安装和配置SnapCenter服务器

SnapCenter software

NetApp
November 06, 2025

目录

安装和配置SnapCenter服务器

准备安装SnapCenter服务器

安装SnapCenter服务器的要求

在 Windows 或 Linux 主机上安装SnapCenter Server 之前，您应该检查并确保满足您的环境的所有要求。

Windows 主机的域和工作组要求

SnapCenter服务器可以安装在域或工作组中的 Windows 主机上。

具有管理员权限的用户可以安装SnapCenter服务器。

- 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 域和信任的 Microsoft 文档包含更多信息。

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

空间和尺寸要求

您应该熟悉空间和尺寸要求。

物品	Windows 主机要求	Linux 主机要求
操作系统	Microsoft Windows 仅支持英语、德语、日语和简体中文版本的操作系统。 有关受支持版本的最新信息，请参阅https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["NetApp 互操作性表工具"^]。	• Red Hat Enterprise Linux (RHEL) 8 和 9 • SUSE Linux 企业服务器 (SLES) 15 有关受支持版本的最新信息，请参阅https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["NetApp 互操作性表工具"^]。
最小 CPU 数量	4 核	4 核

物品	**Windows** 主机要求	**Linux** 主机要求
最低内存	8 GB MySQL 服务器缓冲池使用了总 RAM 的 20%。	8 GB
SnapCenter服务器软件和日志的最小硬盘空间	7 GB 如果SnapCenter存储库与安装SnapCenter Server 的驱动器位于同一驱动器中，则建议使用 15 GB。	15 GB
SnapCenter存储库的最小硬盘空间	8 GB 注意：如果SnapCenter服务器与安装SnapCenter存储库的驱动器相同，则建议使用 15 GB。	不适用
所需的软件包	• ASP.NET Core Runtime 8.0.12（以及所有后续 8.0.x 补丁）托管包 • PowerShell 7.4.2 或更高版本 有关 .NET 特定的故障排除信息，请参阅 "对于没有 Internet 连接的传统系统， SnapCenter升级或安装失败"。	• .NET Framework 8.0.12（以及所有后续的 8.0.x 补丁） • PowerShell 7.4.2 或更高版本 • Nginx 是一个可以用作反向代理的 Web 服务器 • Pam-devel PAM（可插入式身份验证模块）是一种系统安全工具，它允许系统管理员设置身份验证策略，而无需重新编译执行身份验证的程序。

ASP.NET 核心需要 IIS_IUSRS 来访问 Windows 上SnapCenter Server 中的临时文件系统。

SAN 主机要求

SnapCenter不包括主机实用程序或 DSM。如果SnapCenter主机是 SAN（FC/iSCSI）环境的一部分，则可能需要在SnapCenter Server 主机上安装和配置其他软件。

- 主机实用程序：主机实用程序支持 FC 和 iSCSI，它使您能够在 Windows 服务器上使用 MPIO。 "了解更多"

。

- Microsoft DSM for Windows MPIO：该软件与 Windows MPIO 驱动程序配合使用，以管理NetApp和 Windows 主机之间的多条路径。高可用性配置需要 DSM。

> 如果您使用的是ONTAP DSM，则应该迁移到 Microsoft DSM。有关更多信息，请参阅 "如何从ONTAP DSM 迁移到 Microsoft DSM" 。

浏览器要求

SnapCenter software支持 Chrome 125 及更高版本以及 Microsoft Edge 110.0.1587.17 及更高版本。

端口要求

SnapCenter software需要不同的端口来实现不同组件之间的通信。

- 应用程序不能共享端口。
- 对于可自定义的端口，如果您不想使用默认端口，您可以在安装期间选择自定义端口。
- 对于固定端口，您应该接受默认端口号。
- 防火墙
  - 防火墙、代理或其他网络设备不应干扰连接。
  - 如果在安装SnapCenter时指定自定义端口，则应在插件主机上为SnapCenter插件Loader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。

端口名称	端口号	协议	方向	描述
SnapCenter Web 端口	8146	HTTPS	双向	此端口用于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。 您可以自定义端口号。
SnapCenter SMCore 通信端口	8145	HTTPS	双向	此端口用于SnapCenter服务器与安装了SnapCenter插件的主机之间的通信。 您可以自定义端口号。

端口名称	端口号	协议	方向	描述
调度程序服务端口	8154	HTTPS		此端口用于以集中方式协调SnapCenter服务器主机内所有托管插件的SnapCenter调度程序工作流。 您可以自定义端口号。
RabbitMQ 端口	5672	TCP		这是 RabbitMQ 监听的默认端口，用于 Scheduler 服务和SnapCenter之间的发布者-订阅者模型通信。
MySQL 端口	3306	HTTPS		该端口用于与SnapCenter存储库数据库通信。您可以创建从SnapCenter服务器到 MySQL 服务器的安全连接。"了解更多"
Windows 插件主机	135，445	TCP		此端口用于SnapCenter服务器与安装插件的主机之间的通信。Microsoft 指定的其他动态端口范围也应开放。
Linux 或 AIX 插件主机	22	SSH	单向	此端口用于SnapCenter服务器和主机之间的通信，从服务器发起到客户端主机。
适用于 Windows 、Linux 或 AIX 的SnapCenter插件包	8145	HTTPS	双向	该端口用于SMCore与安装插件包的主机进行通信。可定制。 您可以自定义端口号。

端口名称	端口号	协议	方向	描述
适用于 Oracle 数据库的 SnapCenter 插件	27216			Oracle 插件使用默认 JDBC 端口来连接 Oracle 数据库。
适用于 Exchange 数据库的SnapCenter插件	909			Windows 插件使用默认的 NET.TCP 端口来连接 Exchange VSS 回调。
NetApp支持的SnapCenter插件	9090	HTTPS		这是仅在插件主机上使用的内部端口；不需要防火墙例外。 SnapCenter服务器和插件之间的通信通过端口 8145 进行。
ONTAP集群或 SVM 通信端口	• 443（HTTPS） • 80（HTTP）	• HTTPS • HTTP	双向	该端口由 SAL（存储抽象层）用于运行SnapCenter Server 的主机和 SVM 之间的通信。SnapCenter for Windows 插件主机上的 SAL 当前也使用该端口来实现SnapCenter插件主机和 SVM 之间的通信。
适用于 SAP HANA 数据库的SnapCenter插件	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	双向	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。 您可以自定义端口号。
适用于 PostgreSQL 的SnapCenter插件	5432			此端口是 PostgreSQL 插件与 PostgreSQL 集群通信所使用的默认 PostgreSQL 端口。 您可以自定义端口号。

注册以访问SnapCenter software

如果您是Amazon FSx for NetApp ONTAP或Azure NetApp Files 的新用户并且没有现有的NetApp帐户，则应该注册以访问SnapCenter software。

开始之前

- 您应该可以访问公司电子邮件 ID。
- 如果您使用Azure NetApp Files，则应该拥有 Azure 订阅 ID。
- 如果您使用的是Amazon FSx for NetApp ONTAP，则应该拥有 FSx for ONTAP文件系统的文件系统 ID。

关于此任务

您的注册需要经过信息验证，可能需要一天时间才能确认并将新的NetApp支持站点 (NSS) 帐户从 访客 访问权限升级为 完全 访问权限。

步骤

1. 点击 https://mysupport.netapp.com/site/user/registration进行注册。
2. 输入您的公司电子邮件 ID，完成验证码，接受 NetApp 的隐私政策，然后单击“提交”。
3. 通过输入发送到您的电子邮件 ID 的 OTP 来验证注册，然后单击“继续”*。
4. 在注册完成页面，输入以下详细信息以完成注册。
   a. 选择* NetApp客户/最终用户*。
   b. 在序列号字段中，如果您使用的是Azure NetApp Files ，请输入 Azure 订阅 ID；如果您使用的是Amazon FSx for NetApp ONTAP，请输入文件系统 ID。

> 您可以提交以下票证： https://mysupport.netapp.com/site/help如果您在注册过程中遇到任何问题或想了解状态。

多重身份验证 (MFA)

管理多重身份验证 (MFA)

您可以管理 Active Directory 联合身份验证服务 (AD FS) 服务器和SnapCenter服务器中的多重身份验证 (MFA) 功能。

启用多重身份验证 (MFA)

您可以使用 PowerShell 命令为SnapCenter Server 启用 MFA 功能。

关于此任务

- 当在同一 AD FS 中配置其他应用程序时， SnapCenter支持基于 SSO 的登录。在某些 AD FS 配置中，SnapCenter可能出于安全原因要求用户进行身份验证，具体取决于 AD FS 会话持久性。
- 可以通过运行以下命令获取有关可与 cmdlet 一起使用的参数及其描述的信息 `Get-Help command_name`。或者，您也可以查看 "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) 应该在相应的域中启动并运行。

- 您应该拥有 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 服务器时间戳都应该相同。
- 为SnapCenter Server 采购并配置授权 CA 证书。

  由于以下原因，CA 证书是强制性的：

  - 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的升级、修复或灾难恢复 (DR) 期间，不会重新创建自签名证书，从而避免重新配置 MFA。
  - 确保 IP-FQDN 解析。

    有关 CA 证书的信息，请参阅"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. 从以下位置下载 AD FS 联合元数据文件"https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml”。
3. 将下载的文件复制到SnapCenter Server 以启用 MFA 功能。
4. 通过 PowerShell 以SnapCenter管理员用户身份登录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 参数指定在SnapCenter Server 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. SnapCenter `Set-SmMultiFactorAuthentication`命令。
8. （可选）使用以下方式检查 MFA 配置状态和设置 `Get-SmMultiFactorAuthentication`命令。
9. 转到 Microsoft 管理控制台 (MMC) 并执行以下步骤：
   a. 单击“文件”>“添加/删除管理单元”。
   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 > 管理私钥。
   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（层次结构的顶部）。
      iii. 在“位置”弹出窗口中单击“确定”。
      iv. 在对象名称字段中，输入“IIS_IUSRS”，然后单击“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*>*开始*。
    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“下一步”。
    e. 在下一个选项卡中选择默认设置。
    f. 单击“完成”。

    SnapCenter现在反映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“编辑索赔签发政策”。
    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. 选择属性为 **User-Principal-Name**，传出声明类型为 **Name-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. 右键单击信赖方信任并选择“属性”。
    b. 确保端点、标识符和签名字段已填充。
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的会话 cookie，然后再次登录。

SnapCenter MFA 功能也可以使用 REST API 启用。

有关故障排除信息，请参阅 "在多个选项卡中同时尝试登录时显示 MFA 错误"。

更新 **AD FS MFA** 元数据

每当 AD FS 服务器发生任何修改（例如升级、CA 证书续订、DR 等）时，您都应该更新SnapCenter中的 AD FS MFA 元数据。

步骤

1. 从以下位置下载 AD FS 联合元数据文件"https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml”
2. 将下载的文件复制到SnapCenter Server 以更新 MFA 配置。

3. 通过运行以下 cmdlet 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的会话 cookie，然后再次登录。

更新**SnapCenter MFA** 元数据

每当 ADFS 服务器发生任何修改（例如修复、CA 证书续订、DR 等）时，您都应该更新 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. 选择*依赖方信任*。
   b. 右键单击为SnapCenter创建的信赖方信任并选择“删除”。

      将显示依赖方信任的用户定义名称。

   c. 启用多重身份验证 (MFA)。

      看"启用多重身份验证" 。
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的会话 cookie，然后再次登录。

禁用多重身份验证 **(MFA)**

步骤

1. 禁用 MFA 并清理启用 MFA 时创建的配置文件，方法是使用 `Set-SmMultiFactorAuthentication`命令。
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的会话 cookie，然后再次登录。

使用 **Rest API**、**PowerShell** 和 **SCCLI** 管理多重身份验证 **(MFA)**

支持通过浏览器、REST API、PowerShell 和 SCCLI 进行 MFA 登录。 MFA 通过 AD FS 身份管理器支持。您可以从 GUI、REST API、PowerShell 和 SCCLI 启用 MFA、禁用 MFA 和配置 MFA。

将 **AD FS** 设置为 **OAuth/OIDC**

使用 **Windows GUI** 向导配置 **AD FS**

1. 导航到 服务器管理器仪表板 > 工具 > **ADFS** 管理。
2. 导航到 **ADFS** > 应用程序组。
   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*客户端标识符*。

   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*。

   复制秘密值。这是客户的秘密。..单击“下一步”。

5. 在“摘要”页面上，单击“下一步”。
   a. 在*完成*页面上，单击*关闭*。
6. 右键单击新添加的*应用程序组*并选择*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“下一步”。

9. 在配置 Web API 页面上，将上一步中创建的SnapCenter服务器 URL 和客户端标识符输入到标识符部分。
   a. 单击“添加”。
   b. 单击“下一步”。
10. 在*选择访问控制策略*页面上，根据您的要求选择控制策略（例如，允许所有人并要求 MFA），然后单击*下一步*。
11. 在*配置应用程序权限*页面，默认选择openid作为范围，点击*下一步*。
12. 在“摘要”页面上，单击“下一步”。

    在*完成*页面上，单击*关闭*。

13. 在“示例应用程序属性”页面上，单击“确定”。
14. JWT 令牌由授权服务器（AD FS）颁发，供资源使用。

    此令牌的“aud”或受众声明必须与资源或 Web API 的标识符匹配。

15. 编辑选定的 WebAPI 并检查回调 URL（SnapCenter服务器 URL）和客户端标识符是否正确添加。

    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*工具*菜单下的*AD FS 管理*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. 转到发行转换规则选项卡
17. 单击“添加规则”。
    a. 在声明规则模板下拉菜单中选择*将 LDAP 属性作为声明发送*。
    b. 单击“下一步”。
18. 输入*声明规则*名称。

a. 在属性存储下拉菜单中选择*Active Directory*。

b. 在 **LDAP Attribute** 下拉菜单中选择 **User-Principal-Name**，在 O*utgoing Claim Type* 下拉菜单中选择 **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、Web API 并添加范围和声明。这些命令以自动脚本格式提供。欲了解更多信息，请参阅<链接至知识库文章>。

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`您的应用程序组的名称

`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机密。

```
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，因为它只显示一次。

```
"client_id = $identifier"

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

5. 授予 AD FS 应用程序 allatclaims 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 命令更新访问令牌的到期时间。

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。访问令牌不能被撤销，并且在到期前有效。
- 默认情况下，访问令牌的有效期为 60 分钟。此最短到期时间足够且可扩展。您必须提供足够的价值以避免任何正在进行的关键业务工作。

步

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** 获取持有者令牌

您应该在任何 REST 客户端（如 Postman）中填写下面提到的参数，它会提示您填写用户凭据。此外，您应该输入第二因素身份验证（您拥有的东西和您是的东西）来获取承载令牌。

+ 持有者令牌的有效性可根据应用程序从 AD FS 服务器进行配置，默认有效期为 60 分钟。

字段	值

资助类型	授权码
回调URL	如果您没有回调 URL，请输入应用程序的基本 URL。
授权网址	[adfs 域名]/adfs/oauth2/授权
访问令牌 URL	[adfs 域名]/adfs/oauth2/token
客户端 ID	输入 AD FS 客户端 ID
客户端机密	输入 AD FS 客户端机密
范围	OpenID
客户端身份验证	作为基本 AUTH 标头发送
资源	在“高级选项”选项卡中，添加与回调 URL 具有相同值的资源字段，该字段作为 JWT 令牌中的“aud”值出现。

使用 **PowerShell**、**SCCLI** 和 **REST API** 在**SnapCenter Server** 中配置 **MFA**

您可以使用 PowerShell、SCCLI 和 REST API 在SnapCenter Server 中配置 MFA。

SnapCenter MFA CLI 身份验证

在 PowerShell 和 SCCLI 中，现有的 cmdlet（Open-SmConnection）扩展了一个名为“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进一步的SnapCenter cmdlet。

SnapCenter MFA Rest API 身份验证

在 REST API 客户端（如 Postman 或 swagger）中使用格式为 *Authorization=Bearer <access token>* 的承载令牌，并在标头中提及用户 RoleName 以从SnapCenter获得成功响应。

MFA Rest API 工作流程

当使用 AD FS 配置 MFA 时，您应该使用访问（承载）令牌进行身份验证，以通过任何 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，如 Postman、Swagger UI 或 FireCamp。
- 获取访问令牌并使用它来验证后续请求（SnapCenter Rest API）以执行任何操作。

步骤

通过 **AD FS MFA** 进行身份验证

1. 配置 REST 客户端以调用 AD FS 端点来获取访问令牌。

   当您点击按钮获取应用程序的访问令牌时，您将被重定向到 AD FS SSO 页面，您必须在该页面提供您的 AD 凭据并使用 MFA 进行身份验证。1.在 AD FS SSO 页面中，在用户名文本框中输入您的用户名或电子邮件。

   + 用户名必须格式化为 user@domain 或 domain\user。

2. 在密码文本框中，输入您的密码。
3. 单击“登录”。
4. 从*登录选项*部分，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：批准发送到您手机的推送通知。
   - 二维码：使用 AUTH Point 手机应用程序扫描二维码，然后输入应用程序中显示的验证码
   - 一次性密码：输入您的令牌的一次性密码。
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 中使用它来执行操作。

6. 在 Rest API 中，您应该在标题部分传递访问令牌和角色名称。
7. SnapCenter从 AD FS 验证此访问令牌。

   如果它是有效令牌， SnapCenter会对其进行解码并获取用户名。

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

   如果身份验证成功， SnapCenter将返回结果，否则将显示错误消息。

为 **Rest API**、**CLI** 和 **GUI** 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SnapCenter服务器。
2. 单击“设置”>“全局设置”>“多重身份验证 (MFA) 设置”
3. 选择界面（GUI/RST API/CLI）以启用或禁用 MFA 登录。

PowerShell 界面

步骤

1. 运行 PowerShell 或 CLI 命令以启用 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
```

`-IsCliMFAEnabled -Path`

路径参数指定 AD FS MFA 元数据 xml 文件的位置。

使用指定的 AD FS 元数据文件路径配置的SnapCenter GUI、Rest API、PowerShell 和 SCCLI 启用 MFA。

2. 使用 `Get-SmMultiFactorAuthentication`命令。

SCCLI 接口

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. 运行以下帖子 API 以启用 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

参数	值
请求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	发布
请求正文	{ “IsGuiMFAEnabled”：false ，“IsRestApiMFAEnabled”：true ，“IsCliMFAEnabled”：false ，“ADFSConfigFilePath” ：“C:\\ADFS_metadata\\abc.xml”}
响应主体	{ “MFAConfiguration”：{ “IsGuiMFAEnabled”：false ，“ADFSConfigFilePath”：“C：\\ADFS_metadata \\abc.xml”， “SCConfigFilePath”：null ，“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	值
请求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	获取

响应主体	{ “MFAConfiguration”：{ “IsGuiMFAEnabled”：false ，“ADFSConfigFilePath”：“C：\\ADFS_metadata \\abc.xml”， “SCConfigFilePath”：null ，“IsRestApiMFAEnabled”：true ，“IsCliMFAEnabled”：false，“ADFSHostName” ：“win-adfs-sc49.winscedom2.com” } }

安装SnapCenter服务器

在 Windows 主机上安装SnapCenter服务器

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

您可以选择使用 PowerShell cmdlet 执行多个安装和配置过程。您应该使用 PowerShell 7.4.2 或更高版本。

不支持从命令行静默安装SnapCenter服务器。

开始之前

- SnapCenter服务器主机必须保持最新的 Windows 更新，并且无需重新启动系统。
- 您应该确保计划安装SnapCenter服务器的主机上未安装 MySQL 服务器。
- 您应该启用 Windows 安装程序调试。

  有关启用 "Windows 安装程序日志记录"。

  您不应在具有 Microsoft Exchange Server、Active Directory 或域名服务器的主机上安装SnapCenter Server。

步骤

1. 从以下位置下载SnapCenter Server 安装包 "NetApp 支持站点"。
2. 双击下载的 .exe 文件启动SnapCenter Server 安装。

   启动安装后，将执行所有预检查，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，错误应该得到修复。

3. 查看SnapCenter服务器安装所需的预填充值并根据需要进行修改。

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

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

4. 单击“立即安装”。

   如果您指定的任何值无效，则会显示相应的错误消息。您应该重新输入这些值，然后启动安装。

如果点击*取消*按钮，正在执行的步骤将会完成，然后开始回滚操作。 SnapCenter服务器将从主机中完全删除。

但是，如果在执行“SnapCenter Server 站点重新启动”或“等待SnapCenter Server 启动”操作时单击“取消”，则安装将继续进行而不会取消操作。

日志文件始终列在管理员用户的 %temp% 文件夹中（最早的在前）。如果要重定向日志位置，请通过运行以下命令从命令提示符启动SnapCenter Server 安装
：`C:\installer_location\installer_name.exe /log"C:\"`

安装期间在 **Windows** 主机上启用的功能

SnapCenter Server 安装程序在安装期间在 Windows 主机上启用 Windows 功能和角色。这些可能对故障排除和维护主机系统有用。

类别	功能
Web 服务器	• 互联网信息服务 • 万维网服务 • 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 • 健康与诊断 ◦ 自定义日志 ◦ HTTP 日志记录 ◦ 测井工具 ◦ 请求监控 ◦ 追踪 • 性能特点 ◦ 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 ◦ 客户端证书映射认证 ◦ IIS 客户端证书映射身份验证 ◦ IP 和域名限制 ◦ 请求过滤 ◦ URL 授权 ◦ Windows 身份验证 • 应用程序开发功能 ◦ .NET 扩展性 4.5 ◦ 应用程序初始化 ◦ ASP.NET Core Runtime 8.0.12（以及所有后续 8.0.x 补丁）托管包 ◦ 服务器端包含 ◦ 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 8.0.12 功能	• ASP.NET Core Runtime 8.0.12（以及所有后续 8.0.x 补丁）托管包 • Windows Communication Foundation (WCF) HTTP 激活45 ◦ TCP 激活 ◦ HTTP 激活 有关 .NET 特定的故障排除信息，请参阅 "对于没有 Internet 连接的传统系统， SnapCenter升级或安装失败"。
Windows 进程激活服务	流程模型
配置 API	全部

在 **Linux** 主机上安装**SnapCenter**服务器

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

开始之前

- 如果您想使用没有足够权限安装SnapCenter的非 root 用户安装SnapCenter服务器，请从NetApp支持站点获取 sudoers 校验和文件。您应该根据 Linux 版本使用适当的校验和文件。
- 如果 SUSE Linux 中没有 sudo 包，请安装 sudo 包以避免身份验证失败。
- 对于SUSE Linux，请配置主机名以避免安装失败。
- 通过运行以下命令检查 Linux 的安全状态 `sestatus`。如果 _SELinux 状态_为“已启用”且 _当前模式_为“强制”，请执行以下操作：
  - 运行以下命令： `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    WEBAPP_EXTERNAL_PORT 的默认值为 8146
  - 如果防火墙阻止了端口，请运行 `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    WEBAPP_EXTERNAL_PORT 的默认值为 8146
  - 从您具有读写权限的目录运行以下命令：
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

      如果命令返回“无事可做”，请在安装SnapCenter Server 后重新运行该命令。

        - 如果命令创建了_my-nginx.pp_，则运行命令使策略包处于活动状态： `sudo semodule -i my-nginx.pp`
    - MySQL PID 目录使用的路径是 */var/opt/mysqld*。运行以下命令设置MySQL安装的权限。
        - `mkdir /var/opt/mysqld`
        - `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
        - `sudo restorecon -Rv /var/opt/mysqld`
    - MySQL 数据目录使用的路径是 */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*。运行以下命令设置 MySQL 数据目录的权限。
        - `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
        - `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
        - `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

关于此任务

- 当SnapCenter Server 安装在 Linux 主机上时，会安装 MySQL、RabbitMq、Errlang 等第三方服务。您不应该卸载它们。
- Linux 主机上安装的SnapCenter服务器不支持：
    - 高可用性
    - Windows 插件
    - Active Directory（仅支持本地用户，包括具有凭据的 root 用户和非 root 用户）
    - 基于密钥的身份验证以登录SnapCenter
- 在安装 .NET 运行时期间，如果安装无法解析 *libicu* 库的依赖关系，则通过运行以下命令安装 *libicu*： `yum install -y libicu`
- 如果由于_Perl_不可用而导致SnapCenter Server 安装失败，则通过运行以下命令安装_Perl_： `yum install -y perl`

步骤

1. 从以下位置下载 "NetApp 支持站点"到 */home* 目录。
    - SnapCenter服务器安装包 - **snapcenter-linux-server-(el8/el9/sles15).bin**
    - 公钥文件 - **snapcenter_public_key.pub**
    - 相应的签名文件 - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. 验证签名文件。 `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. 对于非 root 用户安装，请添加 .bin 安装程序附带的 **snapcenter_server_checksum_(el8/el9/sles15).txt** 中指定的 visudo 内容。
4. 为.bin安装程序分配执行权限。 `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. 执行其中一项操作来安装SnapCenter Server。

<table>
<tr><th>如果你想表演...</th><th>操作</th></tr>
<tr><td>交互式安装</td><td><code>./snapcenter-linux-server-(el8/el9/sles15).bin</code>

系统将提示您输入以下详细信息：
用于访问 Linux 主机外部的SnapCenter服务器的 webapp 外部端口。默认值为 8146。
将安装SnapCenter Server 的SnapCenter Server 用户。
将安装软件包的安装目录。</td></tr>
</table>

如果你想表演...	操作
非交互式安装	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` 示例：sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log 日志将存储在 */var/opt/snapcenter/logs*。 安装SnapCenter Server 时要传递的参数： • DWEBAPP_EXTERNAL_PORT：用于访问 Linux 主机外部的SnapCenter服务器的 Webapp 外部端口。默认值为 8146。 • DWEBAPP_INTERNAL_PORT：用于访问 Linux 主机内的SnapCenter服务器的 Webapp 内部端口。默认值为 8147。 • DSMCORE_PORT：smcore 服务正在运行的 SMCore 端口。默认值为 8145。 • DSCHEDULER_PORT：运行调度程序服务的调度程序端口。默认值为 8154。 • DSNAPCENTER_SERVER_USER：将安装SnapCenter Server 的SnapCenter Server 用户。对于 *DSNAPCENTER_SERVER_USER*，默认值是运行安装程序的用户。 • DUSER_INSTALL_DIR：将安装包的安装目录。对于_DUSER_INSTALL_DIR_，默认安装目录是_/opt_。 • DINSTALL_LOG_NAME：存储安装日志的日志文件名。这是一个可选参数，如果指定，则控制台上不会显示任何日志。如果不指定此参数，则日志将显示在控制台上，并存储在默认日志文件中。 • DSELINUX：如果_SELinux 状态_为“启用”，_当前模式_为“强制”，并且您已执行“开始之前”部分中提到的命令，则应指定此参数并将其值指定为 1。默认值为 0。 • DUPGRADE：默认值为 0。指定此参数及其值为 0 以外的任何整数来升级SnapCenter服务器。

下一步是什么?

- 如果 _SELinux 状态_为“启用”且 _当前模式_为“强制”，则 **nginx** 服务无法启动。您应该运行以下命令：
  a. 转到主目录。
  b. 运行以下命令： `journalctl -x|grep nginx` 。
  c. 如果不允许Webapp内部端口（8147）监听，则运行以下命令：
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. 跑步 `setsebool -P httpd_can_network_connect on`

安装期间在 **Linux** 主机上启用的功能

SnapCenter服务器安装以下软件包，可帮助排除故障和维护主机系统。

- RabbitMQ
- Erlang

注册**SnapCenter**

如果您是NetApp产品的新用户并且没有现有的NetApp帐户，则应该注册SnapCenter以获得支持。

步骤

1. 安装SnapCenter后，导航至 帮助 **>** 关于。
2. 在“关于 SnapCenter”对话框中，记下SnapCenter实例，这是一个以 971 开头的 20 位数字。
3. 点击 https://register.netapp.com。
4. 单击“我不是注册的**NetApp**客户”。
5. 指定您的详细信息以进行注册。
6. 将NetApp参考 SN 字段留空。
7. 从产品线下拉菜单中选择* SnapCenter*。
8. 选择计费提供商。
9. 输入 20 位SnapCenter实例 ID。
10. 单击“提交”。

使用 **RBAC** 授权登录**SnapCenter**

SnapCenter支持基于角色的访问控制 (RBAC)。 SnapCenter管理员通过SnapCenter RBAC 将角色和资源分配给工作组或活动目录中的用户，或者活动目录中的组。 RBAC 用户现在可以使用分配的角色登录SnapCenter 。

开始之前

- 您应该在 Windows 服务器管理器中启用 Windows 进程激活服务 (WAS)。

- 如果您想使用 Internet Explorer 作为浏览器登录SnapCenter服务器，则应确保 Internet Explorer 中的保护模式已禁用。
- 如果SnapCenter Server 安装在 Linux 主机上，则应使用用于安装SnapCenter Server 的用户帐户登录。

关于此任务

在安装过程中， SnapCenter服务器安装向导会创建一个快捷方式并将其放在桌面上和安装SnapCenter的主机的“开始”菜单中。此外，在安装结束时，安装向导会根据您在安装期间提供的信息显示SnapCenter URL，如果您想从远程系统登录，可以复制该 URL。

如果您在 Web 浏览器中打开了多个选项卡，则仅关闭SnapCenter浏览器选项卡并不会将您退出SnapCenter。要结束与SnapCenter的连接，您必须通过单击“退出”按钮或关闭整个 Web 浏览器来退出SnapCenter 。

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

默认 GUI URL 是与安装SnapCenter Server 的服务器上的默认端口 8146 的安全连接（*https://server:8146*）。如果您在SnapCenter安装期间提供了不同的服务器端口，则将使用该端口。

对于高可用性 (HA) 部署，您必须使用虚拟集群 IP *https://Virtual_Cluster_IP_or_FQDN:8146* 访问SnapCenter 。如果在 Internet Explorer (IE) 中导航到 *https://Virtual_Cluster_IP_or_FQDN:8146* 时没有看到SnapCenter UI ，则必须在每个插件主机上的 IE 中将虚拟集群 IP 地址或 FQDN 添加为受信任的站点，或者必须在每个插件主机上禁用 IE 增强安全性。有关更多信息，请参阅 "无法从外部网络访问群集 IP 地址" 。

除了使用SnapCenter GUI 之外，您还可以使用 PowerShell cmdlet 创建脚本来执行配置、备份和恢复操作。每次发布SnapCenter时，某些 cmdlet 可能会发生变化。这 "SnapCenter软件 Cmdlet 参考指南"有详细信息。

如果您是第一次登录SnapCenter ，则必须使用安装过程中提供的凭据登录。

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. 输入用户凭证。

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\用户名
本地管理员	用户名

3. 如果您被分配了多个角色，请从角色框中选择要用于此登录会话的角色。

   登录后，您当前的用户和相关角色将显示在SnapCenter的右上角。

结果

将显示“仪表板”页面。

如果日志记录失败并出现无法访问站点的错误，则应将 SSL 证书映射到SnapCenter。 "了解更多"

完成后

首次以 RBAC 用户身份登录SnapCenter Server 后，刷新资源列表。

如果您有不受信任的 Active Directory 域并且希望SnapCenter支持这些域，则必须先向SnapCenter注册这些域，然后再为不受信任域上的用户配置角色。"了解更多" 。

如果要在 Linux 主机上运行的SnapCenter中添加插件主机，则应从以下位置获取校验和文件：*/opt/NetApp/snapcenter/SnapManagerWeb/Repository*。

从 6.0 版本开始，桌面上会创建SnapCenter PowerShell 的快捷方式。您可以使用快捷方式直接访问SnapCenter PowerShell cmdlet。

使用多重身份验证 **(MFA)** 登录**SnapCenter**

SnapCenter Server 支持域帐户的 MFA，它是活动目录的一部分。

开始之前

您应该启用 MFA。有关如何启用 MFA 的信息，请参阅"启用多重身份验证"

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，输入用户名和密码。

   当 AD FS 页面上显示用户名或密码无效错误消息时，您应该检查以下内容：

   - 用户名或密码是否有效

     用户帐户应该存在于 Active Directory (AD) 中
   - 您是否超出了 AD 中设置的最大允许尝试次数
   - AD 和 AD FS 是否已启动并运行

修改**SnapCenter**默认 **GUI** 会话超时

您可以修改SnapCenter GUI 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，在默认 15 分钟不活动时间后， SnapCenter会警告您将在 5 分钟内退出 GUI 会话。默认情

况下， SnapCenter会在 20 分钟不活动后将您从 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，输入新的会话超时时间（分钟），然后单击“保存”。

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

出于安全目的，如果您的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 协议存在缺陷，攻击者可以利用这些缺陷导致连接失败，或进行中间人攻击并观察您的网站与其访问者之间的加密流量。

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\。
   - 如果服务器密钥已经存在：
     i. 选择已启用的 DWORD，然后单击 编辑 > 修改。
     ii. 将值更改为 0，然后单击“确定”。
   - 如果服务器密钥不存在：
     i. 单击“编辑”>“新建”>“密钥”，然后将密钥命名为“服务器”。
     ii. 选择新的服务器密钥后，单击*编辑* > 新建 > **DWORD**。
     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SnapCenter服务器

添加并配置存储系统

添加存储系统

您应该设置存储系统，使SnapCenter能够访问ONTAP存储、 ASA r2 系统或Amazon FSx for NetApp ONTAP来执行数据保护和配置操作。

您可以添加独立的 SVM 或由多个 SVM 组成的集群。如果您使用的是Amazon FSx for NetApp ONTAP，则可以使用 fsxadmin 帐户添加由多个 SVM 组成的 FSx 管理 LIF，或者在SnapCenter中添加 FSx SVM。

开始之前

- 您应该拥有基础设施管理员角色所需的权限来创建存储连接。

- 您应该确保插件安装没有正在进行中。

  添加存储系统连接时，不得进行主机插件安装，因为主机缓存可能不会更新，并且数据库状态可能会在SnapCenter GUI 中显示为“不可用于备份”或“不在NetApp存储上”。

- 存储系统名称应该是唯一的。

  SnapCenter不支持不同集群上具有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工具收集有关系统健康状况的数据，并自动将数据发送给NetApp技术支持，使他们能够排除系统故障。

  如果启用这些功能，当资源受到保护、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日志。

- 如果您计划将快照复制到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，计划作业、按需备份和恢复操作可能会失败。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：

对于这个领域...	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 个或更少的字符，并且名称必须可解析。要创建名称超过 15 个字符的存储系统连接，可以使用 Add-SmStorageConnectionPowerShell cmdlet。 对于具有MetroCluster配置 (MCC) 的存储系统，建议同时注册本地集群和对等集群，以实现无中断操作。 SnapCenter不支持不同集群上具有相同名称的多个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。 如果使用短名称或 FQDN 添加了SVM，则它必须能够从SnapCenter和插件主机解析。
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	如果您想要将 EMS 消息发送到存储系统 syslog，或者想要将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。 当您选中 向存储系统发送失败操作的**AutoSupport** 通知 复选框时，也会选中 将**SnapCenter**服务器事件记录到 **syslog** 复选框，因为启用AutoSupport通知需要 EMS 消息传递。

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 是备份关系中的辅助存储系统，请选中 辅助 复选框。当选择“**Secondary**”选项时，SnapCenter不会立即执行许可证检查。

   如果您已在SnapCenter中添加了 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，通常是 HTTPS。

   b. 输入存储系统接受的端口。

默认端口 443 通常有效。

c. 输入停止通信尝试之前应经过的时间（以秒为单位）。

默认值是 60 秒。

d. 如果 SVM 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”。

5. 单击“提交”。

结果

在存储系统页面中，从*类型*下拉菜单中执行以下操作之一：

- 如果要查看已添加的所有 SVM，请选择 * ONTAP SVM *。

  如果您已添加 FSx SVM，则 FSx SVM 将在此处列出。

- 如果要查看所有已添加的集群，请选择* ONTAP集群*。

  如果您已使用 fsxadmin 添加了 FSx 集群，则 FSx 集群将在此处列出。

  单击集群名称时，集群中的所有 SVM 都会显示在存储虚拟机部分。

  如果使用ONTAP GUI 将新的 SVM 添加到ONTAP集群，请单击 重新发现 以查看新添加的 SVM。

完成后

集群管理员必须在每个存储系统节点上启用AutoSupport ，以便从SnapCenter有权访问的所有存储系统发送电子邮件通知，方法是从存储系统命令行运行以下命令：

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

存储虚拟机 (SVM) 管理员无权访问AutoSupport。

存储连接和凭证

在执行数据保护操作之前，您应该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

存储连接使SnapCenter服务器和SnapCenter插件能够访问ONTAP存储。设置这些连接还涉及配置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*\用户名
- 域 *FQDN*\用户名
- 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，请在要安装SnapCenter插件的系统上指定内置的本地管理员。如果用户帐户具有提升的权限或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*

- 各个资源组的凭证

  如果您为单个资源组设置凭据，并且用户名没有完全管理权限，则必须至少为该用户名分配资源组和备份权限。

在 **Windows** 主机上配置存储

创建和管理 **igroup**

您可以创建启动器组 (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。当您将 igroup 映射到 LUN 时，igroup 将在创建磁盘或连接磁盘向导中可用。

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“启动器组”页面中，单击“新建”。
4. 在创建 Igroup 对话框中，定义 igroup：

在这个领域...	操作
存储系统	选择要映射到 igroup 的 LUN 的 SVM。
主机	选择要在其上创建 igroup 的主机。
igroup 名称	输入 igroup 的名称。
启动程序	选择发起者。

在这个领域...	操作
类型	选择启动器类型：iSCSI、FCP 或混合（FCP 和 iSCSI）。

5. 当您对输入的内容满意时，请单击“确定”。

   SnapCenter在存储系统上创建 igroup。

重命名 **igroup**

您可以使用SnapCenter重命名现有的 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. 在启动器组页面中，单击 **Storage Virtual Machine** 字段以显示可用 SVM 的列表，然后选择要重命名的 igroup 的 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将 igroup 启动器添加到现有 igroup。创建 igroup 时，您只能添加一个主机。如果要为集群创建 igroup，则可以修改 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“启动器组”页面中，单击“**Storage Virtual Machine**”字段以显示可用 SVM 的下拉列表，然后选择要修改的 igroup 的 SVM。
4. 在 igroup 列表中，选择一个 igroup 并单击“将启动器添加到 igroup”。
5. 选择主机。
6. 选择启动器并单击“确定”。

删除 **igroup**

当您不再需要某个 igroup 时，可以使用SnapCenter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 **Igroup**。

3. 在“启动器组”页面中，单击“**Storage Virtual Machine**”字段以显示可用 SVM 的下拉列表，然后选择要删除的 igroup 的 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，只允许一个数据分区，对于 MBR，只允许一个主分区，该主分区具有一个使用 NTFS 或 CSVFS 格式化的卷和一个挂载路径。
- 支持的分区样式：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操作将不会成功。

查看主机上的磁盘

您可以使用SnapCenter查看管理的每个 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。

   磁盘已列出。

查看集群磁盘

您可以查看使用SnapCenter管理的群集上的群集磁盘。仅当您从“主机”下拉菜单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。

   磁盘已列出。

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。
- 您必须已经在存储系统上启动了 iSCSI 服务。 "了解更多"

关于此任务

您只能在相同的 IP 版本之间建立 iSCSI 会话，无论是从 IPv6 到 IPv6，还是从 IPv4 到 IPv4。

仅当主机和目标位于同一子网中时，才可以使用链路本地 IPv6 地址进行 iSCSI 会话管理以及主机和目标之间的通信。

如果更改 iSCSI 启动器的名称，则对 iSCSI 目标的访问会受到影响。更改名称后，您可能需要重新配置启动器访问的目标，以便它们能够识别新名称。更改 iSCSI 启动器的名称后，必须确保重新启动主机。

如果您的主机有多个 iSCSI 接口，一旦您使用第一个接口上的 IP 地址建立了与SnapCenter 的iSCSI 会话，您就无法从具有不同 IP 地址的另一个接口建立 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“存储虚拟机”下拉列表中，选择 iSCSI 目标的存储虚拟机 (SVM)。
4. 从“主机”下拉列表中，选择会话的主机。
5. 单击*建立会话*。

   将显示“建立会话”向导。

6. 在建立会话向导中，确定目标：

在这个领域...	进入...
目标节点名称	iSCSI 目标的节点名称 如果存在现有的目标节点名称，则以只读格式显示该名称。
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
发起者门户地址	发起者网络门户的 IP 地址

7. 当您对输入的内容满意时，请单击“连接”。

SnapCenter建立 iSCSI 会话。

8. 重复此过程为每个目标建立会话。

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。

如果您想在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

- 您必须已经在存储系统上为 LUN 创建了一个卷。

  该卷应该仅保存 LUN，并且仅保存使用SnapCenter创建的 LUN。

  除非克隆已被拆分，否则您无法在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。
- 如果您正在使用 iSCSI，则必须与存储系统建立 iSCSI 会话。
- 适用于 Windows 的SnapCenter插件包必须仅安装在要创建磁盘的主机上。

关于此任务

- 除非 Windows Server 故障转移群集中的主机共享 LUN，否则您无法将 LUN 连接到多个主机。
- 如果使用 CSV（群集共享卷）的 Windows Server 故障转移群集中的主机共享 LUN，则必须在拥有该群集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”。

   将打开创建磁盘向导。

5. 在 LUN 名称页面中，识别 LUN：

在这个领域...	操作
存储系统	选择 LUN 的 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。

在这个领域...	操作
簇大小	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	该 LUN 只能被一个主机访问。 忽略*资源组*字段。
共享磁盘	LUN 由 Windows Server 故障转移群集中的主机共享。 在“资源组”字段中输入集群资源组的名称。您只需在故障转移群集中的一个主机上创建磁盘。
集群共享卷 (CSV)	该 LUN 由使用 CSV 的 Windows Server 故障转移群集中的主机共享。 在“资源组”字段中输入集群资源组的名称。确保在其上创建磁盘的主机是群集组的所有者。

7. 在驱动器属性页面中，指定驱动器属性：

财产	描述
自动分配挂载点	SnapCenter根据系统驱动器自动分配卷挂载点。 例如，如果您的系统驱动器是 C:，则自动分配会在您的 C: 驱动器下创建一个卷装入点 (C:\scmnpt\)。共享磁盘不支持自动分配。
分配驱动器号	将磁盘安装到您在相邻下拉列表中选择的驱动器。
使用卷挂载点	将磁盘安装到您在相邻字段中指定的驱动器路径。 卷安装点的根目录必须由您正在创建磁盘的主机拥有。
不要分配驱动器号或卷装入点	如果您希望在 Windows 中手动安装磁盘，请选择此选项。

财产	描述
LUN 大小	指定 LUN 大小；最小 150 MB。 在相邻的下拉列表中选择 MB、GB 或 TB。
对托管此 LUN 的卷使用精简配置	精简配置 LUN。 精简配置一次仅分配所需的存储空间，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，或为主引导记录选择 MBR 分区。 MBR 分区可能会导致 Windows Server 故障转移群集中出现错位问题。 不支持统一可扩展固件接口 (UEFI) 分区磁盘。

8. 在映射 LUN 页面中，选择主机上的 iSCSI 或 FC 启动器：

在这个领域...	操作
主机	双击群集组名称，显示属于该群集的主机的下拉列表，然后选择启动器的主机。 仅当 LUN 由 Windows Server 故障转移群集中的主机共享时，才会显示此字段。
选择主机发起者	选择“光纤通道”或“**iSCSI**”，然后选择主机上的启动器。 如果您使用具有多路径 I/O (MPIO) 的 FC，则可以选择多个 FC 启动器。

9. 在“组类型”页面中，指定是否要将现有 igroup 映射到 LUN，还是创建新的 igroup：

选择...	条件
为选定的启动器创建新的 igroup	您想要为选定的启动器创建一个新的 igroup。

选择...	条件
为选定的启动器选择现有的 igroup 或指定新的 igroup	您想要为选定的启动器指定一个现有的 igroup，或者使用您指定的名称创建一个新的 igroup。 在 **igroup name** 字段中输入 igroup 名称。输入现有 igroup 名称的前几个字母以自动完成该字段。

10. 在“摘要”页面中，检查您的选择，然后单击“完成”。

    SnapCenter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求的变化增加或减少磁盘的大小。

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。
- 对于厚置备 LUN，可扩展大小（卷中的可用大小）显示为最大大小。
- 具有 MBR 样式分区的 LUN 的大小限制为 2 TB。
- 具有 GPT 样式分区的 LUN 的存储系统大小限制为 16 TB。
- 在调整 LUN 大小之前制作快照是一个好主意。
- 如果您需要从调整 LUN 大小之前创建的快照中恢复 LUN， SnapCenter会自动将 LUN 调整为快照的大小。

  恢复操作后，必须从调整大小后创建的快照中恢复调整大小后添加到 LUN 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。

   磁盘已列出。

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，或在“大小”字段中输入新大小。

   如果您手动输入尺寸，则需要单击“尺寸”字段外部，然后才能正确启用“收缩”或“扩展”按钮。此外，您必须单击 MB、GB 或 TB 来指定测量单位。

6. 当您对输入的内容满意时，请根据需要单击“收缩”或“扩展”。

   SnapCenter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。
- 如果您正在使用 iSCSI，则必须与存储系统建立 iSCSI 会话。
- 除非 Windows Server 故障转移群集中的主机共享 LUN，否则您无法将 LUN 连接到多个主机。
- 如果 LUN 由使用 CSV（群集共享卷）的 Windows Server 故障转移群集中的主机共享，则必须连接拥有群集组的主机上的磁盘。
- 仅需在连接磁盘的主机上安装适用于 Windows 的插件。

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”。

   将打开连接磁盘向导。

5. 在 LUN 名称页面中，确定要连接的 LUN：

在这个领域...	操作
存储系统	选择 LUN 的 SVM。
LUN 路径	单击“浏览”以选择包含 LUN 的卷的完整路径。
LUN 名称	输入 LUN 的名称。
簇大小	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	该 LUN 只能被一个主机访问。

选择...	条件
共享磁盘	LUN 由 Windows Server 故障转移群集中的主机共享。 您只需将磁盘连接到故障转移群集中的一台主机。
集群共享卷 (CSV)	该 LUN 由使用 CSV 的 Windows Server 故障转移群集中的主机共享。 确保连接到磁盘的主机是群集组的所有者。

7. 在驱动器属性页面中，指定驱动器属性：

财产	描述
自动分配	让SnapCenter根据系统驱动器自动分配卷挂载点。 例如，如果您的系统驱动器是 C:，则自动分配属性会在您的 C: 驱动器下创建一个卷装入点 (C:\scmnpt\)。共享磁盘不支持自动分配属性。
分配驱动器号	将磁盘安装到您在相邻下拉列表中选择的驱动器。
使用卷挂载点	将磁盘安装到您在相邻字段中指定的驱动器路径。 卷安装点的根目录必须由您正在创建磁盘的主机拥有。
不要分配驱动器号或卷装入点	如果您希望在 Windows 中手动安装磁盘，请选择此选项。

8. 在映射 LUN 页面中，选择主机上的 iSCSI 或 FC 启动器：

在这个领域...	操作
主机	双击集群组名称，显示属于该集群的主机的下拉列表，然后选择启动器的主机。 仅当 LUN 由 Windows Server 故障转移群集中的主机共享时，才会显示此字段。
选择主机发起者	选择“光纤通道”或“**iSCSI**”，然后选择主机上的启动器。 如果您使用带有 MPIO 的 FC，则可以选择多个 FC 启动器。

9. 在“组类型”页面中，指定是否要将现有 igroup 映射到 LUN 或创建新的 igroup：

选择...	条件
为选定的启动器创建新的 igroup	您想要为选定的启动器创建一个新的 igroup。
为选定的启动器选择现有的 igroup 或指定新的 igroup	您想要为选定的启动器指定一个现有的 igroup，或者使用您指定的名称创建一个新的 igroup。 在 **igroup name** 字段中输入 igroup 名称。输入现有 igroup 名称的前几个字母以自动完成该字段。

10. 在“摘要”页面中，检查您的选择并单击“完成”。

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

断开磁盘

您可以将 LUN 与主机断开连接，而不会影响 LUN 的内容，但有一个例外：如果在克隆分离之前断开连接，则会丢失克隆的内容。

开始之前

- 确保 LUN 未被任何应用程序使用。
- 确保 LUN 未被监控软件监控。
- 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都已打开电源、正常运行且可供SnapCenter使用。

关于此任务

如果断开SnapCenter创建的FlexClone卷中的某个 LUN 且该卷上没有连接任何其他 LUN，SnapCenter会删除该卷。在断开 LUN 之前， SnapCenter会显示一条消息，警告您FlexClone卷可能会被删除。

为避免自动删除FlexClone卷，您应该在断开最后一个 LUN 之前重命名该卷。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。

   磁盘已列出。

4. 选择要断开的磁盘，然后单击“断开连接”。
5. 在“断开磁盘”对话框中，单击“确定”。

   SnapCenter断开磁盘连接。

删除磁盘

当您不再需要磁盘时，可以将其删除。删除磁盘后，将无法恢复。

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。

   磁盘已列出。
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删除磁盘。

创建和管理 **SMB** 共享

要在存储虚拟机 (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，因为它使您能够利用SnapCenter提供的模板来自动化共享配置。

模板概括了卷和共享配置的最佳实践。您可以在 Windows 版SnapCenter插件包的安装文件夹中的 Templates 文件夹中找到这些模板。

如果您愿意，您可以按照提供的模型创建自己的模板。在创建自定义模板之前，您应该查看 cmdlet 文档中的参数。

创建 **SMB** 共享

您可以使用SnapCenter共享页面在存储虚拟机 (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“存储虚拟机”下拉列表中选择 SVM。
4. 单击“新建”。

   “新共享”对话框打开。
5. 在新建共享对话框中，定义共享：

在这个领域...	操作
描述	输入共享的描述性文本。
共享名称	输入共享名称，例如 test_share。 您输入的共享名称也将用作卷名称。 共享名称： • 必须是 UTF-8 字符串。 • 不得包含以下字符：从 0x00 到 0x1F（含）的控制字符、0x22（双引号）以及特殊字符 `\ / [ ] : (vertical bar) < > + = ; , ?`
共享路径	• 单击该字段以输入新的文件系统路径，例如 /。 • 双击该字段以从现有文件系统路径列表中进行选择。

6. 当您对输入的内容满意时，请单击“确定”。

   SnapCenter在 SVM 上创建 SMB 共享。

删除 **SMB** 共享

当您不再需要 SMB 共享时，可以将其删除。

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“存储虚拟机”字段以显示一个下拉菜单，其中包含可用存储虚拟机 (SVM) 的列表，然后选择要删除的共享的 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从 SVM 中删除 SMB 共享。

回收存储系统上的空间

尽管 NTFS 在文件被删除或修改时会跟踪 LUN 上的可用空间，但它不会将新信息报告给存储系统。您可以在适用于 Windows 主机的插件上运行空间回收 PowerShell cmdlet，以确保新释放的块在存储中标记为可用。

如果您在远程插件主机上运行 cmdlet，则必须运行 SnapCenterOpen-SMConnection cmdlet 才能打开与SnapCenter服务器的连接。

开始之前

- 您必须确保在执行恢复操作之前空间回收过程已完成。
- 如果 LUN 由 Windows Server 故障转移群集中的主机共享，则必须在拥有该群集组的主机上执行空间回收。
- 为了获得最佳存储性能，您应该尽可能频繁地执行空间回收。

  您应该确保已扫描整个 NTFS 文件系统。

关于此任务

- 空间回收非常耗时且占用大量 CPU 资源，因此最好在存储系统和 Windows 主机使用率较低时运行该操作。
- 空间回收几乎可以回收所有可用空间，但并非 100%。
- 您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。

步

在应用程序服务器 PowerShell 命令提示符下，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 GUI 执行主机配置和空间回收作业，则可以使用 PowerShell cmdlet。您可以直接使用 cmdlet 或将其添加到脚本中。

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

可以通过运行_Get-Help command_name_来获取有关可与 cmdlet 一起使用的参数及其描述的信息。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，请参阅 "卸载SnapDrive for Windows 时SnapCenter cmdlet 损坏"。

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 以及管理快照。

支持的 **VMware** 客户操作系统平台

- 支持的 Windows Server 版本
- Microsoft 群集配置

使用 Microsoft iSCSI Software Initiator 时，VMware 上最多支持 16 个节点，使用 FC 时最多支持两个节点

- RDM LUN

  对于普通 RDMS，最多支持 56 个 RDM LUN，配备四个 LSI Logic SCSI 控制器；对于 Windows 配置，VMware VM MSCS 盒对盒插件最多支持 42 个 RDM LUN，配备三个 LSI Logic SCSI 控制器

  支持 VMware ParaVirtual SCSI 控制器。 RDM 磁盘上可支持 256 个磁盘。

有关受支持版本的最新信息，请参阅 "NetApp 互操作性表工具"。

VMware ESXi 服务器相关限制

- 不支持使用 ESXi 凭据在虚拟机上的 Microsoft 群集上安装适用于 Windows 的插件。

  在集群虚拟机上安装适用于 Windows 的插件时，您应该使用 vCenter 凭据。

- 所有集群节点必须对同一个集群磁盘使用相同的目标 ID（在虚拟 SCSI 适配器上）。
- 当您在适用于 Windows 的插件之外创建 RDM LUN 时，必须重新启动插件服务以使其能够识别新创建的磁盘。
- 您不能在 VMware 客户操作系统上同时使用 iSCSI 和 FC 启动器。

SnapCenter RDM 操作所需的最低 **vCenter** 权限

您应该在主机上拥有以下 vCenter 权限才能在来宾操作系统中执行 RDM 操作：

- 数据存储：删除文件
- 主机：配置 > 存储分区配置
- 虚拟机：配置

您必须将这些权限分配给 Virtual Center Server 级别的角色。您分配了这些权限的角色不能分配给没有 root 权限的任何用户。

分配这些权限后，您可以在来宾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 的插件来管理使用 FC RDM LUN 的 Microsoft 群集，但必须首先在插件外部创建共享 RDM 仲裁和共享存储，然后将磁盘添加到群集中的虚拟机。

从 ESXi 5.5 开始，您还可以使用 ESX iSCSI 和 FCoE 硬件来管理 Microsoft 集群。 Windows 插件包括对 Microsoft 集群的开箱即用支持。

要求

当您满足特定的配置要求时，适用于 Windows 的插件可为 Microsoft 群集提供支持，这些群集使用属于两个不同 ESX 或 ESXi 服务器的两个不同虚拟机上的 FC RDM LUN，也称为跨箱群集。

- 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有两个网络适配器。
- 两个 ESX 或 ESXi 服务器之间必须共享至少一个 VMware 虚拟机文件系统 (VMFS) 数据存储。
- VMware 建议在 FC SAN 上创建共享数据存储。

  如果需要，还可以通过 iSCSI 创建共享数据存储。

- 共享 RDM LUN 必须处于物理兼容模式。
- 必须在 Windows 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。

- 必须在物理兼容模式下在群集中的每个虚拟机上配置 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。如果仅存在一个同类型的控制器并且该控制器已连接到 C: 驱动器，则共享 LUN 无法使用现有的 LSI Logic SAS 控制器。

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

  > 当您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，您必须在 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 虚拟机集群不能成为 VMware 集群的一部分。
- 在属于 Microsoft 群集的虚拟机上安装适用于 Windows 的插件时，必须使用 vCenter 凭据，而不是 ESX 或 ESXi 凭据。
- Windows 插件无法使用来自多个主机的启动器创建单个 igroup。

  在创建将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 主机的启动器的 igroup。

- 确保使用 FC 启动器在 ESXi 5.0 上创建 RDM LUN。

  创建 RDM LUN 时，将使用 ALUA 创建启动器组。

限制

Windows 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 群集。

> ESX 5.5i 之前的版本不支持此功能。

- Windows 插件不支持 ESX iSCSI 和 NFS 数据存储上的群集。
- Windows 插件不支持集群环境中的混合启动器。

  启动器必须是 FC 或 Microsoft iSCSI，但不能同时是两者。

- Microsoft 群集中的共享磁盘不支持 ESX iSCSI 启动器和 HBA。
- 如果虚拟机是 Microsoft 群集的一部分，则适用于 Windows 的插件不支持使用 vMotion 进行虚拟机迁移。

- Windows 插件不支持 Microsoft 群集中虚拟机上的 MPIO。

创建共享 **FC RDM LUN**

在使用 FC RDM LUN 在 Microsoft 群集中的节点之间共享存储之前，您必须首先创建共享仲裁磁盘和共享存储磁盘，然后将它们添加到群集中的两个虚拟机。

共享磁盘不是使用 Windows 插件创建的。您应该创建共享 LUN，然后将其添加到群集中的每个虚拟机。有关信息，请参阅 "跨物理主机集群虚拟机"。

添加基于**SnapCenter Standard** 控制器的许可证

如果您使用FAS、 AFF或ASA存储控制器，则需要基于SnapCenter Standard 控制器的许可证。

基于控制器的许可证具有以下特点：

- 购买 Premium 或 Flash Bundle 即可获得SnapCenter Standard 权利（不包含在基础包中）
- 无限存储使用
- 使用ONTAP系统管理器或ONTAP CLI 直接添加到FAS、 AFF或ASA存储控制器。

  您无需在SnapCenter用户界面中输入基于SnapCenter控制器的许可证的任何许可证信息。

- 锁定到控制器的序列号

有关所需许可证的信息，请参阅"SnapCenter许可证"。

步骤 **1**：验证是否安装了**SnapManager Suite** 许可证

您可以使用SnapCenter用户界面检查FAS、 AFF或ASA主存储系统上是否安装了SnapManager Suite 许可证，并确定哪些系统需要许可证。SnapManager Suite 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有SnapManager Suite 许可证， SnapCenter会自动提供基于标准控制器的许可证授权。SnapManagerSuite 许可证和基于SnapCenter Standard 控制器的许可证这两个名称可以互换使用，但它们指的是同一个许可证。

步骤

1. 在左侧导航窗格中，选择*存储系统*。
2. 在“存储系统”页面中，从“类型”下拉菜单中选择是否查看已添加的所有 SVM 或集群：
   - 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集群”。

     当您选择集群名称时，集群中的所有 SVM 都会显示在 Storage Virtual Machines 部分。
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 Suite 许可证已安装在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 Suite 许可证。
- 不适用表示SnapManager Suite 许可证不适用，因为存储控制器位于Amazon FSx for NetApp ONTAP、Cloud Volumes ONTAP、 ONTAP Select或辅助存储平台上。

第 **2** 步：识别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系统上的集群管理员。

控制器将基于SnapCenter Standard 控制器的许可证显示为 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，然后查看输出以查看是否已安装 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: 1-81-00000000000000000000000xx
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 -
```

   在示例中，已安装 SnapManagerSuite 许可证，因此不需要额外的SnapCenter许可操作。

步骤 **3**：检索控制器序列号

使用ONTAP命令行获取控制器序列号。您必须是FAS、 AFF或ASA系统上的集群管理员才能获取基于控制器的许可证序列号。

步骤

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

   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。

步骤 **4**：检索基于控制器的许可证的序列号

如果您使用的是FAS、 ASA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

- 您应该拥有有效的NetApp支持站点登录凭据。

  如果您没有输入有效的凭证，系统将不会返回任何有关您搜索的信息。

- 您应该有控制器序列号。

步骤

1. 登录 "NetApp 支持站点"。
2. 导航到*系统* > 软件许可证。
3. 在选择标准区域，确保选择了序列号（位于设备背面），输入控制器序列号，然后选择*Go!*。

显示指定控制器的许可证列表。

4. 找到并记录SnapCenter Standard 或 SnapManagerSuite 许可证。

步骤 **5**：添加基于控制器的许可证

当您使用FAS、 AFF或ASA系统并且拥有SnapCenter Standard 或 SnapManagerSuite 许可证时，您可以使用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系统上的集群管理员。
- 您应该拥有SnapCenter Standard 或 SnapManagerSuite 许可证。

关于此任务

如果您想使用FAS、 AFF或ASA存储试用安装SnapCenter ，您可以获取 Premium Bundle 评估许可证以安装在控制器上。

如果您想试用安装SnapCenter ，您应该联系您的销售代表以获取 Premium Bundle 评估许可证以安装在您的控制器上。

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
   ```

   此命令在管理员权限级别可用。

3. 验证是否已安装 SnapManagerSuite 许可证：

   ```
   license show
   ```

步骤 **6**：删除试用许可证

如果您正在使用基于控制器的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 命令手动删除试用许可证。无法使用SnapCenter用户界面删除试用许可证。

仅当您使用基于SnapCenter Standard 控制器的许可证时才需要手动删除试用许可证。

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 帐户与SnapCenter服务器建立连接。
   b. 运行 Set-SmRepositoryPassword 重置 MySQL 密码。

      有关 cmdlet 的信息，请参阅 "SnapCenter软件 Cmdlet 参考指南"。

2. 打开命令提示符并运行mysql -u root -p登录MySQL。

   MySQL 提示您输入密码。输入您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';
   ```

配置高可用性

配置**SnapCenter**服务器以实现高可用性

为了支持在 Windows 或 Linux 上运行的SnapCenter中的高可用性 (HA)，您可以安装 F5 负载平衡器。 F5 使SnapCenter服务器能够支持位于同一位置的最多两台主机的主动-被动配置。要在SnapCenter中使用 F5 负载均衡器，您应该配置SnapCenter服务器并配置 F5 负载均衡器。

您还可以配置网络负载平衡 (NLB) 来设置SnapCenter高可用性。您应该在SnapCenter安装之外手动配置 NLB 以实现高可用性。

对于云环境，您可以使用 Amazon Web Services (AWS) 弹性负载平衡 (ELB) 和 Azure 负载均衡器配置高可用性。

使用 **F5** 配置高可用性

有关使用 F5 负载平衡器配置SnapCenter服务器以实现高可用性的说明，请参阅 "如何使用 F5 负载均衡器配置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（除了分配有 SnapCenterAdmin 角色之外），才能使用以下 cmdlet 添加和删除 F5 群集：

- 添加SmServerCluster
- 添加SmServer
- 删除-SmServerCluster

  有关更多信息，请参阅 "SnapCenter软件 Cmdlet 参考指南" 。

追加信息

- 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，并且还存在现有的SnapCenter会话，则必须关闭浏览器并再次登录SnapCenter 。
- 在负载平衡器设置（NLB 或 F5）中，如果添加由 NLB 或 F5 主机部分解析的主机，并且如果SnapCenter主机无法连接到该主机，则SnapCenter主机页面会在主机关闭和运行状态之间频繁切换。要解决此问题，您应该确保两个SnapCenter主机都能够解析 NLB 或 F5 主机中的主机。
- 应在所有主机上执行 MFA 设置的SnapCenter命令。依赖方配置应使用 F5 群集详细信息在 Active Directory 联合身份验证服务 (AD FS) 服务器中完成。启用 MFA 后，主机级SnapCenter UI 访问将被阻止。
- 在故障转移期间，审计日志设置不会反映在第二台主机上。因此，当 F5 被动主机变为主动主机时，您应该手动重复审核日志设置。

使用网络负载平衡 **(NLB)** 配置高可用性

您可以配置网络负载平衡 (NLB) 来设置SnapCenter高可用性。您应该在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，请参阅 "如何使用SnapCenter配置 NLB"。

使用 **AWS Elastic Load Balancing (ELB)** 配置高可用性

您可以在 Amazon Web Services (AWS) 中配置高可用性SnapCenter环境，方法是在不同的可用区域 (AZ) 中设置两个SnapCenter服务器并对其进行配置以实现自动故障转移。该架构包括虚拟专用IP地址、路由表以及主备MySQL数据库之间的同步。

步骤

1. 在 AWS 中配置虚拟专用覆盖 IP。有关信息，请参阅 "配置虚拟专用覆盖 IP"。
2. 准备 Windows 主机
   a. 强制 IPv4 优先级高于 IPv6：
      - 位置：HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
      - 键：DisabledComponents

- 类型：REG_DWORD
- 值：0x20

b. 确保完全限定域名可以通过 DNS 或本地主机配置解析为 IPv4 地址。

c. 确保您没有配置系统代理。

d. 当使用没有 Active Directory 的设置并且服务器不在一个域中时，请确保两个 Windows Server 上的管理员密码相同。

e. 在两个 Windows 服务器上添加虚拟 IP。

3. 创建SnapCenter集群。

a. 启动 Powershell 并连接到SnapCenter。 `Open-SmConnection`

b. 创建集群。 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`

c. 添加辅助服务器。 `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`

d. 获取高可用性详细信息。 `Get-SmServerConfig`

4. 创建 Lamda 函数以在虚拟私有 IP 端点不可用时调整路由表，并由 AWS CloudWatch 监控。有关信息，请参阅 "创建 Lambda 函数"。

5. 在 CloudWatch 中创建一个监视器来监控SnapCenter端点的可用性。如果端点无法访问，则配置警报以触发 Lambda 函数。 Lambda 函数调整路由表以将流量重定向到活动的SnapCenter服务器。有关信息，请参阅 "创建合成金丝雀"。

6. 使用步骤函数实现工作流作为 CloudWatch 监控的替代方案，从而提供更短的故障转移时间。该工作流程包括一个用于测试SnapCenter URL 的 Lambda 探测函数、一个用于存储故障计数的 DynamoDB 表以及 Step Function 本身。

a. 使用 lambda 函数探测SnapCenter URL。有关信息，请参阅 "创建 Lambda 函数"。

b. 创建一个 DynamoDB 表来存储两次 Step Function 迭代之间的失败计数。有关信息，请参阅 "DynamoDB 表入门"。

c. 创建步进函数。有关信息，请参阅 "Step Function 文档"。

d. 测试单个步骤。

e. 测试完整功能。

f. 创建 IAM 角色并调整权限以允许执行 Lambda 函数。

g. 创建计划以触发 Step Function。有关信息，请参阅 "使用 Amazon EventBridge Scheduler 启动 Step Functions"。

使用 **Azure** 负载均衡器配置高可用性

您可以使用 Azure 负载均衡器配置高可用性SnapCenter环境。

步骤

1. 使用 Azure 门户在规模集中创建虚拟机。 Azure 虚拟机规模集允许您创建和管理一组负载平衡的虚拟机。虚拟机实例的数量可以根据需求或定义的时间表自动增加或减少。有关信息，请参阅 "使用 Azure 门户在规模集中创建虚拟机"。

2. 配置虚拟机后，登录 VM 集中的每个虚拟机并在两个节点上安装SnapCenter Server。
3. 在主机 1 中创建集群。 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. 添加辅助服务器。 `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. 获取高可用性详细信息。 `Get-SmServerConfig`
6. 如果需要，重建辅助主机。 `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. 故障转移到第二台主机。 `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== 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" 。
2. 在SnapCenter服务器主机上，启动 PowerShell。
3. 使用 Open-SmConnection cmdlet 启动会话，然后输入您的凭据。
4. 使用 Update-SmServerCluster cmdlet 更新SnapCenter服务器以指向 F5 集群 IP 地址。

   可以通过运行_Get-Help command_name_来获取有关可与 cmdlet 一起使用的参数及其描述的信息。或者，您也可以参考 "SnapCenter软件 Cmdlet 参考指南"。

SnapCenter MySQL 存储库的高可用性

MySQL 复制是 MySQL 服务器的一项功能，它使您能够将数据从一个 MySQL 数据库服务器（主服务器）复制到另一个 MySQL 数据库服务器（从服务器）。 SnapCenter仅在两个启用网络负载平衡 (NLB) 的节点上支持 MySQL 复制以实现高可用性。

SnapCenter在主存储库上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属存储库。然后从属存储库将成为主存储库。 SnapCenter还支持反向复制，该功能仅在故障转移期间启用。

如果要使用 MySQL 高可用性 (HA) 功能，则必须在第一个节点上配置网络负载均衡器 (NLB)。 MySQL 存储库作为安装的一部分安装在此节点上。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 *Get-SmRepositoryConfig* 和 *Set-SmRepositoryConfig* PowerShell cmdlet 来管理 MySQL 复制。

可以通过运行_Get-Help command_name_来获取有关可与 cmdlet 一起使用的参数及其描述的信息。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 安装或反之亦然，也不支持从 MySQL 独立安装切换到 MySQL HA。
- 如果从属存储库数据与主存储库数据不同步，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。

- 当启动故障转移时，正在运行的作业可能会失败。

  如果由于 MySQL 服务器或SnapCenter服务器关闭而发生故障转移，则任何正在运行的作业都可能失败。故障转移到第二个节点后，所有后续作业均成功运行。

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

配置基于角色的访问控制 (RBAC)

创建角色

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

要创建自己的角色，必须以“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. 为新角色指定名称和描述。

   用户名和组名中只能使用以下特殊字符：空格（ ）、连字符（-）、下划线（_）和冒号（: ）。

5. 选择“此角色的所有成员都可以看到其他成员的对象”，使该角色的其他成员在刷新资源列表后可以看到卷和主机等资源。

   如果您不希望该角色的成员看到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属于同一角色，则无需为用户分配对对象或资源的访问权限。

6. 在“权限”页面中，选择要分配给角色的权限，或单击“全选”将所有权限授予角色。
7. 单击“提交”。

使用安全登录命令添加**NetApp ONTAP RBAC** 角色

当您的存储系统运行集群ONTAP时，您可以使用安全登录命令添加NetApp ONTAP RBAC角色。

开始之前

- 确定您要执行的任务以及执行这些任务所需的权限。
- 授予命令和/或命令目录权限。

  每个命令/命令目录有两种访问级别：全部访问和只读。

  您必须始终首先分配所有访问权限。

- 为用户分配角色。
- 根据您的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内的 SVM 来确定您的配置。

关于此任务

为了简化存储系统上这些角色的配置，您可以使用NetApp ONTAP工具的 RBAC 用户创建器，该工具发布在NetApp社区论坛上。

该工具会自动正确设置ONTAP权限。例如， NetApp ONTAP的 RBAC User Creator 工具会自动按正确的顺序添加权限，以便所有访问权限首先出现。如果您先添加只读权限，然后添加所有访问权限，ONTAP会将所有访问权限标记为重复并忽略它们。

> 如果您稍后升级SnapCenter或ONTAP，则应重新运行NetApp ONTAP的 RBAC User Creator 工具来更新您之前创建的用户角色。为早期版本的SnapCenter或ONTAP创建的用户角色无法与升级后的版本正常配合使用。当您重新运行该工具时，它会自动处理升级。您不需要重新创建角色。

有关设置ONTAP RBAC 角色的更多信息，请参阅 "ONTAP 9 管理员身份验证和 RBAC 电源指南"。

步骤

1. 在存储系统上，输入以下命令创建新角色：

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

   - svm_name 是 SVM 的名称。如果将其留空，则默认为集群管理员。
   - role_name 是您为角色指定的名称。
   - 命令是ONTAP功能。

     > 您必须对每个权限重复此命令。请记住，全访问命令必须列在只读命令之前。

   有关权限列表的信息，请参阅"用于创建角色和分配权限的ONTAP CLI 命令"。

2. 通过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 是您正在创建的用户的名称。

- <password> 是您的密码。如果您未指定密码，系统将提示您输入密码。
- svm_name 是 SVM 的名称。

3. 通过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。此命令允许您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。如果您未指定密码，系统将提示您输入密码。

4. 通过输入以下命令验证用户是否已正确创建：

```
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中为新的 SVM 用户创建角色时，必须运行几个ONTAP CLI 命令。如果您在ONTAP中配置 SVM 以与SnapCenter一起使用并且不想使用 vsadmin 角色，则需要此角色。

步骤

1. 在存储系统上创建一个角色，并为该角色赋予所有权限。

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

您应该对每个权限重复此命令。

2. 创建一个用户并将角色分配给该用户。

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

3. 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 CLI** 命令

您应该运行几个ONTAP CLI 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 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 modify-snaplock-expiry-time" -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 snapshot show-delta" -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
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`

为**ASA r2** 系统创建 **SVM** 角色

您必须运行几个ONTAP CLI 命令才能在ASA r2 系统中为新的 SVM 用户创建角色。如果您在ASA r2 系统中配置 SVM 以与SnapCenter一起使用并且不想使用 vsadmin 角色，则需要此角色。

步骤

1. 在存储系统上创建一个角色，并为该角色赋予所有权限。

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

   您应该对每个权限重复此命令。

2. 创建一个用户并将角色分配给该用户。

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

3. 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 CLI** 命令

您应该运行几个ONTAP CLI 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 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 modify-snaplock-expiry-time" -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 snapshot show-delta" -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
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

创建具有最低权限的**ONTAP**集群角色

您应该创建具有最小权限的ONTAP集群角色，这样您就不必使用ONTAP管理员角色在SnapCenter中执行操作。您可以运行多个ONTAP CLI 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，并为该角色赋予所有权限。

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

   您应该对每个权限重复此命令。

2. 创建一个用户并将角色分配给该用户。

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

3. 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 CLI** 命令

您应该运行几个ONTAP CLI 命令来创建集群角色并分配权限。

- `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 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 "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"nvme subsystem modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- 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 snapshot modify-snaplock-expiry-time" -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 snapshot show-delta" -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`

为**ASA r2** 系统创建**ONTAP**集群角色

您应该创建具有最小权限的ONTAP集群角色，这样您就不必使用ONTAP管理员角色

在SnapCenter中执行操作。您可以运行多个ONTAP CLI 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，并为该角色赋予所有权限。

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

> 您应该对每个权限重复此命令。

2. 创建一个用户并将角色分配给该用户。

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

3. 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 CLI** 命令

您应该运行几个ONTAP CLI 命令来创建集群角色并分配权限。

- `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 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 "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- 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 snapshot modify-snaplock-expiry-time" -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 snapshot show-delta" -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
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all

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。角色决定了SnapCenter用户可以访问的选项。

开始之前

- 您必须以“SnapCenterAdmin”角色登录。
- 您必须已经在操作系统或数据库的 Active Directory 中创建了用户或组帐户。您不能使用SnapCenter创建这些帐户。

  用户名和组名中只能包含以下特殊字符：空格 ( )、连字符 (-)、下划线 (_) 和冒号 (:)。

- SnapCenter包含几个预定义的角色。

  您可以将这些角色分配给用户或创建新角色。

- 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。
- 将角色分配给包含适当权限的用户或组后，必须为该用户分配对SnapCenter资产（例如主机和存储连接）的访问权限。

这使用户能够对分配给他们的资产执行他们有权限执行的操作。

- 您应该在某个时候为用户或组分配一个角色，以利用 RBAC 权限和效率。
- 您可以在创建用户或组时为用户分配主机、资源组、策略、存储连接、插件和凭证等资产。
- 您应分配给用户执行某些操作的最低资产如下：

操作	资产转让
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

- 当将新节点添加到 Windows 群集或 DAG（Exchange Server 数据库可用性组）资产时，如果将此新节点分配给用户，则必须将资产重新分配给用户或组，以将新节点包含到用户或组。

  您应该将 RBAC 用户或组重新分配给群集或 DAG，以将新节点包含到 RBAC 用户或组。例如，您有一个双节点集群，并且已为该集群分配了 RBAC 用户或组。当您向集群添加另一个节点时，您应该将 RBAC 用户或组重新分配给集群，以便为 RBAC 用户或组包含新节点。

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

  您应该在向用户分配访问权限之前添加资产。

如果您使用适用SnapCenter Plug-in for VMware vSphere功能来保护虚拟机、VMDK 或数据存储区，则应使用 VMware vSphere GUI 将 vCenter 用户添加到SnapCenter Plug-in for VMware vSphere角色。有关 VMware vSphere 角色的信息，请参阅 "SnapCenter Plug-in for VMware vSphere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：

对于这个领域...	操作
访问类型	选择域或工作组 对于域身份验证类型，您应该指定要将用户添加到角色的用户或组的域名。 默认情况下，它预先填充了登录的域名。 您必须在*设置* > 全局设置 > *域设置*页面中注册不受信任的域。
类型	选择用户或组 SnapCenter仅支持安全组，不支持分发组。
用户名	a. 输入部分用户名，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。 当您从不同的域或不受信任的域添加用户时，您应该完整地输入用户名，因为没有跨域用户的搜索列表。 重复此步骤以将其他用户或组添加到所选角色。
角色	选择您想要添加用户的角色。

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。

      仅当用户将资产添加到SnapCenter时，才会列出资产。

   c. 对所有所需资产重复此过程。
   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。

配置审核日志设置

SnapCenter服务器的每个活动都会生成审计日志。默认情况下，审计日志保存在默认安装位置 *C:\Program Files\ NetApp\ SnapCenter WebApp\audit*。

通过为每个审计事件生成数字签名摘要来保护审计日志，以防止未经授权的修改。生成的摘要保存在单独的审计校验和文件中，并进行定期的完整性检查以确保内容的完整性。

您应该以“SnapCenterAdmin”角色登录。

关于此任务

- 在以下情况下会发送警报：
  - 审计日志完整性检查计划或 Syslog 服务器已启用或禁用
  - 审计日志完整性检查、审计日志或 Syslog 服务器日志故障
  - 磁盘空间不足
- 仅当完整性检查失败时才发送电子邮件。
- 您应该同时修改审计日志目录和审计校验和日志目录路径。您不能只修改其中一个。
- 当审计日志目录和审计校验和日志目录路径被修改时，无法对先前位置的审计日志执行完整性检查。
- 审计日志目录和审计校验和日志目录路径应位于SnapCenter Server 的本地驱动器上。

  不支持共享或网络安装的驱动器。
- 如果在 Syslog 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 命令来配置审计日志。

  可以通过运行 Get-Help command_name 获取有关可与 cmdlet 一起使用的参数及其描述的信息。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*>*审计日志设置*。
2. 在审计日志部分，输入详细信息。
3. 进入*审计日志目录*和*审计校验和日志目录*
   a. 输入最大文件大小
   b. 输入最大日志文件数
   c. 输入磁盘空间使用率百分比以发送警报
4. （可选）启用*记录 UTC 时间*。
5. （可选）启用*审计日志完整性检查计划*并单击*开始完整性检查*进行按需完整性检查。

   您还可以运行*Start-SmAuditIntegrityCheck*命令来启动按需完整性检查。
6. （可选）启用转发审计日志到远程系统日志服务器并输入系统日志服务器详细信息。

您应该将 Syslog 服务器中的证书导入 TLS 1.2 协议的“受信任的根”。

a. 输入 Syslog 服务器主机
b. 输入 Syslog 服务器端口
c. 输入 Syslog 服务器协议
d. 输入 RFC 格式

7. 单击“保存”。
8. 您可以通过单击“监视”>“作业”查看审计完整性检查和磁盘空间检查。

使用SnapCenter Server 配置安全的 MySQL 连接

如果您想在独立配置或网络负载平衡 (NLB) 配置中保护SnapCenter服务器和 MySQL 服务器之间的通信，则可以生成安全套接字层 (SSL) 证书和密钥文件。

为独立SnapCenter服务器配置配置安全的 MySQL 连接

如果您想确保SnapCenter服务器和 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。

生成以下证书：

- CA 证书
- 服务器公钥和私钥文件
- 客户端公钥和私钥文件

步骤

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

   有关信息，请参阅 "MySQL 版本 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：*您应该使用服务器完全限定域名 (FQDN) 作为服务器证书的通用名称。

2. 将 SSL 证书和密钥文件复制到 MySQL 数据文件夹。

   默认的 MySQL 数据文件夹路径是 `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、服务器公钥、客户端公钥、服务器私钥、客户端私钥路径。

   默认的 MySQL 服务器配置文件（my.ini）路径是 `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、服务器公共证书和服务器私钥路径。

您必须在 MySQL 服务器配置文件（my.ini）的 [client] 部分中指定 CA 证书、客户端公共证书和客户端私钥路径。

以下示例显示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 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 (IIS) 中的SnapCenter Server Web 应用程序。
5. 重新启动 MySQL 服务。
6. 更新SnapManager文件中 MySQLProtocol 键的值。

   以下示例显示了SnapManager文件中更新的 MySQLProtocol 键的值。

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

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

   以下示例显示了 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" />
```

8. 在 IIS 中启动SnapCenter Server Web 应用程序。

为 **HA** 配置配置安全的 **MySQL** 连接

如果您想确保SnapCenter服务器和 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。

生成以下证书：

- CA 证书

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

- 两个 HA 节点的服务器公共证书和服务器私钥文件
- 两个 HA 节点的客户端公共证书和客户端私钥文件

步骤

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

   有关信息，请参阅 "MySQL 版本 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：*您应该使用服务器完全限定域名 (FQDN) 作为服务器证书的通用名称。

2. 将 SSL 证书和密钥文件复制到 MySQL 数据文件夹。

   默认 MySQL 数据文件夹路径为 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、服务器公钥、客户端公钥、服务器私钥、客户端私钥路径。

   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、服务器公共证书和服务器私钥路径。

您必须在 MySQL 服务器配置文件（my.ini）的 [client] 部分中指定 CA 证书、客户端公共证书和客户端私钥路径。

以下示例显示复制到默认文件夹 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 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钥证书、服务器私钥文件、客户端公钥证书和客户端私钥文件。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 文件夹中。

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

      您不能再次创建 CA 证书。您应该只创建服务器公共证书、客户端公共证书、服务器私钥文件和客户端私钥文件。

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

      "MySQL 版本 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 作为服务器证书的通用名称。

c. 将 SSL 证书和密钥文件复制到 MySQL 数据文件夹。

d. 更新MySQL服务器配置文件（my.ini）中的CA证书、服务器公钥、客户端公钥、服务器私钥、客户端私钥路径。

您必须在 MySQL 服务器配置文件（my.ini）的 [mysqld] 部分中指定 CA 证书、服务器公共证书和服务器私钥路径。

您必须在 MySQL 服务器配置文件（my.ini）的 [client] 部分中指定 CA 证书、客户端公共证书和客户端私钥路径。

以下示例显示复制到默认文件夹 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 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. 停止两个 HA 节点上的 Internet 信息服务器 (IIS) 中的SnapCenter Server 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SnapManager.Web.UI.dll.config 文件中 MySQLProtocol 键的值。

   以下示例显示了SnapManager文件中更新的 MySQLProtocol 键的值。

   ```
   <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SnapManager.Web.UI.dll.config 文件。

   以下示例显示了 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" />
   ```

9. 在两个 HA 节点上的 IIS 中启动SnapCenter Server Web 应用程序。
10. 在其中一个 HA 节点上使用带有 -Force 选项的 Set-SmRepositoryConfig -RebuildSlave -Force PowerShell cmdlet 在两个 HA 节点上建立安全的 MySQL 复制。

    即使复制状态良好，-Force 选项也允许您重建从属存储库。

配置基于证书的身份验证

基于证书的身份验证通过验证SnapCenter服务器和插件主机的身份来增强安全性，确保安全和加密的通信。

启用基于证书的身份验证

要为SnapCenter Server 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 时将启用基于证书的身份验证。

- 要启用基于客户端证书的身份验证：

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

- 要禁用基于客户端证书的身份验证：

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

从SnapCenter服务器导出证书颁发机构 (CA) 证书

您应该使用 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

您应该已经配置了双向 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“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 Server 的采购 CA 证书，然后选择 所有任务 > 导出 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	点击*浏览*并指定保存证书的文件路径，然后点击*下一步*。
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SnapCenter Plug-in for VMware vSphere不支持基于证书的身份验证。

将 CA 证书导入 Windows 插件主机

要使用导出的SnapCenter Server CA 证书，您应该使用 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“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. 右键单击文件夹“个人”，然后选择*所有任务* > *导入*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...
商店位置	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”。
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 UNIX 插件主机

您应该将 CA 证书导入到 UNIX 插件主机。

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 密钥库的密码和私钥的所有相关别名的密码应该相同。

步骤

1. 您可以从 SPL 属性文件中检索 SPL 密钥库默认密码。它是键对应的值 `SPL_KEYSTORE_PASS`。
2. 更改密钥库密码： `$ keytool -storepasswd -keystore keystore.jks`
3. 将密钥库中所有私钥条目别名的密码更改为与密钥库相同的密码： `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. 对密钥 SPL_KEYSTORE_PASS 进行相同的更新 `spl.properties``文件。
5. 修改密码后重启服务。

将根证书或中间证书配置到 **SPL** 信任库

您应该将根证书或中间证书配置到 SPL 信任库。您应该添加根 CA 证书，然后添加中间 CA 证书。

步骤

1. 导航到包含 SPL 密钥库的文件夹： `/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到 SPL 信任库后重新启动服务。

将 **CA** 签名密钥对配置到 **SPL** 信任库

您应该将 CA 签名的密钥对配置到 SPL 信任库。

步骤

1. 导航到包含 SPL 密钥库的文件夹 `/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. 添加具有私钥和公钥的 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添加到密钥库的新 CA 证书相对应的别名。
7. 将添加的CA证书私钥密码更改为keystore密码。

   默认 SPL 密钥库密码是密钥 SPL_KEYSTORE_PASS 的值 `spl.properties`文件。

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

8. 如果CA证书中的别名较长，且包含空格或特殊字符（“*”，“，”），请将别名修改为简单名称： `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. 从位于的密钥库配置别名 `spl.properties`文件。根据键 SPL_CERTIFICATE_ALIAS 更新此值。
10. 将 CA 签名密钥对配置到 SPL 信任库后重新启动服务。

导出**SnapCenter**证书

您应该以 .pfx 格式导出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 > 受信任的根证书颁发机构 > 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	选择选项*是，导出私钥*，然后单击*下一步*。
导出文件格式	不做任何更改；单击“下一步”。
安全性	指定导出证书要使用的新密码，然后单击“下一步”。
要导出的文件	指定导出证书的文件名（必须使用.pfx），然后单击“下一步”。
完成证书导出向导	查看摘要，然后单击“完成”开始导出。

为 Windows 主机配置 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。该证书将有一个与之关联的私钥。

CSR 是一段编码文本，提供给授权证书供应商以获取签名的 CA 证书。

CA 证书 RSA 密钥长度必须至少为 3072 位。

有关生成 CSR 的信息，请参阅 "如何生成CA证书CSR文件"。

如果您拥有您的域（*.domain.company.com）或您的系统（machine1.domain.company.com）的 CA 证书，您可以跳过生成 CA 证书 CSR 文件。您可以使用SnapCenter部署现有的 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）和相应的主机名。在获取证书之前，可以通过填写主题备用名称 (SAN) 字段来更新证书。对于通配符证书（*.domain.company.com），该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SnapCenter服务器和 Windows 主机插件。

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“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 > 受信任的根证书颁发机构 > 证书。

5. 右键单击文件夹“受信任的根证书颁发机构”，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	选择选项*是*，导入私钥，然后单击*下一步*。
导入文件格式	不做任何更改；单击“下一步”。
安全性	指定导出证书要使用的新密码，然后单击“下一步”。
完成证书导入向导	查看摘要，然后单击“完成”开始导入。

导入证书时需携带私钥（支持格式为：**.pfx**、.p12、*.p7b）。

7. 对“个人”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出来的。

步骤

1. 在 GUI 上执行以下操作：
   a. 双击该证书。
   b. 在证书对话框中，单击“详细信息”选项卡。
   c. 滚动浏览字段列表并单击“指纹”。
   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”，删除空格后，将为：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 从 PowerShell 执行以下操作：
   a. 运行以下命令列出已安装证书的指纹并通过主题名称识别最近安装的证书。

      Get-ChildItem -Path 证书*:\LocalMachine\My*

   b. 复制指纹。

使用 **Windows** 主机插件服务配置 **CA** 证书

您应该使用 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服务器和所有已部署 CA 证书的插件主机上执行以下步骤。

步骤

1. 通过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
   ```

. 通过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

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

步骤

1. 在安装了SnapCenter的 Windows Server 上打开 IIS 管理器。
2. 在左侧导航窗格中，单击“连接”。
3. 展开服务器的名称和*站点*。
4. 选择要安装 SSL 证书的SnapCenter网站。
5. 导航到*操作* > 编辑站点，单击*绑定*。
6. 在绑定页面中，选择“https 绑定”。
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”。

SnapCenter Scheduler 站点（默认端口：8154，HTTPS）配置了自签名证书。此端口在SnapCenter Server 主机内进行通信，并且不需要使用 CA 证书进行配置。但是，如果您的环境要求您使用 CA 证书，请使用SnapCenter Scheduler 站点重复步骤 5 到 9。

如果下拉菜单中未列出最近部署的 CA 证书，请检查该 CA 证书是否与私钥相关联。

确保使用以下路径添加证书：控制台根 > 证书 - 本地计算机 > 受信任的根证书颁发机构 > 证书。

为SnapCenter启用 CA 证书

您应该配置 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。

可以通过运行_Get-Help command_name_来获取有关可与 cmdlet 一起使用的参数及其描述的信息。或者，您可以参考 "SnapCenter软件 Cmdlet 参考指南"。

步骤

1. 在“设置”页面中，导航至“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

托管主机选项卡主机显示一个挂锁，挂锁的颜色表示SnapCenter服务器和插件主机之间的连接状态。

- * * 表示没有启用或分配给插件主机的 CA 证书。
- * * 表示 CA 证书验证成功。
- * * 表示无法验证 CA 证书。
- * * 表示无法检索连接信息。

当状态为黄色或绿色时，表示数据保护操作成功完成。

为Linux主机配置CA证书

在 Linux 上安装SnapCenter服务器后，安装程序会创建自签名证书。如果要使用 CA 证书，则应配置 nginx 反向代理、审计日志和SnapCenter服务的证书。

配置nginx证书

步骤

1. 导航到_/etc/nginx/conf.d_： `cd /etc/nginx/conf.d`
2. 使用 vi 或任何文本编辑器打开 **snapcenter.conf**。
3. 导航到配置文件中的服务器部分。
4. 修改_ssl_certificate_和_ssl_certificate_key_的路径以指向CA证书。
5. 保存并关闭此文件。
6. 重新加载 nginx： `$nginx -s reload`

配置审核日志证书

步骤

1. 使用 vi 或任何文本编辑器打开 _INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager。

   INSTALL_DIR 的默认值是 */opt*。

2. 编辑 **AUDILOG_CERTIFICATE_PATH** 和 **AUDILOG_CERTIFICATE_PASSWORD** 键以分别包含 CA 证书路径和密码。

   审计日志证书仅支持 *.pfx* 格式。

3. 保存并关闭此文件。
4. 重新启动 **snapmanagerweb** 服务： `$ systemctl restart snapmanagerweb`

配置SnapCenter服务证书

步骤

1. 使用 vi 或任何文本编辑器打开以下配置文件。
   - *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config*
   - 安装目录NetApp
   - 安装目录NetApp

     INSTALL_DIR 的默认值是 */opt*。

2. 编辑 **SERVICE_CERTIFICATE_PATH** 和 **SERVICE_CERTIFICATE_PASSWORD** 键以分别包含 CA 证书路径和密码。

   SnapCenter服务证书仅支持 *.pfx* 格式。

3. 保存并关闭这些文件。
4. 重新启动所有服务。
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

在 Windows 主机上配置并启用双向 SSL 通信

在 Windows 主机上配置双向 SSL 通信

您应该配置双向 SSL 通信以保护 Windows 主机上的SnapCenter服务器与插件之间的相互通信。

开始之前

- 您应该已经生成了具有最小支持密钥长度 3072 的 CA 证书 CSR 文件。
- CA证书应支持服务器认证和客户端认证。
- 您应该拥有一份包含私钥和指纹详细信息的 CA 证书。
- 您应该已经启用单向 SSL 配置。

  有关详细信息，请参阅 "配置CA证书部分。"

- 您必须在所有插件主机和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. 要绑定端口，请使用 PowerShell 命令在SnapCenter Server 主机上对SnapCenter IIS Web 服务器端口 8146（默认）执行以下步骤，并再次对 SMCore 端口 8145（默认）执行以下步骤。

   a. 使用以下 PowerShell 命令删除现有的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. 将新采购的 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，请通过执行以下步骤在证书权限列表中添加 SnapCenter 的默认 IIS Web 服务器用户“**IIS AppPool\ SnapCenter**”来访问新购买的 CA 证书。
   a. 转到 Microsoft 管理控制台 (MMC)，然后单击 文件 > 添加/删除管理单元。
   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 证书并选择 所有任务 > 管理私钥。
   g. 单击“添加”，在“选择用户和组”向导中将位置更改为本地计算机名称（层次结构中的最顶层）
   h. 添加 IIS AppPool\ 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 Server 中添加新的 DWORD 注册表项条目：

   在 Windows 注册表编辑器中，遍历下面提到的路径，

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

4. 在 SCHANNEL 注册表配置上下文中创建新的 DWORD 注册表项条目。

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

配置**SnapCenter Windows** 插件以进行双向 **SSL** 通信

您应该使用 PowerShell 命令配置SnapCenter Windows 插件以进行双向 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 命令删除现有的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. 将新采购的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
```

在 **Windows** 主机上启用双向 **SSL** 通信

您可以启用双向 SSL 通信，以使用 PowerShell 命令保护 Windows 主机上的SnapCenter服务器与插件之间的相互通信。

开始之前

首先执行所有插件和 SMCore 代理的命令，然后执行服务器的命令。

步骤

1. 要启用双向 SSL 通信，请在SnapCenter服务器上运行以下命令，用于插件、服务器以及需要双向 SSL 通信的每个代理。

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

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

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

2. 使用以下命令执行 IIS SnapCenter应用程序池回收操作。 `> Restart-WebAppPool -Name "SnapCenter"`
3. 对于 Windows 插件，通过运行以下 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

- 首先执行所有插件和 SMCore 代理的命令，然后执行服务器的命令。
- 当您禁用双向 SSL 通信时，CA 证书及其配置不会被删除。
- 要向SnapCenter Server 添加新主机，必须禁用所有插件主机的双向 SSL。
- 不支持 NLB 和 F5。

步骤

1. 要禁用双向 SSL 通信，请在SnapCenter Server 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"}
```

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

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

在 **Linux** 主机上配置并启用双向 **SSL** 通信

在 **Linux** 主机上配置双向 **SSL** 通信

您应该配置双向 SSL 通信以保护 Linux 主机上的SnapCenter服务器与插件之间的相互通信。

开始之前

- 您应该已经为 Linux 主机配置了 CA 证书。

- 您必须在所有插件主机和SnapCenter服务器上启用双向 SSL 通信。

步骤

1. 将 **certificate.pem** 复制到 */etc/pki/ca-trust/source/anchors/*。
2. 将证书添加到 Linux 主机的信任列表中。
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. 验证证书是否已添加到信任列表。 `trust list | grep "<CN of your certificate>"`
4. 更新SnapCenter **nginx** 文件中的 **ssl_certificate** 和 **ssl_certificate_key** 并重新启动。
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. 刷新SnapCenter服务器 GUI 链接。
6. 更新位于 _ /<安装路径>/ NetApp /snapcenter/SnapManagerWeb_ 的 * SnapManager .Web.UI.dll.config* 和位于 /<安装路径>/ *NetApp/snapcenter/SMCore* 的 **SMCoreServiceHost.dll.config** 中的以下注册表项的值。
   - <add key="SERVICE_CERTIFICATE_PATH" value="<证书.pfx 的路径>" />
   - <添加键=“SERVICE_CERTIFICATE_PASSWORD”值=“<密码>”/>
7. 重新启动以下服务。
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. 验证证书是否已附加到SnapManager Web 端口。 `openssl s_client -connect localhost:8146 -brief`
9. 验证证书是否已附加到 smcore 端口。 `openssl s_client -connect localhost:8145 -brief`
10. 管理 SPL 密钥库和别名的密码。
    a. 检索分配给 SPL 属性文件中的 **SPL_KEYSTORE_PASS** 键的 SPL 密钥库默认密码。
    b. 更改密钥库密码。 `keytool -storepasswd -keystore keystore.jks`
    c. 更改所有私钥条目别名的密码。 `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. 为 *spl.properties* 中的密钥 **SPL_KEYSTORE_PASS** 更新相同的密码。
    e. 重新启动服务。
11. 在插件 Linux 主机上，在 SPL 插件的密钥库中添加根证书和中间证书。
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`

i. 检查 keystore.jks 中的条目。 `keytool -list -v -keystore <path to keystore.jks>`

ii. 如果需要，重命名任何别名。 `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`

12. 使用存储在 *keystore.jks* 中的 **certificate.pfx** 的别名更新 *spl.properties* 文件中的 **SPL_CERTIFICATE_ALIAS** 的值，然后重新启动 SPL 服务： `systemctl restart spl`

13. 验证证书是否已附加到 smcore 端口。 `openssl s_client -connect localhost:8145 -brief`

在 **Linux** 主机上启用 **SSL** 通信

您可以启用双向 SSL 通信，以使用 PowerShell 命令保护 Linux 主机上的SnapCenter服务器与插件之间的相互通信。

步骤

1. 执行以下操作以启用单向 SSL 通信。
   a. 登录SnapCenter GUI。
   b. 单击“设置”>“全局设置”，然后选择“在**SnapCenter**服务器上启用证书验证”。
   c. 单击“主机”>“托管主机”，然后选择要启用单向 SSL 的插件主机。
   d. 点击图标，然后单击*启用证书验证*。
2. 从SnapCenter Server Linux 主机启用双向 SSL 通信。
   - `Open-SmConnection`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
   - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

配置 **Active Directory**、**LDAP** 和 **LDAPS**

注册不受信任的 **Active Directory** 域

您应该向SnapCenter Server 注册 Active Directory，以管理来自多个不受信任的 Active Directory 域的主机、用户和组。

开始之前

LDAP 和 LDAPS 协议

- 您可以使用 LDAP 或 LDAPS 协议注册不受信任的活动目录域。
- 您应该已经启用插件主机和SnapCenter服务器之间的双向通信。
- 应设置从SnapCenter服务器到插件主机的 DNS 解析，反之亦然。

LDAP 协议

- 完全限定域名 (FQDN) 应该可以从SnapCenter Server 解析。

  您可以使用 FQDN 注册不受信任的域。如果无法从SnapCenter服务器解析 FQDN，则可以使用域控制器 IP 地址进行注册，并且该地址应该可以从SnapCenter服务器解析。

LDAPS 协议

- LDAPS 需要 CA 证书来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）应该可以从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 来注册不受信任的域。

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. 点击 + 注册一个新域名。
5. 在注册新域名页面中，选择 **LDAP** 或 **LDAPS**。
   a. 如果选择 **LDAP**，请指定为 LDAP 注册不受信任域所需的信息：

对于这个领域…	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。 有关更多信息，请参阅 "从 GUI 为不受信任的域添加域控制器 IP" 。

   b. 如果选择 **LDAPS**，请指定为 LDAPS 注册不受信任域所需的信息：

对于这个领域…	操作
域名	指定域的 NetBIOS 名称。

对于这个领域...	操作
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 Server 解析，则应纠正 DNS 解析。

6. 单击“确定”。

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

当您需要为SnapCenter启用 Active Directory 读取权限时，您可以在 Windows Server 上配置 Internet 信息服务 (IIS) 来创建自定义应用程序池帐户。

步骤

1. 在安装了SnapCenter的 Windows Server 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应用程序池身份。
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“OK”。

   自定义帐户取代了SnapCenter应用程序池的内置 ApplicationPoolIdentity 帐户。

为 **LDAPS** 配置 **CA** 客户端证书

当 Windows Active Directory LDAPS 配置了 CA 证书时，您应该在SnapCenter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“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 > 受信任的根证书颁发机构 > 证书。
5. 右键单击文件夹“受信任的根证书颁发机构”，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	单击“浏览”，选择“根证书”，然后单击“下一步”。
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。