多因素身份验证（MFA）

SnapCenter Software 5.0

NetApp
April 04, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/snapcenter/install/enable_multifactor_authentication.html on April 04, 2024. Always check docs.netapp.com for the latest.

目录

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/FedationMetadata。xml"
2. 将下载的文件复制到SnapCenter 服务器以更新MFA配置。
3. 运行以下cmdlet以更新SnapCenter 中的AD FS元数据：

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

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

更新SnapCenter MFA元数据

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

步骤

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

      此时将显示依赖方信任的用户定义名称。

   c. 启用多因素身份验证(MFA)。

      请参见 "启用多因素身份验证"。

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

禁用多因素身份验证(MFA)

步骤

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

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

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

将AD FS设置为OAuth/OIDC

使用Windows GUI向导配置AD FS

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

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

4. 选择*生成共享密钥*。

   复制机密值。这是客户的秘密。 …单击 * 下一步 * 。

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

   选择Web API并单击*Next*。

9. 在配置Web API页面上、在标识符部分中输入上一步创建的SnapCenter服务器URL和客户端标识符。
   a. 单击 * 添加 * 。
   b. 单击 * 下一步 * 。
10. 在*选择访问控制策略*页上，根据您的要求选择控制策略(例如，允许所有人和要求MFA)，然后单击*下一步

*。

11. 在*配置应用程序权限*页上，默认情况下会选择OpenID作为范围，单击*Next*。
12. 在“摘要”页上，单击“下一步”。

    在*完成*页上，单击*关闭*。

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

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

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

    配置OpenID Connect以提供用户名作为声明。

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

使用**PowerShell**命令创建应用程序组

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

1. 使用以下命令在AD FS中创建新的应用程序组。

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

   `ClientRoleIdentifier` 应用程序组的名称

   `redirectURL` 授权后重定向的有效URL

2. 创建AD FS服务器应用程序并生成客户端密钥。

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   ```

```
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
-Identifier $identifier -GenerateClientSecret
```

3. 创建ADFS Web API应用程序并配置其应使用的策略名称。

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

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

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

4. 从以下命令的输出中获取客户端ID和客户端密钥、因为它仅显示一次。

```
"client_id = $identifier"

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

5. 为AD FS应用程序授予allatlaims和OpenID权限。

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

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

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

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 写出转换规则文件。

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

7. 命名Web API应用程序并使用外部文件定义其颁发转换规则。

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile
```

```
$relativePath
```

更新访问令牌到期时间

您可以使用PowerShell命令更新访问令牌到期时间。

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

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

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

从**AD FS**获取承载令牌

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

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

字段	价值
授予类型	授权代码
回调URL	如果没有回调URL，请输入应用程序的基本URL。
身份验证URL	[adfs-domain-name]/adfs/oauth2/authorize
访问令牌URL	[adfs-domain-name]/adfs/oauth2/令牌
客户端 ID	输入AD FS客户端ID
客户端密钥	输入AD FS客户端密钥
范围	OpenID
客户端身份验证	作为基本AUTH标题发送
资源	在*Advance Options *选项卡中，添加与回调URL值相同的“资源”字段，该值在JWT令牌中显示为“aud”值。

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

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

SnapCenter MFA命令行界面身份验证

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

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

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

SnapCenter MFA REST API身份验证

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

MFA REST API工作流

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

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

*通过AD FS MFA*进行身份验证

1. 将REST客户端配置为调用AD FS端点以获取访问令牌。

   单击此按钮获取应用程序的访问令牌后、您将重定向到AD FS SSO页面、在此页面中、您必须提供AD凭据并通过MFA进行身份验证。 1.在AD FS SSO页面的用户名文本框中、键入您的用户名或电子邮件。

   + 用户名的格式必须为user@domain或domain\user。

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

5. 身份验证成功后、将打开一个弹出窗口、其中包含访问、ID和刷新令牌。

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

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

   如果此令牌有效、则SnapCenter会对其进行加密并获取用户名。

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

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

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

图形用户界面

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

PowerShell接口

- 步骤 *

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

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

     path参数用于指定AD FS MFA元数据xml文件的位置。

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

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

sccli Interface

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

REST API

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

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

2. 使用以下API检查MFA配置状态和设置。

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

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，本文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。