



适用于 VMware® vSphere 的 Virtual Storage Console、VASA Provider 和 Storage Replication Adapter

部署和设置指南

9.6 版

2019 年 8 月 | 215-13886_2019-08_zh-cn
ng-gpso-china-documents@netapp.com

目录

VSC、VASA Provider 和 SRA 虚拟设备概述	5
适用于新用户的 VSC、VASA Provider 和 SRA 虚拟设备部署工作流	7
适用于现有用户的 VSC、VASA Provider 和 SRA 部署工作流	7
VSC、VASA Provider 和 SRA 虚拟设备的部署要求	9
VSC 的端口要求	9
VSC、VASA Provider 和 SRA 虚拟设备的空间和规模估算要求	9
VSC、VASA Provider 和 SRA 虚拟设备支持的存储系统、许可和应用程序 ...	10
部署 VSC、VASA Provider 和 SRA 虚拟设备时的注意事项和要求	10
部署或升级 VSC、VASA Provider 和 SRA	13
下载 VSC、VASA Provider 和 SRA 虚拟设备	13
部署 VSC、VASA Provider 和 SRA 虚拟设备	14
启用 VASA Provider 以配置虚拟数据存储库	16
向 VSC、VASA Provider 和 SRA 虚拟设备注册 OnCommand API 服务	16
启用 Storage Replication Adapter	17
安装 NFS VAAI 插件	18
升级到 VSC、VASA Provider 和 SRA 虚拟设备 9.6 版	19
配置适用于 VMware vSphere 的 Virtual Storage Console 环境	21
配置 ESXi 服务器多路径和超时设置	21
适用于 VMware vSphere 的 VSC 设置的 ESXi 主机值	22
配置子操作系统脚本	24
为 Virtual Storage Console 重新生成 SSL 证书	26
在多 vCenter Server 环境中注册 VSC 的要求	26
配置 VSC 首选项文件	27
设置 IPv4 或 IPv6	27
在不同子网中启用数据存储库挂载	28
访问 VSC、VASA Provider 和 SRA 虚拟设备的维护控制台选项	29
访问 Web 命令行界面并更改管理员密码	31
为 VSC、VASA Provider 和 SRA 虚拟设备配置高可用性	31
VMware vSphere HA	31
VMware vSphere Fault Tolerance	32
VSC、VASA Provider 和 SRA 虚拟设备支持的 MetroCluster 配置	32
配置存储系统环境	34
设置存储系统的默认凭据	34
将存储系统添加到 VSC 中	35
发现存储系统和主机	35
刷新存储系统显示	36
适用于 VMware vSphere 的 VSC 中的 vCenter Server 基于角色的访问控制功能	38
vCenter Server 权限的组成部分	38

有关为 vCenter Server 分配和修改权限的要点	39
VSC、VASA Provider 和 SRA 虚拟设备随附的标准角色	40
VSC 标准角色使用准则	41
VSC 任务所需特权	41
适用于 VMware vSphere 的 VSC 所需的产品级特权	41
ONTAP 适用于 VSC、VASA Provider 和 SRA 虚拟设备的基于角色 的访问控制	42
使用适用于 VMware vSphere 的 VSC 时建议的 ONTAP 角色	43
如何为适用于 VMware vSphere 的 VSC 配置 ONTAP 基于角色的访 问控制	43
配置用于灾难恢复的 Storage Replication Adapter	45
为 SAN 环境配置 Storage Replication Adapter	45
为 NAS 环境配置 Storage Replication Adapter	45
为高度扩展的环境配置 Storage Replication Adapter	46
对 VSC、VASA Provider 和 SRA 虚拟设备问题进行故障排除	47
清理 vSphere 缓存的已下载插件软件包	47
卸载程序不会删除标准 VSC 角色	48
Virtual Storage Console 和 VASA Provider 日志文件	48
VSC 和 VASA Provider 服务在高度扩展的环境中重新启动	49
将 VASA Provider 配置为使用 SSH	49
配置 VSC、VASA Provider 和 SRA 虚拟设备以使用 SSH 进行远程诊断访 问	50
SRA 安装失败并显示脚本错误	50
SRA 在高度扩展的环境中无法以最佳性能运行	51
无法安装 SRA 插件	51
版权	52
商标	53
意见反馈及更新通知	54

VSC、VASA Provider 和 SRA 虚拟设备概述

Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备可为使用 NetApp 存储系统的 VMware 环境中的虚拟机提供端到端生命周期管理。它可使管理员在 vCenter Server 中直接管理存储，从而简化了 VMware 环境中的存储和数据管理工作。

在 vSphere 6.5 中，VMware 引入了一个基于 HTML5 的新客户端，称为 vSphere Client。VSC、VASA Provider 和 SRA 虚拟设备 9.6 版仅支持 vSphere Client。VSC、VASA Provider 和 SRA 虚拟设备可与 vSphere Client 集成，并支持使用单点登录 (Single Sign-On, SSO) 服务。在具有多个 vCenter Server 实例的环境中，您要管理的每个 vCenter Server 实例都必须有各自注册的 VSC 实例。

此虚拟设备中的每个组件都可通过一些功能来帮助您更高效地管理存储。

Virtual Storage Console (VSC)

可通过 VSC 执行以下任务：

- 在 VSC 中添加存储控制器、分配凭据以及为存储控制器设置权限，以供 SRA 和 VASA Provider 使用
- 配置数据存储库
- 监控 vCenter Server 环境中数据存储库和虚拟机的性能
- 通过在以下两个级别使用基于角色的访问控制 (Role-Based Access Control, RBAC) 来控制管理员对 vCenter Server 对象的访问：
 - vSphere 对象，例如虚拟机和数据存储库
这些对象可通过 vCenter Server RBAC 进行管理。
 - ONTAP 存储
存储系统通过 ONTAP RBAC 进行管理。
- 查看和更新连接到 NetApp 存储的 ESXi 主机的主机设置

适用于 VMware VAAI 的 NFS 插件可以为 VSC 配置操作带来显著优势。适用于 VMware vStorage APIs for Array Integration (VAAI) 的 NFS 插件是一个软件库，它可将 ESXi 主机上安装的 VMware 虚拟磁盘库集成在一起。通过 VMware VAAI 软件包，可将某些任务从物理主机中负载分流到存储阵列。您可以在阵列级别执行精简配置和硬件加速等任务以减少 ESXi 主机上的工作负载。副本卸载功能和空间预留功能可提高 VSC 操作的性能。

VSC 不会随附适用于 VAAI 的 NetApp NFS 插件。您可以从 NetApp 支持站点下载插件安装包并获取插件安装说明。

VASA Provider

适用于 ONTAP 的 VASA Provider 可通过 VMware vSphere APIs for Storage Awareness (VASA) 将有关 VMware vSphere 所用存储的信息发送到 vCenter Server。在 VSC、VASA Provider 和 SRA 虚拟设备 9.6 版中，VASA Provider 与 VSC 集成在一起。

可通过 VASA Provider 执行以下任务：

- 配置虚拟卷 (VVol) 数据存储库
- 创建和使用存储功能配置文件，为您的环境定义不同的存储服务级别目标 (Service Level Objective, SLO)

- 验证数据存储库与存储功能配置文件之间的合规性
- 设置警报，以便在卷和聚合接近阈值限制时向您发出警告
- 监控虚拟机磁盘 (Virtual Machine Disk, VMDK) 以及 VVol 数据存储库上创建的虚拟机的性能。

VASA Provider 可使用 VASA API 与 vCenter Server 进行通信，并使用称为 ZAPI 的 NetApp API 与 ONTAP 进行通信。要查看 VASA Provider 信息板，必须事先安装 OnCommand API 服务并将其注册到 vCenter Server。

注：VASA Provider 需要使用专用的 OnCommand API 服务实例。一个 OnCommand API 服务实例不能与多个 VASA Provider 实例共享。

Storage Replication Adapter (SRA)

如果启用了 SRA 并将其与 VMware Site Recovery Manager (SRM) 结合使用，则可以在发生故障时恢复 vCenter Server 数据存储库和虚拟机。您可以通过 SRA 在环境中配置受保护站点和恢复站点，以便在发生故障时进行灾难恢复。

相关信息

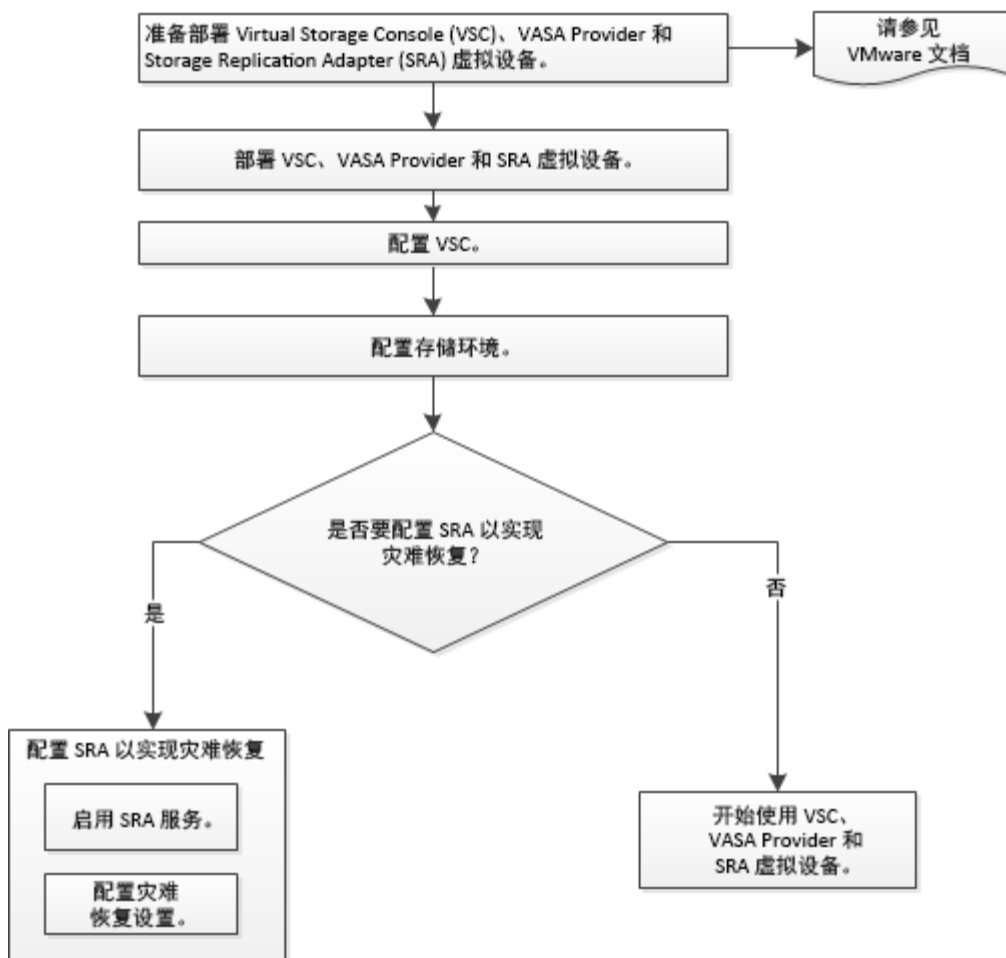
[NetApp 文档：OnCommand API 服务](#)

[NetApp 文档：适用于 VMware VAAI 的 NetApp NFS 插件](#)

[NetApp 支持](#)

适用于新用户的 VSC、VASA Provider 和 SRA 虚拟设备部署 workflow

如果您是 VMware 的新用户且从未使用过 NetApp VSC 产品，则在部署和配置 VSC、VASA Provider 和 SRA 虚拟设备之前，必须配置 vCenter Server 并设置 ESXi 主机。



适用于现有用户的 VSC、VASA Provider 和 SRA 部署 workflow

Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备 7.x 版支持原位升级到最新版本。

早期版本的应用程序（例如 VSC、VASA Provider 和 SRA）分别使用不同的升级过程。如果您的设置中安装了 VSC、VASA Provider 或 SRA，则应执行以下操作：

1. 部署最新版的 VSC、VASA Provider 和 SRA 虚拟设备。
2. 迁移任何现有配置数据。
此配置数据包括存储系统凭据以及 `kaminoprefs.xml` 和 `vscPreferences.xml` 文件中的首选项。

[配置 VSC 首选项文件](#)（第 27 页）

在许多情况下，您可能不需要迁移配置数据。但是，如果您先前自定义了首选项文件，则可能需要查看它们并对新部署的虚拟设备进行类似的更改。可以执行以下操作之一：

- 使用 NetApp 实用程序将存储系统凭据从 VSC 6.X 和 SRA 4.X 迁移到新部署中
- 将存储系统添加到新部署的虚拟设备中，并在添加时指定凭据

如果您要从 VASA Provider 6.X 升级，则应在升级之前取消注册 VASA Provider。有关更多详细信息，请参见当前版本的文档。

如果您还需要从 SRA 4.0 或更早版本升级：

- 如果您使用的是 SRA 4.0，则可以将 SRA 服务器（以虚拟机形式安装的 .ova 文件）原位升级到最新版本。
[升级到 VSC、VASA Provider 和 SRA 虚拟设备 9.6 版](#)（第 19 页）
- 如果您使用的是 SRA 2.1 或 3.0，则应先记下现有站点配置详细信息。
有关详细说明，请参见《适用于 ONTAP 的 Storage Replication Adapter 4.0 安装和设置指南》中的“升级概述”。此外，这些 SRA 版本还会使用 VASA Provider，因此您必须取消注册 VASA Provider，然后部署最新版本的 VSC、VASA Provider 和 SRA 虚拟设备。升级完成后，可以删除先前版本的服务器 (.ova)。

对于任何 SRA 升级，应从 Site Recovery Manager 服务器中删除 SRA 软件（Site Recovery Manager 服务器上使用 .msi 文件安装的适配器）。您可以使用 Windows 系统控制面板卸载此软件，然后在 SRA 服务器上使用 .msi 文件安装最新的 SRA 软件。

如果您已部署 VASA Provider，则在从现有设置升级后，必须使用[编辑设置](#)选项将虚拟设备的内存大小配置为 12 GB。此外，还必须修改预留的虚拟内存大小。要修改此内存大小，必须关闭虚拟机。

如果要部署最新版本的虚拟设备，必须参见“VSC、VASA Provider 和 SRA 虚拟设备的部署要求”主题。“升级到 VSC、VASA Provider 和 SRA 虚拟设备 9.6 版”主题提供了有关如何执行原位升级的信息。

相关概念

[VSC、VASA Provider 和 SRA 虚拟设备的部署要求](#)（第 9 页）

相关任务

[升级到 VSC、VASA Provider 和 SRA 虚拟设备 9.6 版](#)（第 19 页）

相关信息

[NetApp 工具箱：适用于 SnapCenter 和 Virtual Storage Console 的 NetApp 导入实用程序安装和设置 SnapCenter](#)

VSC、VASA Provider 和 SRA 虚拟设备的部署要求

在部署 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备之前，您应了解部署要求，并确定您要执行的任务。您可以根据要执行的任务选择用于部署 VSC、VASA Provider 和 SRA 虚拟设备的部署模式。

VSC 的端口要求

默认情况下，Virtual Storage Console (VSC) 会使用指定的端口使其组件（包括存储系统和 VMware vCenter Server）之间相互通信。如果您启用了防火墙，则必须确保对其进行设置，使其允许例外。

对于非 Windows 防火墙，您必须手动授予对 VSC 所用特定端口的访问权限。如果您不授予对这些端口的访问权限，则会显示错误消息，例如，“Unable to communicate with the server”。

VSC 会使用以下默认双向端口：

默认端口号	说明
9083	启用此端口后，VASA Provider 和 Storage Replication Adapter (SRA) 就会使用此端口与 vCenter Server 通信。获取 TCP/IP 设置时，也需要此端口。
443	根据凭据的配置方式，VMware vCenter Server 和存储系统会侦听此端口上的安全通信。
8143	VSC 会侦听此端口上的安全通信。

VSC、VASA Provider 和 SRA 虚拟设备的空间和规模估算要求

在部署 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备之前，您应事先熟悉部署软件包的空间要求，以及主机系统的一些基本要求。

安装软件包的空间要求

- 2.1 GB（精简配置安装）
- 54.0 GB（厚配置安装）

主机系统容量要求

- ESXi 6.5U2 或更高版本
- 建议的内存：12 GB RAM
- 建议的 CPU 数量：2

VSC、VASA Provider 和 SRA 虚拟设备支持的存储系统、许可和应用程序

在开始部署 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备之前，您应先了解基本存储系统要求、应用程序要求和许可证要求。

互操作性表工具 (IMT) 提供了有关受支持的 ONTAP、vCenter Server、ESXi 主机、插件应用程序和 Site Recovery Manager (SRM) 版本的最新信息。

- [互操作性表工具：VSC 9.6](#)
- [互操作性表工具：VASA Provider 9.6](#)
- [互操作性表工具：SRA 9.6](#)

要对虚拟卷 (VVol) 数据存储库执行虚拟机快照操作和克隆操作，必须启用 FlexClone 许可证。

Storage Replication Adapter (SRA) 需要以下许可证：

- SnapMirror 许可证
要对 SRA 执行故障转移操作，必须启用 SnapMirror 许可证。
- FlexClone 许可证
要对 SRA 执行测试故障转移操作，必须启用 FlexClone 许可证。

要查看数据存储库的 IOPS，您必须启用存储 I/O 控制或取消选中存储 I/O 控制配置中的“禁用存储 I/O 统计信息收集”复选框。只有在从 VMware 获得 Enterprise Plus 许可证后，您才能启用存储 I/O 控制。

- [VMware 知识库文章 1022091：Storage I/O Control 故障排除](#)
- [VMware vSphere 文档：Storage I/O Control 要求](#)

部署 VSC、VASA Provider 和 SRA 虚拟设备时的注意事项和要求

在部署 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备之前，最好对此部署进行规划，并确定希望如何在环境中配置 VSC、VASA Provider 和 SRA。

下表简要介绍了在部署 VSC、VASA Provider 和 SRA 虚拟设备之前应考虑的事项。

注意事项	说明
首次部署 VSC、VASA Provider 和 SRA 虚拟设备	<p>部署 VSC、VASA Provider 和 SRA 虚拟设备时会自动安装 VSC 功能。</p> <p>部署或升级 VSC、VASA Provider 和 SRA（第 13 页）</p> <p>适用于新用户的 VSC、VASA Provider 和 SRA 虚拟设备部署工作流（第 7 页）</p>

注意事项	说明
从现有 VSC 部署升级	<p>从现有 VSC 部署升级到 VSC、VASA Provider 和 SRA 虚拟设备的过程取决于 VSC 的版本以及是否已部署 VASA Provider 和 SRA。有关详细信息，请参见部署工作流程和升级部分。</p> <p>适用于现有用户的 VSC、VASA Provider 和 SRA 部署工作流程（第 7 页）</p> <p>升级前最佳实践：</p> <ul style="list-style-type: none"> 您应记录有关所使用的存储系统及其凭据的信息。 升级完成后，您应确认已自动发现所有存储系统，并且这些存储系统具有正确的凭据。 如果您先前修改了任何标准 VSC 角色，则应复制这些角色以保存所做的更改。 每次重新启动 VSC 服务时，VSC 都会使用当前默认值覆盖这些标准角色。
重新为 VSC 生成 SSL 证书	<p>部署 VSC、VASA Provider 和 SRA 虚拟设备时会自动生成 SSL 证书。要创建站点专用的证书，您可能需要重新生成 SSL 证书。</p> <p>为 Virtual Storage Console 重新生成 SSL 证书（第 26 页）</p>
设置 ESXi 服务器值	<p>虽然默认情况下，大多数 ESXi 服务器值都已设置，但最好检查一下这些值。这些值基于内部测试得出。您可能需要根据具体环境更改某些值以提高性能。</p> <ul style="list-style-type: none"> 配置 ESXi 服务器多路径和超时设置（第 21 页） 适用于 VMware vSphere 的 VSC 设置的 ESXi 主机值（第 22 页）
子操作系统超时值	<p>子操作系统（子 OS）超时脚本用于为受支持的 Linux、Solaris 和 Windows 子操作系统设置 SCSI I/O 超时值，以确保可以正确地进行故障转移。</p>

下表简要介绍了配置 VSC、VASA Provider 和 SRA 虚拟设备时的要求。

注意事项	说明
基于角色的访问控制 (RBAC) 的要求	<p>VSC 既支持 vCenter Server RBAC，又支持 ONTAP RBAC。</p> <p>如果您计划以管理员身份运行 VSC，则必须具有执行所有任务所需的所有权限和特权。</p> <p>如果公司要求您限制对 vSphere 对象的访问，您可以为用户分配标准 VSC 角色，以满足 vCenter Server 的要求。</p> <p>您可以使用适用于 ONTAP 的 RBAC User Creator 工具创建所建议的 ONTAP 角色，此工具可从 NetApp ToolChest 获得。</p> <p>如果用户尝试在没有适当特权和权限的情况下执行某项任务，任务选项会变为灰色。</p> <ul style="list-style-type: none"> VSC、VASA Provider 和 SRA 虚拟设备随附的标准角色（第 40 页） 使用适用于 VMware vSphere 的 VSC 时建议的 ONTAP 角色（第 43 页）
ONTAP 版本	<p>您的存储系统必须运行 ONTAP 9.1、9.3、9.4、9.5 或 9.6 版。</p>

注意事项	说明
存储功能配置文件	<p>要使用存储功能配置文件或设置警报，您必须启用适用于 ONTAP 的 VASA Provider。启用 VASA Provider 后，您可以配置虚拟卷 (Virtual Volume, VVol) 数据存储库，并且可以创建和管理存储功能配置文件以及警报。</p> <p>当卷或聚合容量接近全满或数据存储库不再符合关联存储功能配置文件时，警报功能将向您发出警告。</p>

部署或升级 VSC、VASA Provider 和 SRA

您必须下载并在 VMware vSphere 中部署 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备，然后根据您要使用 VSC、VASA Provider 和 SRA 执行的任务配置所需的应用程序。

相关任务

[启用 VASA Provider 以配置虚拟数据存储库](#)（第 16 页）

下载 VSC、VASA Provider 和 SRA 虚拟设备

您可以从 NetApp 支持站点下载适用于 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备的 .ova 文件。

关于本任务

.ova 文件包含 VSC、VASA Provider 和 SRA。部署完成后，全部这三个产品即会安装在您的环境中。默认情况下，在您确定后续部署模式并根据自己的需要选择是否启用 VASA Provider 和 SRA 后，VSC 便开始工作。

您可以根据自己的需要使用 NetApp 支持站点中的以下任一软件下载页面下载 VSC、VASA Provider 和 SRA 虚拟设备：

- Virtual Storage Console
- NetApp VASA Provider
- Storage Replication Adapter

如果要在 VSC、VASA Provider 和 SRA 虚拟设备部署中启用 SRA，则必须事先在 Site Recovery Manager (SRM) 服务器上安装 SRA 插件。您可以从 Software Downloads 部分中的“Storage Replication Adapter for ONTAP”菜单下载 SRA 适配器插件的安装文件。

步骤

1. 登录到 NetApp 支持站点，然后单击“Downloads”选项卡
2. 在“Downloads”页面中，选择“Software”。
3. 从产品列表中，根据您的需要选择“Virtual Storage Console”、“NetApp VASA Provider”或“Storage Replication Adapter”。
4. 选择要下载的适当软件版本，然后单击“View & Download”。
5. 按照产品说明页面上的说明进行操作，直到显示下载页面为止。
6. 将 .ova 文件下载到 vSphere Client 系统并从此系统部署 OVF 模板。

部署 VSC、VASA Provider 和 SRA 虚拟设备

您应在环境中部署 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备，并指定必要的参数以使用此设备。

开始之前

- 您必须运行受支持的 vCenter Server 版本。
注：VSC、VASA Provider 和 SRA 虚拟设备可以部署在 Windows vCenter Server 部署或 VMware vCenter Server Virtual Appliance (vCSA) 部署中。

[互操作性表工具：VSC 9.6](#)

- 必须已经配置和设置 vCenter Server 环境。
- 必须已经为您的设置 虚拟机 ESXi 主机。
- 必须已经下载 .ova 文件。
- 必须拥有 vCenter Server 实例的管理员登录凭据。
- 必须已注销并关闭 vSphere Client 的所有浏览器会话，并删除浏览器缓存以避免在部署 VSC、VASA Provider 和 SRA 虚拟设备过程中出现任何浏览器缓存问题。

[清理 vSphere 缓存的已下载插件软件包](#)（第 47 页）

- 必须已启用 ICMP。
如果 ICMP 处于禁用状态，则 VSC、VASA Provider 和 SRA 虚拟设备的初始配置将失败，并且在部署后 VSC 将无法启动 VSC 和 VASA Provider 服务。部署后，必须手动启用 VSC 和 VASA Provider 服务。

关于本任务

如果您正在部署全新安装的 VSC、VASA Provider 和 SRA 虚拟设备，则 VASA Provider 会默认处于启用状态。但是，如果从早期版本的虚拟设备升级，则 VASA Provider 的状态会予以保留，您可能需要手动启用 VASA Provider。

[启用 VASA Provider 以配置虚拟数据存储库](#)（第 16 页）

步骤

1. 登录到 vSphere Client。
2. 选择“主页”>“主机和群集”。
3. 右键单击所需的数据中心，然后单击“部署 OVA 模板”。
4. 选择适当方法以提供 VSC、VASA Provider 和 SRA 的部署文件，然后单击“下一步”。

位置	操作
URL	提供 VSC、VASA Provider 和 SRA 虚拟设备的 .ova 文件的 URL。
文件夹	从保存位置选择 VSC、VASA Provider 和 SRA 虚拟设备的 .ova 文件。

5. 输入以下详细信息以自定义部署向导：
 - 部署名称
 - 要应用权限的目标数据中心

- 要部署 VSC、VASA Provider 和 SRA 虚拟设备的主机
- 虚拟磁盘格式、虚拟机存储策略、存储位置和网络
- 管理员用户名和密码

注：

- 您可以在部署 VSC、VASA Provider 和 SRA 虚拟设备时设置 vCenter Server 的管理员凭据。
如果 vCenter Server 的密码发生变化，则可通过以下 URL 更新管理员的密码：
`https://<IP>:8143/Register.html`，其中 IP 地址是您在部署期间提供的 VSC、VASA Provider 和 SRA 虚拟设备 IP 地址。
- 管理员密码不得使用任何空格。
- 您必须使用“maint”用户名来访问维护控制台。
默认情况下，密码设置为“admin123”。
- 如果您未使用 DHCP，请为此虚拟设备指定有效的 DNS 主机名（非限定）和静态 IP 地址以及其他网络参数。要确保正确安装和操作，必须提供所有这些参数。

- 要将 VSC、VASA Provider 和 SRA 虚拟设备注册到的 vCenter Server 实例的 IP 地址（IPv4 或 IPv6）。

生成的 VSC 和 VASA 证书类型取决于您在部署期间提供的 IP 地址（IPv4 或 IPv6）。在部署 VSC、VASA Provider 和 SRA 虚拟设备时，如果未输入任何静态 IP 详细信息，并且 DHCP 网络既提供了 IPv4 地址，又提供了 IPv6 地址：

- 用于注册到 vCenter Server 的 VSC、VASA Provider 和 SRA 虚拟设备 IP 地址取决于在 OVA 部署向导中输入的 vCenter Server IP 地址类型（IPv4 或 IPv6）。
- VSC 和 VASA 证书都会使用注册 vCenter Server 期间所用的相同 IP 地址类型来生成。
- 您可以使用 VSC、VASA Provider 和 SRA 虚拟设备维护控制台中的“应用程序配置”菜单来更改密码。

[访问 VSC、VASA Provider 和 SRA 虚拟设备的维护控制台选项](#)（第 29 页）

重要：只有 vCenter Server 6.7 及更高版本才支持 IPv6。

6. 查看配置数据，然后单击“下一步”完成部署。
在等待部署完成过程中，您可以从“任务”选项卡查看部署进度。
7. 启动虚拟设备虚拟机，然后打开运行此虚拟设备的虚拟机的控制台。
8. 当设备控制台上出现提示时，返回 vCenter Server。
9. 在此设备虚拟机的“摘要”选项卡中，选择“安装/升级 VMware Tools”，然后单击“挂载”。
此时将自动安装 VMware Tools。安装完成后，按照设备控制台中的说明断开 Tools ISO 的连接。
10. 如果 VSC、VASA Provider 和 SRA 虚拟设备未注册到任何 vCenter Server 中，请使用 `https://appliance_ip:8143/Register.html` 注册 VSC 实例。
11. 注销并重新登录到 vSphere Client 以查看已部署的 VSC、VASA Provider 和 SRA 虚拟设备。
 - a. 从现有 vSphere Client 注销并关闭窗口。

- b. 登录到 vSphere Client。

在 vSphere Client 中更新此插件可能需要几分钟的时间。

故障排除：如果在登录后仍无法查看此插件，则必须清理 vSphere Client 缓存。

[清理 vSphere 缓存的已下载插件软件包](#)（第 47 页）

完成之后

注：要查看适用于 ONTAP 的 VASA Provider 信息板，必须下载并安装 OnCommand API 服务。

[向 VSC、VASA Provider 和 SRA 虚拟设备注册 OnCommand API 服务](#)（第 16 页）

启用 VASA Provider 以配置虚拟数据存储库

Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备会默认启用 VASA Provider 功能。您可以通过为每个 VVol 数据存储库配置所需的存储功能配置文件来配置 VVol 数据存储库。

开始之前

- 您必须已设置 vCenter Server 实例并配置 ESXi。
- 您必须已部署 VSC、VASA Provider 和 SRA 虚拟设备。

关于本任务

如果在升级到 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备 9.6 版之前禁用了 VASA Provider 功能，则在升级后，VASA Provider 功能仍会处于禁用状态。

步骤

1. 登录到 VMware vSphere 的 Web 用户界面。
2. 在 vSphere Client 中，单击“菜单”>“Virtual Storage Console”。
3. 单击“设置”。
4. 单击“管理设置”选项卡中的“管理功能”。
5. 在“管理功能”对话框中，选择要启用的 VASA Provider 扩展。
6. 输入 VSC、VASA Provider 和 SRA 虚拟设备的 IP 地址以及管理员密码，然后单击“应用”。

向 VSC、VASA Provider 和 SRA 虚拟设备注册 OnCommand API 服务

只有在为 VASA Provider 注册 OnCommand API 服务后，VVol 信息板才能显示虚拟卷 (VVol) 数据存储库和虚拟机的详细信息。另外，要为 VVol 虚拟机和数据存储库报告获取数据，也需要使用 OnCommand API 服务。

开始之前

您必须已从 NetApp 支持站点下载 OnCommand API 服务 2.1 或更高版本。

注：只有在使用 ONTAP 9.3 或更高版本配置了 VVol 数据存储库和虚拟机的情况下，VVol 信息板才会显示相关性能指标。

步骤

1. 在 Virtual Storage Console (VSC) 的“主页”页面中，单击“设置”。
2. 单击“管理设置”选项卡中的“管理扩展”。
3. 使用“注册 OnCommand API 服务”滑块启用 OnCommand API 服务。
4. 输入 OnCommand API 服务的 IP 地址、服务端口和凭据。

此外，您还可以使用管理 VASA Provider 扩展对话框进行以下修改：

- 在对凭据进行任何更改后更新 OnCommand API 服务注册。
- 不再需要 VASA Provider 信息板时取消注册 OnCommand API 服务。
要删除 VASA Provider 的 OnCommand API 服务注册，您必须清除“注册 OnCommand API 服务”复选框。

5. 单击“应用”。

只有在完成 OnCommand API 服务的注册后，VVol 信息板才会显示相关指标。

相关信息

[NetApp 支持](#)

启用 Storage Replication Adapter

在 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备中，可以选择在 VSC 中使用 SRA 功能来配置灾难恢复。

开始之前

- 您必须已设置 vCenter Server 实例并配置 ESXi。
- 只有在需要配置 Site Recovery Manager (SRM) 灾难恢复解决方案时，才需要为 SRA 插件下载 .msi 文件。
- 您必须已部署 VSC、VASA Provider 和 SRA 虚拟设备。

关于本任务

您可以灵活地启用 VASA Provider 和 SRA 功能，从而仅执行您的企业所需的工作流。

步骤

1. 登录到 VMware vSphere 的 Web 用户界面。
2. 在 vSphere Client 中，单击“菜单”>“Virtual Storage Console”。
3. 单击“设置”。
4. 单击“管理设置”选项卡中的“管理功能”。
5. 在“管理功能”对话框中，选择要启用的 SRA 扩展。
6. 输入 VSC、VASA Provider 和 SRA 虚拟设备的 IP 地址以及管理员密码，然后单击“应用”。
7. 在 Windows SRM 服务器上，双击已下载的 SRA 插件 .msi 安装程序，并按照屏幕上的说明进行操作。

8. 要在 SRM 服务器上完成 SRA 插件的安装，请输入已部署的虚拟设备的 IP 地址和密码。
您必须注销 vSphere Web Client 并重新登录，以验证是否可配置选定扩展。

相关概念

[配置用于灾难恢复的 Storage Replication Adapter](#)（第 45 页）

安装 NFS VAAI 插件

您可以使用 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备的图形用户界面安装适用于 VMware vStorage APIs for Array Integration (VAAI) 的 NetApp NFS 插件。

开始之前

- 您必须已从 NetApp 支持站点下载适用于 VAAI 的 NFS 插件的安装包 (.vib)。
[NetApp 支持](#)
- 您必须已安装 ESXi 主机 6.5 或更高版本以及 ONTAP 9.1 或更高版本。
- 您必须已启动 ESXi 主机并已挂载 NFS 数据存储库。
- 您必须已将 `DataMover.HardwareAcceleratedMove`、`DataMover.HardwareAcceleratedInit` 和 `VMFS3.HardwareAcceleratedLocking` 主机设置的值设置为“1”。
这些值可通过 VSC 主机设置进行设置。
- 您必须已使用 `vserver nfs modify -vserver vserver_name -vstorage enabled` 命令在 Storage Virtual Machine (SVM) 上启用 vstorage 选项。

步骤

1. 将从 NetApp 支持站点下载的 .vib 文件重命名为 `NetAppNasPlugin.vib`，以便与 VSC 使用的预定义名称匹配。
2. 单击 VSC 的“主页”页面中的“设置”。
3. 单击“NFS VAAI 工具”选项卡。
4. 单击“现有版本”部分中的“更改”。
5. 浏览并选择已重命名的 .vib 文件，然后单击“上传”将此文件上传到虚拟设备。
6. 在“安装在 ESXi 主机上”部分中，选择要安装 NFS VAAI 插件的 ESXi 主机，然后单击“安装”。

您应按照屏幕上的说明完成安装。您可以在 vSphere Web Client 的“任务”部分监控安装进度。

7. 安装完成后，请重新启动 ESXi 主机。

重新启动 ESXi 主机时，VSC 会自动检测 NFS VAAI 插件。启用此插件不需要执行任何其他步骤。

升级到 VSC、VASA Provider 和 SRA 虚拟设备 9.6 版

您可以按照此处提供的说明从现有设置原位升级到 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备 9.6 版。

开始之前


- 您必须已下载 VSC、VASA Provider 和 SRA 虚拟设备 9.6 版的 .iso 文件。
- 要使 VSC、VASA Provider 和 SRA 虚拟设备在升级后以最佳状态运行，您必须至少预留 12 GB RAM。
- 您必须清理 vSphere Client 浏览器缓存。
清理 vSphere 缓存的已下载插件软件包（第 47 页）

关于本任务

现有部署中的 VASA Provider 状态将在升级后保留下来。升级后，您应根据需要手动启用或禁用 VASA Provider。但是，即使未使用 VVol，NetApp 也建议启用 VASA Provider，因为它可使用存储功能配置文件配置传统数据存储库，并支持存储警报。

注：您只能从现有的 VSC、VASA Provider 和 SRA 虚拟设备 7.x 版原位升级到虚拟设备 9.6 版。

步骤

1. 将下载的 .iso 文件挂载到虚拟设备：
 - a. 单击“编辑设置”>“DVD/CD-ROM 驱动器”。
 - b. 从下拉列表中选择“数据存储 ISO 文件”文件。
 - c. 浏览并选择已下载的 .iso 文件，然后选中“打开电源时连接”复选框。
2. 访问已部署虚拟设备的“摘要”选项卡。
3. 单击  以启动维护控制台。
4. 在“Main Menu”提示符处，输入选项 2（表示“System Configuration”），然后输入选项 8（表示“Upgrade”）。
升级完成后，此虚拟设备将重新启动。VSC、VASA Provider 和 SRA 虚拟设备将使用与升级前相同的 IP 地址注册到 vCenter Server。
5. 如果您希望 VSC、VASA Provider 和 SRA 虚拟设备使用 IPv6 地址注册到 vCenter Server，必须执行以下操作：
 - a. 取消注册 VSC、VASA Provider 和 SRA 虚拟设备。
 - b. 使用“注册”页面将 VSC、VASA Provider 和 SRA 虚拟设备的 IPv6 地址注册到 vCenter Server。
 - c. 完成注册后，重新生成 VSC 和 VASA Provider 证书。

重要：只有 vCenter Server 6.7 及更高版本才支持 IPv6。
6. 注销并重新登录到 vSphere Client 以查看已部署的 VSC、VASA Provider 和 SRA 虚拟设备。

- a. 从现有 vSphere Web Client 或 vSphere Client 注销，然后关闭窗口。
- b. 登录到 vSphere Client。

在 vSphere Client 中更新此插件可能需要几分钟的时间。

相关任务

[启用 VASA Provider 以配置虚拟数据存储库](#)（第 16 页）

配置适用于 VMware vSphere 的 Virtual Storage Console 环境

Virtual Storage Console (VSC) 支持多种环境。这些环境中的某些功能可能需要额外配置。

您可能需要执行以下某些任务来配置 ESXi 主机、子操作系统和 VSC：

- 验证 ESXi 主机设置（包括 UNMAP 设置）
- 为子操作系统添加超时值
- 重新生成 VSC SSL 证书
- 创建存储功能配置文件和阈值警报
- 修改首选项文件，以便能够跨不同子网挂载数据存储库

配置 ESXi 服务器多路径和超时设置

适用于 VMware vSphere 的 Virtual Storage Console 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。

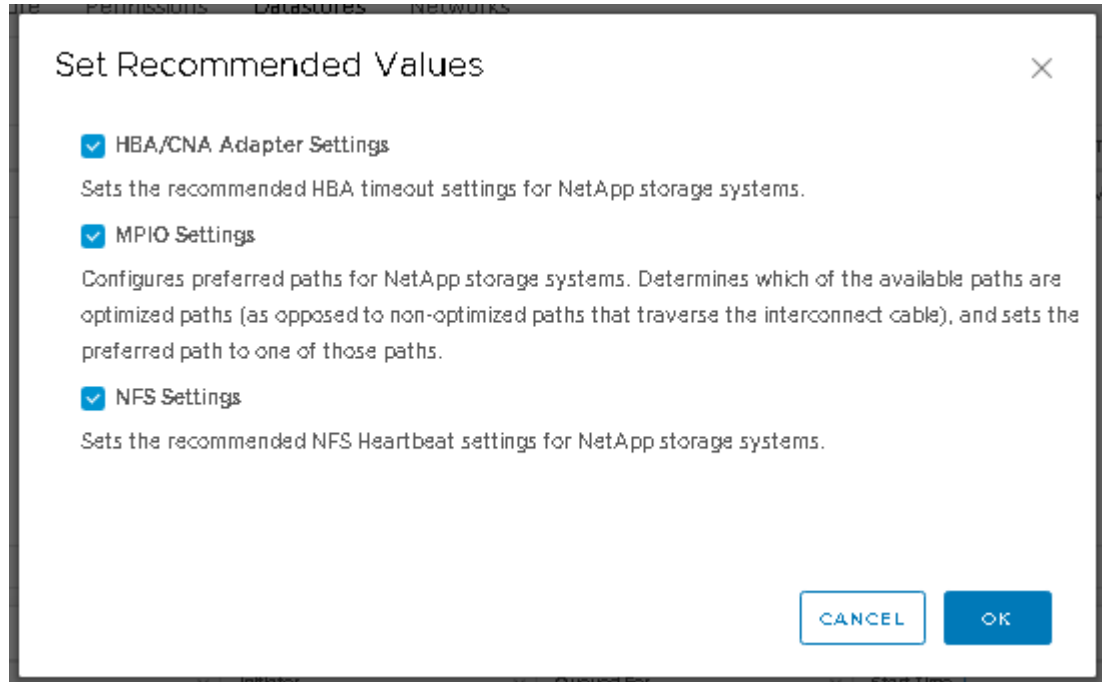
关于本任务

此过程可能需要很长时间，具体取决于您的配置和系统负载。近期任务面板会显示任务进度。任务完成后，主机状态“警报”图标将替换为“正常”图标或“等待重新启动”图标。

步骤

1. 从 VMware vSphere Web Client “主页”中，单击“vCenter”>“主机”。
2. 右键单击一个主机并选择“操作”>“NetApp VSC”>“设置建议值”。
3. 在“NetApp 建议设置”对话框中，选择最适合您系统的值。

默认情况下会设置标准的建议值。



4. 单击“确定”。

适用于 VMware vSphere 的 VSC 设置的 ESXi 主机值

适用于 VMware vSphere 的 Virtual Storage Console 将设置 ESXi 主机超时值和其他值，以确保性能最佳并成功完成故障转移。Virtual Storage Console (VSC) 设置的值基于 NetApp 内部测试。

VSC 可在 ESXi 主机上设置以下值：

ESXi 高级配置

VMFS3.HardwareAcceleratedLocking

应将此值设置为 1。

VMFS3.EnableBlockDelete

应将此值设置为 0。

NFS 设置

Net.TcpipHeapSize

应将此值设置为 32。

对于所有其他 NFS 配置，应将此值设置为 30。

Net.TcpipHeapMax

如果使用的是 vSphere 6.0 或更高版本，应将此值设置为 1536。

如果使用的是 vSphere 5.5，应将此值设置为 512。

如果使用的是 vSphere 5.0 或 5.1，应将此值设置为 128。

如果使用的是 vSphere 5.0 或更早版本，应将此值设置为 120。

NFS.MaxVolumes

如果使用的是 vSphere 5.0 或更高版本，应将此值设置为 256。

对于所有其他 NFS 配置，应将此值设置为 64。

NFS41.MaxVolumes

如果使用的是 vSphere 6.0 或更高版本，应将此值设置为 256。

NFS.MaxQueueDepth

如果在 ESXi 主机上使用的是 vSphere 6.0 或更高版本，应将此值设置为 128 或以上，以避免出现队列瓶颈。

对于 vSphere 6.0 之前的版本，应将此值设置为 64。

NFS.HeartbeatMaxFailures

对于所有 NFS 配置，应将此值设置为 10。

NFS.HeartbeatFrequency

对于所有 NFS 配置，应将此值设置为 12。

NFS.HeartbeatTimeout

对于所有 NFS 配置，应将此值设置为 5。

FC/FCoE 设置**路径选择策略**

如果使用采用 ALUA 的 FC 路径，应将此值设置为“RR”。

对于所有其他配置，应将此值设置为“FIXED”。

将此值设置为“RR”有助于在所有主动/优化路径之间实现负载平衡。值“FIXED”适用于较早的非 ALUA 配置，可防止出现代理 I/O。也就是说，在使用 7-模式 Data ONTAP 的环境中，它有助于防止 I/O 流向高可用性 (HA) 对中的另一节点。

Disk.QFullSampleSize

对于所有配置，应将此值设置为 32。设置此值有助于防止出现 I/O 错误。

Disk.QFullThreshold

对于所有配置，应将此值设置为 8。设置此值有助于防止出现 I/O 错误。

Emulex FC HBA 超时

使用默认值。

QLogic FC HBA 超时

使用默认值。

iSCSI 设置**路径选择策略**

对于所有 iSCSI 路径，应将此值设置为“RR”。

将此值设置为“RR”有助于在所有主动/优化路径之间实现负载平衡。

Disk.QFullSampleSize

对于所有配置，应将此值设置为 32。设置此值有助于防止出现 I/O 错误。

Disk.QFullThreshold

对于所有配置，应将此值设置为 8。设置此值有助于防止出现 I/O 错误。

配置子操作系统脚本

子操作系统 (OS) 脚本的 ISO 映像会挂载在适用于 VMware vSphere 的 Virtual Storage Console Virtual Storage Console 服务器上。要使用子操作系统脚本为虚拟机设置存储超时，必须从 vSphere Client 挂载此脚本。

表 1: 子操作系统的 ISO 位置

操作系统类型	60 秒超时设置	190 秒超时设置
Linux	https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout-install.iso	https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout_190-install.iso
Windows	https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout.iso	https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout_190.iso
Solaris	https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout-install.iso	https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout_190-install.iso

您应从一个 VSC 实例副本安装此脚本，此实例副本必须已注册到用于管理虚拟机的 vCenter Server 中。如果您的环境包含多个 vCenter Server，则应选择要设置存储超时值的虚拟机所在的服务器。

您应登录到此虚拟机，然后运行此脚本以设置存储超时值。

为 Windows 子操作系统设置超时值

此子操作系统 (GOS) 超时脚本用于为 Windows 子操作系统设置 SCSI I/O 超时设置。您可以指定 60 秒超时或 190 秒超时。您必须重新启动 Windows 子操作系统，这些设置才能生效。

开始之前

您必须已挂载包含 Windows 脚本的 ISO 映像。

步骤

1. 访问 Windows 虚拟机的控制台，并登录到具有管理员权限的帐户。
2. 如果此脚本没有自动启动，请打开 CD 驱动器，然后运行 windows_gos_timeout.reg 脚本。
此时将显示“注册表编辑器”对话框。
3. 单击“是”继续。
此时将显示以下消息：“D:\windows_gos_timeout.reg 中包含的项和值已成功添加到注册表中。”
4. 重新启动 Windows 子操作系统。
5. 卸载 ISO 映像。

为 Solaris 子操作系统设置超时值

此子操作系统 (GOS) 超时脚本用于为 Solaris 10 设置 SCSI I/O 超时设置。您可以指定 60 秒超时或 190 秒超时。

开始之前

您必须已挂载包含 Solaris 脚本的 ISO 映像。

步骤

1. 访问 Solaris 虚拟机的控制台，并登录到具有 root 权限的帐户。
2. 运行 `solaris_gos_timeout-install.sh` 脚本。

对于 Solaris 10，将显示类似如下内容的消息：

```
Setting I/O Timeout for /dev/s-a - SUCCESS!
```

3. 卸载 ISO 映像。

为 Linux 子操作系统设置超时值

此子操作系统 (GOS) 超时脚本用于为 Red Hat Enterprise Linux 4、5、6 和 7 以及 SUSE Linux Enterprise Server 9、10 和 11 设置 SCSI I/O 超时设置。您可以指定 60 秒超时或 190 秒超时。每当升级到新版 Linux 时，您都必须运行此脚本。

开始之前

您必须已挂载包含 Linux 脚本的 ISO 映像。

步骤

1. 访问 Linux 虚拟机的控制台，并登录到具有 root 权限的帐户。
2. 运行 `linux_gos_timeout-install.sh` 脚本。

对于 Red Hat Enterprise Linux 4 或 SUSE Linux Enterprise Server 9，将显示类似以下内容的消息：

```
Restarting udev... this may take a few seconds.
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

对于 Red Hat Enterprise Linux 5、Red Hat Enterprise Linux 6 和 Red Hat Enterprise Linux 7，将显示类似以下内容的消息：

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
Restarting udev... this may take a few seconds.
```

```
Starting udev: [ OK ]
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

对于 SUSE Linux Enterprise Server 10 或 SUSE Linux Enterprise Server 11，将显示类似以下内容的消息：

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev: done
```

3. 卸载 ISO 映像。

为 Virtual Storage Console 重新生成 SSL 证书

安装 Virtual Storage Console (VSC) 时会生成 SSL 证书。为 SSL 证书生成的可分辨名称 (Distinguished Name, DN) 可能不是客户端计算机可识别的公用名 (Common Name, CN)。您可以通过更改密钥库和专用密钥密码来重新生成证书，并创建站点专用的证书。

关于本任务

您可以使用维护控制台启用远程诊断并生成站点专用的证书。

[NetApp 知识库解答 1075654: Virtual Storage Console 7.x: Implementing CA signed certificates](#)

步骤

1. 登录到维护控制台。
2. 输入 **1** 以访问 Application Configuration 菜单。
3. 在 Application Configuration 菜单中，输入 **3** 以停止 VSC 服务。
4. 输入 **7** 以重新生成 SSL 证书。

在多 vCenter Server 环境中注册 VSC 的要求

如果在您的环境中，一个 VMware vSphere Web Client 管理着多个 vCenter Server 实例，而您要在此环境中使用适用于 VMware vSphere 的 Virtual Storage Console，则必须向每个 vCenter Server 注册一个 VSC 实例，以使 VSC 与 vCenter Server 呈现 1:1 配对关系。这样，您就可以通过一个 vSphere Web Client 在链接模式和非链接模式下管理运行 vCenter 6.0 或更高版本的所有服务器了。

注：如果您要将 VSC 与 vCenter Server 结合使用，则必须为您要管理的每个 vCenter Server 实例设置或注册一个 VSC 实例。每个已注册 VSC 实例的版本都必须相同。

在 vCenter Server 部署期间，系统会自动安装链接模式。链接模式会使用 Microsoft Active Directory Application Mode (ADAM) 跨多个 vCenter Server 系统存储和同步数据。

使用 vSphere Web Client 跨多个 vCenter Server 执行 VSC 任务需要满足以下要求：

- VMware 清单中要管理的每个 vCenter Server 都必须注册一个 VSC 服务器，并使两者保持 1:1 的配对关系。

例如，可以将 VSC 服务器 A 注册到 vCenter Server A，将 VSC 服务器 B 注册到 vCenter Server B，将 VSC 服务器 C 注册到 vCenter Server C，依此类推。

您**不能**将 VSC 服务器 A 同时注册到 vCenter Server A 和 vCenter Server B。

此外，如果 VMware 清单中的某个 vCenter Server 未注册 VSC 服务器，则即使 VMware 清单中有一个或多个 vCenter Server 注册了 VSC，您也无法看到任何 VSC 实例。

- 对于已向单点登录 (SSO) 注册的每个 vCenter Server，您必须拥有 VSC 专用的查看特权。此外，还必须拥有正确的 RBAC 权限。

在执行需要指定 vCenter Server 的任务时，“vCenter Server”下拉框会按字母顺序显示可用的 vCenter Server。此下拉列表中的第一个服务器始终为默认的 vCenter Server。

如果存储位置已知（例如使用配置向导且数据存储库位于由特定 vCenter Server 管理的主机上时），则 vCenter Server 列表会显示为一个只读选项。只有在使用右键单击选项选择 vSphere Web Client 中的某一项时，才会发生这种情况。

如果尝试选择不受 VSC 管理的对象，则 VSC 会向您发出警告。

您可以根据 VSC 摘要页面上的特定 vCenter Server 筛选存储系统。对于向 vCenter Server 注册的每个 VSC 实例，都会显示一个摘要页面。您可以管理与特定 VSC 实例和 vCenter Server 相关的存储系统，但是，如果您正在运行多个 VSC 实例，则每个存储系统的注册信息应该分开。

配置 VSC 首选项文件

首选项文件包含用于控制适用于 VMware vSphere 的 Virtual Storage Console 操作的设置。在大多数情况下，您无需修改这些文件中的设置。了解 Virtual Storage Console (VSC) 使用哪些首选项文件很有用。

VSC 具有若干个首选项文件。这些文件包含一些输入项和值，用于确定 VSC 执行各种操作的方式。以下是 VSC 使用的一些首选项文件：

```
/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml
```

```
/opt/netapp/vscserver/etc/vsc/vscPreferences.xml
```

在某些情况下，您可能需要修改这些首选项文件。例如，如果您使用 iSCSI 或 NFS，并且 ESXi 主机和存储系统的子网不同，则必须修改这些首选项文件。如果您不修改首选项文件中的设置，则数据存储库配置操作就会因 VSC 无法挂载数据存储库而失败。

设置 IPv4 或 IPv6

首选项文件 `kaminoprefs.xml` 中添加了一个新选项，您可以通过设置此选项来为添加到 VSC 中的所有存储系统启用 IPv4 或 IPv6 支持。

- `kaminoprefs.xml` 首选项文件添加了 `default.override.option.provision.mount.datastore.address.family` 参数，用于为数据存储库配置设置首选数据 LIF 协议。
此首选项适用于添加到 VSC 中的所有存储系统。
- 此新选项的值为 IPv4、IPv6 和 NONE。
- 默认情况下，此值设置为 NONE。

值	说明
NONE	<ul style="list-style-type: none"> 使用与用于添加存储的集群或 SVM 管理 LIF 的类型相同的 IPv6 或 IPv4 地址类型数据 LIF 进行配置。 如果此 SVM 没有相同 IPv6 或 IPv4 地址类型的数据 LIF，则会通过其他类型的数据 LIF（如果有）进行配置。
IPv4	<ul style="list-style-type: none"> 使用选定 SVM 中的 IPv4 数据 LIF 进行配置。 如果此 SVM 没有 IPv4 数据 LIF，则会通过 IPv6 数据 LIF（如果此 SVM 中存在）进行配置。
IPv6	<ul style="list-style-type: none"> 使用选定 SVM 中的 IPv6 数据 LIF 进行配置。 如果此 SVM 没有 IPv6 数据 LIF，则会通过 IPv4 数据 LIF（如果此 SVM 中存在）进行配置。

在不同子网中启用数据存储库挂载

如果您使用 iSCSI 或 NFS，并且 ESXi 主机和存储系统的子网不同，则必须修改适用于 VMware vSphere 的 Virtual Storage Console 首选项文件。如果您不修改这些首选项文件，则数据存储库配置会失败，因为 Virtual Storage Console VSC 无法挂载此数据存储库。

关于本任务

如果数据存储库配置失败，则 VSC 会记录以下错误消息：

```
"Unable to continue. No ip addresses found when cross-referencing kernel ip addresses and addresses on the controller."
```

```
"Unable to find a matching network to NFS mount volume to these hosts."
```

步骤

1. 登录到 vCenter Server 实例。
2. 使用统一设备虚拟机启动维护控制台。
访问 [VSC、VASA Provider 和 SRA 虚拟设备的维护控制台选项](#)（第 29 页）
3. 输入 4 以访问“Support and Diagnostics”选项。
4. 输入 2 以访问“Access Diagnostic Shell”选项。
5. 输入 `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` 以更新 kaminoprefs.xml 文件。
6. 更新 kaminoprefs.xml 文件。

使用的协议	操作
iSCSI	将输入项 <code>default.allow.iscsi.mount.networks</code> 的值从 ALL 更改为您的 ESXi 主机网络值。
NFS	将输入项 <code>default.allow.nfs.mount.networks</code> 的值从 ALL 更改为您的 ESXi 主机网络值。

这些首选项文件包含这些输入项的示例值。

注：“ALL”值并不表示所有网络。“ALL”值用于使用主机和存储系统之间的所有匹配网络来挂载数据存储库。如果您指定了主机网络，则只能跨指定子网进行挂载。

7. 保存并关闭 `kaminoprefs.xml` 文件。

访问 VSC、VASA Provider 和 SRA 虚拟设备的维护控制台选项

您可以通过 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备的维护控制台管理您的应用程序、系统和网络配置。您可以更改管理员密码和维护密码。此外，还可以生成支持包、设置不同的日志级别、查看和管理 TLS 配置以及启动远程诊断。

开始之前


部署 VSC、VASA Provider 和 SRA 虚拟设备后，必须已安装 VMware Tools。

关于本任务

- 必须分别使用“maint”和“admin123”作为用户名和密码登录到 VSC、VASA Provider 和 SRA 虚拟设备的维护控制台。
- 在启用远程诊断时，必须为“diag”用户设置密码。

步骤

1. 访问已部署虚拟设备的“Summary”选项卡。

2. 单击  以启动维护控制台。

可以访问以下维护控制台选项：

应用程序配置

可用选项如下：

- 显示服务器状态摘要
- 启动 Virtual Storage Console 服务
- 停止 Virtual Storage Console 服务
- 启动 VASA Provider 和 SRA 服务
- 停止 VASA Provider 和 SRA 服务
- 更改“administrator”用户密码
- 重新生成证书
- 硬重置密钥库和证书
- 硬重置数据库

- 更改 Virtual Storage Console 的日志级别
- 更改 VASA Provider 和 SRA 服务的日志级别
- 显示 TLS 配置
- 启用 TLS 协议
- 禁用 TLS 协议

系统配置

可用选项如下：

- 重新启动虚拟机
- 关闭虚拟机
- 更改 “maint” 用户密码
- 更改时区
- 更改 NTP 服务器
您可以为 NTP 服务器提供 IPv6 地址。
- 启用/禁用 SSH 访问
- 增加 jail 磁盘大小 (/jail)
- 升级
- 安装 VMware Tools

网络配置

可用选项如下：

- 显示 IP 地址设置
- 更改 IP 地址设置
您可以使用此选项将部署后的 IP 地址更改为 IPv6。
- 显示域名搜索设置
- 更改域名搜索设置
- 显示静态路由
- 更改静态路由
您可以使用此选项添加 IPv6 路由。
- 提交更改
- 对主机进行 Ping 操作
您可以使用此选项对 IPv6 主机进行 Ping 操作。
- 还原默认设置

支持和诊断

可用选项如下：

- 生成支持包
- 访问诊断 Shell

- 启用远程诊断访问

相关概念

[Virtual Storage Console 和 VASA Provider 日志文件](#)（第 48 页）

访问 Web 命令行界面并更改管理员密码

您可以在部署后访问 VSC、VASA Provider 和 SRA 虚拟设备的 Web 命令行界面并更改管理员密码。

步骤

1. 使用 `https://<IP>:9083` 访问 Web 命令行界面 (CLI)。此 IP 地址是您在部署期间为 VSC、VASA Provider 和 SRA 虚拟设备提供的 IP 地址。
2. 使用您在部署期间提供的管理员用户名和密码登录到此 Web 命令行界面。
3. 创建一个介于 8 到 63 个字符之间的密码。

为 VSC、VASA Provider 和 SRA 虚拟设备配置高可用性

Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备支持高可用性 (HA) 配置，用于实现 VSC、VASA Provider 和 SRA 的无中断运行。

VSC、VASA Provider 和 SRA 虚拟设备可利用 VMware vSphere 高可用性 (HA) 功能以及 vSphere Fault Tolerance (FT) 功能来提供高可用性。通过高可用性 (HA) 解决方案，您可以从由于以下原因而导致的中断中快速恢复：

- 主机故障
- 网络故障
- 虚拟机故障（客户机操作系统故障）
- 应用程序 (VSC、VASA Provider 和 SRA) 崩溃

要提供高可用性，不需要对此虚拟设备执行任何其他配置。只需根据 vCenter Server 和 ESXi 主机的要求，为其配置 VMware vSphere HA 功能或 vSphere FT 功能即可。HA 和 FT 都需要使用集群模式主机和共享存储。此外，FT 还具有其他要求和限制。

除了 VMware vSphere HA 解决方案和 vSphere FT 解决方案之外，此虚拟设备还有助于保持 VSC、VASA Provider 和 SRA 服务不间断运行。虚拟设备 watchdog 进程会定期监控所有这三项服务，并在检测到任何类型的故障时自动重新启动它们。这样有助于防止发生应用程序故障。

VMware vSphere HA

您可以为部署了 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备的 vSphere 环境配置高可用性 (HA)。通过 VMware HA 功能，可以在虚拟环境出现硬件故障和操作系统故障时提供故障转移保护。

VMware HA 功能可对虚拟机进行监控，以检测操作系统故障和硬件故障。一旦检测到故障，VMware HA 功能将在资源池中的另一台物理服务器上重新启动这些虚拟机。检测到服务器故障后，不需要手动操作。

用来配置 VMware HA 的过程取决于您的 vCenter Server 版本。例如，您可以访问以下参考链接并选择所需 vCenter Server 版本来查看配置 VMware HA 的步骤。

[VMware vSphere 文档：创建和使用 vSphere HA 集群](#)

VMware vSphere Fault Tolerance

VMware vSphere Fault Tolerance (FT) 功能可以在更高级别提供高可用性 (HA)，可用于在保护虚拟机的同时不丢失任何数据或连接。您必须从 vCenter Server 为 VSC、VASA Provider 和 SRA 虚拟设备启用或禁用 vSphere FT。

请确保您的 vSphere 许可证支持 FT 以及您环境中的虚拟设备所需的 vCPU 数量（至少 2 个 vCPU；对于大型环境，则为 4 个 vCPU）。

借助 vSphere FT，即使服务器发生故障，虚拟机也可以持续运行。在对某个虚拟机启用 vSphere FT 后，系统会在 Distributed Resource Scheduler (DRS) 选择的另一台主机（二级虚拟机）上自动为主虚拟机创建一份副本。如果未启用 DRS，则系统将从可用主机中选择目标主机。vSphere FT 会使主虚拟机和二级虚拟机同步运行，并将主虚拟机的执行状态镜像到二级虚拟机。

如果出现硬件故障，进而导致主虚拟机失败，则二级虚拟机会立即从主虚拟机的停止位置开始接管。二级虚拟机会继续运行，而不会断开任何网络连接，也不会丢失事务或数据。

要为 vCenter Server 实例配置 vSphere FT，系统必须满足 CPU 要求、虚拟机限制要求以及许可要求。

用来配置 HA 的过程取决于您的 vCenter Server 版本。例如，您可以访问以下参考链接并选择所需 vCenter Server 版本来查看配置 HA 的步骤。

[VMware vSphere 文档：Fault Tolerance 要求、限制和许可](#)

VSC、VASA Provider 和 SRA 虚拟设备支持的 MetroCluster 配置

Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备支持对 ONTAP 使用 MetroCluster 配置的环境。大多数情况下，系统会自动提供这种支持，但是，在将 MetroCluster 环境与 VSC 和 VASA Provider 结合使用时，您可能会发现一些差别。

MetroCluster 配置和 VSC

您必须确保 VSC 可以发现主站点和二级站点上的存储系统控制器。通常，VSC 会自动发现存储控制器。如果您正在使用集群管理 LIF，则最好确认一下 VSC 已发现这两个站点上的集群。否则，您可以手动将这些存储控制器添加到 VSC 中。此外，您还可以修改 VSC 用于连接到存储控制器的用户名和密码对。

一旦发生切换，二级站点上的 SVM 就会进行接管。这些 SVM 会在名称后面附加“-mc”后缀。如果在发生切换操作时正在执行某些操作（例如配置），则数据存储库所在 SVM 的名称会发生更改，即附加“-mc”后缀。切回时会删除此后缀，同时，主站点上的 SVM 将恢复控制。

注：如果已将采用 MetroCluster 配置的直接 SVM 添加到 VSC 中，则在执行切换后，不会反映 SVM 名称的变化（即添加了后缀 -mc）。所有其他切换操作将继续正常执行。

发生切换或切回时，VSC 可能需要几分钟的时间来自动检测和发现集群。如果发生这种情况时，您正在执行 VSC 操作（例如配置数据存储库），则可能会发生延迟。

MetroCluster 配置和 VASA Provider

VASA Provider 会自动支持采用 MetroCluster 配置的环境。在 VASA Provider 环境中，切换操作是透明的。您不能将直接 SVM 添加到 VASA Provider 中。

注：在执行切换后，VASA Provider 不会为二级站点上的 SVM 的名称附加后缀“-mc”。

MetroCluster 配置和 SRA

SRA 不支持 MetroCluster 配置。

配置存储系统环境

适用于 VMware vSphere 的 Virtual Storage Console 提供了一种发现存储系统以及设置存储凭据的机制。这些凭据提供了 Virtual Storage Console (VSC) 用户使用存储系统执行任务所需的 ONTAP 权限。

要显示和管理存储资源，VSC 必须先发现存储系统。在发现过程中，您必须提供存储系统的 ONTAP 凭据。这些凭据是与分配给每个存储系统的用户名和密码对相关特权（或角色）。这些用户名和密码对会使用 ONTAP 基于角色的访问控制 (Role-Based Access Control, RBAC)，并且必须在 ONTAP 中进行设置。您不能在 VSC 中更改这些凭据。您可以使用适用于 ONTAP 的 RBAC User Creator 等工具定义 ONTAP RBAC 角色。您不能在 VSC 中更改这些凭据。

注：如果以管理员身份登录，则您将自动拥有对该存储系统的所有特权。

如果您要向 VSC 添加存储系统，则必须提供该存储系统的 IP 地址以及与该系统关联的用户名和密码对。您可以设置 VSC 在存储系统发现过程中要使用的默认凭据，也可以在发现存储系统后手动输入凭据。已添加到 VSC 的存储系统详细信息会自动推送到您在部署中启用的扩展。因此，您无需手动将存储添加到 VASA Provider 和 Storage Replication Adapter (SRA)。VSC 和 SRA 支持在集群级别和 Storage Virtual Machine (SVM) 级别添加凭据。VASA Provider 仅支持使用集群级别的凭据来添加存储系统。

如果您的环境包含多个 vCenter Server 实例，则在通过存储系统页面向 VSC 添加存储系统时，“添加存储系统”对话框会显示一个“vCenter Server”框，您可以在此处指定要将该存储系统添加到的 vCenter Server 实例。如果您通过右键单击数据中心名称来添加存储系统，则无法指定 vCenter Server 实例，因为该服务器已经与该数据中心相关联。

可通过以下方式之一执行发现。在每种情况下，您都必须为任何新发现的存储系统提供凭据。

- 一旦 VSC 服务启动，VSC 就会自动开始后台发现过程。
- 您可以在“存储系统”页面中单击“重新发现全部”按钮，也可以在主机或数据中心上，从操作菜单中选择此选项（“操作”>“NetApp VSC”>“更新主机和存储数据”），或者单击“概述”中“开始使用”选项卡上的“发现”。

注：不支持 IPv6 地址。

所有 VSC 功能都需要特定权限才能执行相关任务。您可以根据与 ONTAP 角色关联的凭据限制用户可以执行的操作。所有具有相同存储系统用户名和密码对的用户都将共享一组相同的存储系统凭据，并可执行相同的操作。

设置存储系统的默认凭据

您可以使用适用于 VMware vSphere 的 Virtual Storage Console 为 vCenter Server 中的存储系统设置默认凭据。

开始之前

您必须已选择要用于创建默认凭据的 vCenter Server。

关于本任务

如果为存储系统设置了默认凭据，Virtual Storage Console (VSC) 将使用这些凭据来登录到 VSC 刚刚发现的存储系统。如果这些默认凭据不起作用，您必须手动登录到此存储系统。VSC 和 SRA 支持在集群级别或 SVM 级别添加存储系统凭据。但是，VASA Provider 仅能使用集群级别凭据。

步骤

1. 在 VSC 的“主页”页面中，单击“设置”>“管理设置”>“配置存储系统的默认凭据”。
2. 在“存储系统默认凭据”对话框中，输入此存储系统的用户名和密码。
存储控制器凭据是根据用户名和密码对在 ONTAP 中分配的。此存储控制器凭据可以是管理员帐户，也可以是使用基于角色的访问控制 (Role-Based Access Control, RBAC) 的自定义帐户。
您不能使用 VSC 更改与存储控制器用户名和密码对相关角色。要更改存储控制器凭据，您必须使用适用于 ONTAP 的 RBAC User Creator 等工具。
3. 单击“确定”保存默认凭据。

完成之后

如果由于存储系统报告“身份验证失败”状态而更新了存储系统凭据，则应单击“存储系统”页面中的“重新发现全部”选项。执行此操作时，VSC 会尝试使用新凭据连接到存储系统。

将存储系统添加到 VSC 中

您可以手动将存储系统添加到 Virtual Storage Console (VSC) 中。如果存储系统数量很多，则手动添加新存储系统可能比使用“重新发现全部”选项来发现存储系统速度更快。

关于本任务

每当启动 Virtual Storage Console (VSC) 或选择“重新发现全部”选项时，VSC 都会自动发现可用的存储系统。或者，您也可以手动向 VSC 添加存储系统。

步骤

1. 使用 VSC 的“主页”页面将存储系统添加到 VSC 中：
 - 单击“存储系统”>“添加”。
 - 单击“概述”>“开始使用”，然后单击添加存储系统下的“添加”按钮。
2. 在“添加存储系统”对话框中，输入该存储系统的管理 IP 地址和凭据。
此外，您还可以使用集群或 SVM 的 IPv6 地址添加存储系统。在此对话框中，您还可以更改 TLS 和端口号的默认设置。
从 VSC 中的“存储系统”页面添加存储时，您还必须指定要将该存储放置到的 vCenter Server 实例。“添加存储系统”对话框提供了一个下拉列表，其中列出了可用的 vCenter Server 实例。如果要将存储添加到已经与某个 vCenter Server 实例关联的数据中心，则 VSC 不会显示此选项。
3. 添加完所有必需的信息后，单击“确定”。

发现存储系统和主机

首次在 vSphere Client 中运行 Virtual Storage Console (VSC) 时，VSC 将发现 ESXi 主机、它们的 LUN 和 NFS 导出以及这些 LUN 和导出所属的 NetApp 存储系统。

开始之前

- 所有 ESXi 主机都必须已启动且已连接。

- 待发现卷的 Storage Virtual Machine (SVM) 必须正在运行，并且每个集群节点必须至少为正在使用的存储协议（NFS、iSCSI 或 FC）配置一个数据 LIF。

关于本任务

您可以随时发现新的存储系统或更新有关现有存储系统的信息，以获取最新容量和配置信息。此外，还可以修改 VSC 用于登录到存储系统的凭据。

发现存储系统时，VSC 会从 vCenter Server 实例管理的 ESXi 主机收集信息。

步骤

- 在 vSphere Client “主页” 页面中，选择 “主机和群集”。
- 右键单击所需的数据中心，然后选择 “NetApp VSC” > “更新主机和存储数据”。
VSC 会显示一个确认对话框，告知您此操作可能需要很长时间。
- 单击 “确定”。
- 选择状态为 “身份验证失败” 的已发现存储控制器，然后单击 “操作” > “修改”。
- 在 “修改存储系统” 对话框中填入所需信息。
- 对状态为 “身份验证失败” 的所有存储控制器重复步骤 4 和 5。

完成之后

完成发现过程后，请执行以下操作：

- 使用 VSC 为在 “适配器设置” 列、“MPIO 设置” 列或 “NFS 设置” 列显示警报图标的主机配置 ESXi 主机设置。
- 提供存储系统凭据。

刷新存储系统显示

可以使用适用于 VMware vSphere 的 Virtual Storage Console 提供的更新功能来刷新有关存储系统的信息，并强制 Virtual Storage Console (VSC) 发现存储系统。

关于本任务

如果您在收到身份验证错误后更改了存储系统的默认凭据，则 “刷新” 选项会很有用。如果您在存储系统报告 “身份验证失败状态” 后更改了存储系统凭据，则应及时执行更新操作。执行更新操作期间，VSC 会尝试使用新凭据连接到存储系统。

此任务可能需要较长时间才能完成，具体取决于您的系统设置。

步骤

- 在 VMware vSphere Client 的 “主页” 页面上，单击 “存储系统”。
- 开始更新：

所处位置	单击项
Virtual Storage Console	“重新发现全部” 图标。
数据中心	右键单击数据中心，然后单击 “NetApp VSC” > “更新主机和存储数据”。

- 在 “更新主机和存储数据” 对话框中，单击 “确定”。

发现操作可能需要几分钟的时间，具体取决于数据中心中的主机和存储系统数量。此发现操作将在后台运行。

4. 单击“成功”对话框中的“确定”。

适用于 VMware vSphere 的 VSC 中的 vCenter Server 基于角色的访问控制功能

vCenter Server 可通过基于角色的访问控制 (RBAC) 来使您控制对 vSphere 对象的访问权限。在适用于 VMware vSphere 的 Virtual Storage Console 中，vCenter Server RBAC 可以与 ONTAP RBAC 结合使用来确定某个特定用户可以对特定存储系统上的对象执行的 VSC 任务。

要成功完成任务，您必须具有适当的 vCenter Server RBAC 权限。执行任务时，VSC 将首先检查用户的 vCenter Server 权限，然后再检查 ONTAP 特权。

您可以在根对象（也称为根文件夹）上设置 vCenter Server 权限。然后，您可以通过限制不需要这些权限的子实体来细化安全设置。

vCenter Server 权限的组成部分

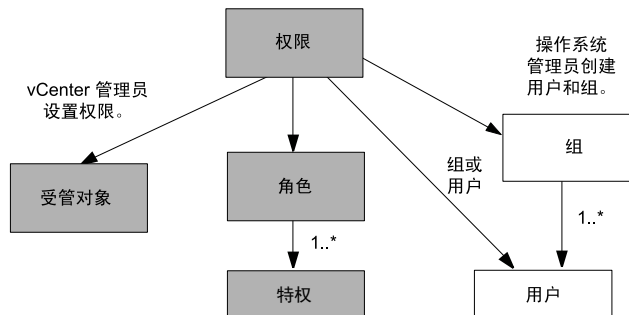
vCenter Server 可识别权限，而不是特权。每个 vCenter Server 权限都包含三个组成部分。

vCenter Server 包含以下组成部分：

- 一个或多个特权（角色）
特权用于定义用户可执行的任务。
- vSphere 对象
对象是任务的目标。
- 用户或组
用户或组用于定义可执行任务的人员。

如下图所示，一个权限必须具备所有三个要素。

注：在此图中，灰色方框表示 vCenter Server 中的组成部分，白色方框表示运行 vCenter Server 的操作系统中的组成部分。



特权

与适用于 VMware vSphere 的 Virtual Storage Console 关联的特权有两种：

- 本机 vCenter Server 特权
这些特权随 vCenter Server 一起提供。
- VSC 专用特权
这些特权是为特定 VSC 任务定义的。它们是 VSC 特有的。

VSC 任务既需要 VSC 专用特权，也需要 vCenter Server 本机特权。这些特权构成了用户的“角色”。一个权限可以具有多个特权。

注：为了简化 vCenter Server RBAC 的使用，VSC 提供了几个标准角色，这些角色包含执行 VSC 任务所需的所有 VSC 专用特权和本机特权。

如果更改了某个权限中的特权，则与此权限关联的用户应先注销并登录，才能启用更新后的权限。

表 2: VSC 特权

权限	角色	任务
“NetApp Virtual Storage Console” > “查看”	<ul style="list-style-type: none"> • VSC 管理员 • VSC 配置 • VSC 只读 	所有 VSC 和 VASA Provider 专用任务都需要查看特权。
“NetApp Virtual Storage Console” > “基于策略的管理” > “管理” 或 “privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label” > “管理”	VSC 管理员	与存储功能配置文件和阈值设置相关的 VSC 和 VASA Provider 任务。

vSphere 对象

权限与 vSphere 对象（例如 vCenter Server、ESXi 主机、虚拟机、数据存储库、数据中心和文件夹）相关联。您可以向任何 vSphere 对象分配权限。根据分配给 vSphere 对象的权限，vCenter Server 可确定哪些用户可以对此对象执行哪些任务。对于 VSC 专用任务，只会在根文件夹级别 (vCenter Server) 分配和验证权限，而不会在任何其他实体上分配和验证权限。但是，VAAI 插件操作除外，其中会对相关 ESXi 验证权限。

用户和组

您可以使用 Active Directory（或本地 vCenter Server 计算机）设置用户和用户组，然后，可以使用 vCenter Server 权限向这些用户或组授予访问权限，使其可以执行特定 VSC 任务。

注：这些 vCenter Server 权限适用于 VSC vCenter 用户，而不适用于 VSC 管理员。默认情况下，VSC 管理员对产品拥有完全访问权限，因此无需为其分配权限。

用户和组不具有分配的角色。他们会通过加入 vCenter Server 权限来获得某个角色。

有关为 vCenter Server 分配和修改权限的要点

在使用 vCenter Server 的权限时，需要注意几个要点。适用于 VMware vSphere 的 Virtual Storage Console 任务是否成功，可能取决于您分配权限的位置或修改权限后用户执行的操作。

只有希望限制对 vSphere 对象和任务的访问时，您才需要设置 vCenter Server 权限。否则，可以使用管理员身份登录。这种登录方式会自动允许您访问所有 vSphere 对象。

分配权限

您分配权限的位置将决定用户可执行的 VSC 任务。

有时，为了确保任务完成，必须在较高级别（例如根对象）分配权限。如果某项任务需要的特权不适用于特定 vSphere 对象（例如跟踪任务），或者所需特权适用于非 vSphere 对象（例如存储系统），即属于此情况。

此时，您可以设置一个权限，以供子实体继承。您也可以为子实体分配其他权限。为子实体分配的权限始终会覆盖从父实体继承的权限。这意味着，您可以通过为子实体分配权限来限制分配给根对象并由此子实体继承的权限的范围。

提示：除非贵公司的安全策略要求使用限制性更强的权限，否则最好为根对象（也称为根文件夹）分配权限。

权限和非 vSphere 对象

您创建的权限将应用于非 vSphere 对象。例如，存储系统不是 vSphere 对象。如果某个特权适用于存储系统，则必须将包含该特权的权限分配给 VSC 根对象，因为此时没有可分配权限的 vSphere 对象。

例如，包含“添加/修改/跳过存储系统”等 VSC 特权的权限必须分配给根对象级别。

修改权限

您可以随时修改某个权限。

如果您更改了权限中的特权，与该权限关联的用户应退出并重新登录，以启用更新后的权限。

VSC、VASA Provider 和 SRA 虚拟设备随附的标准角色

为了简化 vCenter Server 特权和基于角色的访问控制 (Role-Based Access Control, RBAC) 的使用，Virtual Storage Console (VSC) 提供了若干标准 VSC 角色，用于执行关键 VSC 任务。此外，还提供了一个只读角色，可以通过此角色查看 VSC 信息，但不能执行任何任务。

标准 VSC 角色具有用户执行 VSC 任务所需的 VSC 专用特权以及本机 vCenter Server 特权。此外，这些角色已经过设置，具有所有受支持的 vCenter Server 版本所需的特权。

作为管理员，您可以根据需要为用户分配这些角色。

注：在将 VSC 升级到最新版本时，这些标准角色会自动升级，以适用于新版本的 VSC。

您可以通过单击 vSphere Client 的“主页”页面上的“角色”来查看 VSC 标准角色。

可以使用 VSC 提供的角色执行以下任务：

角色	说明
VSC 管理员	提供执行所有 VSC 任务所需的所有本机 vCenter Server 特权和 VSC 专用特权。
VSC 只读	提供对 VSC 的只读访问权限。 这些用户无法执行受访问权限控制的任何 VSC 操作。
VSC 配置	提供配置存储所需的所有本机 vCenter Server 特权和 VSC 专用特权。 您可以执行以下任务： <ul style="list-style-type: none">创建新数据存储库销毁数据存储库查看有关存储功能配置文件的信息

VSC 标准角色使用准则

使用标准适用于 VMware vSphere 的 Virtual Storage Console 角色时，您应遵循特定准则。

您不应直接修改标准角色。如果直接修改，则在每次升级 VSC 时，VSC 将覆盖您所做的更改。安装程序会在您每次升级 VSC 时更新标准角色定义。这样可以确保这些角色对于您的 VSC 版本和所有受支持的 vCenter Server 版本均为最新。

但是，您可以使用标准角色为您的环境创建量身定制的角色。要执行此操作，您应该复制 VSC 标准角色，然后编辑已复制的角色。通过创建新角色，即使重新启动或升级 VSC Windows 服务，也可以保持此角色。

您可以使用 VSC 标准角色的部分方法有：

- 对所有 VSC 任务使用标准 VSC 角色。
这种情况下，标准角色提供用户执行 VSC 任务所需的所有特权。
- 合并角色，以扩展用户可以执行的任务。
如果标准 VSC 角色为您的环境提供的细化程度过高，您可以创建包含多个角色的更高级别的组来扩展角色。
如果用户需要执行其他非 VSC 任务，而这些任务需要其他本机 vCenter Server 特权，您可以创建一个角色来提供这些特权并将其添加到组中。
- 创建更加精细的角色。
如果公司要求您实施比标准 VSC 角色限制性更强的角色，您可以使用 VSC 角色创建新角色。
在这种情况下，您可以克隆必要的 VSC 角色，然后编辑已克隆的角色，使其仅具有用户所需的特权。

VSC 任务所需特权

不同的适用于 VMware vSphere 的 Virtual Storage Console 任务需要使用 Virtual Storage Console (VSC) 专用特权与本机 vCenter Server 特权的不同组合。

有关 VSC 任务所需特权的信息，请参见 NetApp 知识库文章 1032542。

[NetApp 知识库解答 1032542: How to configure RBAC for Virtual Storage Console](#)

适用于 VMware vSphere 的 VSC 所需的产品级特权

要访问适用于 VMware vSphere 的 Virtual Storage Console 的图形用户界面，您必须在正确的 vSphere 对象级别分配有产品级 VSC 专用查看特权。如果您不使用此特权登录，则在单击 NetApp 图标时，VSC 会显示错误消息，并阻止您访问 VSC。

下面的信息说明了 VSC 的产品级查看特权。

特权	说明	分配级别
查看	您可以访问 VSC 图形用户界面。 此特权并不能使您在 VSC 中执行任务。要执行任何 VSC 任务，您必须具有这些任务所需的正确 VSC 专用特权和本机 vCenter Server 特权。	分配级别将决定您可以查看到的用户界面部分。 通过在根对象（文件夹）上分配查看特权，您便可通过单击 NetApp 图标进入 VSC。 您可以将查看特权分配给其他 vSphere 对象级别，但是这样做会限制您可以查看和使用的 VSC 菜单。 建议将包含查看特权的任何权限分配给根对象。

ONTAP 适用于 VSC、VASA Provider 和 SRA 虚拟设备的基于角色的访问控制

使用 ONTAP 基于角色的访问控制 (Role-Based Access Control, RBAC)，您可以控制对特定存储系统的访问以及用户可对这些存储系统执行的操作。在适用于 VMware vSphere 的 Virtual Storage Console 中，可以通过 ONTAP RBAC 与 vCenter Server RBAC 来确定特定用户可以对特定存储系统中的对象执行哪些 Virtual Storage Console (VSC) 任务。

VSC 会使用您在 VSC 中设置的凭据（用户名和密码）来对每个存储系统进行身份验证，并确定可对该存储系统执行的存储操作。VSC 会对每个存储系统使用一组凭据。这些凭据决定了可对该存储系统执行的 VSC 任务，换言之，这些凭据是为 VSC 提供的，而不是为个别 VSC 用户提供的。

ONTAP RBAC 仅适用于访问存储系统以及执行与存储相关的 VSC 任务（例如配置虚拟机）。如果您对特定存储系统没有相应的 ONTAP RBAC 特权，则无法对该存储系统上托管的 vSphere 对象执行任何任务。您可以将 ONTAP RBAC 和 VSC 专用的特权结合使用来控制用户可执行的 VSC 任务：

- 监控和配置存储或存储系统中的 vCenter Server 对象
- 配置存储系统中的 vSphere 对象

通过将 ONTAP RBAC 与 VSC 专用的特权结合使用，可以提供面向存储的安全层，并可供存储管理员进行管理。因此，与单独使用 ONTAP RBAC 或 vCenter Server RBAC 相比，您可以更精细地实施访问控制。例如，通过 vCenter Server RBAC，您可以允许 vCenterUserB 在 NetApp 存储上配置数据仓库，同时防止 vCenterUserA 配置数据仓库。如果特定存储系统的存储系统凭据不支持创建存储，则 vCenterUserB 和 vCenterUserA 都无法在该存储系统上配置数据仓库。

当您启动 VSC 任务时，VSC 会首先确认您是否具有执行此任务的正确 vCenter Server 权限。如果您的 vCenter Server 权限不足以执行此任务，则 VSC 就不需要检查对该存储系统的 ONTAP 特权，因为您未通过最初的 vCenter Server 安全检查。这样，您就无法访问该存储系统。

如果您有足够的 vCenter Server 权限，则 VSC 会检查与该存储系统的凭据（用户名和密码）关联的 ONTAP RBAC 特权（您的 ONTAP 角色），以确定您是否有足够的特权来对该存储系统执行此 VSC 任务所需的存储操作。如果您具有正确的 ONTAP 特权，您就可以访问该存储系统并执行 VSC 任务。ONTAP 角色决定了您可以对存储系统执行的 VSC 任务。

每个存储系统都有一组关联的 ONTAP 特权。

使用 ONTAP RBAC 和 vCenter Server RBAC 可提供以下优势：

- 安全性
管理员可以在精细的 vCenter Server 对象级别和存储系统级别控制哪些用户可以执行哪些任务。

- 审核信息
在许多情况下，VSC 都会在存储系统上提供审核跟踪，用于追溯事件是由哪个修改存储的 vCenter Server 用户触发的。
- 可用性
您可以在一个位置维护所有控制器凭据。

使用适用于 VMware vSphere 的 VSC 时建议的 ONTAP 角色

您可以设置若干个建议的 ONTAP 角色，以使用适用于 VMware vSphere 的 Virtual Storage Console 和基于角色的访问控制 (Role-Based Access Control, RBAC)。这些角色包含执行必要的存储操作所需的 ONTAP 特权，可通过 Virtual Storage Console (VSC) 任务来执行这些操作。

要创建新用户角色，您必须以管理员身份登录到运行 ONTAP 的存储系统。您可以采用以下方式之一创建 ONTAP 角色：

- 适用于 ONTAP 的 RBAC User Creator 工具
[NetApp 社区文档：适用于 Data ONTAP 的 RBAC User Creator](#)
- ONTAP System Manager，可以下载到 Windows 平台或 Linux 平台上

每个 ONTAP 角色都有关联的用户名和密码对，它们构成该角色的凭据。如果不使用这些凭据登录，则无法访问与该角色关联的存储操作。您创建的每个 ONTAP 角色都会与一个用户名关联。如果要存储系统执行上述基于角色的任务，则必须使用相应的用户名和密码对登录到该存储系统。

作为一项安全措施，VSC 专用的 ONTAP 角色会按分层结构进行排序。这意味着，第一个角色的限制性最强，它只包含与一组最基本的 VSC 存储操作关联的特权。下一个角色既包含自身的特权，也包含与上一个角色关联的所有特权。对于受支持的存储操作，每增加一个角色，限制性就会相应地降低。

下面列出了一些使用 VSC 时建议设置的 ONTAP RBAC 角色。创建这些角色后，您可以将其分配给需要执行存储相关任务（例如配置虚拟机）的用户。

1. 发现
使用此角色可以添加存储系统。
2. 创建存储
使用此角色可以创建存储。另外，此角色还包含与“发现”角色关联的所有特权。
3. 修改存储
使用此角色可以修改存储。另外，此角色还包含与“发现”角色和“创建存储”角色关联的所有特权。
4. 销毁存储
使用此角色可以销毁存储。另外，此角色还包含与“发现”角色、“创建存储”角色和“修改存储”角色关联的所有特权。

如果您要使用适用于 ONTAP 的 VASA Provider，则还应设置基于策略的管理 (Policy-Based Management, PBM) 角色。使用此角色可以通过存储策略来管理存储。此角色还要求您设置发现角色。

如何为适用于 VMware vSphere 的 VSC 配置 ONTAP 基于角色的访问控制

如果要在适用于 VMware vSphere 的 Virtual Storage Console (VSC) 中使用基于角色的访问控制，则必须在存储系统上配置 ONTAP 基于角色的访问控制 (Role-Based Access Control, RBAC) 功能。您可以使用 ONTAP 的 RBAC 功能创建一个或多个具有有限访问特权的自定义用户帐户。

VSC 和 SRA 可以在集群级别或 SVM 级别访问存储系统。如果要在集群级别添加存储系统，则必须提供管理员用户的凭据，以提供所需的全部功能。如果要通过直接添加 SVM 详细信息

来添加存储系统，请务必注意，“vsadmin”用户不具有执行某些任务所需的所有角色和功能。

VASA Provider 只能在集群级别访问存储系统。如果某个存储控制器需要 VASA Provider，则必须在集群级别将该存储系统添加到 VSC 中，即便正在使用 VSC 或 SRA 也是如此。

要创建新用户并将集群或 SVM 连接到 VSC、VASA Provider 和 SRA，您应执行以下操作：

- 使用 ONTAP 创建集群管理员或 SVM 管理员角色

注：您可以使用适用于 ONTAP 的 RBAC User Creator 工具来创建这些角色。

[NetApp 社区文档：适用于 Data ONTAP 的 RBAC User Creator](#)

- 使用 ONTAP 创建具有所分配角色和适当应用程序集的用户

您需要使用这些存储系统凭据来为 VSC 配置存储系统。您可以通过在 VSC 中输入凭据来为 VSC 配置存储系统。每次使用这些凭据登录到存储系统时，您都将有权访问创建这些凭据时在 ONTAP 中设置的 VSC 功能。

- 将存储系统添加到 VSC 并提供您刚创建的用户凭据

VSC 角色

VSC 会将 ONTAP 特权分为以下几组 VSC 角色：

- 发现
用于发现所有已连接的存储控制器。
- 创建存储
用于创建卷和逻辑单元号 (Logical Unit Number, LUN)。
- 修改存储
用于对存储系统执行大小调整和重复数据删除。
- 销毁存储
用于销毁卷和 LUN。

VASA Provider 角色

您只能在集群级别创建基于策略的管理。通过此角色，可以使用存储功能配置文件对存储实施基于策略的管理。

SRA 角色

SRA 会在集群级别或 SVM 级别将 ONTAP 特权分为 SAN 或 NAS 角色。这样，用户便可运行 SRM 操作。

注：要使用 ONTAP 命令手动配置角色和特权，必须参考 NetApp 知识库文章。

- [NetApp 知识库解答 1001058: FAQ: VSC, VASA, and SRA 7.0 ONTAP RBAC Configuration](#)
- [NetApp 知识库解答 1001056: FAQ: Roll up of all commands for VSC and SRA for SVM level](#)

在将集群添加到 VSC 时，VSC 会对 ONTAP RBAC 角色执行初始特权验证。如果您添加的是直接 SVM 存储 IP，则 VSC 不会执行此初始验证，而是稍后在任务工作流检查并强制实施特权。

配置用于灾难恢复的 Storage Replication Adapter

如果要配置 vCenter Server 以实现灾难恢复，必须在部署 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备之后启用 Storage Replication Adapter (SRA)。默认情况下，部署此虚拟设备时将安装 VSC。在部署此虚拟设备之后，必须为 vCenter Server 启用 SRA。

相关任务

[启用 Storage Replication Adapter](#)（第 17 页）

为 SAN 环境配置 Storage Replication Adapter

在运行适用于 Site Recovery Manager (SRM) 的 Storage Replication Adapter (SRA) 之前，必须先设置存储系统。

开始之前

受保护站点和恢复站点上必须已安装以下程序：

- SRM
VMware 站点上提供了有关安装 SRM 的文档。
[VMware Site Recovery Manager 文档](#)
- SRA
此适配器已安装在 SRM 和 SRA 服务器上。

步骤

1. 验证主 ESXi 主机是否已连接到受保护站点上的主存储系统中的 LUN。
2. 验证这些 LUN 是否位于主存储系统上 `ostype` 选项设置为 `vmware` 的 `igroup` 中。
3. 验证恢复站点上的 ESXi 主机是否与 Storage Virtual Machine (SVM) 建立了适当的 FC 或 iSCSI 连接。

要执行此操作，可以验证 ESXi 主机是否在 SVM 上连接了本地 LUN，或者在 SVM 上使用 `fcpl show initiators` 命令或 `iscsi show initiators` 命令。

为 NAS 环境配置 Storage Replication Adapter

在运行适用于 VMware vCenter Site Recovery Manager (SRM) 的 Storage Replication Adapter (SRA) 之前，必须先配置存储系统。

开始之前

受保护站点和恢复站点上必须已安装以下程序：

- SRM
可从 VMware 站点获取有关安装 SRM 的文档。
[VMware Site Recovery Manager 文档](#)
- SRA
此适配器已安装在 SRM 和 SRA 服务器上。

步骤

1. 验证受保护站点上的数据存储库是否包含已注册到 vCenter Server 的虚拟机。
2. 验证受保护站点上的 ESXi 主机是否已从 Storage Virtual Machine (SVM) 中挂载 NFS 导出卷。
3. 验证在使用“阵列管理器”向导向 SRM 添加阵列时是否在“NFS 地址”字段中为 NFS 导出指定了有效的地址（例如 IP 地址、主机名或 FQDN）。
4. 对恢复站点的每个 ESXi 主机使用 ping 命令以验证此主机是否具有一个 VMkernel 端口，且此端口可访问用于从 SVM 提供 NFS 导出的 IP 地址。

相关信息

[NetApp 支持](#)

为高度扩展的环境配置 Storage Replication Adapter

您必须按照建议的设置来配置存储超时间隔，以使 Storage Replication Adapter (SRA) 能够在高度扩展的环境中以最佳性能运行。

存储提供程序设置

- 必须将 `StorageProvider.resignatureTimeout` 设置的值从 900 秒增加到 12000 秒。
- 必须启用 `StorageProvider.autoResignatureMode` 选项。

有关修改存储提供程序设置的详细信息，请参见 VMware 文档。

[VMware vSphere 文档：更改存储提供程序设置](#)

存储设置

必须将高度扩展的环境下的 `storage.commandTimeout` 超时间隔值设置为 12,000 秒。

注：指定的超时间隔为最大值。不必等到此最大超时时间。大多数命令会在设置的最大超时间隔内完成。

[NetApp 知识库解答 1001111：NetApp Storage Replication Adapter 4.0/7.X for ONTAP Sizing Guide](#)

有关详细信息，请参见关于修改 SAN Provider 设置的 VMware 文档。

[VMware Site Recovery Manager 文档：更改存储设置](#)

对 VSC、VASA Provider 和 SRA 虚拟设备问题进行故障排除

如果您在安装或配置 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备期间遇到意外行为，可以按照特定的故障排除过程确定此类问题的原因并予以解决。

清理 vSphere 缓存的已下载插件软件包

如果在部署或升级 VSC、VASA Provider 和 SRA 虚拟设备后未自动更新插件，则应清理浏览器和 vCenter Server 上缓存的下载插件软件包以解决 vCenter Server 插件问题。

步骤

- 1. 从现有的 vSphere Web Client 或 vSphere Client 中注销。
- 2. 删除浏览器缓存。
- 3. 删除 vSphere Client 缓存的插件软件包。

使用的网桥	操作
Windows vCenter Server	<div>删除位于以下路径的文件夹中的 com.netapp.vasa.vvol.webclient-x.x.x.xxxx、com.netapp.nvpf.webclient-x.x.x.xxxx 和 com.netapp.vsch5-x.x.x.xxxx：</div> <ul style="list-style-type: none">• vSphere Web Client 路径： C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity• vSphere Client (HTML5) 路径： C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity

使用的网桥	操作
VCSA	<div><div>a. 通过 SSH 连接到 VCSA 设备。</div><div>b. 使用 <code>cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity</code> 将目录更改为 vCenter Web Client UI 扩展目录</div><div>c. 使用以下命令删除缓存的插件软件包：<div><div><code>rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx</code></div><div><code>rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx</code></div><div><code>rm -rf com.netapp.vsch5-x.x.x.xxxx</code></div></div></div><div>d. 使用 <code>cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity</code> 将目录更改为 vCenter Client (HTML5) UI 扩展目录</div><div>e. 使用以下命令删除缓存的插件软件包：<div><div><code>rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx</code></div><div><code>rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx</code></div><div><code>rm -rf com.netapp.vsch5-x.x.x.xxxx</code></div></div></div></div>

4. 使用以下命令登录到 vSphere 并重新启动 vSphere Web Client 和 vSphere Client 服务：
- `service-control --stop vsphere-client vsphere-ui`

`service-control --start vsphere-client vsphere-ui`

卸载程序不会删除标准 VSC 角色

卸载适用于 VMware vSphere 的 Virtual Storage Console (VSC) 后，标准 VSC 角色将保持不变。这是预期行为，不会影响 VSC 性能，也不会影响升级到新版本 VSC 的功能。您可以根据需要手动删除这些角色。

虽然卸载操作不会删除 VSC 角色，但它会删除 VSC 专用特权的本地化名称，并为其附加以下前缀：“XXX missing privilege”。例如，如果您在安装 VSC 后打开 vSphere “编辑角色”对话框，则会看到 VSC 专用特权显示为 `xxx missing privilege.<privilege name>.label not found XXX`。

之所以出现此行为，是因为 vCenter Server 不提供删除特权的选项。

在重新安装 VSC 或升级到更高版本的 VSC 时，所有标准 VSC 角色以及 VSC 专用特权都会被还原。

Virtual Storage Console 和 VASA Provider 日志文件

遇到错误时，您可以检查 `/opt/netapp/vscserver/logs` 目录和 `/opt/netapp/vpserver/logs` 目录中的日志文件。

在确定问题时，以下两个日志文件可能会很有帮助：

- `cxfl.log`，其中包含有关传入和传出 VASA Provider 的 API 流量的信息

- `kamino.log`，其中包含有关 VSC 设置的信息
- `vvolvp.log`，其中包含有关 VASA Provider 的所有日志信息

您可以通过 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备的维护菜单根据需要设置不同的日志级别。可用日志级别如下：

- 信息
- 调试
- 错误
- 跟踪

设置日志级别后，以下文件将会更新：

- VSC 服务器：`kamino.log` 和 `vvolvp.log`
- VASA Provider 服务器：`vvolvp.log`、`error.log` 和 `netapp.log`

此外，VASA Provider Web 命令行界面 (CLI) 页面还会显示已发出的 API 调用、返回的错误以及性能相关的若干计数器。可通过 `https://<IP_address_or_hostname>:9083/stats` 访问此 Web 命令行界面页面。

VSC 和 VASA Provider 服务在高度扩展的环境中重新启动

问题

VSC、VASA Provider 和 SRA 虚拟设备可能无法在高度扩展的环境中以最佳状态运行，您可能会发现 VSC 和 VASA Provider 服务频繁重新启动等问题。

更正操作

修改 VSC、VASA Provider 和 SRA 虚拟设备的 RAM 和堆内存要求。

[NetApp 知识库解答 1079321: How to tune memory settings of virtual appliance for VSC, VASA Provider, and SRA for scale and performance](#)

将 VASA Provider 配置为使用 SSH

您可以通过配置 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备来设置 VASA Provider，以便使用 SSH 实现安全访问。

关于本任务

在配置 SSH 时，您必须以维护用户身份登录。这是因为对 VASA Provider 的 root 访问已被禁用。如果您使用其他登录凭据，则不能使用 SSH 来访问 VASA Provider。

步骤

1. 从 vCenter Server 中，打开一个 VSC、VASA Provider 和 SRA 虚拟设备控制台。
2. 以维护用户身份登录。
3. 输入 **3** 以选择 “System Configuration”。
4. 输入 **6** 以选择 “Enable SSH Access”。
5. 在确认对话框中输入 **y**。

配置 VSC、VASA Provider 和 SRA 虚拟设备以使用 SSH 进行远程诊断访问

您可以对 Virtual Storage Console (VSC)、VASA Provider 和 Storage Replication Adapter (SRA) 虚拟设备进行配置，以便为 diag 用户启用 SSH 访问。

开始之前

必须为 vCenter Server 实例启用 VASA Provider 扩展。

关于本任务

使用 SSH 访问 diag 用户具有以下限制：

- 每次激活 SSH 仅允许登录一次。
- 如果发生以下情况之一，则不允许为 diag 用户启用 SSH 访问：
 - 时间已到。
登录会话的有效期限截止到第二天午夜。
 - 您再次使用 SSH 以 diag 用户身份登录。

步骤

1. 在 vCenter Server 中，打开一个 VASA Provider 控制台。
2. 以 maint 用户身份登录。
3. 输入 4 以选择 “Support and Diagnostics”。
4. 输入 3 以选择 “Enable remote diagnostics access”。
5. 在 “Confirmation” 对话框中输入 **y**，以启用远程诊断访问。
6. 输入远程诊断访问的密码。

SRA 安装失败并显示脚本错误

问题

在 Windows 2008 R2 上安装 Storage Replication Adapter (SRA) 失败，并显示凭据无效错误。

原因

之所以出现此错误，可能的原因是在 VSC、VASA Provider 和 SRA 虚拟设备和 Windows 2008 R2 上启用了不同版本的传输层安全 (Transport Layer Security, TLS)。

更正操作

如果您尝试在 Windows 2008 R2 上安装 SRA，则必须在维护控制台中执行以下步骤来为 VSC、VASA Provider 和 SRA 虚拟设备启用 TLSv1.0：

1. 使用 “maint” 用户凭据登录到维护控制台。
2. 从主菜单中，选择 “1” 以访问 “Application configuration” 菜单。

3. 在“Application configuration”菜单中输入“13”以从“Application Configuration”菜单中选择“Enable TLS Protocol”。
 4. 在 TLS 协议列表中选择“TLSv1”。
- 此时将重新启动 VSC 和 VASA Provider 服务并启用 TLSv1.0。

您也可以在 Windows 2008 R2 上启用 TLSv1.2。

SRA 在高度扩展的环境中无法以最佳性能运行

问题

SRA 在高度扩展的环境中无法以最佳性能运行，并且您发现超时错误或 ONTAP 超时等问题。

更正操作

必须修改超时间隔。

为高度扩展的环境配置 [Storage Replication Adapter](#)（第 46 页）

注：此外，您还可以在高度扩展的设置中修改内存设置以提高 VSC、VASA Provider 和 SRA 虚拟设备的可扩展能力和性能。

[NetApp 知识库解答 1079321: How to tune memory settings of virtual appliance for VSC, VASA Provider, and SRA for scale and performance](#)

无法安装 SRA 插件

问题

在安装 Storage Replication Adapter (SRA) 插件期间，系统停留在服务器 IP 地址和密码屏幕，并显示以下错误消息：“The credentials you entered are not valid. Please enter a valid hostname and password.”

原因

此错误可能是由于以下原因之一导致的：

- 输入的管理员凭据不正确。
- WinHTTP 代理设置不正确。

更正操作

- 验证您的管理员凭据。
- 有关解决 WinHTTP 代理设置问题的详细信息，请参见 NetApp 知识库文章。
[NetApp 知识库解答 1005074: Installing of SRA 4.0P1 client plugin \(netapp_sra_4.0P1_ontap_64bit.msi\) hangs at the server IP and password screen](#)

版权

版权所有 © 2019 NetApp, Inc.。保留所有权利。中国印刷。

未经版权所有者优先书面许可，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。

根据 FAR 2.101 中的定义，本产品所含数据属于商业项目，并归 NetApp, Inc. 专有。美国政府使用此类数据需遵守非独占、不可转让、不可再许可、全球性、有限不可撤销的许可证的要求，且对此类数据的使用仅能出于履行美国政府就此类数据的交付缔结的合约并为此类合约提供支持之目的。除非本文另有规定，否则未经 NetApp, Inc. 事先书面批准，不得使用、披露、再现、修正、执行或显示此类数据。美国国防部享有的美国政府许可权利仅限于 DFARS 第 252.227-7015(b) 条中规定的权利。

商标

NetApp、NetApp 标识以及“NetApp 商标”页面所列的标志是 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。

<http://www.netapp.com/cn/legal/netapptmlist.aspx>

意见反馈及更新通知

您可以向我们发送反馈意见，帮助我们提高文档质量。初次发行生产级 (GA/FCS) 文档或者对现有生产级文档进行重要更改时，您可以收到自动通知。

如果您对改进本文档有任何建议，请发送电子邮件。

ng-gpso-china-documents@netapp.com

为了方便我们将您的意见或建议转发给相关主管部门，请在主题行写明产品名称、版本和操作系统。

您也可以通过以下方式与我们联系：

- 北京市朝阳区东大桥路 9 号侨福芳草地 C 座 6 层 606 室 100020
- 电话：86-10-59293000
- 传真：86-10-59293099
- 支持电话：86-10-59293008