Autenticação multifator (MFA)

SnapCenter software

NetApp
November 06, 2025

Índice

Autenticação multifator (MFA)

Gerenciar autenticação multifator (MFA)

Você pode gerenciar a funcionalidade de autenticação multifator (MFA) no servidor do Serviço de Federação do Active Directory (AD FS) e no SnapCenter Server.

Habilitar autenticação multifator (MFA)

Você pode habilitar a funcionalidade MFA para o SnapCenter Server usando comandos do PowerShell.

Sobre esta tarefa

- O SnapCenter oferece suporte a logins baseados em SSO quando outros aplicativos são configurados no mesmo AD FS. Em determinadas configurações do AD FS, o SnapCenter pode exigir autenticação do usuário por motivos de segurança, dependendo da persistência da sessão do AD FS.
- As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando `Get-Help command_name` . Alternativamente, você também pode ver "Guia de referência do cmdlet do software SnapCenter" .

Antes de começar

- O Serviço de Federação do Active Directory (AD FS) do Windows deve estar ativo e em execução no respectivo domínio.
- Você deve ter um serviço de autenticação multifator compatível com AD FS, como Azure MFA, Cisco Duo e assim por diante.
- O registro de data e hora do servidor SnapCenter e AD FS deve ser o mesmo, independentemente do fuso horário.
- Obtenha e configure o certificado de CA autorizado para o SnapCenter Server.

  O Certificado CA é obrigatório pelos seguintes motivos:

  - Garante que as comunicações ADFS-F5 não sejam interrompidas porque os certificados autoassinados são exclusivos no nível do nó.
  - Garante que durante a atualização, o reparo ou a recuperação de desastres (DR) em uma configuração autônoma ou de alta disponibilidade, o certificado autoassinado não seja recriado, evitando assim a reconfiguração do MFA.
  - Garante resoluções IP-FQDN.

    Para obter informações sobre o certificado CA, consulte"Gerar arquivo CSR de certificado CA" .

Passos

1. Conecte-se ao host dos Serviços de Federação do Active Directory (AD FS).
2. Baixe o arquivo de metadados da federação do AD FS em"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copie o arquivo baixado para o SnapCenter Server para habilitar o recurso MFA.
4. Efetue login no SnapCenter Server como usuário administrador do SnapCenter por meio do PowerShell.
5. Usando a sessão do PowerShell, gere o arquivo de metadados do SnapCenter MFA usando o cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

O parâmetro path especifica o caminho para salvar o arquivo de metadados MFA no host do SnapCenter Server.

6. Copie o arquivo gerado para o host do AD FS para configurar o SnapCenter como a entidade do cliente.
7. Habilite o MFA para o SnapCenter Server usando o `Set-SmMultiFactorAuthentication` cmdlet.
8. (Opcional) Verifique o status e as configurações da configuração do MFA usando `Get-SmMultiFactorAuthentication` cmdlet.
9. Acesse o console de gerenciamento da Microsoft (MMC) e execute as seguintes etapas:
   a. Clique em **Arquivo** > **Adicionar/Remover Snapin**.
   b. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
   c. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
   d. Clique em **Console Root** > **Certificados – Computador local** > **Pessoal** > **Certificados**.
   e. Clique com o botão direito do mouse no certificado CA vinculado ao SnapCenter e selecione **Todas as tarefas** > **Gerenciar chaves privadas**.
   f. No assistente de permissões, execute as seguintes etapas:
      i. Clique em **Adicionar**.
      ii. Clique em **Locais** e selecione o host em questão (topo da hierarquia).
      iii. Clique em **OK** na janela pop-up **Locais**.
      iv. No campo de nome do objeto, digite 'IIS_IUSRS', clique em **Verificar nomes** e clique em **OK**.

      Se a verificação for bem-sucedida, clique em **OK**.
10. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
    a. Clique com o botão direito em **Relying Party Trusts** > **Adicionar Relying Party Trust** > **Iniciar**.
    b. Selecione a segunda opção, navegue pelo arquivo de metadados do SnapCenter MFA e clique em **Avançar**.
    c. Especifique um nome de exibição e clique em **Avançar**.
    d. Escolha uma política de controle de acesso conforme necessário e clique em **Avançar**.
    e. Selecione as configurações na próxima aba como padrão.
    f. Clique em **Concluir**.

    O SnapCenter agora é refletido como uma parte confiável com o nome de exibição fornecido.
11. Selecione o nome e execute os seguintes passos:
    a. Clique em **Editar política de emissão de reivindicações**.
    b. Clique em **Adicionar regra** e clique em **Avançar**.
    c. Especifique um nome para a regra de reivindicação.
    d. Selecione **Active Directory** como o armazenamento de atributos.
    e. Selecione o atributo como **User-Principal-Name** e o tipo de declaração de saída como **Name-ID**.
    f. Clique em **Concluir**.
12. Execute os seguintes comandos do PowerShell no servidor ADFS.

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

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

13. Execute as seguintes etapas para confirmar se os metadados foram importados com sucesso.
    a. Clique com o botão direito do mouse na parte confiável e selecione **Propriedades**.
    b. Certifique-se de que os campos Endpoints, Identificadores e Assinatura estejam preenchidos.
14. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

A funcionalidade SnapCenter MFA também pode ser habilitada usando APIs REST.

Para obter informações sobre solução de problemas, consulte "Tentativas simultâneas de login em várias guias mostram erro de MFA" .

Atualizar metadados do AD FS MFA

Você deve atualizar os metadados do AD FS MFA no SnapCenter sempre que houver qualquer modificação no servidor AD FS, como atualização, renovação de certificado CA, DR e assim por diante.

Passos

1. Baixe o arquivo de metadados da federação do AD FS em"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copie o arquivo baixado para o SnapCenter Server para atualizar a configuração do MFA.
3. Atualize os metadados do AD FS no SnapCenter executando o seguinte cmdlet:

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

4. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Atualizar metadados do SnapCenter MFA

Você deve atualizar os metadados do SnapCenter MFA no AD FS sempre que houver qualquer modificação no servidor ADFS, como reparo, renovação de certificado CA, DR e assim por diante.

Passos

1. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
    a. Selecione **Relying Party Trusts**.
    b. Clique com o botão direito do mouse na parte confiável que foi criada para o SnapCenter e selecione **Excluir**.

    O nome definido pelo usuário da parte confiável será exibido.

    c. Habilite a autenticação multifator (MFA).

    Ver "Habilitar autenticação multifator" .

2. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Desativar autenticação multifator (MFA)

Passos

1. Desabilite o MFA e limpe os arquivos de configuração que foram criados quando o MFA foi habilitado usando o `Set-SmMultiFactorAuthentication` cmdlet.
2. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Gerenciar autenticação multifator (MFA) usando Rest API, PowerShell e SCCLI

O login MFA é compatível com navegador, API REST, PowerShell e SCCLI. O MFA é suportado por um gerenciador de identidade do AD FS. Você pode habilitar o MFA, desabilitar o MFA e configurar o MFA a partir da GUI, API REST, PowerShell e SCCLI.

Configurar o AD FS como OAuth/OIDC

Configurar o AD FS usando o assistente da GUI do Windows

1. Navegue até **Painel do Gerenciador de Servidores** > **Ferramentas** > **Gerenciamento do ADFS**.
2. Navegue até **ADFS** > **Grupos de Aplicativos**.
   a. Clique com o botão direito do mouse em **Grupos de aplicativos**.
   b. Selecione **Adicionar grupo de aplicativos** e insira **Nome do aplicativo**.
   c. Selecione **Aplicativo do Servidor**.
   d. Clique em **Avançar**.
3. Copie **Identificador do Cliente**.

   Este é o ID do cliente. .. Adicione URL de retorno de chamada (URL do SnapCenter Server) na URL de redirecionamento. .. Clique em **Avançar**.

4. Selecione **Gerar segredo compartilhado**.

   Copie o valor secreto. Este é o segredo do cliente. .. Clique em **Avançar**.

5. Na página **Resumo**, clique em **Avançar**.
   a. Na página **Concluído**, clique em **Fechar**.
6. Clique com o botão direito do mouse no **Grupo de Aplicativos** recém-adicionado e selecione **Propriedades**.
7. Selecione **Adicionar aplicativo** em Propriedades do aplicativo.
8. Clique em **Adicionar aplicativo**.

   Selecione Web API e clique em **Avançar**.

9. Na página Configurar API da Web, insira a URL do SnapCenter Server e o Identificador do Cliente criados

na etapa anterior na seção Identificador.

a. Clique em **Adicionar**.

b. Clique em **Avançar**.

10. Na página **Escolher política de controle de acesso**, selecione a política de controle com base em suas necessidades (por exemplo, Permitir todos e exigir MFA) e clique em **Avançar**.
11. Na página **Configurar permissão do aplicativo**, por padrão o openid é selecionado como um escopo, clique em **Avançar**.
12. Na página **Resumo**, clique em **Avançar**.

    Na página **Concluído**, clique em **Fechar**.

13. Na página **Propriedades do aplicativo de exemplo**, clique em **OK**.
14. Token JWT emitido por um servidor de autorização (AD FS) e destinado a ser consumido pelo recurso.

    A declaração 'aud' ou de público deste token deve corresponder ao identificador do recurso ou da API da Web.

15. Edite a WebAPI selecionada e verifique se o URL de retorno de chamada (URL do SnapCenter Server) e o identificador do cliente foram adicionados corretamente.

    Configure o OpenID Connect para fornecer um nome de usuário como declarações.

16. Abra a ferramenta **Gerenciamento do AD FS** localizada no menu **Ferramentas** no canto superior direito do Gerenciador do Servidor.

    a. Selecione a pasta **Grupos de Aplicativos** na barra lateral esquerda.

    b. Selecione a API da Web e clique em **EDITAR**.

    c. Guia de regras de transformação de emissão

17. Clique em **Adicionar regra**.

    a. Selecione **Enviar atributos LDAP como declarações** no menu suspenso Modelo de regra de declaração.

    b. Clique em **Avançar**.

18. Digite o nome da **Regra de reivindicação**.

    a. Selecione **Active Directory** no menu suspenso Armazenamento de atributos.

    b. Selecione **Nome-Principal-do-Usuário** no menu suspenso **Atributo LDAP** e **UPN** no menu suspenso Tipo de Reivindicação de Saída*.

    c. Clique em **Concluir**.

Criar grupo de aplicativos usando comandos do PowerShell

Você pode criar o grupo de aplicativos, a API da Web e adicionar o escopo e as declarações usando comandos do PowerShell. Esses comandos estão disponíveis em formato de script automatizado. Para mais informações, consulte <link para o artigo da KB>.

1. Crie o novo Grupo de Aplicativos no AD FS usando o seguinte comando.

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

`ClientRoleIdentifier`nome do seu grupo de aplicação

`redirectURL`URL válida para redirecionamento após autorização

2. Crie o aplicativo do servidor AD FS e gere o segredo do cliente.

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

3. Crie o aplicativo ADFS Web API e configure o nome da política que ele deve usar.

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

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

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

4. Obtenha o ID do cliente e o segredo do cliente da saída dos comandos a seguir, pois eles são exibidos apenas uma vez.

```
"client_id = $identifier"

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

5. Conceda ao aplicativo AD FS as permissões allatclaims e openid.

```
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. Escreva o arquivo de regras de transformação.

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

7. Nomeie o aplicativo Web API e defina suas regras de transformação de emissão usando um arquivo externo.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Atualizar tempo de expiração do token de acesso

Você pode atualizar o tempo de expiração do token de acesso usando o comando do PowerShell.

Sobre esta tarefa

- Um token de acesso pode ser usado somente para uma combinação específica de usuário, cliente e recurso. Os tokens de acesso não podem ser revogados e são válidos até expirarem.
- Por padrão, o tempo de expiração de um token de acesso é de 60 minutos. Este tempo mínimo de expiração é suficiente e dimensionado. Você deve fornecer valor suficiente para evitar quaisquer trabalhos críticos para os negócios em andamento.

Etapa

Para atualizar o tempo de expiração do token de acesso para um grupo de aplicativos WebApi, use o seguinte comando no servidor AD FS.

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

Obter o token do portador do AD FS

Você deve preencher os parâmetros mencionados abaixo em qualquer cliente REST (como o Postman) e ele solicitará que você preencha as credenciais do usuário. Além disso, você deve inserir a autenticação de segundo fator (algo que você tem e algo que você é) para obter o token do portador.

+ A validade do token portador é configurável no servidor AD FS por aplicativo e o período de validade padrão é de 60 minutos.

Campo	Valor
Tipo de subsídio	Código de autorização
URL de retorno de chamada	Insira a URL base do seu aplicativo se você não tiver uma URL de retorno de chamada.
URL de autenticação	[adfs-nome-de-domínio]/adfs/oauth2/autorizar
URL do token de acesso	[nome-de-domínio-adfs]/adfs/oauth2/token
ID do cliente	Insira o ID do cliente do AD FS

Segredo do cliente	Digite o segredo do cliente do AD FS
Escopo	OpenID
Autenticação do cliente	Enviar como cabeçalho AUTH básico
Recurso	Na aba **Opções Avançadas**, adicione o campo Recurso com o mesmo valor que o URL de retorno de chamada, que vem como um valor “aud” no token JWT.

Configurar MFA no SnapCenter Server usando PowerShell, SCCLI e REST API

Você pode configurar o MFA no SnapCenter Server usando PowerShell, SCCLI e REST API.

Autenticação SnapCenter MFA CLI

No PowerShell e no SCCLI, o cmdlet existente (Open-SmConnection) é estendido com mais um campo chamado "AccessToken" para usar o token do portador para autenticar o usuário.

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

Após a execução do cmdlet acima, uma sessão é criada para o respectivo usuário executar outros cmdlets do SnapCenter .

Autenticação SnapCenter MFA Rest API

Use o token portador no formato *Authorization=Bearer <access token>* no cliente REST API (como Postman ou swagger) e mencione o RoleName do usuário no cabeçalho para obter uma resposta bem-sucedida do SnapCenter.

Fluxo de trabalho da API REST do MFA

Quando o MFA é configurado com o AD FS, você deve autenticar usando um token de acesso (portador) para acessar o aplicativo SnapCenter por qualquer API Rest.

Sobre esta tarefa

- Você pode usar qualquer cliente REST, como Postman, Swagger UI ou FireCamp.
- Obtenha um token de acesso e use-o para autenticar solicitações subsequentes (SnapCenter Rest API) para executar qualquer operação.

Passos

Para autenticar através do AD FS MFA

1. Configure o cliente REST para chamar o ponto de extremidade do AD FS para obter o token de acesso.

   Ao clicar no botão para obter um token de acesso para um aplicativo, você será redirecionado para a página SSO do AD FS, onde deverá fornecer suas credenciais do AD e autenticar com o MFA. 1. Na página SSO do AD FS, digite seu nome de usuário ou e-mail na caixa de texto Nome de usuário.

   + Os nomes de usuário devem ser formatados como usuário@domínio ou domínio\usuário.

2. Na caixa de texto Senha, digite sua senha.
3. Clique em **Entrar**.
4. Na seção **Opções de login**, selecione uma opção de autenticação e autentique (dependendo da sua configuração).
   - Push: aprove a notificação push que é enviada para seu telefone.
   - Código QR: Use o aplicativo móvel AUTH Point para escanear o código QR e digite o código de verificação mostrado no aplicativo
   - Senha de uso único: digite a senha de uso único para seu token.
5. Após a autenticação bem-sucedida, um pop-up será aberto contendo o acesso, o ID e o token de atualização.

   Copie o token de acesso e use-o na API Rest do SnapCenter para executar a operação.

6. Na API Rest, você deve passar o token de acesso e o nome da função na seção de cabeçalho.
7. O SnapCenter valida esse token de acesso do AD FS.

   Se for um token válido, o SnapCenter o decodifica e obtém o nome de usuário.

8. Usando o nome de usuário e o nome da função, o SnapCenter autentica o usuário para uma execução de API.

   Se a autenticação for bem-sucedida, o SnapCenter retornará o resultado, caso contrário, uma mensagem de erro será exibida.

Habilitar ou desabilitar a funcionalidade SnapCenter MFA para REST API, CLI e GUI

GUI

Passos

1. Efetue login no SnapCenter Server como Administrador do SnapCenter .
2. Clique em **Configurações** > **Configurações globais** > **Configurações de autenticação multifator (MFA)**
3. Selecione a interface (GUI/RST API/CLI) para habilitar ou desabilitar o login MFA.

Interface do PowerShell

Passos

1. Execute os comandos do PowerShell ou da CLI para habilitar o MFA para GUI, REST API, PowerShell e SCCLI.

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

O parâmetro path especifica o local do arquivo XML de metadados do AD FS MFA.

Habilita o MFA para SnapCenter GUI, Rest API, PowerShell e SCCLI configurados com o caminho de arquivo de metadados do AD FS especificado.

2. Verifique o status e as configurações da configuração do MFA usando o `Get-SmMultiFactorAuthentication` cmdlet.

Interface SCCLI

Passos

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

APIs REST

1. Execute a seguinte API de postagem para habilitar MFA para GUI, REST API, PowerShell e SCCLI.

Parâmetro	Valor
URL solicitada	/api/4.9/settings/autenticação multifator
Método HTTP	Publicar
Corpo da solicitação	{ "IsGuiMFAEnabled": falso, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }
Corpo de Resposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": nulo, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

2. Verifique o status e as configurações da configuração do MFA usando a seguinte API.

Parâmetro	Valor
URL solicitada	/api/4.9/settings/autenticação multifator
Método HTTP	Pegar

Corpo de Resposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": nulo, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

Informações sobre direitos autorais

Informações sobre marcas comerciais