



准备安装 **SnapCenter** 服务器

SnapCenter Software 4.9

NetApp
March 20, 2024

目录

准备安装 SnapCenter 服务器	1
域和工作组要求	1
空间和规模估算要求	1
SAN主机要求	2
支持的存储系统和应用程序	3
支持的浏览器	3
连接和端口要求	3
SnapCenter 许可证	6
凭据的身份验证方法	8
存储连接和凭据	9
多因素身份验证 (MFA)	10

准备安装 SnapCenter 服务器

域和工作组要求

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

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

- * Active Directory 域 *

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

- * 工作组 *

您必须使用具有本地管理员权限的本地帐户。

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





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

空间和规模估算要求

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

项目	要求
操作系统	Microsoft Windows 操作系统仅支持英语，德语，日语和简体中文版。 有关受支持版本的最新信息，请参见 " NetApp 互操作性表工具 "。
最小 CPU 计数	4 个核心
最小 RAM	8 GB MySQL Server 缓冲区池使用的 RAM 占总 RAM 的 20%。

项目	要求
SnapCenter 服务器软件和日志的最小硬盘驱动器空间	4 GB  如果 SnapCenter 存储库位于安装 SnapCenter 服务器的同一驱动器中，则建议使用 10 GB。
SnapCenter 存储库的最小硬盘空间	6 GB  注意：如果 SnapCenter 服务器位于安装 SnapCenter 存储库的同一驱动器中，则建议具有 10 GB。
所需的软件包	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2或更高版本 • Windows Management Framework (WMF) 4.0 或更高版本 • PowerShell 4.0 或更高版本 <p>有关.NET专用的故障排除信息、请参见 "对于没有Internet连接的原有系统、SnapCenter 升级或安装失败"。</p>

SAN主机要求

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

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

- Host Utilities

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

- 适用于 Windows MPIO 的 Microsoft DSM

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

高可用性配置需要使用 DSM。



如果您使用的是 ONTAP DSM，则应迁移到 Microsoft DSM。有关详细信息，请参见 ["如何从 ONTAP DSM 迁移到 Microsoft DSM"](#)。

支持的存储系统和应用程序

您应了解支持的存储系统，应用程序和数据库。

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

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

有关适用于 NetApp ONTAP 的 Amazon FSX 的信息，请参见 ["Amazon FSX for NetApp ONTAP 文档"](#)。

- SnapCenter 支持保护不同的应用程序和数据库。

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

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

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

支持的浏览器

SnapCenter 软件可在多个浏览器上使用。

- Chrome

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

- Internet Explorer

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

- 仅支持默认级别的安全性。

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

- 必须禁用 Internet Explorer 兼容性视图。

- Microsoft Edge

有关受支持版本的最新信息，请参见 ["NetApp 互操作性表工具"](#)。

连接和端口要求

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

- 应用程序无法共享端口。

每个端口都必须专用于相应的应用程序。

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

您可以在安装后使用修改主机向导更改插件端口。

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

下表列出了不同的端口及其默认值。

端口类型	默认端口
SnapCenter 端口	8146 (HTTPS)、双向、可自定义、如URL _https://server:8146_中所示 用于 SnapCenter 客户端（SnapCenter 用户）与 SnapCenter 服务器之间的通信。也用于从插件主机到 SnapCenter 服务器的通信。 要自定义端口、请参见 "使用安装向导安装SnapCenter 服务器。"
SnapCenter SMCORE 通信端口	8145（HTTPS），双向，可自定义 此端口用于在 SnapCenter 服务器与安装 SnapCenter 插件的主机之间进行通信。 要自定义端口、请参见 "使用安装向导安装SnapCenter 服务器。"
MySQL 端口	3306（HTTPS），双向 此端口用于在 SnapCenter 和 MySQL 存储库数据库之间进行通信。 您可以创建从 SnapCenter 服务器到 MySQL 服务器的安全连接。 "了解更多信息。" 要自定义端口、请参见 "使用安装向导安装SnapCenter 服务器。"


端口类型	默认端口
Windows 插件主机	<p>135 , 445 (TCP)</p> <p>除了端口 135 和 445 之外, Microsoft 指定的动态端口范围也应处于打开状态。远程安装操作使用 Windows Management Instrumentation (WMI) 服务, 该服务会动态搜索此端口范围。</p> <p>有关支持的动态端口范围的信息, 请参见 "Windows 的服务概述和网络端口要求"</p> <p>这些端口用于在 SnapCenter 服务器与要安装此插件的主机之间进行通信。要将插件软件包二进制文件推送到 Windows 插件主机, 这些端口只能在插件主机上打开, 并且可以在安装后关闭。</p>
Linux 或 AIX 插件主机	<p>22 (SSH)</p> <p>这些端口用于在 SnapCenter 服务器与要安装此插件的主机之间进行通信。SnapCenter 使用这些端口将插件软件包二进制文件复制到 Linux 或 AIX 插件主机, 这些端口应处于打开状态或从防火墙或 IP 表中排除。</p>
适用于 Windows 的 SnapCenter 插件软件包, 适用于 Linux 的 SnapCenter 插件软件包或适用于 AIX 的 SnapCenter 插件软件包	<p>8145 (HTTPS) , 双向, 可自定义</p> <p>此端口用于在 SMCORE 与安装了插件软件包的主机之间进行通信。</p> <p>此外, 还需要在 SVM 管理 LIF 和 SnapCenter 服务器之间打开通信路径。</p> <p>要自定义端口、请参见 "添加主机并安装适用于 Microsoft Windows 的 SnapCenter 插件" 或 "添加主机并安装适用于 Linux 或 AIX 的 SnapCenter 插件软件包。"</p>
适用于 Oracle 数据库的 SnapCenter 插件	<p>27216 , 可自定义</p> <p>适用于 Oracle 的插件使用默认 JDBC 端口连接到 Oracle 数据库。</p> <p>要自定义端口、请参见 "添加主机并安装适用于 Linux 或 AIX 的 SnapCenter 插件软件包。"</p>
适用于 SnapCenter 的自定义插件	<p>9090 (HTTPS) , 已修复</p> <p>这是一个仅在自定义插件主机上使用的内部端口; 不需要防火墙异常。</p> <p>SnapCenter 服务器与自定义插件之间的通信通过端口 8145 进行路由。</p>

端口类型	默认端口
ONTAP 集群或 SVM 通信端口	443 (HTTPS), 双向 80 (HTTP), 双向 SAL (存储抽象层) 使用此端口在运行 SnapCenter 服务器的主机与 SVM 之间进行通信。SnapCenter for Windows 插件主机上的 SAL 当前也使用此端口在 SnapCenter 插件主机与 SVM 之间进行通信。
适用于SAP HANA数据库的SnapCenter 插件vCode编写检查程序	3 个 instance_number13 或 3 个 instance_number15, HTTP 或 HTTPS, 双向且可自定义 对于多租户数据库容器 (MDC) 单租户, 端口号以 13 结尾; 对于非 MDC, 端口号以 15 结尾。 例如, 32013 是实例 20 的端口号, 31015 是实例 10 的端口号。 要自定义端口、请参见 "添加主机并在远程主机上安装插件软件包。"
域控制器通信端口	请参见 Microsoft 文档以确定域控制器上应在防火墙中打开的端口, 以便身份验证能够正常工作。 必须在域控制器上打开 Microsoft 所需的端口, 以便 SnapCenter 服务器, 插件主机或其他 Windows 客户端能够对用户进行身份验证。


要修改端口详细信息, 请参见 ["修改插件主机"](#)。

SnapCenter 许可证

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

许可证	必要时
基于 SnapCenter 标准控制器	<p>对于FAS、AFF、全SAN阵列(ASA)为必需项</p> <p>SnapCenter 标准版许可证是一种基于控制器的许可证, 作为高级包的一部分提供。如果您拥有 SnapManager 套件许可证, 则还可以获得 SnapCenter 标准许可证授权。如果您要在FAS、AFF或ASA存储中试用SnapCenter、可以联系销售代表获取超值包评估许可证。</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  SnapCenter 也作为数据保护包的一部分提供。如果您购买的是 A400 或更高版本, 则应购买数据保护包。 </div>

许可证	必要时
基于 SnapCenter 标准容量	<p>ONTAP Select 和 Cloud Volumes ONTAP 必需</p> <p>如果您是 Cloud Volumes ONTAP 或 ONTAP Select 客户，则需要根据 SnapCenter 管理的数据购买基于每 TB 容量的许可证。默认情况下，SnapCenter 会提供一个内置 90 天 100 TB SnapCenter 标准容量试用许可证。有关其他详细信息，请联系销售代表。</p>
SnapMirror 或 SnapVault	<p>ONTAP</p> <p>如果在 SnapCenter 中启用了复制，则需要 SnapMirror 或 SnapVault 许可证。</p>
SnapRestore	<p>用于还原和验证备份。</p> <p>在主存储系统上</p> <ul style="list-style-type: none"> 在 SnapVault 目标系统上执行远程验证和从备份中还原时需要使用。 SnapMirror 目标系统上执行远程验证所需的。
FlexClone	<p>克隆数据库和验证操作所需。</p> <p>在主存储系统和二级存储系统上。</p> <ul style="list-style-type: none"> 在 SnapVault 目标系统上需要此功能才能从二级存储备份创建克隆。 在 SnapMirror 目标系统上需要使用此功能从二级 SnapMirror 备份创建克隆。
协议	<ul style="list-style-type: none"> LUN 的 iSCSI 或 FC 许可证 SMB 共享的 CIFS 许可证 NFS 类型 VMDK 的 NFS 许可证 VMFS 类型 VMDK 的 iSCSI 或 FC 许可证 <p>如果源卷不可用，则 SnapMirror 目标系统需要提供数据。</p>

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



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

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

单邮箱恢复（SMBR）许可证

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

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

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

凭据的身份验证方法

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

Windows 身份验证

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

不可信域身份验证

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

本地工作组身份验证

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

SQL Server 身份验证

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

Linux 身份验证

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

AIX 身份验证

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

Oracle 数据库身份验证

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

Oracle ASM 身份验证

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

RMAN 目录身份验证

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

存储连接和凭据

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

- * 存储连接 *

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

- * 凭据 *

- 域管理员或管理员组的任何成员

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

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

- 本地管理员（仅适用于工作组）

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

用户名字段的有效格式为： `username`

- 单个资源组的凭据

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

多因素身份验证（MFA）

管理多因素身份验证(MFA)

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

启用多因素身份验证(MFA)

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

关于此任务

- 如果在同一AD FS中配置了其他应用程序、则SnapCenter 支持基于SSO的登录。在某些AD FS配置中、出于安全原因、SnapCenter 可能需要用户身份验证、具体取决于AD FS会话持久性。
- 有关可与cmdlet结合使用的参数及其说明的信息、可以通过运行来获取 `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)应在相应的域中启动并运行。
- 您应该拥有一个AD FS支持的多因素身份验证服务、例如Azure MFA、Cisco Duo等。
- 无论时区如何、SnapCenter 和AD FS服务器的时间戳都应相同。
- 获取并配置SnapCenter 服务器的授权CA证书。

CA证书为必填项、原因如下：

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

有关CA证书的信息、请参见 "[生成 CA 证书 CSR 文件](#)"。

步骤

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

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

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

如果检查成功、请单击*确定*。

10. 在AD FS主机中、打开AD FS管理向导并执行以下步骤：
 - a. 右键单击*依赖方信任*>*添加依赖方信任*>*启动*。
 - b. 选择第二个选项并浏览SnapCenter MFA元数据文件、然后单击*下一步*。
 - c. 指定显示名称并单击*下一步*。

- d. 根据需要选择访问控制策略，然后单击*Next*。
- e. 在下一个选项卡中选择默认设置。
- f. 单击 * 完成 *。

现在、SnapCenter 已被视为具有所提供显示名称的依赖方。

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

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

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

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

也可以使用REST API启用SnapCenter MFA功能。

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

更新AD FS MFA元数据

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

步骤

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

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

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

更新SnapCenter MFA元数据

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

步骤

1. 在AD FS主机中、打开AD FS管理向导并执行以下步骤：

- a. 单击*依赖方信任*。
- b. 右键单击为SnapCenter 创建的依赖方信任、然后单击*删除*。

此时将显示依赖方信任的用户定义名称。

- c. 启用多因素身份验证(MFA)。

请参见 "[启用多因素身份验证](#)"。

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

禁用多因素身份验证(MFA)

步骤

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

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

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

将AD FS设置为OAuth/OIDC

使用Windows GUI向导配置AD FS

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

这是客户端ID。 ...在重定向URL中添加回调URL (SnapCenter服务器URL)。 ...单击 * 下一步 *。

4. 选择*生成共享密钥*。

复制机密值。这是客户的秘密。 ...单击 * 下一步 * 。

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

选择Web API并单击*Next*。

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

在*完成*页上，单击*关闭*。

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

此令牌的"aud"或访问群体声明必须与资源或Web API的标识符匹配。

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

配置OpenID Connect以提供用户名作为声明。

16. 打开位于服务器管理器右上角的*Tools*菜单下的*AD FS Management*工具。
 - a. 从左侧边栏中选择*应用程序组*文件夹。
 - b. 选择Web API并单击*edit*。
 - c. 转至“颁发转换规则”选项卡

17. 单击 * 添加规则 * 。

- a. 在“声明规则模板”下拉列表中选择*将LDAP属性作为声明发送*。
- b. 单击 * 下一步 * 。

18. 输入*申请规则*名称。

- a. 在“属性存储”下拉列表中选择*Active Directory*。
- b. 在*LDAP Attribute*下拉列表中选择*User-Principal-Name*，在O*utgoing款项申请类型*下拉列表中选择*UPN*。
- c. 单击 * 完成 * 。

使用PowerShell命令创建应用程序组

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

1. 使用以下命令在AD FS中创建新的应用程序组。

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

ClientRoleIdentifier 应用程序组的名称

redirectURL 授权后重定向的有效URL

2. 创建AD FS服务器应用程序并生成客户端密钥。

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

3. 创建ADFS Web API应用程序并配置其应使用的策略名称。

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

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier  
-Name "App Web API"  
  
-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 从以下命令的输出中获取客户端ID和客户端密钥、因为它仅显示一次。

```
"client_id = $identifier"  
  
"client_secret: "$($ADFSApp.ClientSecret)
```

5. 为AD FS应用程序授予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命令更新访问令牌到期时间。

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

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

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

从AD FS获取承载令牌

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

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

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

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

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

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

SnapCenter MFA命令行界面身份验证

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

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

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

SnapCenter MFA REST API身份验证

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

MFA REST API workflow

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

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

*通过AD FS MFA*进行身份验证

1. 将REST客户端配置为调用AD FS端点以获取访问令牌。

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

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

+ 用户名的格式必须为user@domain或domain\user。

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

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

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

如果此令牌有效、则SnapCenter会对其进行加密并获取用户名。

8. SnapCenter使用用户名和角色名称对执行API的用户进行身份验证。
如果身份验证成功、SnapCenter将返回结果、否则会显示错误消息。

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

图形用户界面

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

PowerShell接口

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

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

path参数用于指定AD FS MFA元数据xml文件的位置。

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

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

sccli Interface

- 步骤 *

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

REST API

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

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

2. 使用以下API检查MFA配置状态和设置。

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

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。