准备安装SnapCenter服务器

SnapCenter software

NetApp
November 06, 2025

目录

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” } }