准备安装 SnapCenter 服务器

SnapCenter Software 4.7

NetApp
January 18, 2024

目录

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	• Microsoft .NET Framework 4.7.2或更高版本 • Windows Management Framework （ WMF ） 4.0 或更高版本 • PowerShell 4.0 或更高版本 有关.NET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。" 有关受支持版本的最新信息，请参见 "NetApp 互操作性表工具"。

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"。

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* 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。"

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

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

要修改端口详细信息，请参见 "修改插件主机"。

SnapCenter 许可证

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

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

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

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

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

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

单邮箱恢复（ SMBR ）许可证

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

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

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

凭据的身份验证方法

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

Windows 身份验证

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

不可信域身份验证

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

本地工作组身份验证

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

SQL Server 身份验证

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

Linux 身份验证

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

AIX 身份验证

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

Oracle 数据库身份验证

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

Oracle ASM 身份验证

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

RMAN 目录身份验证

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

存储连接和凭据

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

- * 存储连接 *

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

- * 凭据 *
  - 域管理员或管理员组的任何成员

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

    - *netbios\username*
    - 域 FQDN\username_
    - 用户名@UPN_
  - 本地管理员（仅适用于工作组）

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

  用户名字段的有效格式为： *username*

  - 单个资源组的凭据

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

启用多因素身份验证(MFA)

要启用MFA功能、您应在Active Directory联合身份验证服务(AD FS)服务器和SnapCenter服务器中执行一些步骤。

- 您需要的内容 *
- 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。
- 您应拥有任何AD FS支持的多因素身份验证服务、例如Azure MFA、Cisco双核等。
- 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"。

- 关于此任务 *
- 如果在同一AD FS中配置了其他应用程序、则SnapCenter 支持基于SSO的登录。在某些AD FS配置中、出于安全原因、SnapCenter 可能需要用户身份验证、具体取决于AD FS会话持久性。

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

1. 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年06月/FedationMetadata。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_set-SmMultiFactorAuthentication -Enable -Path_ cmdlet为SnapCenter 服务器启用MFA。

   path参数指定在步骤3中复制到SnapCenter 服务器的AD FS MFA元数据xml文件的位置。

8. (可选)使用_Get-SmMultiFactorAuthentication_cmdlet检查MFA配置状态和设置。
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. 根据需要选择并访问控制策略、然后单击*下一步*。
    e. 将下一个选项卡中的设置设置设置为默认值。

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‘<显示依赖方名称>'-SigningCertificateRevocationCheck NONE _

_Set-AdfsRelyingPartyTrust -targetName‘<显示依赖方的名称>'-EncryptionCertificateRevocationCheck NONE _

1. 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。

也可以使用REST API启用SnapCenter MFA功能。

- 完成后 *

在SnapCenter 中启用、更新或禁用MFA设置后、请关闭所有浏览器选项卡并重新打开浏览器以重新登录。此操作将清除现有或活动的会话Cookie。

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

更新AD FS MFA元数据

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

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

       *Set-SmMultiFactorAuthentication -Path < ADFS MFA*元数据*xml*文件的位置>

- 完成后 *

在SnapCenter 中启用、更新或禁用MFA设置后、请关闭所有浏览器选项卡并重新打开浏览器以重新登录。此操作将清除现有或活动的会话Cookie。

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"

- 完成后 *

在SnapCenter 中启用、更新或禁用MFA设置后、请关闭所有浏览器选项卡并重新打开浏览器以重新登录。此操作将清除现有或活动的会话Cookie。

禁用多因素身份验证(MFA)

使用_set-SmMultiFactorAuthentication -Disable_ cmdlet禁用MFA并清理启用MFA时创建的配置文件。

- 完成后 *

在SnapCenter 中启用、更新或禁用MFA设置后、请关闭所有浏览器选项卡并重新打开浏览器以重新登录。此操作将清除现有或活动的会话Cookie。