SnapCenter 服务器安装

SnapCenter Software 4.9

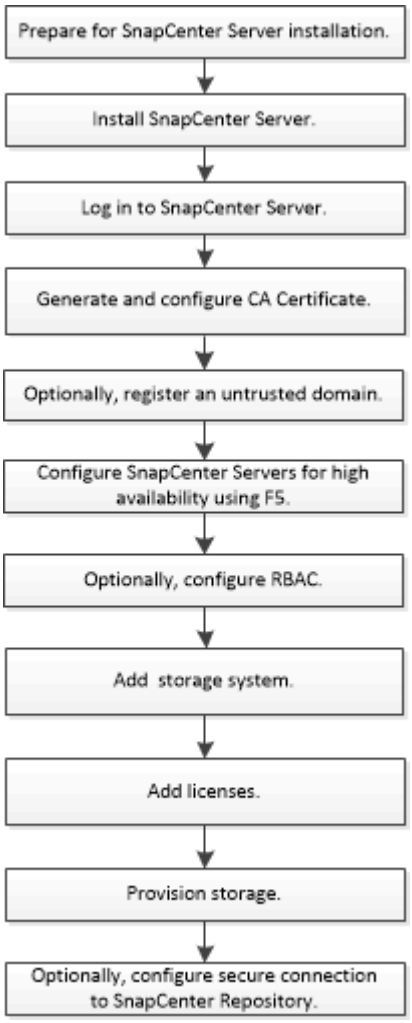
NetApp
September 26, 2025

目录

SnapCenter 服务器安装

安装工作流

此工作流显示了安装和配置 SnapCenter 服务器所需的不同任务。



准备安装 SnapCenter 服务器

域和工作组要求

SnapCenter 服务器可以安装在域或工作组中的系统上。用于安装的用户应在工作组和域的情况下对计算机具有管理员权限。

要在 Windows 主机上安装 SnapCenter 服务器和 SnapCenter 插件，应使用以下方法之一：

- * Active Directory 域 *

  您必须使用具有本地管理员权限的域用户。域用户必须是 Windows 主机上本地管理员组的成员。

- * 工作组 *

  您必须使用具有本地管理员权限的本地帐户。

虽然支持域信任，多域林和跨域信任，但不支持跨林域。有关 Active Directory 域和信任关系的 Microsoft 文档包含详细信息。

> 安装 SnapCenter 服务器后，不应更改 SnapCenter 主机所在的域。如果从安装 SnapCenter 服务器时所在的域中删除 SnapCenter 服务器主机，然后尝试卸载 SnapCenter 服务器，则卸载操作将失败。

空间和规模估算要求

在安装 SnapCenter 服务器之前，您应熟悉空间和规模估算要求。您还应应用可用的系统和安全更新。

项目	要求
操作系统	Microsoft Windows 操作系统仅支持英语，德语，日语和简体中文版。 有关受支持版本的最新信息，请参见 "NetApp 互操作性表工具"。
最小 CPU 计数	4 个核心
最小 RAM	8 GB MySQL Server 缓冲区池使用的 RAM 占总 RAM 的 20% 。
SnapCenter 服务器软件和日志的最小硬盘驱动器空间	4 GB 如果 SnapCenter 存储库位于安装 SnapCenter 服务器的同一驱动器中，则建议使用 10 GB 。
SnapCenter 存储库的最小硬盘空间	6 GB 注意：如果 SnapCenter 服务器位于安装 SnapCenter 存储库的同一驱动器中，则建议具有 10 GB 。

项目	要求
所需的软件包	• Microsoft .NET Framework 4.7.2或更高版本 • Windows Management Framework （ WMF ） 4.0 或更高版本 • PowerShell 4.0 或更高版本 有关.NET专用的故障排除信息、请参见 "对于没有Internet连接的原有系统、SnapCenter 升级或安装失败"。

SAN主机要求

如果 SnapCenter 主机属于 FC/iSCSI 环境，则可能需要在系统上安装其他软件才能访问 ONTAP 存储。

SnapCenter 不包括 Host Utilities 或 DSM 。如果 SnapCenter 主机属于 SAN 环境，则可能需要安装和配置以下软件：

- Host Utilities

  Host Utilities 支持 FC 和 iSCSI ，并可用于在 Windows 服务器上使用 MPIO 。 有关信息，请参见 "Host Utilities 文档"。

- 适用于 Windows MPIO 的 Microsoft DSM

  此软件可与 Windows MPIO 驱动程序结合使用，用于管理 NetApp 和 Windows 主机计算机之间的多个路径。

  高可用性配置需要使用 DSM 。

  > ⓘ 如果您使用的是 ONTAP DSM ，则应迁移到 Microsoft DSM 。有关详细信息，请参见 "如何从 ONTAP DSM 迁移到 Microsoft DSM"。

支持的存储系统和应用程序

您应了解支持的存储系统，应用程序和数据库。

- SnapCenter 支持 ONTAP 8.3.0 及更高版本来保护数据。
- SnapCenter 支持适用于 NetApp ONTAP 的 Amazon FSx ，以保护您的数据免受 SnapCenter 软件 4.5 P1 修补版本的影响。

  如果您使用的是适用于 NetApp ONTAP 的 Amazon FSx ，请确保 SnapCenter 服务器主机插件升级到 4.5 P1 或更高版本以执行数据保护操作。

  有关适用于 NetApp ONTAP 的 Amazon FSX 的信息，请参见 "Amazon FSX for NetApp ONTAP 文档"。

- SnapCenter 支持保护不同的应用程序和数据库。

有关支持的应用程序和数据库的详细信息，请参见 "NetApp 互操作性表工具"。

- SnapCenter 4.9 P1及更高版本支持在基于Amazon Web Services (AWS)的VMware Cloud软件定义的数据中心(SDDC)环境中保护Oracle和Microsoft SQL工作负载。

  有关详细信息，请参见 "在AWS SDDC环境中的VMware Cloud中使用NetApp SnapCenter保护Oracle、MS SQL工作负载"。

支持的浏览器

SnapCenter 软件可在多个浏览器上使用。

- Chrome

  如果您使用的是 v66 ，则可能无法启动 SnapCenter 图形用户界面。

- Internet Explorer

  如果您使用的是 IE 10 或更早版本，则无法正确加载 SnapCenter UI 。您应升级到 IE 11 。

  - 仅支持默认级别的安全性。

    更改 Internet Explorer 安全设置会导致出现严重的浏览器显示问题。

  - 必须禁用 Internet Explorer 兼容性视图。

- Microsoft Edge

有关受支持版本的最新信息，请参见 "NetApp 互操作性表工具"。

连接和端口要求

在安装 SnapCenter 服务器和应用程序或数据库插件之前，应确保满足连接和端口要求。

- 应用程序无法共享端口。

  每个端口都必须专用于相应的应用程序。

- 对于可自定义的端口，如果您不想使用默认端口，则可以在安装期间选择自定义端口。

  您可以在安装后使用修改主机向导更改插件端口。

- 对于固定端口，您应接受默认端口号。
- 防火墙
  - 防火墙，代理或其他网络设备不应干扰连接。
  - 如果您在安装 SnapCenter 时指定了自定义端口，则应在插件主机上为 SnapCenter 插件加载程序的该端口添加防火墙规则。

下表列出了不同的端口及其默认值。

端口类型	默认端口
SnapCenter 端口	8146 (HTTPS)、双向、可自定义、如URL _\https://server:8146_中所示 用于 SnapCenter 客户端（ SnapCenter 用户）与 SnapCenter 服务器之间的通信。也用于从插件主机到 SnapCenter 服务器的通信。 要自定义端口、请参见 "使用安装向导安装SnapCenter服务器。"
SnapCenter SMCore 通信端口	8145 （ HTTPS ），双向，可自定义 此端口用于在 SnapCenter 服务器与安装 SnapCenter 插件的主机之间进行通信。 要自定义端口、请参见 "使用安装向导安装SnapCenter服务器。"
MySQL 端口	3306 （ HTTPS ），双向 此端口用于在 SnapCenter 和 MySQL 存储库数据库之间进行通信。 您可以创建从 SnapCenter 服务器到 MySQL 服务器的安全连接。 "了解更多信息。" 要自定义端口、请参见 "使用安装向导安装SnapCenter服务器。"
Windows 插件主机	135 ， 445 （ TCP ） 除了端口 135 和 445 之外， Microsoft 指定的动态端口范围也应处于打开状态。远程安装操作使用 Windows Management Instrumentation （ WMI ）服务，该服务会动态搜索此端口范围。 有关支持的动态端口范围的信息，请参见 "Windows 的服务概述和网络端口要求" 这些端口用于在 SnapCenter 服务器与要安装此插件的主机之间进行通信。要将插件软件包二进制文件推送到 Windows 插件主机，这些端口只能在插件主机上打开，并且可以在安装后关闭。

端口类型	默认端口
Linux 或 AIX 插件主机	22 （ SSH ） 这些端口用于在 SnapCenter 服务器与要安装此插件的主机之间进行通信。SnapCenter 使用这些端口将插件软件包二进制文件复制到 Linux 或 AIX 插件主机，这些端口应处于打开状态或从防火墙或 IP 表中排除。
适用于 Windows 的 SnapCenter 插件软件包，适用于 Linux 的 SnapCenter 插件软件包或适用于 AIX 的 SnapCenter 插件软件包	8145 （ HTTPS ），双向，可自定义 此端口用于在 SMCore 与安装了插件软件包的主机之间进行通信。 此外，还需要在 SVM 管理 LIF 和 SnapCenter 服务器之间打开通信路径。 要自定义端口、请参见 "添加主机并安装适用于 Microsoft Windows 的 SnapCenter 插件" 或 "添加主机并安装适用于Linux或AIX的SnapCenter插件软件包。"
适用于 Oracle 数据库的 SnapCenter 插件	27216 ，可自定义 适用于 Oracle 的插件使用默认 JDBC 端口连接到 Oracle 数据库。 要自定义端口、请参见 "添加主机并安装适用于Linux或AIX的SnapCenter插件软件包。"
适用于 SnapCenter 的自定义插件	9090 （ HTTPS ），已修复 这是一个仅在自定义插件主机上使用的内部端口；不需要防火墙异常。 SnapCenter 服务器与自定义插件之间的通信通过端口 8145 进行路由。
ONTAP 集群或 SVM 通信端口	443 （ HTTPS ），双向 80 （ HTTP ），双向 SAL （存储抽象层）使用此端口在运行 SnapCenter 服务器的主机与 SVM 之间进行通信。SnapCenter for Windows 插件主机上的 SAL 当前也使用此端口在 SnapCenter 插件主机与 SVM 之间进行通信。

端口类型	默认端口
适用于SAP HANA数据库的SnapCenter 插件vCode拼写检查程序	3 个 instance_number13 或 3 个 instance_number15 ， HTTP 或 HTTPS ，双向且可自定义 对于多租户数据库容器（ MDC ）单租户，端口号以 13 结尾；对于非 MDC ，端口号以 15 结尾。 例如， 32013 是实例 20 的端口号， 31015 是实例 10 的端口号。 要自定义端口、请参见 "添加主机并在远程主机上安装插件软件包。"
域控制器通信端口	请参见 Microsoft 文档以确定域控制器上应在防火墙中打开的端口，以便身份验证能够正常工作。 必须在域控制器上打开 Microsoft 所需的端口，以便 SnapCenter 服务器，插件主机或其他 Windows 客户端能够对用户进行身份验证。

要修改端口详细信息，请参见 "修改插件主机"。

SnapCenter 许可证

SnapCenter 需要多个许可证才能对应用程序，数据库，文件系统和虚拟机进行数据保护。您安装的 SnapCenter 许可证类型取决于您的存储环境和要使用的功能。

许可证	必要时
基于 SnapCenter 标准控制器	对于FAS、AFF、全SAN阵列(ASA)为必需项 SnapCenter 标准版许可证是一种基于控制器的许可证，作为高级包的一部分提供。如果您拥有 SnapManager 套件许可证，则还可以获得 SnapCenter 标准许可证授权。如果您要在FAS、AFF或ASA存储中试用SnapCenter、可以联系销售代表获取超值包评估许可证。 SnapCenter 也作为数据保护包的一部分提供。如果您购买的是 A400 或更高版本，则应购买数据保护包。

许可证	必要时
基于 SnapCenter 标准容量	ONTAP Select 和 Cloud Volumes ONTAP 必需 如果您是 Cloud Volumes ONTAP 或 ONTAP Select 客户，则需要根据 SnapCenter 管理的数据购买基于每 TB 容量的许可证。默认情况下， SnapCenter 会提供一个内置 90 天 100 TB SnapCenter 标准容量试用许可证。有关其他详细信息，请联系销售代表。
SnapMirror 或 SnapVault	ONTAP 如果在 SnapCenter 中启用了复制，则需要 SnapMirror 或 SnapVault 许可证。
SnapRestore	用于还原和验证备份。 在主存储系统上 • 在 SnapVault 目标系统上执行远程验证和从备份中还原时需要使用。 • SnapMirror 目标系统上执行远程验证所需的。
FlexClone	克隆数据库和验证操作所需。 在主存储系统和二级存储系统上。 • 在 SnapVault 目标系统上需要此功能才能从二级存储备份创建克隆。 • 在 SnapMirror 目标系统上需要使用此功能从二级 SnapMirror 备份创建克隆。
协议	• LUN 的 iSCSI 或 FC 许可证 • SMB 共享的 CIFS 许可证 • NFS 类型 VMDK 的 NFS 许可证 • VMFS 类型 VMDK 的 iSCSI 或 FC 许可证 如果源卷不可用，则 SnapMirror 目标系统需要提供数据。

许可证	必要时
SnapCenter 标准许可证（可选）	二级目标 建议（但不要求）将 SnapCenter 标准版许可证添加到二级目标。如果二级目标上未启用 SnapCenter 标准许可证，则在执行故障转移操作后，您将无法使用 SnapCenter 备份二级目标上的资源。但是，要执行克隆和验证操作，二级目标需要 FlexClone 许可证。

SnapCenter 高级版和 SnapCenter NAS 文件服务许可证已弃用，不再可用。

您应安装一个或多个 SnapCenter 许可证。有关如何添加许可证的信息，请参见 "添加基于 SnapCenter 标准控制器的许可证" 或 "添加基于 SnapCenter 标准容量的许可证"。

单邮箱恢复（ **SMBR** ）许可证

如果您使用适用于 Exchange 的 SnapCenter 插件管理 Microsoft Exchange Server 数据库和单邮箱恢复（ SMBR ），则需要为 SMBR 提供额外的许可证，此许可证需要根据用户邮箱单独购买。

NetApp®Single Mailbox Recovery已于2023年5月12日终止提供(EOA)。有关详细信息、请参见 "CP-00507"。在支持授权期间、NetApp将继续通过2020年6月24日推出的营销部件号为已购买邮箱容量、维护和支持的客户提供支持。

NetApp Single Mailbox Recovery是Ontrack提供的合作伙伴产品。Ontrack PowerControls提供的功能与NetApp Single Mailbox Recovery类似。在EOA日期2023年5月12日之后、客户可以从Ontrack (通过licensingteam@ontrack.com)购买新的Ontrack PowerControls软件许可证以及Ontrack PowerControls维护和支持续订、以实现邮箱粒度恢复。

凭据的身份验证方法

凭据使用不同的身份验证方法，具体取决于应用程序或环境。凭据用于对用户进行身份验证，以便用户可以执行 SnapCenter 操作。您应创建一组用于安装插件的凭据，并创建另一组用于数据保护操作的凭据。

Windows 身份验证

Windows 身份验证方法根据 Active Directory 进行身份验证。对于 Windows 身份验证， Active Directory 是在 SnapCenter 之外设置的。SnapCenter 无需进行额外配置即可进行身份验证。要执行添加主机，安装插件软件包和计划作业等任务，您需要 Windows 凭据。

不可信域身份验证

SnapCenter 允许使用属于不可信域的用户和组创建 Windows 凭据。要成功进行身份验证，您应向 SnapCenter 注册不可信域。

本地工作组身份验证

SnapCenter 允许使用本地工作组用户和组创建 Windows 凭据。本地工作组用户和组的 Windows 身份验证不会在创建 Windows 凭据时进行，而是会延迟到主机注册和其他主机操作执行之后再进行。

SQL Server 身份验证

SQL 身份验证方法针对 SQL Server 实例进行身份验证。这意味着必须在 SnapCenter 中发现 SQL Server 实例。因此，在添加 SQL 凭据之前，您必须添加主机，安装插件软件包并刷新资源。要执行在 SQL Server 上计划或发现资源等操作，您需要进行 SQL Server 身份验证。

Linux 身份验证

Linux 身份验证方法可针对 Linux 主机进行身份验证。在从 SnapCenter 图形用户界面远程添加 Linux 主机和安装适用于 Linux 的 SnapCenter 插件软件包的初始步骤中，您需要进行 Linux 身份验证。

AIX身份验证

AIX 身份验证方法可针对 AIX 主机进行身份验证。在从 SnapCenter 图形用户界面远程添加 AIX 主机和安装适用于 AIX 的 SnapCenter 插件软件包的初始步骤中，您需要 AIX 身份验证。

Oracle 数据库身份验证

Oracle 数据库身份验证方法可针对 Oracle 数据库进行身份验证。如果在数据库主机上禁用了操作系统（ OS ）身份验证，则需要使用 Oracle 数据库身份验证对 Oracle 数据库执行操作。因此，在添加 Oracle 数据库凭据之前，您应在 Oracle 数据库中创建一个具有 sysdba 权限的 Oracle 用户。

Oracle ASM 身份验证

Oracle ASM 身份验证方法可针对 Oracle 自动存储管理（ Automatic Storage Management ， ASM ）实例进行身份验证。如果需要访问 Oracle ASM 实例，并且在数据库主机上禁用了操作系统（ OS ）身份验证，则需要 Oracle ASM 身份验证。因此，在添加 Oracle ASM 凭据之前，您应在 ASM 实例中创建一个具有 sysASM 特权的 Oracle 用户。

RMAN 目录身份验证

RMAN 目录身份验证方法根据 Oracle Recovery Manager （ RMAN ）目录数据库进行身份验证。如果您已配置外部目录机制并将数据库注册到目录数据库，则需要添加 RMAN 目录身份验证。

存储连接和凭据

在执行数据保护操作之前，您应设置存储连接并添加 SnapCenter 服务器和 SnapCenter 插件将使用的凭据。

- * 存储连接 *

  通过存储连接， SnapCenter 服务器和 SnapCenter 插件可以访问 ONTAP 存储。设置这些连接还需要配置 AutoSupport 和事件管理系统（ EMS ）功能。

- * 凭据 *

- 域管理员或管理员组的任何成员

  指定要安装 SnapCenter 插件的系统上的域管理员或管理员组的任何成员。用户名字段的有效格式为：

  - *netbios\username*
  - 域 FQDN\username_
  - 用户名@UPN_

- 本地管理员（仅适用于工作组）

  对于属于工作组的系统，请指定要安装 SnapCenter 插件的系统上的内置本地管理员。如果用户帐户具有提升的权限或在主机系统上禁用了用户访问控制功能，则可以指定属于本地管理员组的本地用户帐户。

用户名字段的有效格式为： *username*

- 单个资源组的凭据

  如果您为各个资源组设置了凭据，并且用户名不具有完全管理员权限，则必须至少为此用户名分配资源组和备份权限。

多因素身份验证（ **MFA** ）

管理多因素身份验证**(MFA)**

您可以在Active Directory联合身份验证服务(AD FS)服务器和SnapCenter服务器中管理多因素身份验证(MFA)功能。

启用多因素身份验证**(MFA)**

您可以使用PowerShell命令为SnapCenter服务器启用MFA功能。

关于此任务

- 如果在同一AD FS中配置了其他应用程序、则SnapCenter 支持基于SSO的登录。在某些AD FS配置中、出于安全原因、SnapCenter 可能需要用户身份验证、具体取决于AD FS会话持久性。
- 有关可与cmdlet结合使用的参数及其说明的信息，可通过运行来获取 `Get-Help command_name`。或者，您也可以参见 "《 SnapCenter 软件 cmdlet 参考指南》"。

开始之前

- Windows Active Directory联合身份验证服务(AD FS)应在相应的域中启动并运行。
- 您应该拥有一个AD FS支持的多因素身份验证服务、例如Azure MFA、Cisco Duo等。
- 无论时区如何、SnapCenter 和AD FS服务器的时间戳都应相同。
- 获取并配置SnapCenter 服务器的授权CA证书。

  CA证书为必填项、原因如下：

  - 确保ADFS-F5通信不会中断、因为自签名证书在节点级别是唯一的。
  - 确保在独立或高可用性配置中升级、修复或灾难恢复(DR)期间、不会重新创建自签名证书、从而避

免MFA重新配置。

- 确保IP-FQDN解决。

有关CA证书的信息、请参见 "生成 CA 证书 CSR 文件"。

步骤

1. 连接到Active Directory联合身份验证服务(AD FS)主机。
2. 从下载AD FS联合元数据文件 "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"。
3. 将下载的文件复制到SnapCenter 服务器以启用MFA功能。
4. 通过PowerShell以SnapCenter 管理员用户身份登录到SnapCenter 服务器。
5. 使用PowerShell会话、使用_New-SmMultifactorAuthenticationMetadata -path_ cmdlet生成SnapCenter MFA元数据文件。

   path参数用于指定在SnapCenter 服务器主机中保存MFA元数据文件的路径。

6. 将生成的文件复制到AD FS主机、以将SnapCenter 配置为客户端实体。
7. 使用为SnapCenter 服务器启用MFA `Set-SmMultiFactorAuthentication` cmdlet。
8. (可选)使用检查MFA配置状态和设置 `Get-SmMultiFactorAuthentication` cmdlet。
9. 转至Microsoft管理控制台(MMC)并执行以下步骤：
   a. 单击*文件*>*添加/删除Snapin *。
   b. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
   c. 在证书管理单元窗口中，选择 * 计算机帐户 * 选项，然后单击 * 完成 * 。
   d. 单击*控制台根*>*证书–本地计算机*>*个人*>*证书*。
   e. 右键单击绑定到SnapCenter 的CA证书、然后选择*所有任务*>*管理专用密钥*。
   f. 在权限向导上、执行以下步骤：
      i. 单击 * 添加 * 。
      ii. 单击*位置*并选择相关主机(层次结构顶部)。
      iii. 单击*位置*弹出窗口中的*确定*。
      iv. 在对象名称字段中、输入'IIS_IUSRS '并单击*检查名称*、然后单击*确定*。

      如果检查成功、请单击*确定*。
10. 在AD FS主机中、打开AD FS管理向导并执行以下步骤：
    a. 右键单击*依赖方信任*>*添加依赖方信任*>*启动*。
    b. 选择第二个选项并浏览SnapCenter MFA元数据文件、然后单击*下一步*。
    c. 指定显示名称并单击*下一步*。
    d. 根据需要选择访问控制策略，然后单击*Next*。
    e. 在下一个选项卡中选择默认设置。

f. 单击 * 完成 * 。

现在、SnapCenter 已被视为具有所提供显示名称的依赖方。

11. 选择名称并执行以下步骤：
    a. 单击*编辑款项申请发放策略*。
    b. 单击*添加规则*、然后单击*下一步*。
    c. 指定声明规则的名称。
    d. 选择* Active Directory*作为属性存储。
    e. 选择*用户主体名称*属性、并选择传出声明类型*名称ID *。
    f. 单击 * 完成 * 。
12. 在ADFS服务器上运行以下PowerShell命令。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. 执行以下步骤以确认元数据已成功导入。
    a. 右键单击依赖方信任并选择*属性*。
    b. 确保已填充"端点"、"标识符"和"签名"字段。
14. 关闭所有浏览器选项卡并重新打开浏览器以清除现有或活动会话Cookie、然后重新登录。

也可以使用REST API启用SnapCenter MFA功能。

有关故障排除的信息、请参阅 "在多个选项卡中同时尝试登录时会显示MFA错误"。

更新**AD FS MFA**元数据

只要对AD FS服务器进行了任何修改、例如升级、CA证书续订、灾难恢复等、您就应在SnapCenter 中更新AD FS MFA元数据。

步骤

1. 从下载AD FS联合元数据文件 "https://<host FQDN>/FederationMetadata、2007年06月/FedationMetadata。xml"
2. 将下载的文件复制到SnapCenter 服务器以更新MFA配置。
3. 运行以下cmdlet以更新SnapCenter 中的AD FS元数据：

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. 关闭所有浏览器选项卡并重新打开浏览器以清除现有或活动会话Cookie、然后重新登录。

更新**SnapCenter MFA**元数据

只要在ADFS服务器中进行任何修改、例如修复、CA证书续订、DR等、您就应更新AD FS中的SnapCenter

MFA元数据。

步骤

1. 在AD FS主机中、打开AD FS管理向导并执行以下步骤：
   a. 单击*依赖方信任*。
   b. 右键单击为SnapCenter 创建的依赖方信任、然后单击*删除*。

      此时将显示依赖方信任的用户定义名称。

   c. 启用多因素身份验证(MFA)。

      请参见 "启用多因素身份验证"。
2. 关闭所有浏览器选项卡并重新打开浏览器以清除现有或活动会话Cookie、然后重新登录。

禁用多因素身份验证**(MFA)**

步骤

1. 使用禁用MFA并清理在启用MFA时创建的配置文件 `Set-SmMultiFactorAuthentication` cmdlet。
2. 关闭所有浏览器选项卡并重新打开浏览器以清除现有或活动会话Cookie、然后重新登录。

使用**REST API**、**PowerShell**和**sccli**管理多因素身份验证**(MFA)**

支持从浏览器、REST API、PowerShell和sccli登录MFA。MFA可通过AD FS身份管理器获得支持。您可以通过GUI、REST API、PowerShell和sccli启用MFA、禁用MFA以及配置MFA。

将**AD FS**设置为**OAuth/OIDC**

使用**Windows GUI**向导配置**AD FS**

1. 导航到*Server Manager Dashboard (服务器管理器仪表板)**>*Tools**(工具)>*ADFS Management*(ADFS管理)。
2. 导航到*ADFS*>*Application Groups*。
   a. 右键单击*应用程序组*。
   b. 选择*添加应用程序组*并输入*应用程序名称*。
   c. 选择*服务器应用程序*。
   d. 单击 * 下一步 * 。
3. 复制*客户标识符*。

   这是客户端ID。 …在重定向URL中添加回调URL (SnapCenter服务器URL)。 …单击 * 下一步 * 。
4. 选择*生成共享密钥*。

   复制机密值。这是客户的秘密。 …单击 * 下一步 * 。

5. 在“摘要”页上，单击“下一步”。
    a. 在*完成*页上，单击*关闭*。
6. 右键单击新添加的*应用程序组*，然后选择*属性*。
7. 从“应用程序属性”中选择*添加应用程序*。
8. 单击*添加应用程序*。

    选择Web API并单击*Next*。

9. 在配置Web API页面上、在标识符部分中输入上一步创建的SnapCenter服务器URL和客户端标识符。
    a. 单击 * 添加 * 。
    b. 单击 * 下一步 * 。
10. 在*选择访问控制策略*页上，根据您的要求选择控制策略(例如，允许所有人和要求MFA)，然后单击*下一步*。
11. 在*配置应用程序权限*页上，默认情况下会选择OpenID作为范围，单击*Next*。
12. 在“摘要”页上，单击“下一步”。

    在*完成*页上，单击*关闭*。

13. 在“示例应用程序属性”页上，单击*OK*。
14. 由授权服务器(AD FS)颁发并打算由资源使用的JWT令牌。

    此令牌的"aud"或访问群体声明必须与资源或Web API的标识符匹配。

15. 编辑选定的WebAPI并检查是否已正确添加回调URL (SnapCenter服务器URL)和客户端标识符。

    配置OpenID Connect以提供用户名作为声明。

16. 打开位于服务器管理器右上角的*Tools*菜单下的*AD FS Management*工具。
    a. 从左侧边栏中选择*应用程序组*文件夹。
    b. 选择Web API并单击*edit*。
    c. 转至"颁发转换规则"选项卡
17. 单击 * 添加规则 * 。
    a. 在“声明规则模板”下拉列表中选择*将LDAP属性作为声明发送*。
    b. 单击 * 下一步 * 。
18. 输入*申请规则*名称。
    a. 在“属性存储”下拉列表中选择*Active Directory*。
    b. 在*LDAP Attribute*下拉列表中选择*User-Principal-Name*，在O*utgoing款项申请类型*下拉列表中选择*UPN*。
    c. 单击 * 完成 * 。

使用**PowerShell**命令创建应用程序组

您可以使用PowerShell命令创建应用程序组和Web API、并添加范围和声明。这些命令以自动脚本格式提供。有关详细信息、请参见<link to KB article>。

1. 使用以下命令在AD FS中创建新的应用程序组。

   ```
   New-AdfsApplicationGroup -Name $ClientRoleIdentifier
   -ApplicationGroupIdentifier $ClientRoleIdentifier
   ```

   `ClientRoleIdentifier` 应用程序组的名称

   `redirectURL` 授权后重定向的有效URL

2. 创建AD FS服务器应用程序并生成客户端密钥。

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   -ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
   -Identifier $identifier -GenerateClientSecret
   ```

3. 创建ADFS Web API应用程序并配置其应使用的策略名称。

   ```
   $identifier = (New-Guid).Guid

   Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
   -Name "App Web API"

   -Identifier $identifier -AccessControlPolicyName "Permit everyone"
   ```

4. 从以下命令的输出中获取客户端ID和客户端密钥、因为它仅显示一次。

   ```
   "client_id = $identifier"

   "client_secret: "$($ADFSApp.ClientSecret)
   ```

5. 为AD FS应用程序授予allatlaims和OpenID权限。

   ```
   Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
   -ServerRoleIdentifier $identifier -ScopeNames @('openid')

   $transformrule = @"

   @RuleTemplate = "LdapClaims"

   @RuleName = "AD User properties and Groups"

   c:[Type ==
   "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
   Issuer ==

   "AD AUTHORITY"]

   ⇒ issue(store = "Active Directory", types =
   ```

```
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 写出转换规则文件。

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 命名Web API应用程序并使用外部文件定义其颁发转换规则。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

更新访问令牌到期时间

您可以使用PowerShell命令更新访问令牌到期时间。

- 关于此任务 *
- 访问令牌只能用于用户、客户端和资源的特定组合。访问令牌不能撤消、在到期之前有效。
- 默认情况下、访问令牌的到期时间为60分钟。 这种最短到期时间足以满足要求。您必须提供足够的价值、以避免执行任何持续的业务关键型作业。
- 步骤 *

要更新应用程序组WebApi的访问令牌到期时间、请在AD FS服务器中使用以下命令。

+ `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

从**AD FS**获取承载令牌

您应在任何REST客户端(如Postman)中填写以下参数、并提示您填写用户凭据。此外、您还应输入第二因素身份验证(您拥有的和您所拥有的)以获取承载令牌。

+ 可从AD FS服务器为每个应用程序配置承载令牌的有效期、默认有效期为60分钟。

字段	价值
授予类型	授权代码
回调URL	如果没有回调URL，请输入应用程序的基本URL。
身份验证URL	[adfs-domain-name]/adfs/oauth2/authorize

访问令牌URL	[adfs-domain-name]/adfs/oauth2/令牌
客户端 ID	输入AD FS客户端ID
客户端密钥	输入AD FS客户端密钥
范围	OpenID
客户端身份验证	作为基本AUTH标题发送
资源	在*Advance Options *选项卡中，添加与回调URL值相同的“资源”字段，该值在JWT令牌中显示为“aud”值。

使用**PowerShell**、**sccli**和**REST API**在**SnapCenter**服务器中配置**MFA**

您可以使用PowerShell、sccli和REST API在SnapCenter服务器中配置MFA。

SnapCenter MFA命令行界面身份验证

在PowerShell和sccli中、现有cmdlet (Open-SmConnection)扩展为另外一个名为"AccessToken "的字段、以使用承载令牌对用户进行身份验证。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

执行上述cmdlet后、将为相应用户创建一个会话、以执行其他SnapCenter cmdlet。

SnapCenter MFA REST API身份验证

在REST <access token>客户端(如Postman或swagger)中使用格式为_Authorization=Bearer API_的承载令牌、并在标题中提及用户RoleName、以从SnapCenter获得成功响应。

MFA REST API工作流

如果为MFA配置了AD FS、则应使用访问(承载)令牌进行身份验证、以便通过任何REST API访问SnapCenter应用程序。

- 关于此任务 *
- 您可以使用任何REST客户端、例如Postman、Swagger UI或FireCamp。
- 获取访问令牌并使用它对后续请求(SnapCenter REST API)进行身份验证、以执行任何操作。
- 步骤 *

*通过AD FS MFA*进行身份验证

1. 将REST客户端配置为调用AD FS端点以获取访问令牌。

   单击此按钮获取应用程序的访问令牌后、您将重定向到AD FS SSO页面、在此页面中、您必须提供AD凭据

并通过MFA进行身份验证。 1.在AD FS SSO页面的用户名文本框中、键入您的用户名或电子邮件。

+ 用户名的格式必须为user@domain或domain\user。

2. 在密码文本框中、键入您的密码。
3. 单击*登录*。
4. 从*登录选项*部分中，选择一个身份验证选项并进行身份验证(取决于您的配置)。
   - 推送：批准发送到您的电话的推送通知。
   - QR码：使用AUTH Point移动应用程序扫描QR码、然后键入应用程序中显示的验证码
   - 一次性密码：键入令牌的一次性密码。
5. 身份验证成功后、将打开一个弹出窗口、其中包含访问、ID和刷新令牌。

   复制访问令牌并在SnapCenter REST API中使用它来执行此操作。

6. 在REST API中、您应在标题部分中传递访问令牌和角色名称。
7. SnapCenter将从AD FS验证此访问令牌。

   如果此令牌有效、则SnapCenter会对其进行加密并获取用户名。

8. SnapCenter使用用户名和角色名称对执行API的用户进行身份验证。

   如果身份验证成功、SnapCenter将返回结果、否则会显示错误消息。

为**REST API**、命令行界面和图形用户界面启用或禁用**SnapCenter MFA**功能

图形用户界面

- 步骤 *
  1. 以SnapCenter管理员身份登录到SnapCenter服务器。
  2. 单击*Settings*>*Global Settings*>*MultiFacorAuthentication (MFA) Settings*
  3. 选择接口(GUI/RST API/CLI)以启用或禁用MFA登录。

PowerShell接口

- 步骤 *
  1. 运行PowerShell或CLI命令为GUI、REST API、PowerShell和sccli启用MFA。

     ```
     Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
     -IsCliMFAEnabled -Path
     ```

     path参数用于指定AD FS MFA元数据xml文件的位置。

为配置有指定AD FS元数据文件路径的SnapCenter图形用户界面、REST API、PowerShell和sccli启用MFA。

1. 使用检查MFA配置状态和设置 `Get-SmMultiFactorAuthentication` cmdlet。

sccli Interface

- 步骤 *

1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. `# sccli Get-SmMultiFactorAuthentication`

REST API

1. 运行以下POST API、以便为GUI、REST API、PowerShell和sccli启用MFA。

参数	价值
请求的URL	/API/4.9/SETTINGS/multifactorauthentication
HTTP 方法	发布
请求正文	｛"isiMFAEnabled"：false、"IsRestApiMFAEnabled"：true、 "IsCliMFAEnabled"：false、 "ADFSConfigFilePath"："c：\\ADFS_METADA\\abc.xml" }
响应正文	｛"MFAConfiguration"： ｛"isiMFAEnabled"：false、 "ADFSConfigFilePath"："c：\\ADFS_metadata\\abc.xml"、 "SCConfigFilePath"：空、 "IsRestApiMFAEnabled"：true、 "IsCliMFAEnabled"：false、 "ADFSHostName"：win-adfs-sc49.winscedom2.com } }

2. 使用以下API检查MFA配置状态和设置。

参数	价值
请求的URL	/API/4.9/SETTINGS/multifactorauthentication
HTTP 方法	获取
响应正文	｛"MFAConfiguration"： ｛"isiMFAEnabled"：false、 "ADFSConfigFilePath"："c：\\ADFS_metadata\\abc.xml"、 "SCConfigFilePath"：空、 "IsRestApiMFAEnabled"：true、 "IsCliMFAEnabled"：false、 "ADFSHostName"：win-adfs-sc49.winscedom2.com } }

安装 SnapCenter 服务器

您可以运行 SnapCenter 服务器安装程序可执行文件来安装 SnapCenter 服务器。

您可以选择使用 PowerShell cmdlet 执行多个安装和配置过程。

不支持使用命令行静默安装 SnapCenter 服务器。

开始之前

- SnapCenter 服务器主机必须是最新的 Windows 更新，并且不会发生待定系统重新启动。
- 您应确保计划安装 SnapCenter 服务器的主机上未安装 MySQL 服务器。
- 您应已启用 Windows 安装程序调试。

  有关启用的信息，请参见 Microsoft 网站 "Windows 安装程序日志记录"。

  您不应将 SnapCenter 服务器安装在具有 Microsoft Exchange Server ， Active Directory 或域名服务器的主机上。

- 步骤 *

1. 从下载 SnapCenter 服务器安装包 "NetApp 支持站点"。
2. 双击下载的 .exe 文件启动 SnapCenter 服务器安装。

   启动安装后，系统将执行所有预检，如果不满足最低要求，则会显示相应的错误或警告消息。

   您可以忽略警告消息并继续安装；但是，错误应予以修复。

3. 查看安装 SnapCenter 服务器所需的预填充值，并根据需要进行修改。

   您不必指定 MySQL Server 存储库数据库的密码。在 SnapCenter 服务器安装期间，系统会自动生成密码。

   特殊字符"`%`" is not supported in the custom path for the repository database. If you include “%”、安装失败。

4. 单击 * 立即安装 * 。

   如果指定的值无效，则会显示相应的错误消息。您应重新输入这些值，然后启动安装。

   如果单击 * 取消 * 按钮，则正在执行的步骤将完成，然后启动回滚操作。SnapCenter 服务器将从主机中完全删除。

   但是，如果在执行 SnapCenter 服务器站点重新启动或等待 SnapCenter 服务器启动操作时单击 * 取消 * ，则安装将继续进行，而不会取消此操作。

日志文件始终列在管理员用户的 %temp% 文件夹中（最早的先列出）。如果要重定向日志位置、请从命令提示符处运行以下命令来启动SnapCenter 服务器安装
：`C:\installer_location\installer_name.exe /log"C:\"`

使用RBAC授权登录到SnapCenter

SnapCenter 支持基于角色的访问控制（ Role-Based Access Control ， RBAC ）。SnapCenter 管理员通过 SnapCenter RBAC 将角色和资源分配给工作组或 Active Directory 中的用户或 Active Directory 中的组。现在， RBAC 用户可以使用分配的角色登录到 SnapCenter 。

开始之前

- 您应在 Windows Server Manager 中启用 Windows 进程激活服务（ Wwas ）。
- 如果要使用 Internet Explorer 作为浏览器登录到 SnapCenter 服务器，应确保已禁用 Internet Explorer 中的保护模式。
- 关于此任务 *

安装期间， SnapCenter 服务器安装向导会创建一个快捷方式，并将其放置在桌面上以及安装 SnapCenter 的主机的 " 开始 " 菜单中。此外，安装向导将在安装结束时根据您在安装期间提供的信息显示 SnapCenter URL ，如果您要从远程系统登录，可以复制这些 URL 。

如果您在 Web 浏览器中打开了多个选项卡，则仅关闭 SnapCenter 浏览器选项卡不会将您从 SnapCenter 中注销。要结束与 SnapCenter 的连接，您必须单击 * 注销 * 按钮或关闭整个 Web 浏览器以注销 SnapCenter 。

* 最佳实践： * 出于安全原因，建议不要启用浏览器来保存 SnapCenter 密码。

默认图形用户界面URL是与安装SnapCenter服务器的服务器上的默认端口8146 (https://server:8146_).如果您在 SnapCenter 安装期间提供了其他服务器端口，则会改用该端口。

对于高可用性(HA)部署、您必须使用虚拟集群IP *Data https://Virtual_Cluster_IP_or_FQDN:8146*.访问SnapCenter如果在Internet Explorer (IE)中导航到_FQDN时看不到SnapCenter UI、则必须在每个插件主机上将虚拟集群IP地址或\https://Virtual_Cluster_IP_or_FQDN:8146_添加为IE中的受信任站点、或者必须在每个插件主机上禁用IE增强安全。 有关详细信息，请参见 "无法从外部网络访问集群 IP 地址"。

除了使用 SnapCenter 图形用户界面之外，您还可以使用 PowerShell cmdlet 创建脚本以执行配置，备份和还原操作。某些 cmdlet 可能会随每个 SnapCenter 版本而发生更改。 "《 SnapCenter 软件 cmdlet 参考指南》"具有详细信息。

如果您是首次登录到 SnapCenter ，则必须使用安装过程中提供的凭据进行登录。

- 步骤 *

1. 从本地主机桌面上的快捷方式，安装结束时提供的 URL 或 SnapCenter 管理员提供的 URL 启动 SnapCenter 。
2. 输入用户凭据。

要指定以下内容 ...	使用以下格式之一 ...
域管理员	• netbios\ 用户名 • 用户名@UPN 后缀 例如， username@netapp.com • 域 FQDN\username
本地管理员	Username

3. 如果您分配了多个角色，请从角色框中选择要用于此登录会话的角色。

   登录后，您的当前用户和关联角色将显示在 SnapCenter 的右上角。

- 结果 *

此时将显示信息板页面。

如果日志记录失败并显示错误，指出无法访问站点，则应将 SSL 证书映射到 SnapCenter 。 "了解更多信息。"

- 完成后 *

首次以 RBAC 用户身份登录到 SnapCenter 服务器后，刷新资源列表。

如果您希望 SnapCenter 支持不可信的 Active Directory 域，则必须先向 SnapCenter 注册这些域，然后再为不可信域上的用户配置角色。 "了解更多信息。"

使用多因素身份验证(Multi-Factor Authentication、MFA)登录到SnapCenter

SnapCenter 服务器支持将MFA用于域帐户、此帐户属于活动目录。

开始之前

- 您应已启用MFA。

  有关如何启用MFA的信息、请参见 "启用多因素身份验证"

- 关于此任务 *
- 仅支持FQDN
- 工作组和跨域用户无法使用MFA登录
- 步骤 *

1. 从本地主机桌面上的快捷方式，安装结束时提供的 URL 或 SnapCenter 管理员提供的 URL 启动 SnapCenter 。
2. 在AD FS登录页面中、输入用户名和密码。

   如果AD FS页面上显示用户名或密码无效错误消息、则应检查以下内容：

- 用户名或密码是否有效

  此用户帐户应位于Active Directory (AD)中

- 是否超过在AD中设置的允许的最大尝试次数
- AD和AD FS是否已启动且正在运行

修改 **SnapCenter** 默认 **GUI** 会话超时

您可以修改 SnapCenter 图形用户界面会话超时期限，使其小于或大于默认超时期限 20 分钟。

作为一项安全功能，默认情况下处于非活动状态 15 分钟后， SnapCenter 会向您发出警告，指出您将在 5 分钟内从图形用户界面会话中注销。默认情况下， SnapCenter 会在不活动 20 分钟后从 GUI 会话中注销，您必须重新登录。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 设置 * > * 全局设置 * 。
  2. 在全局设置页面中，单击 * 配置设置 * 。
  3. 在会话超时字段中，以分钟为单位输入新会话超时，然后单击 * 保存 * 。

通过禁用 **SSL 3.0** 来保护 **SnapCenter Web** 服务器的安全

出于安全考虑，如果在 SnapCenter Web 服务器上启用了安全套接字层（ SSL ） 3.0 协议，则应在 Microsoft IIS 中禁用该协议。

SSL 3.0 协议存在一些缺陷，攻击者可以使用这些缺陷来处理发生原因连接故障，或者执行中间人攻击并观察您的网站与其访客之间的加密流量。

- 步骤 *
  1. 要在 SnapCenter Web 服务器主机上启动注册表编辑器，请单击 * 开始 * > * 运行 * ，然后输入 regedit 。
  2. 在注册表编辑器中，导航到 HKEY_LOCAL_MACHINE ， system\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols\SSL 3.0\ 。
     - 如果服务器密钥已存在：
       i. 选择已启用的 DWORD ，然后单击 * 编辑 * > * 修改 * 。
       ii. 将此值更改为 0 ，然后单击 * 确定 * 。
     - 如果服务器密钥不存在：
       i. 单击 * 编辑 * > * 新增 * > * 密钥 * ，然后将密钥服务器命名为。
       ii. 选择新服务器密钥后，单击 * 编辑 * > * 新建 * > * 双字节 * 。
       iii. 将新的 DWORD 命名为 Enabled ，然后输入 0 作为值。
  3. 关闭注册表编辑器。

配置 CA 证书

生成 CA 证书 CSR 文件

您可以生成证书签名请求（ CSR ），并导入可使用生成的 CSR 从证书颁发机构（ CA ）获取的证书。此证书将具有一个关联的专用密钥。

CSR 是一个编码文本块，提供给授权证书供应商以采购签名的 CA 证书。

CA证书RSA密钥长度应至少为3072位。

有关生成 CSR 的信息，请参见 "如何生成 CA 证书 CSR 文件"。

如果您拥有域（ * .domain.company.com ）或系统（ machine1.domain.company.com ）的 CA 证书，则可以跳过生成 CA 证书 CSR 文件。 您可以使用 SnapCenter 部署现有 CA 证书。

对于集群配置， CA 证书中应提及集群名称（虚拟集群 FQDN ）以及相应的主机名。 可以通过在获取证书之前填写使用者替代名称(SAN)字段来更新此证书。 对于通配符证书（ * .domain.company.com ），此证书将隐式包含域的所有主机名。

导入 CA 证书

您必须使用 Microsoft 管理控制台（ MMC ）将 CA 证书导入到 SnapCenter 服务器和 Windows 主机插件中。

步骤

1. 转到 Microsoft 管理控制台（ MMC ），然后单击 * 文件 * > * 添加 / 删除 Snapin * 。
2. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
3. 在证书管理单元窗口中，选择 * 计算机帐户 * 选项，然后单击 * 完成 * 。
4. 单击 * 控制台根 * > * 证书–本地计算机 * > * 可信根证书颁发机构 * > * 证书 * 。
5. 右键单击文件夹 " 可信根证书颁发机构 " ，然后选择 * 所有任务 * > * 导入 * 以启动导入向导。
6. 完成向导，如下所示：

在此向导窗口中 ...	执行以下操作 ...
导入私钥	选择 * 是 * 选项，导入私钥，然后单击 * 下一步 * 。
导入文件格式	不进行任何更改；单击 * 下一步 * 。
安全性	指定要用于导出的证书的新密码，然后单击 * 下一步 * 。
正在完成证书导入向导	查看摘要，然后单击 * 完成 * 开始导入。

导入证书应与私钥捆绑在一起(支持的格式为：。**pfx**、。p12和*。p7b)。

7. 对 "Personal" 文件夹重复步骤 5 。

获取 **CA** 证书指纹

证书指纹是用于标识证书的十六进制字符串。指纹是使用指纹算法根据证书内容计算得出的。

步骤

1. 在 GUI 上执行以下操作：
   a. 双击证书。
   b. 在证书对话框中，单击 * 详细信息 * 选项卡。
   c. 滚动字段列表，然后单击 * 缩略图 * 。
   d. 从框中复制十六进制字符。
   e. 删除十六进制数之间的空格。

      例如，如果指纹为 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b" ，则在删除空格后，指纹将为 "a909502dd82ae41433e6f83886b00d4277a32a7b" 。

2. 从 PowerShell 执行以下操作：
   a. 运行以下命令以列出已安装证书的指纹，并按主题名称标识最近安装的证书。

      *Get-*子 项 *-Path Cert* ： *\LOCALLMACHINE\My*

   b. 复制指纹。

使用 **Windows** 主机插件服务配置 **CA** 证书

您应使用 Windows 主机插件服务配置 CA 证书，以激活已安装的数字证书。

在 SnapCenter 服务器以及已部署 CA 证书的所有插件主机上执行以下步骤。

步骤

1. 运行以下命令，删除与 SMCore 默认端口 8145 的现有证书绑定：

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   例如：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

. 运行以下命令，将新安装的证书与 `Windows` 主机插件服务绑定：

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

使用 **SnapCenter** 站点配置 **CA** 证书

您应在 Windows 主机上使用 SnapCenter 站点配置 CA 证书。

- 步骤 *
  1. 在安装了 SnapCenter 的 Windows 服务器上打开 IIS 管理器。
  2. 在左侧导航窗格中，单击 * 连接 * 。
  3. 展开服务器和 * 站点 * 的名称。
  4. 选择要安装 SSL 证书的 SnapCenter 网站。
  5. 导航到*Actions*>*Edit Site*，单击*BINDENTS*。
  6. 在绑定页面中，选择 * 绑定 https * 。
  7. 单击 * 编辑 * 。
  8. 从 SSL 证书下拉列表中，选择最近导入的 SSL 证书。
  9. 单击 * 确定 * 。

如果最近部署的 CA 证书未在下拉菜单中列出，请检查此 CA 证书是否与专用密钥关联。

确保使用以下路径添加证书： * 控制台根 > 证书–本地计算机 > 可信根证书颁发机构 > 证书 * 。

为 **SnapCenter** 启用 **CA** 证书

您应配置 CA 证书并为 SnapCenter 服务器启用 CA 证书验证。

开始之前

- 您可以使用 Set-SmCertificateSettings cmdlet 启用或禁用 CA 证书。
- 您可以使用 Get-SmCertificateSettings cmdlet 显示 SnapCenter 服务器的证书状态。

有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 *get-help command_name* 来获取。或者，您也

可以参考 "《 SnapCenter 软件 cmdlet 参考指南》"。

- 步骤 *
  1. 在设置页面中，导航到 * 设置 * > * 全局设置 * > * CA 证书设置 * 。
  2. 选择 * 启用证书验证 * 。
  3. 单击 * 应用 * 。
- 完成后 *

受管主机选项卡主机会显示一个挂锁，挂锁的颜色表示 SnapCenter 服务器与插件主机之间的连接状态。

- ** 表示没有为插件主机启用或分配CA证书。
- ** 表示CA证书已成功验证。
- ** 表示无法验证CA证书。
- *]* 表示无法检索到连接信息。

如果状态为黄色或绿色，则表示数据保护操作已成功完成。

配置并启用双向SSL通信

配置双向SSL通信

您应配置双向SSL通信、以确保SnapCenter服务器与插件之间的相互通信安全。

- 开始之前 *
- 您应已生成支持的最小密钥长度为3072的CA证书CSR文件。
- CA证书应支持服务器身份验证和客户端身份验证。
- 您应拥有一个CA证书、其中应包含私钥和指纹详细信息。
- 您应已启用单向SSL配置。

  有关详细信息，请参见 "配置CA证书部分。"
- 您必须已在所有插件主机和SnapCenter服务器上启用双向SSL通信。

  不支持某些主机或服务器未启用双向SSL通信的环境。
- 步骤 *
  1. 要绑定此端口、请在SnapCenter服务器主机上对SnapCenter IIS Web服务器端口8146 (默认)执行以下步骤、并使用PowerShell命令对SMCore端口8145 (默认)再次执行以下步骤。
     a. 使用以下PowerShell命令删除现有SnapCenter自签名证书端口绑定。

        ```
        > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
        ```

        例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145

> netsh http delete sslcert ipport=0.0.0.0:8146
```

b. 将新获取的CA证书与SnapCenter服务器和SMCore端口绑定。

```
> $cert = "<CA_certificate thumbprint>"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
certhash=$cert appid="$guid" clientcertnegotiation=enable
verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

例如：

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. 要访问CA证书的权限、请执行以下步骤以访问新购买的CA证书、从而将SnapCenter的默认IIS Web服务器用户"**IIS AppPoool\SnapCenter**"添加到证书权限列表中。
   a. 转到Microsoft管理控制台(MMC)，然后单击*File*>*Add/Remove snapin。
   b. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
   c. 在证书管理单元窗口中，选择 * 计算机帐户 * 选项，然后单击 * 完成 * 。
   d. 单击*控制台根*>*证书–本地计算机*>*个人*>*证书*。
   e. 选择SnapCenter证书。
   f. 要启动添加用户\权限向导，请右键单击CA证书，然后选择*All Tasks*>*Manage private keys*。
   g. 单击*Add*，在Select Users and Groups (选择用户和组)向导中将位置更改为本地计算机名称(层次结构中最顶端)
   h. 添加IIS Appool\SnapCenter用户、授予完全控制权限。
3. 对于*CA证书IIS权限*，从以下路径在SnapCenter服务器中添加新的DWORD注册表项条目：

   在Windows注册表编辑器中，遍历以下路径：

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
ders\SCHANNEL
```

4. 在Schchannel注册表配置环境下创建新的DWORD注册表项条目。

```
SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
```

配置**SnapCenter Windows**插件以实现双向**SSL**通信

您应使用PowerShell命令配置SnapCenter Windows插件以实现双向SSL通信。

- 开始之前 *

确保CA证书指纹可用。

- 步骤 *

1. 要绑定端口、请在Windows插件主机上对SMCore端口8145 (默认)执行以下操作。

   a. 使用以下PowerShell命令删除现有SnapCenter自签名证书端口绑定。

   ```
   > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
   ```

   例如：

   ```
   > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   b. 将新获得的CA证书与SMCore端口绑定。

   ```
   > $cert = "<CA_certificate thumbprint>"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
   appid="$guid" clientcertnegotiation=enable
   verifyclientcertrevocation=disable

   > netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
   ```

   例如：

   ```
   > $cert = "abc123abc123abc123abc123"

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
   clientcertnegotiation=enable verifyclientcertrevocation=disable

   > netsh http show sslcert ipport=0.0.0.0:8145
   ```

启用双向SSL通信

您可以使用PowerShell命令启用双向SSL通信、以确保SnapCenter服务器与插件之间的相互通信安全。

- 开始之前 *

先对所有插件和SMCore代理执行命令、然后再对服务器执行命令。

- 步骤 *

1. 要启用双向SSL通信、请在SnapCenter服务器上为需要双向SSL通信的插件、服务器和每个代理运行以下命令。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

1. 使用以下命令执行IIS SnapCenter应用程序池回收操作。 `> Restart-WebAppPool -Name "SnapCenter"`
2. 对于Windows插件、运行以下PowerShell命令重新启动SMCore服务：

```
> Restart-Service -Name SnapManagerCoreService
```

禁用双向SSL通信

您可以使用PowerShell命令禁用双向SSL通信。

- 关于此任务 *
- 先对所有插件和SMCore代理执行命令、然后再对服务器执行命令。
- 禁用双向SSL通信时、不会删除CA证书及其配置。
- 要向SnapCenter服务器添加新主机、必须对所有插件主机禁用双向SSL。
- 不支持NLB和F5。
- 步骤 *

1. 要禁用双向SSL通信、请在SnapCenter服务器上对所有插件主机和SnapCenter主机运行以下命令。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

1. 使用以下命令执行IIS SnapCenter应用程序池回收操作。 `> Restart-WebAppPool -Name "SnapCenter"`
2. 对于Windows插件、运行以下PowerShell命令重新启动SMCore服务：

```
> Restart-Service -Name SnapManagerCoreService
```

配置基于证书的身份验证

从**SnapCenter**服务器导出证书颁发机构**(CA)**证书

您应使用Microsoft管理控制台(MMC)将CA证书从SnapCenter服务器导出到插件主机。

开始之前

您应已配置双向SSL。

- 步骤 *
  1. 转到 Microsoft 管理控制台（ MMC ），然后单击 * 文件 * > * 添加 / 删除 Snapin * 。
  2. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
  3. 在"证书管理单元"窗口中，选择*计算机帐户*选项，然后单击*完成*。
  4. 单击*控制台根*>*证书-本地计算机*>*个人*>*证书*。
  5. 右键单击用于SnapCenter服务器的已获得CA证书，然后选择*All Tasks*>*Export*以启动导出向导。
  6. 在向导中执行以下操作。

对于此选项...	执行以下操作 ...
导出私钥	选择*否，不导出私钥*，然后单击*下一步*。
导出文件格式	单击 * 下一步 * 。
文件名	单击*浏览*并指定保存证书的文件路径，然后单击*下一步*。
正在完成证书导出向导	查看摘要，然后单击 * 完成 * 开始导出。

SnapCenter HA配置和适用于VMware vSphere的SnapCenter插件不支持基于证书的身份验证。

将证书颁发机构**(Certificate Authority**、**CA)**证书导入到**Windows**插件主机

要使用导出的SnapCenter服务器CA证书、应使用Microsoft管理控制台(MMC)将相关证书导入到SnapCenter Windows插件主机。

- 步骤 *

1. 转到 Microsoft 管理控制台（ MMC ），然后单击 * 文件 * > * 添加 / 删除 Snapin * 。
2. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
3. 在"证书管理单元"窗口中，选择*计算机帐户*选项，然后单击*完成*。
4. 单击*控制台根*>*证书-本地计算机*>*个人*>*证书*。
5. 右键单击“个人”文件夹，然后选择*All Tasks*>*Import*以启动导入向导。
6. 在向导中执行以下操作。

对于此选项...	执行以下操作 ...
存储位置	单击 * 下一步 * 。
要导入的文件	选择以.cer扩展名结尾的SnapCenter服务器证书。
证书存储	单击 * 下一步 * 。
正在完成证书导出向导	查看摘要，然后单击 * 完成 * 开始导入。

将**CA**证书导入到**UNIX**主机插件、并将根证书或中间证书配置到**SPL**信任存储库

将**CA**证书导入到**UNIX**插件主机

您应将CA证书导入到UNIX插件主机中。

- 关于此任务 *
- 您可以管理SPL密钥库的密码以及正在使用的CA签名密钥对的别名。
- SPL密钥库的密码和专用密钥的所有关联别名密码应相同。
- 步骤 *
  1. 您可以从 SPL 属性文件检索 SPL 密钥库默认密码。它是与密钥对应的值 `SPL_KEYSTORE_PASS`。
  2. 更改密钥库密码： `$ keytool -storepasswd -keystore keystore.jks`
  3. 将密钥库中私钥条目的所有别名的密码更改为密钥库使用的相同密码： `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. 为中的密钥SPL_KEYORE_Pass更新相同的值 `spl.properties`` 文件
  5. 更改密码后重新启动服务。

配置根证书或中间证书以 **SPL** 信任存储

您应将根证书或中间证书配置为SPL信任存储库。您应先添加根 CA 证书，然后再添加中间 CA 证书。

- 步骤 *
  1. 导航到SPL密钥库所在的文件夹： `/var/opt/snapcenter/spl/etc`。

2. 找到文件 `keystore.jks`。
3. 列出密钥库中添加的证书： `$ keytool -list -v -keystore keystore.jks`
4. 添加根证书或中间证书： `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. 将根证书或中间证书配置为 SPL 信任存储后重新启动服务。

将 **CA** 签名密钥对配置为 **SPL** 信任存储

您应将CA签名密钥对配置为SPL信任存储库。

- 步骤 *

1. 导航到SPL密钥库所在的文件夹 `/var/opt/snapcenter/spl/etc`。
2. 找到文件 `keystore.jks`。
3. 列出密钥库中添加的证书： `$ keytool -list -v -keystore keystore.jks`
4. 添加同时具有私钥和公有密钥的 CA 证书。 `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. 列出密钥库中添加的证书。 `$ keytool -list -v -keystore keystore.jks`
6. 验证密钥库是否包含与已添加到密钥库中的新 CA 证书对应的别名。
7. 将为 CA 证书添加的私钥密码更改为密钥库密码。

   默认SPL密钥库密码是输入的SPL_keykeykeyStore传递密钥的值 `spl.properties` 文件

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

1. 如果 CA 证书中的别名较长，并且包含空格或特殊字符（"*"，"，"），请将别名更改为简单名称： `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. 从中的密钥库配置别名 `spl.properties` 文件 根据密钥 SPL_certificate_alias 更新此值。
3. 将 CA 签名密钥对配置为 SPL 信任存储后重新启动服务。

启用基于证书的身份验证

要为SnapCenter服务器和Windows插件主机启用基于证书的身份验证、请运行以下PowerShell cmdlet。 对于Linux插件主机、启用双向SSL后、将启用基于证书的身份验证。

- 启用基于客户端证书的身份验证：

```
Set-SmConfigSettings -Agent –configSettings @{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 禁用基于客户端证书的身份验证：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

配置 Active Directory ， LDAP 和 LDAPS

注册不可信的 Active Directory 域

您应向 SnapCenter 服务器注册 Active Directory ，以管理多个不可信 Active Directory 域中的主机，用户和组。

开始之前

- LDAP 和 LDAPS 协议 *
- 您可以使用 LDAP 或 LDAPS 协议注册不可信的 Active Directory 域。
- 您应已在插件主机和 SnapCenter 服务器之间启用双向通信。
- 应在 SnapCenter 服务器和插件主机之间设置 DNS 解析，反之亦然。
- LDAP 协议 *
- 完全限定域名（ FQDN ）应可从 SnapCenter 服务器解析。

  您可以将不可信域注册到 FQDN 中。如果无法从 SnapCenter 服务器解析 FQDN ，您可以向域控制器 IP 地址注册，此地址应可从 SnapCenter 服务器解析。

- LDAPS 协议 *
- LDAPS 需要 CA 证书才能在活动目录通信期间提供端到端加密。

  "为 LDAPS 配置 CA 客户端证书"

- 域控制器主机名（ DCHostName ）应可从 SnapCenter 服务器访问。
- 关于此任务 *
- 您可以使用 SnapCenter 用户界面， PowerShell cmdlet 或 REST API 注册不可信域。
- 步骤 *
  1. 在左侧导航窗格中，单击 * 设置 * 。
  2. 在设置页面中，单击 * 全局设置 * 。
  3. 在全局设置页面中，单击 * 域设置 * 。
  4. 单击  以注册新域。
  5. 在注册新域页面中，选择 * LDAP * 或 * LDAPS* 。
     a. 如果选择 * LDAP * ，请指定为 LDAP 注册不可信域所需的信息：

对于此字段 ...	执行此操作 ...
域名	指定域的 NetBIOS 名称。
域 FQDN	指定 FQDN 并单击 * 解析 * 。
域控制器 IP 地址	如果无法从 SnapCenter 服务器解析域 FQDN ，请指定一个或多个域控制器 IP 地址。 有关详细信息，请参见 "从图形用户界面中为不可信域添加域控制器 IP"。

b. 如果选择 * LDAP* ，请指定为 LDAPS 注册不可信域所需的信息：

对于此字段 ...	执行此操作 ...
域名	指定域的 NetBIOS 名称。
域 FQDN	指定FQDN。
域控制器名称	指定一个或多个域控制器名称，然后单击 * 解析 * 。
域控制器 IP 地址	如果域控制器名称无法从 SnapCenter 服务器解析，则应更正 DNS 解析。

6. 单击 * 确定 * 。

为 **LDAPS** 配置 **CA** 客户端证书

如果为 SnapCenter Active Directory LDAPS 配置了 CA 证书，则应在 服务器上为 LDAPS 配置 CA 客户端证书。

- 步骤 *

1. 转到 Microsoft 管理控制台（ MMC ），然后单击 * 文件 * > * 添加 / 删除 Snapin * 。
2. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
3. 在证书管理单元窗口中，选择 * 计算机帐户 * 选项，然后单击 * 完成 * 。
4. 单击 * 控制台根 * > * 证书–本地计算机 * > * 可信根证书颁发机构 * > * 证书 * 。
5. 右键单击文件夹 " 可信根证书颁发机构 " ，然后选择 * 所有任务 * > * 导入 * 以启动导入向导。
6. 完成向导，如下所示：

在此向导窗口中 ...	执行以下操作 ...
在向导的第二页中	单击 * 浏览 * ，选择根证书 _ ，然后单击 * 下一步 * 。
正在完成证书导入向导	查看摘要，然后单击 * 完成 * 开始导入。

7. 对中间证书重复步骤5和6。

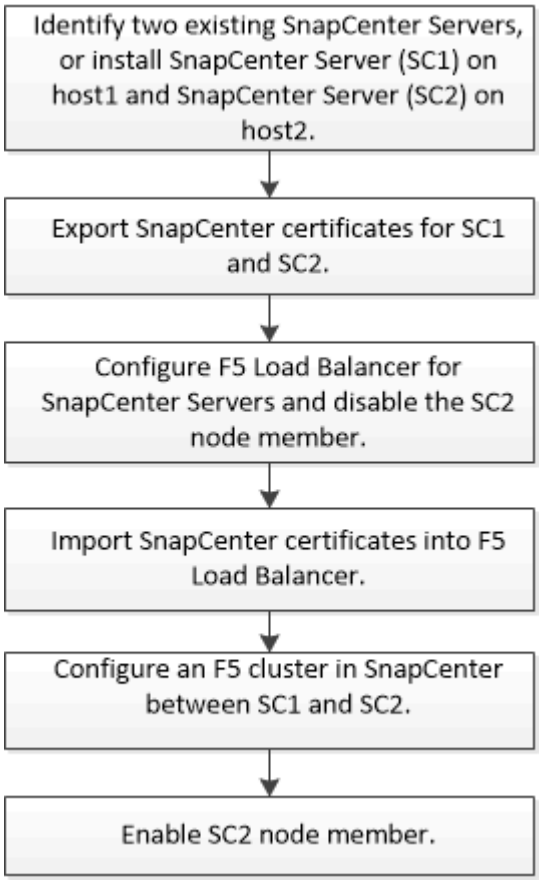
配置高可用性

使用 **F5** 配置 **SnapCenter** 服务器以实现高可用性

要在 SnapCenter 中支持高可用性（ HA ），您可以安装 F5 负载平衡器。F5 允许 SnapCenter 服务器在最多两个位于同一位置的主机中支持主动 - 被动配置。要在 SnapCenter 中使用 F5 负载平衡器，您应配置 SnapCenter 服务器并配置 F5 负载平衡器。

如果您已从 SnapCenter 4.2.x 升级，并且先前使用的是网络负载平衡（ NLB ），则可以继续使用该配置或切换到 F5 。

此工作流图列出了使用 F5 负载平衡器配置 SnapCenter 服务器以实现高可用性的步骤。有关详细说明，请参见 "如何使用 F5 负载平衡器配置 SnapCenter 服务器以实现高可用性"。



您必须是 SnapCenter 服务器上本地管理员组的成员（除了分配给 SnapCenterAdmin 角色之外），才能使用以下 cmdlet 添加和删除 F5 集群：

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

  有关详细信息，请参见 "《 SnapCenter 软件 cmdlet 参考指南》"。

其他 **F5** 配置信息

- 安装并配置 SnapCenter 以实现高可用性后，编辑 SnapCenter 桌面快捷方式以指向 F5 集群 IP 。
- 如果 SnapCenter 服务器之间发生故障转移，并且还存在现有 SnapCenter 会话，则必须关闭浏览器并重新登录到 SnapCenter 。
- 在负载平衡器设置（ NLB 或 F5 ）中，如果您添加的节点已由 NLB 或 F5 节点部分解决，并且 SnapCenter 节点无法访问此节点，则 SnapCenter 主页会频繁在主机关闭和运行状态之间切换。要解决此问题描述，您应确保两个 SnapCenter 节点都能够解析 NLB 或 F5 节点中的主机。
- 应在所有节点上执行用于MFA设置的SnapCenter 命令。应使用F5集群详细信息在Active Directory联合身份验证服务(AD FS)服务器中完成依赖方配置。 启用MFA后、将阻止节点级别的SnapCenter UI访问。
- 在故障转移期间、审核日志设置不会反映在第二个节点上。 因此、当F5被动节点变为活动状态时、您应在该节点上手动重复审核日志设置。

手动配置 **Microsoft** 网络负载平衡器

您可以配置 Microsoft 网络负载平衡（ NLB ）以设置 SnapCenter 高可用性。在 SnapCenter 4.2 中，您应在 SnapCenter 安装之外手动配置 NLB 以实现高可用性。

有关如何使用 SnapCenter 配置网络负载平衡（ NLB ）的信息，请参见 "如何使用 SnapCenter 配置 NLB"。

SnapCenter 4.1.1 或更早版本支持在安装 SnapCenter 时配置网络负载平衡（ NLB ）。

从 **NLB** 切换到 **F5** 以实现高可用性

您可以将 SnapCenter HA 配置从网络负载平衡（ NLB ）更改为使用 F5 负载平衡器。

- 步骤 *
  1. 使用 F5 配置 SnapCenter 服务器以实现高可用性。 "了解更多信息。"。
  2. 在 SnapCenter 服务器主机上，启动 PowerShell 。
  3. 使用 Open-SmConnection cmdlet 启动会话，然后输入凭据。
  4. 使用 Update-SmServerCluster cmdlet 更新 SnapCenter 服务器以指向 F5 集群 IP 地址。

     有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 *get-help command_name* 来获取。或者、您也可以参考 https://docs.netapp.com/us-en/snapcenter-cmdlets-49/index.html

SnapCenter MySQL 存储库的高可用性

MySQL 复制是 MySQL Server 的一项功能，可用于将数据从一个 MySQL 数据库服务器（主）复制到另一个 MySQL 数据库服务器（从）。SnapCenter 仅支持在两个启用了网络负载平衡（启用了 NLB ）的节点上进行 MySQL 复制以实现高可用性。

SnapCenter 对主存储库执行读取或写入操作，并在主存储库出现故障时将其连接路由到从存储库。然后，从存储库将成为主存储库。SnapCenter 还支持反向复制，此功能仅在故障转移期间启用。

如果要使用 MySQL 高可用性（ High Availability ， HA ）功能，必须在第一个节点上配置网络负载平衡器（ Network Load Balancer ， NLB ）。在安装过程中， MySQL 存储库安装在此节点上。在第二个节点上安装 SnapCenter 时，您必须加入第一个节点的 F5 并在第二个节点上创建 MySQL 存储库的副本。

SnapCenter 提供了 *Get-SmRepositoryConfig* 和 *Set-SmRepositoryConfig* PowerShell cmdlet 来管理 MySQL 复制。

有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 *get-help command_name* 来获取。或者，您也可以参考 "《 SnapCenter 软件 cmdlet 参考指南》"。

您必须了解与 MySQL HA 功能相关的限制：

- 两个节点以上不支持 NLB 和 MySQL HA 。
- 不支持从 SnapCenter 独立安装切换到 NLB 安装，反之亦然，也不支持从 MySQL 独立设置切换到 MySQL HA 。
- 如果从存储库数据未与主存储库数据同步，则不支持自动故障转移。

  您可以使用 *set-SmRepositoryConfig* cmdlet 启动强制故障转移。

- 启动故障转移后，正在运行的作业可能会失败。

  如果由于 MySQL 服务器或 SnapCenter 服务器已关闭而发生故障转移，则正在运行的任何作业可能会失败。故障转移到第二个节点后，所有后续作业均会成功运行。

有关配置高可用性的信息，请参见 "如何使用 SnapCenter 配置 NLB 和 ARR"。

导出 SnapCenter 证书

- 步骤 *
  1. 转到 Microsoft 管理控制台 （ MMC ），然后单击 * 文件 * > * 添加 / 删除管理单元 * 。
  2. 在添加或删除管理单元窗口中，选择 * 证书 * ，然后单击 * 添加 * 。
  3. 在证书管理单元窗口中，选择 * 我的用户帐户 * 选项，然后单击 * 完成 * 。
  4. 单击 * 控制台根 * > * 证书 - 当前用户 * > * 可信根证书颁发机构 * > * 证书 * 。
  5. 右键单击具有 SnapCenter 友好名称的证书，然后选择 * 所有任务 * > * 导出 * 以启动导出向导。
  6. 完成向导，如下所示：

在此向导窗口中 ...	执行以下操作 ...
导出私钥	选择 * 是，导出私钥 * 选项，然后单击 * 下一步 * 。
导出文件格式	不进行任何更改；单击 * 下一步 * 。
安全性	指定要用于导出的证书的新密码，然后单击 * 下一步 * 。
要导出的文件	为导出的证书指定文件名（必须使用 .pfx ），然后单击 * 下一步 * 。
正在完成证书导出向导	查看摘要，然后单击 * 完成 * 开始导出。

- 结果 *

证书以 .pfx 格式导出。

配置基于角色的访问控制（ RBAC ）

添加用户或组并分配角色和资产

要为 SnapCenter 用户配置基于角色的访问控制，您可以添加用户或组并分配角色。此角色决定了 SnapCenter 用户可以访问的选项。

开始之前

- 您必须已以 "SnapCenterAdmin" 角色登录。
- 您必须已在操作系统或数据库的 Active Directory 中创建用户或组帐户。您不能使用 SnapCenter 创建这些帐户。

> 从 SnapCenter 4.5 开始，您只能在用户名和组名称中包含以下特殊字符：空格（），连字符（ - ），下划线（ _ ）和冒号（：）。 如果要使用在早期版本的 SnapCenter 中创建的角色以及这些特殊字符，您可以通过在安装 SnapCenter WebApp 的 web.config 文件中将 "DisableSQLInjectionValidation " 参数的值更改为 true 来禁用角色名称验证。修改此值后，您无需重新启动此服务。

- SnapCenter 包括多个预定义角色。

  您可以将这些角色分配给用户，也可以创建新角色。

- 添加到 SnapCenter RBAC 的 AD 用户和 AD 组必须对 Active Directory 中的用户容器和计算机容器具有读取权限。
- 为包含相应权限的用户或组分配角色后，您必须为用户分配对 SnapCenter 资产（例如主机和存储连接）的访问权限。

  这样，用户就可以执行对分配给他们的资产具有权限的操作。

- 您应在某个时刻为用户或组分配一个角色，以利用 RBAC 权限和效率。
- 您可以分配主机，资源组，策略，存储连接，插件， 创建用户或组时提供给用户的凭据。
- 应分配给用户以执行某些操作的最小资产如下：

操作	资产分配
保护资源	主机，策略
备份	主机，资源组，策略
还原	主机，资源组
克隆	主机，资源组，策略
克隆生命周期	host
创建资源组	host

- 将新节点添加到 Windows 集群或 DAG （ Exchange Server 数据库可用性组）资产中后，如果将此新节点分配给用户，则必须将此资产重新分配给用户或组，以便将此新节点包含到用户或组中。

  您应将 RBAC 用户或组重新分配给集群或 DAG ，以便将新节点包含给 RBAC 用户或组。例如，您有一个双节点集群，并且已为此集群分配 RBAC 用户或组。向集群添加另一个节点时，应将 RBAC 用户或组重新分配给集群，以便为 RBAC 用户或组添加新节点。

- 如果您计划复制 Snapshot 副本，则必须将源卷和目标卷的存储连接分配给执行此操作的用户。

  您应先添加资产，然后再为用户分配访问权限。

如果您使用适用于 VMware vSphere 的 SnapCenter 插件功能来保护 VM ， VMDK 或数据存储库，则应使用 VMware vSphere GUI 将 vCenter 用户添加到适用于 VMware vSphere 的 SnapCenter 插件角色中。有关 VMware vSphere 角色的信息，请参见 "适用于 VMware vSphere 的 SnapCenter 插件附带的预定义角色"。

- 步骤 *

1. 在左侧导航窗格中，单击 * 设置 * 。
2. 在设置页面中，单击 * 用户和访问 * > 
3. 在从 Active Directory 或工作组添加用户 / 组页面中：

对于此字段 ...	执行此操作 ...
访问类型	选择域或工作组 对于域身份验证类型，您应指定要将用户添加到角色的用户或组的域名。 默认情况下，它会预先填充已登录的域名。 您必须在 * 设置 * > * 全局设置 * > * 域设置 * 页面中注册不可信域。
Type	选择用户或组 SnapCenter 仅支持安全组，而不支持分发组。
用户名	a. 键入部分用户名，然后单击 * 添加 * 。 用户名区分大小写。 b. 从搜索列表中选择用户名。 在添加来自其他域或不可信域的用户时，应完整键入用户名，因为没有跨域用户的搜索列表。 重复此步骤，向选定角色添加其他用户或组。
角色	选择要将用户添加到的角色。

4. 单击 * 分配 * ，然后在分配资产页面中：
   a. 从 * 资产 * 下拉列表中选择资产类型。
   b. 在资产表中，选择资产。

      只有在用户已将资产添加到 SnapCenter 后，才会列出这些资产。

   c. 对所有所需资产重复此操作步骤。
   d. 单击 * 保存 * 。
5. 单击 * 提交 * 。

添加用户或组并分配角色后，刷新资源列表。

创建角色

除了使用现有 SnapCenter 角色之外，您还可以创建自己的角色并自定义权限。

您应已以 "SnapCenterAdmin" 角色登录。

- 步骤 *

1. 在左侧导航窗格中，单击 * 设置 * 。
2. 在设置页面中，单击 * 角色 * 。
3. 单击 。
4. 在添加角色页面中，指定新角色的名称和问题描述。

> 从 SnapCenter 4.5 开始，您只能在用户名和组名称中包含以下特殊字符：空格（），连字符（ - ），下划线（ _ ）和冒号（：）。 如果要使用在早期版本的 SnapCenter 中创建的角色以及这些特殊字符，您可以通过在安装 SnapCenter WebApp 的 web.config 文件中将 "DisableSQLInjectionValidation " 参数的值更改为 true 来禁用角色名称验证。修改此值后，您无需重新启动此服务。

5. 选择 * 此角色的所有成员均可查看其他成员的对象 * ，以使该角色的其他成员能够在刷新资源列表后查看卷和主机等资源。

   如果不希望此角色的成员查看分配给其他成员的对象，则应取消选择此选项。

> 启用此选项后，如果用户与创建对象或资源的用户具有相同的角色，则不需要为用户分配对对象或资源的访问权限。

1. 在权限页面中，选择要分配给角色的权限，或者单击 * 全选 * 授予该角色的所有权限。
2. 单击 * 提交 * 。

使用 **security login** 命令添加 **ONTAP RBAC** 角色

如果存储系统运行的是集群模式 ONTAP ，则可以使用 security login 命令添加 ONTAP RBAC 角色。

开始之前

- 在为运行集群模式 ONTAP 的存储系统创建 ONTAP RBAC 角色之前，您必须确定以下内容：
  - 要执行的一项或多项任务
  - 执行这些任务所需的权限
- 配置 RBAC 角色需要执行以下操作：
  - 为命令和 / 或命令目录授予权限。

    每个命令 / 命令目录有两个访问级别： all-access 和 read-only 。

您必须始终先分配所有访问权限。

- 为用户分配角色。
- 根据 SnapCenter 插件是连接到整个集群的集群管理员 IP 还是直接连接到集群中的 SVM ，更改您的配置。

• 关于此任务 *

要简化在存储系统上配置这些角色的过程，您可以使用适用于 Data ONTAP 的 RBAC User Creator 工具，该工具已发布在 NetApp 社区论坛上。

此工具会自动正确设置 ONTAP 权限。例如，适用于 Data ONTAP 的 RBAC User Creator 工具会自动按正确顺序添加权限，以便首先显示所有访问权限。如果先添加只读权限，然后再添加纯访问权限，则 ONTAP 会将纯访问权限标记为重复项并忽略它们。

如果稍后升级 SnapCenter 或 ONTAP ，则应重新运行适用于 Data ONTAP 的 RBAC 用户创建程序工具以更新先前创建的用户角色。为早期版本的 SnapCenter 或 ONTAP 创建的用户角色无法在升级后的版本中正常工作。重新运行此工具时，它会自动处理升级。您无需重新创建角色。

有关设置 ONTAP RBAC 角色的详细信息，请参见 "《 ONTAP 9 管理员身份验证和 RBAC 高级指南》"。

为了确保一致性， SnapCenter 文档将角色称为使用特权。OnCommand 系统管理器图形用户界面使用术语_attribute_、而不是_privilege。设置ONTAP RBAC角色时、这两个术语的含义相同。

• 步骤 *

1. 在存储系统上，输入以下命令以创建新角色：

```
security login role create <role_name\> -cmddirname "command" -access all
-vserver <svm_name\>
```

   - svm_name 是 SVM 的名称。如果将此字段留空，则默认为集群管理员。
   - role_name 是为角色指定的名称。
   - command 是 ONTAP 功能。

     您必须对每个权限重复此命令。请记住，必须先列出所有访问命令，然后再列出只读命令。

   有关权限列表的信息，请参见 "用于创建角色和分配权限的 ONTAP 命令行界面命令"。

2. 输入以下命令创建用户名：

```
security login create -username <user_name\> -application ontapi -authmethod
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
"user_description"
```

   - user_name 是要创建的用户的名称。
   - <password> 是您的密码。如果不指定密码，系统将提示您输入一个密码。
   - svm_name 是 SVM 的名称。

3. 输入以下命令，将角色分配给用户：

```
security login modify username <user_name\> -vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod
<password\>
```

- <user_name> 是您在步骤 2 中创建的用户的名称。此命令可用于修改用户以将其与角色关联。
- <SVM_name> 是 SVM 的名称。
- <role_name> 是您在步骤 1 中创建的角色的名称。
- <password> 是您的密码。如果不指定密码，系统将提示您输入一个密码。

4. 输入以下命令，验证是否已正确创建用户：

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

user_name 是您在步骤 3 中创建的用户的名称。

创建具有最低权限的 **SVM** 角色

在 ONTAP 中为新 SVM 用户创建角色时，必须运行多个 ONTAP 命令行界面命令。如果您在 ONTAP 中将 SVM 配置为与 SnapCenter 结合使用，而您不想使用 vsadmin 角色，则需要此角色。

- 步骤 *

1. 在存储系统上，创建一个角色并为该角色分配所有权限。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

您应对每个权限重复此命令。

1. 创建一个用户并将该角色分配给该用户。

```
security login create -user <user_name\> -vserver <svm_name\> -application
ontapi -authmethod password -role <SVM_Role_Name\>
```

2. 解除用户锁定。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

用于创建 **SVM** 角色和分配权限的 **ONTAP** 命令行界面命令

您应运行多个 ONTAP 命令行界面命令来创建 SVM 角色并分配权限。

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"job history show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume modify" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`

创建具有最低权限的 ONTAP 集群角色

您应创建一个具有最低权限的 ONTAP 集群角色，以便不必使用 ONTAP 管理员角色在 SnapCenter 中执行操作。您可以运行多个 ONTAP 命令行界面命令来创建 ONTAP 集群角色并分配最低权限。

- 步骤 *

1. 在存储系统上，创建一个角色并为该角色分配所有权限。

```
security login role create -vserver <cluster_name\>- role <role_name\>
-cmddirname <permission\>
```

> 您应对每个权限重复此命令。

1. 创建一个用户并将该角色分配给该用户。

```
security login create -user <user_name\> -vserver <cluster_name\>
-application ontapi -authmethod password -role <role_name\>
```

2. 解除用户锁定。

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

用于创建集群角色和分配权限的 **ONTAP** 命令行界面命令

您应运行多个 ONTAP 命令行界面命令来创建集群角色和分配权限。

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"snapmirror policy add-rule" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume snapshot promote" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

配置 **IIS** 应用程序池以启用 **Active Directory** 读取权限

如果需要为 SnapCenter 启用 Active Directory 读取权限，您可以在 Windows 服务器上配置 Internet 信息服务（ Internet Information Services ， IIS ）以创建自定义应用程序池帐户。

- 步骤 *
  1. 在安装了 SnapCenter 的 Windows 服务器上打开 IIS 管理器。
  2. 在左侧导航窗格中，单击 * 应用程序池 * 。
  3. 在应用程序池列表中选择 SnapCenter ，然后单击操作窗格中的 * 高级设置 * 。
  4. 选择身份，然后单击 * 。 * 以编辑 SnapCenter 应用程序池标识。
  5. 在自定义帐户字段中，输入具有 Active Directory 读取权限的域用户或域管理员帐户名称。
  6. 单击确定。

     自定义帐户将替换 SnapCenter 应用程序池的内置 ApplicationPoolIdentity 帐户。

配置审核日志设置

系统会为SnapCenter 服务器的每个活动生成审核日志。默认情况下、审核日志会在默认安装位置_C：\Program Files\NetApp\SnapCenter WebApp\audit中受到保护。

通过为每个审核事件生成数字签名摘要来保护审核日志、防止未经授权的修改。生成的摘要保存在单独的审核校验和文件中、并定期进行完整性检查以确保内容的完整性。

您应已以 "SnapCenterAdmin" 角色登录。

- 关于此任务 *
- 在以下情况下会发送警报：
  - 已启用或禁用审核日志完整性检查计划或系统日志服务器

- 审核日志完整性检查、审核日志或系统日志服务器日志失败
- 磁盘空间不足

- 只有在完整性检查失败时、才会发送电子邮件。
- 您应同时修改审核日志目录和审核校验和日志目录路径。您不能仅修改其中一个。
- 修改审核日志目录和审核校验和日志目录路径后、无法对早期位置的审核日志执行完整性检查。
- 审核日志目录和审核校验和日志目录路径应位于SnapCenter 服务器的本地驱动器上。

  不支持共享驱动器或网络挂载驱动器。

- 如果在系统日志服务器设置中使用UDP协议、则由于端口关闭或不可用而导致的错误无法在SnapCenter 中捕获为错误或警报。
- 您可以使用Set-SmAuditSettings和Get－SmAuditSettings命令配置审核日志。

  有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 get-help command_name 来获取。或者，您也可以参考 "《 SnapCenter 软件 cmdlet 参考指南》"。

- 步骤 *

1. 在*设置*页面中、导航到*设置*>*全局设置*>*审核日志设置*。
2. 在Audit log部分中、输入详细信息。
3. 输入*审核日志目录*和*审核校验和日志目录*
   a. 输入最大文件大小
   b. 输入最大日志文件数
   c. 输入要发送警报的磁盘空间使用量百分比
4. (可选)启用*记录UTC时间*。
5. (可选)启用*审核日志完整性检查计划*并单击*启动完整性检查*以进行按需完整性检查。

   您还可以运行*启动-小型审核集成检查*命令来启动按需完整性检查。

6. (可选)启用转发到远程系统日志服务器的审核日志并输入系统日志服务器详细信息。

   您应将证书从系统日志服务器导入到TLS 1.2协议的"可信根"中。

   a. 输入系统日志服务器主机
   b. 输入系统日志服务器端口
   c. 输入系统日志服务器协议
   d. 输入RFC格式
7. 单击 * 保存 * 。
8. 您可以通过单击*监控*>*作业*来查看审核完整性检查和磁盘空间检查。

添加存储系统

您应设置存储系统，使 SnapCenter 能够访问 ONTAP 存储或适用于 NetApp ONTAP 的 Amazon FSX ，以执行数据保护和配置操作。

您可以添加一个独立 SVM ，也可以添加一个由多个 SVM 组成的集群。如果您使用的是适用于 NetApp ONTAP 的 Amazon FSX ，则可以使用 fsxadmin 帐户添加由多个 SVM 组成的 FSX 管理 LIF ，也可以在 SnapCenter 中添加 FSX SVM 。

开始之前

- 您应具有创建存储连接所需的基础架构管理员角色权限。
- 您应确保插件安装未在进行中。

  添加存储系统连接时，主机插件安装不得正在进行中，因为主机缓存可能不会更新，并且数据库状态可能会在 SnapCenter 图形用户界面中显示为 "`不可用于备份` " 或 "`不在 NetApp 存储` 上 " 。

- 存储系统名称应是唯一的。

  SnapCenter 不支持在不同集群上使用相同名称的多个存储系统。SnapCenter 支持的每个存储系统都应具有唯一的名称和唯一的数据 LIF IP 地址。

- 关于此任务 *
- 配置存储系统时，您还可以启用事件管理系统（ EMS ）和 AutoSupport 功能。AutoSupport 工具可收集有关系统运行状况的数据，并自动将这些数据发送给 NetApp 技术支持，使其能够对系统进行故障排除。

  如果启用了这些功能，则在资源受保护，还原或克隆操作成功完成或操作失败时， SnapCenter 会将 AutoSupport 信息发送到存储系统，并将 EMS 消息发送到存储系统系统系统日志。

- 如果您计划将 Snapshot 副本复制到 SnapMirror 目标或 SnapVault 目标，则必须为目标 SVM 或集群以及源 SVM 或集群设置存储系统连接。

  如果更改存储系统密码，计划的作业，按需备份和还原操作可能会失败。更改存储系统密码后，您可以通过单击存储选项卡中的 * 修改 * 来更新密码。

- 步骤 *

1. 在左侧导航窗格中，单击 * 存储系统 * 。
2. 在存储系统页面中，单击 * 新建 * 。
3. 在添加存储系统页面中，提供以下信息：

对于此字段 ...	执行此操作 ...
存储系统	输入存储系统名称或 IP 地址。 存储系统名称(不包括域名)必须包含15个或更少字符、并且这些名称必须可进行析。要创建名称包含超过 15 个字符的存储系统连接，可以使用 Add-SmStorageConnectionPowerShell cmdlet 。 对于采用 MetroCluster 配置（ MCC ）的存储系统，建议同时注册本地集群和对等集群，以实现无中断运行。 SnapCenter 不支持在不同集群上使用相同名称的多个 SVM 。SnapCenter 支持的每个 SVM 都必须具有唯一的名称。 将存储连接添加到 SnapCenter 后，不应使用 ONTAP 重命名 SVM 或集群。 如果添加的 SVM 使用短名称或 FQDN ，则必须可从 SnapCenter 和插件主机解析此 SVM 。
用户名 / 密码	输入具有访问存储系统所需权限的存储用户的凭据。
事件管理系统（ EMS ）和 AutoSupport 设置	如果要将 EMS 消息发送到存储系统系统系统日志，或者要将 AutoSupport 消息发送到存储系统以应用保护，完成还原操作或失败操作，请选中相应的复选框。 如果选中 * 向存储系统发送失败操作的 AutoSupport 通知 * 复选框，则还会选中 * 将 SnapCenter 服务器事件记录到系统日志 * 复选框，因为要启用 AutoSupport 通知，需要 EMS 消息传送。

4. 如果要修改分配给平台，协议，端口和超时的默认值，请单击 * 更多选项 * 。
   a. 在平台中，从下拉列表中选择一个选项。

      如果 SVM 是备份关系中的二级存储系统，请选中 * 二级 * 复选框。如果选择 * 二级 * 选项，则 SnapCenter 不会立即执行许可证检查。

如果您已在SnapCenter中添加SVM、则用户需要从下拉列表中手动选择平台类型。

a. 在协议中，选择在 SVM 或集群设置期间配置的协议，通常为 HTTPS 。
b. 输入存储系统可接受的端口。

   默认端口 443 通常有效。

c. 输入暂停通信尝试之前应经过的时间（以秒为单位）。

   默认值为60秒。

d. 如果 SVM 具有多个管理接口，请选中 * 首选 IP* 复选框，然后输入 SVM 连接的首选 IP 地址。
e. 单击 * 保存 * 。
   1. 单击 * 提交 * 。

- 结果 *

在存储系统页面中，从 * 类型 * 下拉列表中执行以下操作之一：

- 如果要查看已添加的所有 ONTAP SVM* ，请选择 * SVM* 。

  如果已添加 FSX SVM ，此处将列出 FSX SVM 。

- 如果要查看已添加的所有集群，请选择 * ONTAP Clusters* 。

  如果您已使用 fsxadmin 添加 FSX 集群，此处将列出 FSX 集群。

  单击集群名称后，属于集群的所有 SVM 都会显示在 Storage Virtual Machine 部分中。

  如果使用 ONTAP 图形用户界面将新的 SVM 添加到 ONTAP 集群中，请单击 * 重新发现 * 以查看新添加的 SVM 。

如果已将FAS或AFF存储系统升级到全SAN阵列(ASA)、则必须刷新SnapCenter服务器中的存储连接、以在SnapCenter中反映新的存储类型。

- 完成后 *

集群管理员必须在每个存储系统节点上启用 AutoSupport ，才能通过在存储系统命令行中运行以下命令从 SnapCenter 有权访问的所有存储系统发送电子邮件通知：

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```

Storage Virtual Machine （ SVM ）管理员无法访问 AutoSupport 。

添加基于 SnapCenter 标准控制器的许可证

如果您使用的是FAS、AFF或全SAN阵列(ASA)存储控制器、则需要一个基于控制器的SnapCenter标准许可证。

基于控制器的许可证具有以下特征：

- 购买高级版或闪存捆绑包时附带的 SnapCenter 标准权益（不随基础包一起提供）
- 存储使用量无限制
- 可通过使用ONTAP系统管理器或存储集群命令行将其直接添加到FAS、AFF或ASA存储控制器来启用

> 对于基于 SnapCenter 控制器的许可证，您不会在 SnapCenter 图形用户界面中输入任何许可证信息。

- 锁定到控制器的序列号

有关所需许可证的信息，请参见 "SnapCenter 许可证"。

第1步：验证是否已安装SnapManager 套件许可证

您可以使用SnapCenter图形用户界面查看FAS、AFF或ASA主存储系统上是否安装了SnapManager套件许可证、并确定哪些存储系统可能需要SnapManager套件许可证。SnapManager套件许可证仅适用于主存储系统上的FAS、AFF和ASA SVM或集群。

> 如果您的控制器上已安装 SnapManagerSuite 许可证，则系统会自动提供基于 SnapCenter 标准控制器的许可证授权。SnapManagerSuite 许可证和基于 SnapCenter 标准控制器的许可证这两个名称可以互换使用，但它们表示的是同一个许可证。

步骤

1. 在左侧导航窗格中，选择*存储系统*。
2. 在存储系统页面的 * 类型 * 下拉列表中，选择是要查看已添加的所有 SVM 还是集群：
   - 要查看已添加的所有 SVM ，请选择 * ONTAP SVM* 。
   - 要查看已添加的所有集群，请选择 * ONTAP Clusters* 。

     选择集群名称后、集群中的所有SVM都会显示在Storage Virtual Machine部分中。
3. 在存储连接列表中，找到控制器许可证列。

   控制器许可证列显示以下状态：

   -  表示SnapManager套件许可证安装在FAS、AFF或ASA主存储系统上。
   -  表示FAS、AFF或ASA主存储系统上未安装SnapManager套件许可证。
   - 不适用表示 SnapManager 套件许可证不适用，因为存储控制器位于 Cloud Volumes ONTAP ， ONTAP Select 或二级存储平台上。

第2步：确定控制器上安装的许可证

您可以使用 ONTAP 命令行查看控制器上安装的所有许可证。您应该是FAS、AFF或ASA系统的集群管理员。

基于 SnapCenter 标准控制器的许可证在控制器上显示为 SnapManagerSuite 许可证。

步骤

1. 使用 ONTAP 命令行登录到 NetApp 控制器。
2. 输入 license show 命令，然后查看输出以确定是否已安装 SnapManagerSuite 许可证。

   示例输出

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
Base              site     Cluster Base License     -

Serial Number: 1-81-0000000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

   在此示例中，安装了 SnapManagerSuite 许可证，因此无需执行其他 SnapCenter 许可操作。

第3步：检索控制器序列号

您需要具有控制器序列号才能检索基于控制器的许可证的序列号。您可以使用 ONTAP 命令行检索控制器序列号。您应该是FAS、AFF或ASA系统的集群管理员。

步骤

1. 使用 ONTAP 命令行登录到控制器。
2. 输入 system show -instance 命令，然后查看输出以查找控制器序列号。

示例输出

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. 记录序列号。

第4步：检索基于控制器的许可证的序列号

如果您使用的是 FAS 或 AFF 存储，则可以先从 NetApp 支持站点检索基于 SnapCenter 控制器的许可证，然后再使用 ONTAP 命令行进行安装。

开始之前

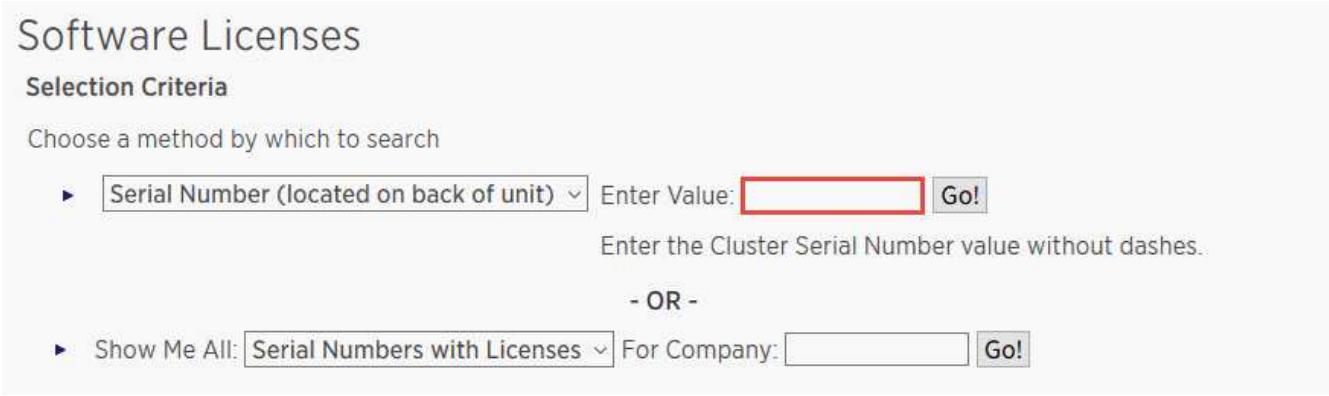
- 您应具有有效的 NetApp 支持站点登录凭据。

如果未输入有效凭据，则不会为搜索返回任何信息。

- 您应具有控制器序列号。

步骤

1. 登录到 "NetApp 支持站点"。
2. 导航到 * 系统 * > * 软件许可证 * 。
3. 在"Selection Criteral"(选择条件)区域中，确保选择了"Serial Number"(序列号)(位于设备背面)，输入控制器序列号，然后选择*GO！*。



此时将显示指定控制器的许可证列表。

4. 找到并记录 SnapCenter 标准版或 SnapManagerSuite 许可证。

第5步：添加基于控制器的许可证

如果您使用的是FAS、AFF或ASA系统、并且拥有SnapCenter标准版或SnapManagerSuite许可证、则可以使用ONTAP命令行添加基于SnapCenter控制器的许可证。

开始之前

- 您应该是FAS、AFF或ASA系统的集群管理员。
- 您应具有 SnapCenter 标准版或 SnapManagerSuite 许可证。

关于此任务

如果您要使用FAS、AFF或ASA存储试用SnapCenter、则可以获取超值包评估许可证、以便在控制器上安装。

如果要试用 SnapCenter ，应联系销售代表以获取要在控制器上安装的超值包评估许可证。

步骤

1. 使用 ONTAP 命令行登录到 NetApp 集群。
2. 添加 SnapManagerSuite 许可证密钥：

```
system license add -license-code license_key
```

此命令可在管理员权限级别使用。

3. 验证是否已安装 SnapManagerSuite 许可证：

```
license show
```

第6步：删除试用许可证

如果您使用的是基于控制器的 SnapCenter 标准许可证，并且需要删除基于容量的试用许可证（序列号以 "`50` " 结尾），则应使用 MySQL 命令手动删除此试用许可证。无法使用 SnapCenter 图形用户界面删除试用许可证。

> 只有在使用基于 SnapCenter 标准控制器的许可证时，才需要手动删除试用许可证。如果您购买了基于 SnapCenter 标准容量的许可证并将其添加到 SnapCenter 图形用户界面中，则试用许可证将自动被覆盖。

步骤

1. 在 SnapCenter 服务器上，打开 PowerShell 窗口以重置 MySQL 密码。
   a. 运行 Open-SmConnection cmdlet ，为 SnapCenterAdmin 帐户启动与 SnapCenter 服务器的连接会话。
   b. 运行 Set-SmRepositoryPassword 以重置 MySQL 密码。

      有关cmdlet的信息，请参见 "《 SnapCenter 软件 cmdlet 参考指南》"。
2. 打开命令提示符并运行 mysql -u root -p 以登录到 MySQL 。

   MySQL 将提示您输入密码。输入在重置密码时提供的凭据。
3. 从数据库中删除试用许可证：

   ```
   use nsm;``DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
   ```

添加基于 SnapCenter 标准容量的许可证

您可以使用 SnapCenter 标准容量许可证来保护 ONTAP Select 和 Cloud Volumes ONTAP 平台上的数据。

容量许可证具有以下特征：

- 由一个九位数序列号组成，格式为 51xxxxxxx

  您可以使用许可证序列号和有效的 NetApp 支持站点登录凭据通过 SnapCenter 图形用户界面启用许可证。
- 作为单独的永久许可证提供，成本基于已用存储容量或要保护的数据大小（以较低者为准），并且数据由 SnapCenter 管理
- 每 TB 可用

  例如，您可以获取 1 TB ， 2 TB ， 4 TB 等基于容量的许可证。
- 提供 90 天试用许可证，可获得 100 TB 容量授权

  有关所需许可证的信息，请参见 "SnapCenter 许可证"。

SnapCenter 每天午夜自动计算其管理的 ONTAP Select 和 Cloud Volumes ONTAP 存储的容量使用量。使用标准容量许可证时， SnapCenter 会从总许可容量中扣除所有卷上的已用容量，从而计算未用容量。如果已用容量超过许可容量， SnapCenter 信息板上将显示过度使用警告。如果您在 SnapCenter 中配置了容量阈值和通知，则在已用容量达到您指定的阈值时，系统会发送电子邮件。

第1步：计算容量要求

在获取基于 SnapCenter 容量的许可证之前，您应计算要由 SnapCenter 管理的主机上的容量。

您应是 Cloud Volumes ONTAP 或 ONTAP Select 系统上的集群管理员。

关于此任务

SnapCenter 将计算实际使用的容量。如果文件系统或数据库的大小为 1 TB ，但仅使用了 500 GB 的空间，则 SnapCenter 将计算 500 GB 的已用容量。卷容量是在重复数据删除和数据压缩之后计算得出的，它基于整个卷的已用容量。

步骤

1. 使用 ONTAP 命令行登录到 NetApp 控制器。
2. 要查看已用卷容量，请输入命令。

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

这两个卷的总已用容量小于 5 TB ；因此，如果要保护所有 5 TB 的数据，则基于 SnapCenter 容量的最低许可证要求为 5 TB 。

但是，如果您只想保护已用总容量 5 TB 中的 2 TB ，则可以获取 2 TB 基于容量的许可证。

第2步：检索基于容量的许可证的序列号

您的订单确认函或文档包中提供了基于 SnapCenter 容量的许可证序列号；但是，如果您没有此序列号，则可以从 NetApp 支持站点检索此序列号。

您应具有有效的 NetApp 支持站点登录凭据。

步骤

1. 登录到 "NetApp 支持站点"。
2. 导航到 * 系统 * > * 软件许可证 * 。
3. 在选择条件区域中，从全部显示：序列号和许可证下拉菜单中选择 * SC_STANDARE* 。

4. 键入您的公司名称，然后选择*GO！*。

   显示格式为 51xxxxxxx 的九位 SnapCenter 许可证序列号。

5. 记录序列号。

第**3**步：生成**NetApp**许可证文件

如果您不想在SnapCenter 图形用户界面中输入NetApp 支持站点 凭据和SnapCenter 许可证序列号、或者无法从SnapCenter 通过Internet访问NetApp 支持站点 、则可以生成NetApp许可证文件(NLG)。然后、您可以将文件下载并存储在可从SnapCenter 主机访问的位置。

开始之前

- 您应将 SnapCenter 与 ONTAP Select 或 Cloud Volumes ONTAP 结合使用。
- 您应具有有效的 NetApp 支持站点登录凭据。
- 您应具有格式为 51xxxxxxx 的九位数许可证序列号。

步骤

1. 导航到 "NetApp 许可证文件生成器"。
2. 输入所需信息。
3. 在产品线字段中，从下拉菜单中选择 * SnapCenter 标准（基于容量） * 。
4. 在产品序列号字段中，输入 SnapCenter 许可证序列号
5. 阅读并接受NetApp数据隐私政策、然后选择*提交*。
6. 保存许可证文件，然后记录文件位置。

第**4**步：添加基于容量的许可证

如果您将 SnapCenter 与 ONTAP Select 或 Cloud Volumes ONTAP 平台结合使用，则应安装一个或多个基于 SnapCenter 容量的许可证。

开始之前

- 您应以 SnapCenter 管理员用户身份登录。
- 您应具有有效的 NetApp 支持站点登录凭据。
- 您应具有格式为 51xxxxxxx 的九位数许可证序列号。

如果您使用 NetApp 许可证文件（ NLF ）添加许可证，则应知道许可证文件的位置。

关于此任务

您可以在设置页面中执行以下任务：

- 添加许可证
- 查看许可证详细信息以快速查找有关每个许可证的信息。
- 如果要替换现有许可证，例如，要更新许可证容量或更改阈值通知设置，请修改许可证。
- 如果要替换现有许可证或不再需要许可证，请删除此许可证。

无法使用 SnapCenter 图形用户界面删除试用许可证（序列号以 50 结尾）。添加已获取的基于 SnapCenter 标准容量的许可时，试用许可证会自动被覆盖。

步骤

1. 在左侧导航窗格中，选择*Settings*。
2. 在设置页面中，选择*软件*。
3. 在“软件”页面的“许可证”部分中，选择*Add*。
4. 在添加 SnapCenter 许可证向导中，选择以下方法之一以获取要添加的许可证：

对于此字段 ...	执行此操作 ...
输入 NetApp 支持站点 (NSS) 登录凭据以导入许可证	a. 输入您的 NSS 用户名。 b. 输入 NSS 密码。 c. 输入基于控制器的许可证的序列号。
NetApp 许可证文件	a. 浏览到许可证文件的位置，然后选择它。 b. 选择 * 打开 * 。

5. 在 Notifications 页面中，输入 SnapCenter 发送电子邮件， EMS 和 AutoSupport 通知的容量阈值。

   默认阈值为 90% 。

6. 要为电子邮件通知配置SMTP服务器，请选择*Settings*>*Global Settings*>*Notification Server Settings*，然后输入以下详细信息：

对于此字段 ...	执行此操作 ...
电子邮件首选项	选择 * 始终 * 或 * 从不 * 。

对于此字段 ...	执行此操作 ...
提供电子邮件设置	如果选择 * 始终 * ，请指定以下内容： • 发件人电子邮件地址 • 收件人电子邮件地址 • 可选：编辑默认主题行 默认主题如下所示： SnapCenter 许可证容量通知。

7. 如果要将事件管理系统（ EMS ）消息发送到存储系统系统系统日志或将 AutoSupport 消息发送到存储系统以处理失败的操作，请选中相应的复选框。建议启用AutoSupport 以帮助您解决可能遇到的问题。
8. 选择 * 下一步 * 。
9. 查看摘要，然后选择*完成*。

配置存储系统

在 **Windows** 主机上配置存储

配置 **LUN** 存储

您可以使用 SnapCenter 配置 FC 连接或 iSCSI 连接的 LUN 。您还可以使用 SnapCenter 将现有 LUN 连接到 Windows 主机。

LUN 是 SAN 配置中的基本存储单元。Windows 主机将系统上的 LUN 视为虚拟磁盘。有关详细信息，请参见 "《 ONTAP 9 SAN 配置指南》"。

建立 **iSCSI** 会话

如果您使用 iSCSI 连接到 LUN ，则必须在创建 LUN 之前建立 iSCSI 会话以启用通信。

- 开始之前 *
- 您必须已将存储系统节点定义为 iSCSI 目标。
- 您必须已在存储系统上启动 iSCSI 服务。 "了解更多信息。"
- 关于此任务 *

您只能在从 IPv6 到 IPv6 或从 IPv4 到 IPv4 的相同 IP 版本之间建立 iSCSI 会话。

您可以使用链路本地 IPv6 地址进行 iSCSI 会话管理，并且只有当主机和目标位于同一子网中时，才能在两者之间进行通信。

如果更改 iSCSI 启动程序的名称，对 iSCSI 目标的访问将受到影响。更改名称后，您可能需要重新配置启动程序访问的目标，以便它们能够识别新名称。更改 iSCSI 启动程序的名称后，必须确保重新启动主机。

如果主机具有多个 iSCSI 接口，则在使用第一个接口上的 IP 地址与 SnapCenter 建立 iSCSI 会话后，您将无法

使用其他 IP 地址从另一个接口建立 iSCSI 会话。

- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 在主机页面中，单击 * iSCSI 会话 * 。
3. 从 * Storage Virtual Machine* 下拉列表中，选择 iSCSI 目标的 Storage Virtual Machine （ SVM ）。
4. 从 * 主机 * 下拉列表中，选择会话的主机。
5. 单击 * 建立会话 * 。

   此时将显示建立会话向导。

6. 在建立会话向导中，确定目标：

在此字段中 ...	输入 ...
目标节点名称	iSCSI 目标的节点名称 如果存在现有目标节点名称，则此名称将以只读格式显示。
目标门户地址	目标网络门户的 IP 地址
目标门户端口	目标网络门户的 TCP 端口
启动程序门户地址	启动程序网络门户的 IP 地址

7. 对输入内容感到满意后，单击 * 连接 * 。

   SnapCenter 将建立 iSCSI 会话。

8. 重复此操作步骤，为每个目标建立一个会话。

断开 **iSCSI** 会话的连接

有时，您可能需要将 iSCSI 会话与具有多个会话的目标断开连接。

- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 在主机页面中，单击 * iSCSI 会话 * 。
3. 从 * Storage Virtual Machine* 下拉列表中，选择 iSCSI 目标的 Storage Virtual Machine （ SVM ）。
4. 从 * 主机 * 下拉列表中，选择会话的主机。
5. 从 iSCSI 会话列表中，选择要断开连接的会话，然后单击 * 断开会话 * 。
6. 在断开会话对话框中，单击 * 确定 * 。

   SnapCenter 会断开 iSCSI 会话的连接。

创建和管理 igroup

您可以创建启动程序组（ igroup ）来指定哪些主机可以访问存储系统上的给定 LUN 。您可以使用 SnapCenter 在 Windows 主机上创建，重命名，修改或删除 igroup 。

创建 igroup

您可以使用 SnapCenter 在 Windows 主机上创建 igroup 。将 igroup 映射到 LUN 时，可以在创建磁盘或连接磁盘向导中使用此 igroup 。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。
  2. 在主机页面中，单击 * igroup* 。
  3. 在启动程序组页面中，单击 * 新建 * 。
  4. 在创建 igroup 对话框中，定义 igroup ：

在此字段中 ...	执行此操作 ...
存储系统	为要映射到 igroup 的 LUN 选择 SVM 。
主机	选择要创建 igroup 的主机。
igroup 名称	输入 igroup 的名称。
启动程序	选择启动程序。
Type	选择启动程序类型 iSCSI ， FCP 或混合（ FCP 和 iSCSI ）。

  5. 对输入的内容感到满意后，单击 * 确定 * 。

     SnapCenter 会在存储系统上创建 igroup 。

重命名 igroup

您可以使用 SnapCenter 重命名现有 igroup 。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。
  2. 在主机页面中，单击 * igroup* 。
  3. 在启动程序组页面中，单击 * Storage Virtual Machine* 字段以显示可用 SVM 的列表，然后为要重命名的 igroup 选择 SVM 。
  4. 在 SVM 的 igroup 列表中，选择要重命名的 igroup ，然后单击 * 重命名 * 。
  5. 在重命名 igroup 对话框中，输入 igroup 的新名称，然后单击 * 重命名 * 。

修改 **igroup**

您可以使用 SnapCenter 向现有 igroup 添加 igroup 启动程序。创建 igroup 时，只能添加一个主机。如果要为集群创建 igroup ，可以修改 igroup 以将其他节点添加到该 igroup 。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。
  2. 在主机页面中，单击 * igroup* 。
  3. 在启动程序组页面中，单击 * Storage Virtual Machine* 字段以显示可用 SVM 的下拉列表，然后为要修改的 igroup 选择 SVM 。
  4. 在 igroup 列表中，选择一个 igroup ，然后单击 * 将启动程序添加到 igroup* 。
  5. 选择一个主机。
  6. 选择启动程序并单击 * 确定 * 。

删除 **igroup**

您可以使用 SnapCenter 删除不再需要的 igroup 。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。
  2. 在主机页面中，单击 * igroup* 。
  3. 在启动程序组页面中，单击 * Storage Virtual Machine* 字段以显示可用 SVM 的下拉列表，然后为要删除的 igroup 选择 SVM 。
  4. 在 SVM 的 igroup 列表中，选择要删除的 igroup ，然后单击 * 删除 * 。
  5. 在删除 igroup 对话框中，单击 * 确定 * 。

     SnapCenter 将删除 igroup 。

创建和管理磁盘

Windows 主机将存储系统上的 LUN 视为虚拟磁盘。您可以使用 SnapCenter 创建和配置 FC 连接或 iSCSI 连接的 LUN 。

- SnapCenter 仅支持基本磁盘。不支持动态磁盘。
- 对于 GPT ，仅允许一个数据分区，对于 MBR ，允许一个主分区具有一个使用 NTFS 或 CSVFS 格式化的卷且具有一个挂载路径。
- 支持的分区模式： GPT ， MBR ；在 VMware UEFI VM 中，仅支持 iSCSI 磁盘

SnapCenter 不支持重命名磁盘。如果重命名由 SnapCenter 管理的磁盘， SnapCenter 操作将失败。

查看主机上的磁盘

您可以查看使用 SnapCenter 管理的每个 Windows 主机上的磁盘。

- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 在主机页面中，单击 * 磁盘 * 。
3. 从 * 主机 * 下拉列表中选择主机。

   此时将列出这些磁盘。

查看集群模式磁盘

您可以查看使用 SnapCenter 管理的集群上的集群磁盘。只有在从主机下拉列表中选择集群时，才会显示集群磁盘。

- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 在主机页面中，单击 * 磁盘 * 。
3. 从 * 主机 * 下拉列表中选择集群。

   此时将列出这些磁盘。

创建 **FC** 连接或 **iSCSI** 连接的 **LUN** 或磁盘

Windows 主机将存储系统上的 LUN 视为虚拟磁盘。您可以使用 SnapCenter 创建和配置 FC 连接或 iSCSI 连接的 LUN 。

如果要在 SnapCenter 之外创建和格式化磁盘，则仅支持 NTFS 和 CSVFS 文件系统。

开始之前

- 您必须已为存储系统上的 LUN 创建卷。

  此卷应仅包含 LUN ，而只能包含使用 SnapCenter 创建的 LUN 。

  除非已拆分此克隆，否则无法在 SnapCenter 创建的克隆卷上创建 LUN 。

- 您必须已在存储系统上启动 FC 或 iSCSI 服务。
- 如果您使用的是 iSCSI ，则必须已与存储系统建立 iSCSI 会话。
- 适用于 Windows 的 SnapCenter 插件软件包只能安装在要创建磁盘的主机上。
- 关于此任务 *
- 除非 LUN 由 Windows Server 故障转移集群中的主机共享，否则不能将 LUN 连接到多个主机。
- 如果 LUN 由使用 CSV （集群共享卷）的 Windows Server 故障转移集群中的主机共享，则必须在拥有集群组的主机上创建磁盘。
- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 在主机页面中，单击 * 磁盘 * 。

3. 从 * 主机 * 下拉列表中选择主机。
4. 单击 * 新建 * 。

   此时将打开创建磁盘向导。

5. 在 LUN 名称页面中，确定 LUN ：

在此字段中 ...	执行此操作 ...
存储系统	为 LUN 选择 SVM 。
LUN 路径	单击 * 浏览 * 以选择包含 LUN 的文件夹的完整路径。
LUN名称	输入 LUN 的名称。
集群大小	选择集群的 LUN 块分配大小。 集群大小取决于操作系统和应用程序。
LUN 标签	或者，输入 LUN 的描述性文本。

6. 在磁盘类型页面中，选择磁盘类型：

选择 ...	条件
专用磁盘	LUN 只能由一台主机访问。 忽略 * 资源组 * 字段。
共享磁盘	LUN 由 Windows Server 故障转移集群中的主机共享。 在 * 资源组 * 字段中输入集群资源组的名称。您只需要在故障转移集群中的一个主机上创建磁盘。
集群共享卷（ CSV ）	LUN 由使用 CSV 的 Windows Server 故障转移集群中的主机共享。 在 * 资源组 * 字段中输入集群资源组的名称。确保要创建磁盘的主机是集群组的所有者。

7. 在驱动器属性页面中，指定驱动器属性：

属性	Description
自动分配挂载点	SnapCenter 会根据系统驱动器自动分配卷挂载点。 例如，如果系统驱动器为 C： ，则 auto assign 会在 C： 驱动器（ C： \scmnpt\ ）下创建一个卷挂载点。 共享磁盘不支持自动分配。
分配驱动器号	将磁盘挂载到相邻下拉列表中选择的驱动器。
使用卷挂载点	将磁盘挂载到相邻字段中指定的驱动器路径。 卷挂载点的根目录必须归要创建磁盘的主机所有。
请勿分配驱动器号或卷挂载点	如果您希望在 Windows 中手动挂载磁盘，请选择此选项。
LUN 大小	指定 LUN 大小；最小值为 150 MB 。 在相邻下拉列表中选择 MB ， GB 或 TB 。
对托管此 LUN 的卷使用精简配置	对 LUN 进行精简配置。 精简配置一次只会根据需要分配尽可能多的存储空间，从而使 LUN 能够高效地增长到最大可用容量。 确保卷上有足够的可用空间来容纳您认为需要的所有 LUN 存储。
选择分区类型	为 GUID 分区表选择 GPT 分区，为主启动记录选择 MBR 分区。 发生原因分区可能会在 Windows Server 故障转移集群中出现 MBR 不对齐问题。 不支持统一可扩展固件接口（ Unified 可扩展固件接口， UEFI ）分区磁盘。

8. 在映射 LUN 页面中，选择主机上的 iSCSI 或 FC 启动程序：

在此字段中 ...	执行此操作 ...
主机	双击集群组名称以显示一个下拉列表，其中显示了属于集群的主机，然后选择启动程序的主机。 只有当 LUN 由 Windows Server 故障转移集群中的主机共享时，才会显示此字段。
选择主机启动程序	选择 * 光纤通道 * 或 * iSCSI * ，然后选择主机上的启动程序。 如果您使用的是具有多路径 I/O （ MPIO ）的 FC ，则可以选择多个 FC 启动程序。

9. 在组类型页面中，指定是要将现有 igroup 映射到 LUN ，还是要创建新的 igroup ：

选择 ...	条件
为选定启动程序创建新的 igroup	要为选定启动程序创建新的 igroup 。
选择一个现有 igroup 或为选定启动程序指定一个新的 igroup	您希望为选定启动程序指定一个现有 igroup ，或者使用指定的名称创建一个新的 igroup 。 在 * igroup name* 字段中键入 igroup 名称。键入现有 igroup 名称的前几个字母以自动填写此字段。

10. 在摘要页面中，查看所做的选择，然后单击 * 完成 * 。

    SnapCenter 将创建 LUN 并将其连接到主机上的指定驱动器或驱动器路径。

调整磁盘大小

您可以根据存储系统需要的变化增加或减小磁盘大小。

- 关于此任务 *
- 对于精简配置的 LUN ， ONTAP LUN 几何大小显示为最大大小。
- 对于厚配置 LUN ，可扩展大小（卷中的可用大小）显示为最大大小。
- 具有 MBR 模式分区的 LUN 的大小限制为 2 TB 。
- 具有 GPT 模式分区的 LUN 的存储系统大小限制为 16 TB 。
- 最好在调整 LUN 大小之前创建 Snapshot 副本。
- 如果需要从调整 LUN 大小之前创建的 Snapshot 副本还原 LUN ， SnapCenter 会自动将 LUN 大小调整为 Snapshot 副本的大小。

  执行还原操作后，必须从调整大小后创建的 Snapshot 副本还原在调整 LUN 大小后添加到 LUN 中的数据。

- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 在主机页面中，单击 * 磁盘 * 。
3. 从主机下拉列表中选择主机。

   此时将列出这些磁盘。

4. 选择要调整大小的磁盘，然后单击 * 调整大小 * 。
5. 在调整磁盘大小对话框中，使用滑块工具指定磁盘的新大小，或者在大小字段中输入新大小。

   如果您手动输入大小，则需要在大小字段外单击，然后才能正确启用缩减或扩展按钮。此外，您还必须单击 MB ， GB 或 TB 以指定度量单位。

6. 对输入的内容感到满意后，根据需要单击 * 缩减 * 或 * 扩展 * 。

   SnapCenter 会调整磁盘大小。

连接磁盘

您可以使用连接磁盘向导将现有 LUN 连接到主机，或者重新连接已断开连接的 LUN 。

开始之前

- 您必须已在存储系统上启动 FC 或 iSCSI 服务。
- 如果您使用的是 iSCSI ，则必须已与存储系统建立 iSCSI 会话。
- 除非 LUN 由 Windows Server 故障转移集群中的主机共享，否则不能将 LUN 连接到多个主机。
- 如果 LUN 由使用 CSV （集群共享卷）的 Windows Server 故障转移集群中的主机共享，则必须将磁盘连接到拥有集群组的主机上。
- 适用于 Windows 的插件只需安装在要连接磁盘的主机上。
- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 在主机页面中，单击 * 磁盘 * 。
3. 从 * 主机 * 下拉列表中选择主机。
4. 单击 * 连接 * 。

   此时将打开连接磁盘向导。

5. 在 LUN 名称页面中，确定要连接到的 LUN ：

在此字段中 ...	执行此操作 ...
存储系统	为 LUN 选择 SVM 。
LUN 路径	单击 * 浏览 * 以选择包含 LUN 的卷的完整路径。

在此字段中 ...	执行此操作 ...
LUN名称	输入 LUN 的名称。
集群大小	选择集群的 LUN 块分配大小。 集群大小取决于操作系统和应用程序。
LUN 标签	或者，输入 LUN 的描述性文本。

6. 在磁盘类型页面中，选择磁盘类型：

选择 ...	条件
专用磁盘	LUN 只能由一台主机访问。
共享磁盘	LUN 由 Windows Server 故障转移集群中的主机共享。 您只需将磁盘连接到故障转移集群中的一台主机即可。
集群共享卷（ CSV ）	LUN 由使用 CSV 的 Windows Server 故障转移集群中的主机共享。 确保要连接到磁盘的主机是集群组的所有者。

7. 在驱动器属性页面中，指定驱动器属性：

属性	**Description**
自动分配	让 SnapCenter 根据系统驱动器自动分配卷挂载点。 例如，如果系统驱动器为 C： ，则 auto assign 属性会在 C： 驱动器（ C： \scmnpt\ ）下创建一个卷挂载点。 共享磁盘不支持自动分配属性。
分配驱动器号	将磁盘挂载到相邻下拉列表中选择的驱动器。
使用卷挂载点	将磁盘挂载到相邻字段中指定的驱动器路径。 卷挂载点的根目录必须归要创建磁盘的主机所有。
请勿分配驱动器号或卷挂载点	如果您希望在 Windows 中手动挂载磁盘，请选择此选项。

8. 在映射 LUN 页面中，选择主机上的 iSCSI 或 FC 启动程序：

在此字段中 ...	执行此操作 ...
主机	双击集群组名称以显示一个下拉列表，其中显示了属于集群的主机，然后选择启动程序的主机。 只有当 LUN 由 Windows Server 故障转移集群中的主机共享时，才会显示此字段。
选择主机启动程序	选择 * 光纤通道 * 或 * iSCSI * ，然后选择主机上的启动程序。 如果将 FC 与 MPIO 结合使用，则可以选择多个 FC 启动程序。

9. 在组类型页面中，指定要将现有 igroup 映射到 LUN 还是创建新的 igroup ：

选择 ...	条件
为选定启动程序创建新的 igroup	要为选定启动程序创建新的 igroup 。
选择一个现有 igroup 或为选定启动程序指定一个新的 igroup	您希望为选定启动程序指定一个现有 igroup ，或者使用指定的名称创建一个新的 igroup 。 在 * igroup name* 字段中键入 igroup 名称。键入现有 igroup 名称的前几个字母以自动填写此字段。

10. 在摘要页面中，查看所做的选择并单击 * 完成 * 。

    SnapCenter 会将 LUN 连接到主机上的指定驱动器或驱动器路径。

断开磁盘连接

您可以在不影响 LUN 内容的情况下将 LUN 与主机断开连接，但有一个例外：如果在拆分克隆之前断开克隆的连接，则克隆的内容将丢失。

开始之前

- 确保 LUN 未被任何应用程序使用。
- 确保监控软件不会监控 LUN 。
- 如果 LUN 是共享的，请确保从 LUN 中删除集群资源依赖关系，并验证集群中的所有节点是否均已打开电源，正常运行并可供 SnapCenter 使用。
- 关于此任务 *

如果断开 SnapCenter 创建的 FlexClone 卷中的 LUN ，并且该卷上没有连接任何其他 LUN ，则 SnapCenter 会删除该卷。断开 LUN 连接之前， SnapCenter 会显示一条消息，警告您可能会删除 FlexClone 卷。

为避免自动删除 FlexClone 卷，应在断开最后一个 LUN 的连接之前重命名此卷。重命名卷时，请确保更改多个字符，而不仅仅是名称中的最后一个字符。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。
  2. 在主机页面中，单击 * 磁盘 * 。
  3. 从 * 主机 * 下拉列表中选择主机。

     此时将列出这些磁盘。
  4. 选择要断开连接的磁盘，然后单击 * 断开连接 * 。
  5. 在断开磁盘连接对话框中，单击 * 确定 * 。

     SnapCenter 将断开磁盘连接。

删除磁盘

您可以删除不再需要的磁盘。删除磁盘后，您将无法取消删除该磁盘。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。
  2. 在主机页面中，单击 * 磁盘 * 。
  3. 从 * 主机 * 下拉列表中选择主机。

     此时将列出这些磁盘。
  4. 选择要删除的磁盘，然后单击 * 删除 * 。
  5. 在删除磁盘对话框中，单击 * 确定 * 。

     SnapCenter 将删除该磁盘。

创建和管理 **SMB** 共享

要在 Storage Virtual Machine （ SVM ）上配置 SMB3 共享，您可以使用 SnapCenter 用户界面或 PowerShell cmdlet 。

* 最佳实践： * 建议使用 cmdlet ，因为它可以让您利用 SnapCenter 提供的模板自动配置共享。

这些模板包含卷和共享配置的最佳实践。您可以在适用于 Windows 的 SnapCenter 插件软件包安装文件夹中的 "Templates" 文件夹中找到这些模板。

如果您愿意这样做，可以按照提供的型号创建自己的模板。在创建自定义模板之前，应查看 cmdlet 文档中的参数。

创建 SMB 共享

您可以使用 SnapCenter 共享页面在 Storage Virtual Machine （ SVM ）上创建 SMB3 共享。

您不能使用 SnapCenter 备份 SMB 共享上的数据库。SMB 支持仅限于配置。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。
  2. 在主机页面中，单击 * 共享 * 。
  3. 从 * Storage Virtual Machine* 下拉列表中选择 SVM 。
  4. 单击 * 新建 * 。

     此时将打开 " 新建共享 " 对话框。

  5. 在新建共享对话框中，定义共享：

在此字段中 ...	执行此操作 ...
Description	输入共享的描述性文本。
Share name	输入共享名称，例如 test_share 。 您为共享输入的名称也将用作卷名称。 共享名称： • 必须为 UTF-8 字符串。 • 不得包含以下字符：0x00到0x1F之间的控制字符(包括两个字符)、0x22 (双引号)和特殊字符 `\ / [ ] : (vertical bar) < > + = ; , ?`
共享路径	• 单击字段以输入新的文件系统路径，例如 / 。 • 双击字段可从现有文件系统路径列表中进行选择。

  6. 对输入的内容感到满意后，单击 * 确定 * 。

     SnapCenter 会在 SVM 上创建 SMB 共享。

删除 SMB 共享

您可以在不再需要 SMB 共享时将其删除。

- 步骤 *
  1. 在左侧导航窗格中，单击 * 主机 * 。

2. 在主机页面中，单击 * 共享 * 。
3. 在共享页面中，单击 * Storage Virtual Machine* 字段以显示包含可用 Storage Virtual Machine （ SVM ）列表的下拉列表，然后为要删除的共享选择 SVM 。
4. 从 SVM 上的共享列表中，选择要删除的共享，然后单击 * 删除 * 。
5. 在删除共享对话框中，单击 * 确定 * 。

   SnapCenter 将从 SVM 中删除 SMB 共享。

回收存储系统上的空间

虽然在删除或修改文件时 NTFS 会跟踪 LUN 上的可用空间，但它不会向存储系统报告新信息。您可以在适用于 Windows 的插件主机上运行空间回收 PowerShell cmdlet ，以确保新释放的块在存储中标记为可用。

如果要在远程插件主机上运行 cmdlet ，则必须先运行 SnapCenterOpen-SMConnection cmdlet 以打开与 SnapCenter 服务器的连接。

开始之前

- 在执行还原操作之前，您必须确保空间回收过程已完成。
- 如果 LUN 由 Windows Server 故障转移集群中的主机共享，则必须在拥有集群组的主机上执行空间回收。
- 为了获得最佳存储性能，您应尽可能频繁地执行空间回收。

  您应确保已扫描整个 NTFS 文件系统。

- 关于此任务 *
- 空间回收耗时且需要占用大量 CPU 资源，因此，通常最好在存储系统和 Windows 主机使用率较低时运行此操作。
- 空间回收几乎会回收所有可用空间，但不会回收 100% 的空间。
- 不应在执行空间回收的同时运行磁盘碎片整理。

  这样做会减慢回收过程的速度。

- 步骤 *

在应用程序服务器 PowerShell 命令提示符处，输入以下命令：

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path 是映射到 LUN 的驱动器路径。

使用 **PowerShell cmdlet** 配置存储

如果您不想使用 SnapCenter 图形用户界面执行主机配置和空间回收作业，则可以使用适用于 Microsoft Windows 的 SnapCenter 插件提供的 PowerShell cmdlet 。您可以直接使用 cmdlet 或将其添加到脚本中。

如果要在远程插件主机上运行 cmdlet ，则必须运行 SnapCenter Open-SMConnection cmdlet 以打开与 SnapCenter 服务器的连接。

有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 *get-help command_name* 来获取。或者，您也可以参考 "《 SnapCenter 软件 cmdlet 参考指南》"。

如果由于从服务器中删除 SnapDrive for Windows 而导致 SnapCenter PowerShell cmdlet 损坏，请参见 "卸载 SnapDrive for Windows 后， SnapCenter cmdlet 断开"。

在 **VMware** 环境中配置存储

您可以在VMware环境中使用适用于Microsoft Windows的SnapCenter 插件来创建和管理LUN以及管理Snapshot副本。

支持的 **VMware** 子操作系统平台

- 支持的 Windows Server 版本
- Microsoft 集群配置

  使用 Microsoft iSCSI 软件启动程序时，最多支持 VMware 上支持 16 个节点，或者使用 FC 最多支持两个节点

- RDM LUN

  对于普通 RDM ，最多支持 56 个 RDM LUN 以及 4 个 LSI Logic SCSI 控制器；对于适用于 Windows 的 VMware VM MSCS 盒对盒插件配置，最多支持 42 个 RDM LUN 以及 3 个 LSI Logic SCSI 控制器

  支持 VMware 半虚拟 SCSI 控制器。RDM 磁盘可支持 256 个磁盘。

有关受支持版本的最新信息，请参见 "NetApp 互操作性表工具"。

VMware ESXi 服务器相关限制

- 不支持在使用 ESXi 凭据的虚拟机上的 Microsoft 集群上安装适用于 Windows 的插件。

  在集群模式虚拟机上安装适用于 Windows 的插件时，应使用 vCenter 凭据。

- 所有集群节点必须对同一集群磁盘使用相同的目标 ID （在虚拟 SCSI 适配器上）。
- 在适用于 Windows 的插件之外创建 RDM LUN 时，必须重新启动此插件服务才能使其识别新创建的磁盘。
- 不能在 VMware 子操作系统上同时使用 iSCSI 和 FC 启动程序。

SnapCenter RDM 操作所需的最小 **vCenter** 特权

要在子操作系统中执行 RDM 操作，您应在主机上具有以下 vCenter 权限：

- 数据存储库：删除文件
- Host ： 配置 > 存储分区配置
- Virtual Machine ： 配置

您必须将这些特权分配给 Virtual Center Server 级别的角色。不能将分配这些特权的角色分配给没有 root 权限的任何用户。

分配这些权限后，您可以在子操作系统上安装适用于 Windows 的插件。

管理 **Microsoft** 集群中的 **FC RDM LUN**

您可以使用适用于 Windows 的插件管理使用 FC RDM LUN 的 Microsoft 集群，但必须先在该插件外部创建共享 RDM 仲裁和共享存储，然后将磁盘添加到集群中的虚拟机。

从 ESXi 5.5 开始，您还可以使用 ESX iSCSI 和 FCoE 硬件来管理 Microsoft 集群。适用于 Windows 的插件为 Microsoft 集群提供了开箱即用支持。

要求

如果您满足特定配置要求，适用于 Windows 的插件可为在属于两个不同 ESX 或 ESXi 服务器的两个不同虚拟机上使用 FC RDM LUN 的 Microsoft 集群提供支持，这两个虚拟机也称为跨机集群。

- 虚拟机（ VM ）必须运行相同的 Windows Server 版本。
- 每个 VMware 父主机的 ESX 或 ESXi 服务器版本必须相同。
- 每个父主机必须至少具有两个网络适配器。
- 两个 ESX 或 ESXi 服务器之间必须至少共享一个 VMware 虚拟机文件系统（ VMFS ）数据存储库。
- VMware 建议在 FC SAN 上创建共享数据存储库。

  如有必要，还可以通过 iSCSI 创建共享数据存储库。

- 共享 RDM LUN 必须处于物理兼容模式。
- 必须在适用于 Windows 的插件之外手动创建共享 RDM LUN 。

  您不能将虚拟磁盘用于共享存储。

- 必须在集群中的每个虚拟机上以物理兼容模式配置 SCSI 控制器：

  Windows Server 2008 R2 要求您在每个虚拟机上配置 LSI Logic SAS SCSI 控制器。如果只有一种类型的 LSI Logic SAS 控制器存在，并且该控制器已连接到 C ： 驱动器，则共享 LUN 无法使用现有 LSI Logic SAS 控制器。

  VMware Microsoft 集群不支持半虚拟类型的 SCSI 控制器。

  > 在物理兼容模式下将 SCSI 控制器添加到虚拟机上的共享 LUN 时，必须在 VMware Infrastructure Client 中选择 * 原始设备映射 * （ RDM ）选项，而不是 * 创建新磁盘 * 选项。

- Microsoft 虚拟机集群不能属于 VMware 集群。
- 在属于 Microsoft 集群的虚拟机上安装适用于 Windows 的插件时，您必须使用 vCenter 凭据，而不是 ESX 或 ESXi 凭据。
- 适用于 Windows 的插件无法使用多个主机中的启动程序创建一个 igroup 。

  在创建要用作共享集群磁盘的 RDM LUN 之前，必须在存储控制器上创建包含所有 ESXi 主机中的启动程序的 igroup 。

- 确保使用 FC 启动程序在 ESXi 5.0 上创建 RDM LUN 。

  创建 RDM LUN 时，系统将使用 ALUA 创建启动程序组。

限制

适用于 Windows 的插件支持在属于不同 ESX 或 ESXi 服务器的不同虚拟机上使用 FC/iSCSI RDM LUN 的 Microsoft 集群。

ESX 5.5i 之前的版本不支持此功能。

- 适用于 Windows 的插件不支持 ESX iSCSI 和 NFS 数据存储库上的集群。
- 适用于 Windows 的插件不支持在集群环境中使用混合启动程序。

  启动程序必须为 FC 或 Microsoft iSCSI ，但不能同时为这两者。

- Microsoft 集群中的共享磁盘不支持 ESX iSCSI 启动程序和 HBA 。
- 如果虚拟机属于 Microsoft 集群，则适用于 Windows 的插件不支持使用 vMotion 迁移虚拟机。
- 适用于 Windows 的插件不支持在 Microsoft 集群中的虚拟机上运行 MPIO 。

创建共享 **FC RDM LUN**

在使用 FC RDM LUN 在 Microsoft 集群中的节点之间共享存储之前，必须先创建共享仲裁磁盘和共享存储磁盘，然后将其添加到集群中的两个虚拟机。

共享磁盘不是使用适用于 Windows 的插件创建的。您应创建共享 LUN ，然后将其添加到集群中的每个虚拟机。 有关信息，请参见 "跨物理主机的集群虚拟机"。

配置与 SnapCenter 服务器的安全 MySQL 连接

如果要在独立配置或网络负载平衡（ NLB ）配置中确保 SnapCenter 服务器与 MySQL 服务器之间的通信安全，可以生成安全套接字层（ SSL ）证书和密钥文件。

为独立的 SnapCenter 服务器配置配置安全的 MySQL 连接

如果要保护 SnapCenter 服务器与 MySQL 服务器之间的通信安全，可以生成安全套接字层（ SSL ）证书和密钥文件。您必须在 MySQL 服务器和 SnapCenter 服务器中配置证书和密钥文件。

此时将生成以下证书：

- CA 证书
- 服务器公有证书和专用密钥文件
- 客户端公有证书和专用密钥文件
- 步骤 *

  1. 使用 openssl 命令在 Windows 上为 MySQL 服务器和客户端设置 SSL 证书和密钥文件。

有关信息，请参见 "MySQL 5.7 ： 使用 openssl 创建 SSL 证书和密钥"

> 用于服务器证书，客户端证书和密钥文件的通用名称值必须与用于 CA 证书的通用名称值不同。如果通用名称值相同，则使用 OpenSSL 编译的服务器的证书和密钥文件将失败。

* 最佳实践： * 您应使用服务器完全限定域名（ FQDN ）作为服务器证书的公用名。

2. 将 SSL 证书和密钥文件复制到 MySQL Data 文件夹。

   默认MySQL Data文件夹路径为 `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`。

3. 更新 MySQL 服务器配置文件（ my.ini ）中的 CA 证书，服务器公有证书，客户端公有证书，服务器专用密钥和客户端专用密钥路径。

   默认MySQL服务器配置文件(my.ini)路径为 `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`。

   > 您必须在 MySQL 服务器配置文件（ my.ini ）的 "mysqld" 部分中指定 CA 证书，服务器公有证书和服务器专用密钥路径。

   您必须在 MySQL 服务器配置文件（ my.ini ）的 [client] 部分中指定 CA 证书，客户端公有证书和客户端专用密钥路径。

   以下示例显示了复制到默认文件夹中my.ini文件的[mysqld]部分的证书和密钥文件 `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

   以下示例显示了在 my.ini 文件的 [client] 部分中更新的路径。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
   ```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. 停止 Internet 信息服务器（ Internet Information Server ， IIS ）中的 SnapCenter 服务器 Web 应用程序。
5. 重新启动 MySQL 服务。
6. 更新 web.config 文件中 MySQLProtocol 密钥的值。

   以下示例显示了在 web.config 文件中更新的 MySQLProtocol 密钥的值。

```
<add key="MySQLProtocol" value="SSL" />
```

7. 使用 my.ini 文件的 [client] 部分中提供的路径更新 web.config 文件。

   以下示例显示了在 my.ini 文件的 [client] 部分中更新的路径。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
```

+

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem" />
```

+

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem" />
```

1. 在 IIS 中启动 SnapCenter 服务器 Web 应用程序。

为 **HA** 配置配置安全 **MySQL** 连接

如果要确保 SnapCenter 服务器与 MySQL 服务器之间的通信安全，您可以为高可用性（ HA ）节点生成安全套接字层（ SSL ）证书和密钥文件。您必须在 MySQL 服务器和 HA 节点上配置证书和密钥文件。

此时将生成以下证书：

- CA 证书

  在其中一个 HA 节点上生成一个 CA 证书，并将此 CA 证书复制到另一个 HA 节点。

- 两个 HA 节点的服务器公有证书和服务器专用密钥文件

- 两个 HA 节点的客户端公有证书和客户端专用密钥文件
- 步骤 *

1. 对于第一个 HA 节点，请使用 openssl 命令在 Windows 上为 MySQL 服务器和客户端设置 SSL 证书和密钥文件。

   有关信息，请参见 "MySQL 5.7 ： 使用 openssl 创建 SSL 证书和密钥"

   > 用于服务器证书，客户端证书和密钥文件的通用名称值必须与用于 CA 证书的通用名称值不同。如果通用名称值相同，则使用 OpenSSL 编译的服务器的证书和密钥文件将失败。

   * 最佳实践： * 您应使用服务器完全限定域名（ FQDN ）作为服务器证书的公用名。

2. 将 SSL 证书和密钥文件复制到 MySQL Data 文件夹。

   默认 MySQL Data 文件夹路径为 C ： \ProgramData\NetApp\SnapCenter\MySQL Data\Data\ 。

3. 更新 MySQL 服务器配置文件（ my.ini ）中的 CA 证书，服务器公有证书，客户端公有证书，服务器专用密钥和客户端专用密钥路径。

   默认 MySQL 服务器配置文件（ my.ini ）路径为 C ： \ProgramData\NetApp\SnapCenter\MySQL Data\my.in

   > 您必须在 MySQL 服务器配置文件（ my.ini ）的 "mysqld" 部分中指定 CA 证书，服务器公有证书和服务器专用密钥路径。

   您必须在 MySQL 服务器配置文件（ my.ini ）的 [client] 部分中指定 CA 证书，客户端公有证书和客户端专用密钥路径。

   以下示例显示了复制到默认文件夹 C ： /ProgramData/NetApp/SnapCenter/MySQL Data/Data 中 my.ini 文件的 [mysqld] 部分的证书和密钥文件。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

   以下示例显示了在 my.ini 文件的 [client] 部分中更新的路径。

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. 对于第二个 HA 节点，复制 CA 证书并生成服务器公有证书，服务器专用密钥文件，客户端公有证书和客户端专用密钥文件。执行以下步骤：

   a. 将第一个 HA 节点上生成的 CA 证书复制到第二个 NLB 节点的 MySQL Data 文件夹。

      默认 MySQL Data 文件夹路径为 C： \ProgramData\NetApp\SnapCenter\MySQL Data\Data\ 。

      > 您不能再次创建 CA 证书。您应仅创建服务器公有证书，客户端公有证书，服务器专用密钥文件和客户端专用密钥文件。

   b. 对于第一个 HA 节点，请使用 openssl 命令在 Windows 上为 MySQL 服务器和客户端设置 SSL 证书和密钥文件。

      "MySQL 5.7 ： 使用 openssl 创建 SSL 证书和密钥"

      > 用于服务器证书，客户端证书和密钥文件的通用名称值必须与用于 CA 证书的通用名称值不同。如果通用名称值相同，则使用 OpenSSL 编译的服务器的证书和密钥文件将失败。

      建议使用服务器 FQDN 作为服务器证书的公用名。

   c. 将 SSL 证书和密钥文件复制到 MySQL Data 文件夹。

   d. 更新 MySQL 服务器配置文件（ my.ini ）中的 CA 证书，服务器公有证书，客户端公有证书，服务器专用密钥和客户端专用密钥路径。

      > 您必须在 MySQL 服务器配置文件（ my.ini ）的 "mysqld" 部分中指定 CA 证书，服务器公有证书和服务器专用密钥路径。

      您必须在 MySQL 服务器配置文件（ my.ini ）的 [client] 部分中指定 CA 证书，客户端公有证书和客户端专用密钥路径。

      以下示例显示了复制到默认文件夹 C： /ProgramData/NetApp/SnapCenter/MySQL Data/Data 中 my.ini 文件的 [mysqld] 部分的证书和密钥文件。

      ```
      ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
      ```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

以下示例显示了在 my.ini 文件的 [client] 部分中更新的路径。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. 在两个 HA 节点上停止 Internet 信息服务器（ Internet Information Server ， IIS ）中的 SnapCenter 服务器 Web 应用程序。
6. 在两个 HA 节点上重新启动 MySQL 服务。
7. 更新两个 HA 节点的 web.config 文件中 MySQLProtocol 密钥的值。

   以下示例显示了在 web.config 文件中更新的 MySQLProtocol 密钥的值。

   ```
   <add key="MySQLProtocol" value="SSL" />
   ```

8. 使用您在 my.ini 文件的 [client] 部分中为两个 HA 节点指定的路径更新 web.config 文件。

   以下示例显示了在 my.ini 文件的 [client] 部分中更新的路径。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
```

+

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

+

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

1. 在两个 HA 节点上的 IIS 中启动 SnapCenter 服务器 Web 应用程序。
2. 在其中一个 HA 节点上使用 Set-SmRepositoryConfig -RebuildSlave -Force PowerShell cmdlet 和 -Force 选项，以便在两个 HA 节点上建立安全的 MySQL 复制。

   即使复制状态正常， -Force 选项也允许您重建从属存储库。

安装期间在 **Windows** 主机上启用的功能

SnapCenter 服务器安装程序可在安装期间在 Windows 主机上启用 Windows 功能和角色。出于故障排除和主机系统维护的目的，这些功能可能会很重要。

类别	功能
Web 服务器	• Internet 信息服务 • 全球 Web 服务 • 常见 HTTP 功能 ◦ 默认文档 ◦ 目录浏览 ◦ HTTP 错误 ◦ HTTP 重定向 ◦ 静态内容 ◦ WebDAV 发布 • 运行状况和诊断 ◦ 自定义日志记录 ◦ HTTP 日志记录 ◦ 日志记录工具 ◦ 请求监控器 ◦ 跟踪 • 性能功能 ◦ 静态内容压缩 • 安全性 ◦ IP 安全性 ◦ 基本身份验证 ◦ 集中式 SSL 证书支持 ◦ 客户端证书映射身份验证 ◦ IIS 客户端证书映射身份验证 ◦ IP 和域限制 ◦ 请求筛选 ◦ URL 授权 ◦ Windows 身份验证 • 应用程序开发功能 ◦ .NET 可扩展性 4.5 ◦ 应用程序初始化 ◦ ASP.NET 4.7.2 ◦ 服务器端包括 ◦ WebSocket 协议 管理工具 IIS 管理控制台

类别	功能
IIS 管理脚本和工具	• IIS 管理服务 • Web 管理工具
.NET Framework 4.7.2功能	• .NET Framework 4.7.2 • ASP.NET 4.7.2 • Windows Communication Foundation （ WCF ） HTTP 激活 45 ◦ TCP 激活 ◦ HTTP激活 ◦ 消息队列（ MSMQ ）激活 有关.NET专用的故障排除信息、请参见 "对于没有Internet连接的原有系统、SnapCenter 升级或安装失败"。
消息队列	• 消息队列服务 确保没有其他应用程序使用 SnapCenter 创建和管理的 MSMQ 服务。 • MSMQ服务器
Windows 进程激活服务	• 流程模型
配置 API	全部