 ONTAP CLI 命令升级到 10.3 版本。

对于产品功能：

- VSC
- VSC 和 VASA Provider
- VSC 和 SRA
- VSC、VASA Provider 和 SRA。

集群权限：

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all

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

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

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

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

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

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

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all

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

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

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

对于具有使用 json 文件创建的 SVM 范围用户的 ONTAP tools for VMware vSphere 10.1 用户，请使用具有管理员用户权限的 ONTAP CLI 命令升级到 10.3 版本。

SVM 权限：

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

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

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

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

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

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

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

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>

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

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

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

要启用以下命令，请将命令 *vserver nvme namespace show* 和 *vserver nvme subsystem 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** 的 **ONTAP tools 10.3** 用户升级到 **10.4** 用户

从 ONTAP 9.16.1 开始，将适用于 VMware vSphere 的 ONTAP tools 10.3 用户升级到 10.4 用户。

对于使用 JSON 文件创建了集群范围用户且 ONTAP 版本为 9.16.1 或更高版本的 ONTAP tools for VMware vSphere 10.3 用户，请使用具有管理员用户权限的 ONTAP CLI 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。

集群权限：

```
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。您可以加载集群或 SVM、启用 MetroCluster 支持，并验证证书以实现安全连接。您可以使用 ONTAP tools Manager 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 tools 界面中使用集群或 SVM 凭据。本地存储后端仅对所选 vCenter Server 可用。ONTAP tools 将 SVM 映射到 vCenter Server，以进行 vVols 或 VMFS 数据存储管理。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 tools Manager 中使用 ONTAP 集群凭据。全局存储后端使发现工作流能够识别 vVol 管理所需的集群资源。在多租户环境中，您可以在本地添加 SVM 用户以管理 vVols 数据存储区。

有关全局和本地存储后端的更多信息，请参见 KB 文章： "OTV 10：什么是存储后端全局和本地范围"。

如果 ONTAP 中启用了 MetroCluster 支持，请将源集群和目标集群均作为本地或全局存储后端载入。

开始之前

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

使用 **ONTAP tools Manager**

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 tools Manager：
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用部署期间提供的 ONTAP tools for VMware vSphere 管理员凭据登录。
3. 从侧边栏中选择 **Storage Backends**。
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 LIF。

5. 自动获取 ONTAP 集群证书并授权证书，或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使用者备用名称(SAN)验证。有关说明，请参见 "更改证书验证标志"。

6. 如果添加的存储后端是 MetroCluster 配置的一部分，则 ONTAP tools Manager 将显示一条弹出消息以添加对等集群。选择 **Add** 并提供 MetroCluster 对等存储后端的详细信息。

   在 ONTAP 系统执行切换和切回后，手动运行 ONTAP tools 发现。

使用 **vSphere** 客户端用户界面

vVols 数据存储区不支持通过 vSphere 客户端用户界面直接添加 SVM 用户。

1. 登录到 vSphere 客户端。
2. 在快捷方式页面中，在插件部分下选择*NetApp ONTAP tools*。
3. 从侧边栏中选择 **Storage Backends**。
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。

   您可以使用具有 IPv4 或 IPv6 管理 LIF 的基于集群的凭据添加存储后端。要直接添加 SVM 用户，请提供基于 SVM 的凭据以及 SVM 管理 LIF。如果集群已启用，则无法再次从该集群启用 SVM 用户。

5. 自动获取 ONTAP 集群证书并授权证书，或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 tools 将显示*添加 MetroCluster 对等项*屏幕。选择*添加对等端*以添加对等端存储后端。

   在 ONTAP 系统执行切换和切回后，手动运行 ONTAP tools 发现。

ONTAP tools 在*存储后端*页面上列出新添加的存储后端。如果证书在 30 天或更短时间内过期，ONTAP tools 会在证书过期日期列中显示警告。到期后，ONTAP tools 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

"OTV 10：什么是存储后端全局和本地范围"

"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，以启用对所有 vCenter Server 实例的访问。对于 MetroCluster 配置，当您关联存储后端集群时，请确保也将其对等集群与 vCenter Server 关联。

步骤

1. 从 Web 浏览器启动 ONTAP tools Manager：
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用部署期间提供的 ONTAP tools for VMware vSphere 管理员凭据登录。
3. 从侧边栏中选择 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，选择要与选定 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，从 ESXi 主机发现的所有 IP 地址都会自动添加到导出策略中，除非您配置了网络访问权限。您可以修改导出策略以仅允许从特定 IP 地址进行访问。如果排除的 ESXi 主机尝试挂载操作，则该操作会失败。

步骤

1. 登录到 vSphere 客户端。
2. 在插件部分下的快捷方式页面中选择 **NetApp ONTAP tools**。
3. 在 ONTAP tools 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，请用逗号、范围、无类域间路由 (CIDR) 或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

在主机集群级别创建数据存储区时，ONTAP tools 会将其挂载到所有目标主机上，并仅在您具有所需权限时才启用此操作。

本机数据存储与 **vCenter Server** 和 **ONTAP tools** 托管数据存储之间的互操作性

从 ONTAP tools for VMware vSphere 10.4 开始，ONTAP tools 为数据存储区创建嵌套 igroup，父 igroup 特定于数据存储区，子 igroup 映射到主机。您可以从 ONTAP System Manager 创建平面 igroup，并使用它们在不使用 ONTAP tools 的情况下创建 VMFS 数据存储区。有关详细信息，请参见 "管理 SAN 启动器和 igroup"。

加载存储并运行数据存储区发现后，ONTAP tools 会将 VMFS 数据存储区中的平面 igroup 更改为嵌套 igroup。您不能使用较早的平面 igroup 来创建新数据存储区。使用 ONTAP tools 界面或 REST API 重新使用嵌套 igroup。

创建 **vVols** 数据存储库

从 ONTAP tools for VMware vSphere 10.3 开始，您可以在 ASA r2 系统上创建空间效率为精简的 vVols 数据存储库。vVol。VASA Provider 在创建 vVol 数据存储库时会创建容器和所需的协议端点。VASA Provider 不会将任何备份卷分配给此容器。

开始之前

- 确保根聚合未映射到 SVM。
- 确保已将 VASA Provider 注册到所选的 vCenter。
- 在 ASA r2 存储系统中，应将 SVM 映射到 SVM 用户的聚合。

步骤

1. 登录到 vSphere 客户端。
2. 右键单击主机系统、主机群集或数据中心，然后选择*NetApp ONTAP tools* > 创建数据存储。
3. 选择 vVols 作为 数据存储类型。
4. 输入*数据存储库名称*和*协议*信息。

   ASA r2 系统支持 iSCSI 和 FC 协议用于 vVols。

5. 选择希望在其中创建数据存储库的存储虚拟机。
6. 在高级选项下：
   - 如果选择*自定义导出策略*，请确保在 vCenter 中为所有对象运行发现。建议您不要使用此选项。
   - 您可以为 iSCSI 和 FC 协议选择*自定义启动器组*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，您不能将这两种类型的卷组合起来创建 vVols 数据存储区。

   创建新卷时，可以在数据存储区上启用 QoS。默认情况下，为每个 LUN 创建请求创建一个卷。对于 ASA r2 存储系统上的 vVols 数据存储，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** 数据存储区

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 客户端。
2. 右键单击主机系统、主机群集或数据中心，然后选择*NetApp ONTAP tools* > 创建数据存储。
3. 在*数据存储类型*字段中选择 NFS。
4. 在*名称和协议*窗格中输入数据存储区名称、大小和协议信息。在高级选项中选择*数据存储群集*和*

Kerberos 身份验证*。

仅当选择了 NFS 4.1 协议时，Kerberos 身份验证才可用。

5. 在 **Storage** 窗格中选择 **Platform** 和 **Storage VM**。
6. 如果在高级选项下选择*自定义导出策略*，请在 vCenter 中对所有对象运行发现。建议您不要使用此选项。

无法使用 SVM 的默认或根卷策略创建 NFS 数据存储库。

- 在高级选项中，*非对称*切换按钮仅在平台下拉列表中选择性能或容量时才可见。
- 当您在平台下拉列表中选择*任何*选项时，您可以在 vCenter 中看到所有 SVM。平台和非对称标志不会影响可见性。

7. 在*存储属性*窗格中选择用于卷创建的聚合。在高级选项中，根据需要选择*空间预留*和*启用 QoS*。
8. 查看*摘要*窗格中的选择，然后选择*完成*。

ONTAP tools 创建 NFS 数据存储区并将其挂载到所有主机上。

创建 **VMFS** 数据存储区

VMFS 是一个用于存储虚拟机文件的群集文件系统。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。

在受保护的集群上：

- 您只能创建 VMFS 数据存储。将 VMFS 数据存储添加到受保护的集群将自动对其进行保护。
- 无法在具有一个或多个受保护主机群集的数据中心上创建数据存储区。
- 如果父主机集群受"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。
- 只能在受异步关系保护的 ESXi 主机上创建 VMFS 数据存储区。您不能在受"Automated Failover Duplex"策略保护的主机集群中的 ESXi 主机上创建和挂载数据存储区。

开始之前

- 在 ONTAP 存储端为每个协议启用服务和 LIF。
- 将 ASA r2 存储系统中的 SVM 映射到 SVM 用户的聚合。
- 如果使用 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) 供应商是否支持使用 NVMe/TCP 协议的 ESXi NIC。
  c. 根据 NIC 供应商规格设置 NVMe/TCP 的 ESXi NIC。
  d. 使用 VMware vSphere 7 版本时，请按照 VMware 站点上的说明 "为 NVMe over TCP 适配器配置 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 NVMe over TCP"配置 NVMe/TCP 端口绑定。

e. 对于 VMware vSphere 7 版本，请按照第 "启用 NVMe over RDMA 或 NVMe over TCP 软件适配器"页上的说明配置 NVMe/TCP 软件适配器。对于 VMware vSphere 8 版本，请按照 "添加软件 NVMe over RDMA 或 NVMe over TCP 适配器"配置 NVMe/TCP 软件适配器。

f. 在 ESXi 主机上运行 "发现存储系统和主机" 操作。有关详细信息，请参见 "如何使用 vSphere 8.0 Update 1 和 ONTAP 9.13.1 为 VMFS 数据存储配置 NVMe/TCP"。

- 如果使用 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 NVMe over Fabrics (NVMe-oF)。

b. 完成 SCSI 分区。

c. 确保 ESXi 主机和 ONTAP 系统在物理和逻辑层连接。

要为 FC 协议配置 ONTAP SVM，请参阅 "为 FC 配置 SVM"。

有关在 VMware vSphere 8.0 中使用 NVMe/FC 协议的更多信息，请参阅 "适用于带 ONTAP 的 ESXi 8.x 的 NVMe-oF 主机配置"。

有关在 VMware vSphere 7.0 中使用 NVMe/FC 的更多信息，请参阅 "ONTAP NVMe/FC 主机配置指南"和 "TR-4684"。

步骤

1. 登录到 vSphere 客户端。
2. 右键单击主机系统、主机群集或数据中心，然后选择*NetApp ONTAP tools* > 创建数据存储。
3. 选择 VMFS 数据存储类型。
4. 在*名称和协议*窗格中输入数据存储区名称、大小和协议信息。要将新数据存储添加到现有 VMFS 群集，请在高级选项中选择数据存储群集。
5. 在 **Storage** 窗格中选择一个存储 VM。根据需要在 高级选项 部分中提供 自定义启动器组名称。您可以为数据存储区选择现有的 igroup，也可以使用自定义名称创建新的 igroup。

   选择 NVMe/FC 或 NVMe/TCP 协议时，将创建一个新的命名空间子系统并用于命名空间映射。ONTAP tools 使用包含数据存储区名称的自动生成名称创建命名空间子系统。您可以在 **Storage** 窗格的高级选项中的 **custom namespace subsystem name** 字段中重命名命名空间子系统。

6. 在*存储属性*窗格中：

   a. 从下拉选项中选择 **Aggregate**。

   对于 ASA r2 存储系统，不显示 **Aggregate** 选项，因为存储是分解的。当您选择 ASA r2 存储系统类型 SVM 时，存储属性页面将显示启用 QoS 的选项。

   b. ONTAP tools 根据选定协议创建具有精简空间保留的存储单元（LUN/命名空间）。

   从 ONTAP 9.16.1 开始，ASA r2 存储系统每个集群最多支持 12 个节点。

   c. 为具有 12 个节点 SVM 的异构集群的 ASA r2 存储系统选择*性能服务级别*。如果选定的 SVM 是同构集群或使用 SVM 用户，则此选项不可用。

"Any"是默认的性能服务级别 (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限选项。

d. 根据需要选择 **Use existing volume**、**Enable 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/Namespace）。因此，这些选项不会显示。

无法使用现有卷通过 NVMe/FC 或 NVMe/TCP 协议创建 VMFS 数据存储区。为 VMFS 数据存储区创建新卷。

7. 在*摘要*窗格中查看数据存储库详细信息，然后选择*完成*。

如果在受保护的集群上创建数据存储库，则可以看到一条只读消息："The datastore is being mounted on a protected Cluster."

结果

ONTAP tools 创建 VMFS 数据存储区并将其挂载到所有主机上。

版权信息

商标信息