Autenticação multifator (MFA)

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

Autenticação multifator (MFA)

Gerenciamento da autenticação multifator (MFA)

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

Habilitar a autenticação multifator (MFA)

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

Sobre esta tarefa

- O SnapCenter suporta logins baseados em SSO quando outros aplicativos são configurados no mesmo AD FS. Em certas configurações do AD FS, o SnapCenter pode exigir autenticação de 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`o . Alternativamente, você também pode "Guia de referência de cmdlet do software SnapCenter"ver .

Antes de começar

- O Serviço de Federação do ative Directory do Windows (AD FS) deve estar ativo e em execução no respetivo domínio.
- Você deve ter um serviço de autenticação multifator compatível com AD FS, como Azure MFA, Cisco Duo, etc.
- O carimbo de data/hora do servidor SnapCenter e AD FS deve ser o mesmo, independentemente do fuso horário.
- Procure e configure o certificado de CA autorizado para o servidor SnapCenter.

  O certificado CA é obrigatório pelos seguintes motivos:

  - Garante que as comunicações ADFS-F5 não quebrem porque os certificados autoassinados são exclusivos no nível do nó.
  - Garante que durante a atualização, reparo ou 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, "Gerar arquivo CSR do certificado CA"consulte .

Passos

1. Conete-se ao host dos Serviços de Federação do ative Directory (AD FS).
2. Faça download do arquivo de metadados de federação do AD FS de "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copie o arquivo baixado para o servidor SnapCenter para ativar o recurso MFA.
4. Faça login no servidor SnapCenter como o usuário Administrador do SnapCenter através 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 servidor SnapCenter.

6. Copie o arquivo gerado para o host do AD FS para configurar o SnapCenter como a entidade cliente.
7. Habilite o MFA para servidor SnapCenter usando `Set-SmMultiFactorAuthentication` o cmdlet.
8. (Opcional) Verifique o status e as configurações do MFA usando `Get-SmMultiFactorAuthentication` o cmdlet.
9. Vá para o console de gerenciamento da Microsoft (MMC) e execute as seguintes etapas:
   a. Clique em **File** > **Add/Remove Snapin**.
   b. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
   c. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
   d. Clique em **raiz da consola** > **certificados – computador local** > **Pessoal** > **certificados**.
   e. Clique com o botão direito do rato no certificado CA vinculado ao SnapCenter e selecione **todas as tarefas** > **gerir chaves privadas**.
   f. No assistente de permissões, execute as seguintes etapas:
      i. Clique em **Add**.
      ii. Clique em **locais** e selecione o host em questão (topo da hierarquia).
      iii. Clique em **OK** na janela pop-up **Locations**.
      iv. No campo Nome do objeto, digite 'IIS_IUSRS' e 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 do rato em **confiar em parte** > **Adicionar confiança de parte dependente** > **Iniciar**.
    b. Selecione a segunda opção e navegue no arquivo de metadados do SnapCenter MFA e clique em **Avançar**.
    c. Especifique um nome de exibição e clique em **Next**.
    d. Escolha uma política de controle de acesso conforme necessário e clique em **Next**.
    e. Selecione as configurações na próxima guia como padrão.
    f. Clique em **Finish**.

    O SnapCenter é agora refletido como uma parte dependente com o nome de exibição fornecido.
11. Selecione o nome e execute as seguintes etapas:
    a. Clique em **Editar Política de emissão de reclamação**.
    b. Clique em **Adicionar regra** e clique em **seguinte**.
    c. Especifique um nome para a regra de reclamação.
    d. Selecione **ative Directory** como o armazenamento de atributos.
    e. Selecione o atributo como **User-Principal-Name** e o tipo de reclamação enviada como **Name-ID**.
    f. Clique em **Finish**.
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 etapas a seguir para confirmar se os metadados foram importados com êxito.
    a. Clique com o botão direito do rato na confiança da parte dependente e selecione **Propriedades**.
    b. Certifique-se de que os campos Endpoints, Identificadores e assinatura estão preenchidos.
14. Feche todas as guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

A funcionalidade de MFA do SnapCenter também pode ser ativada usando APIS REST.

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

Atualizar metadados MFA do AD FS

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

Passos

1. Faça download do arquivo de metadados de federação do AD FS de "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copie o arquivo baixado para o servidor SnapCenter para atualizar a configuração 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 guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Atualizar os 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 da CA, DR, etc.

Passos

1. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
    a. Clique em **confiança de parte**.
    b. Clique com o botão direito do Mouse na confiança de quem confia que foi criada para o SnapCenter e clique em **Excluir**.

    O nome definido pelo utilizador da confiança da parte dependente será apresentado.

    c. Habilite a autenticação multifator (MFA).

    "Ativar a autenticação multifator"Consulte .

2. Feche todas as guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Desativar a autenticação multifator (MFA)

Passos

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

Gerencie a autenticação multifator (MFA) usando API REST, PowerShell e SCCLI

O login no MFA é compatível com navegador, API REST, PowerShell e SCCLI. O MFA é suportado por um gerenciador de identidade do AD FS. Você pode ativar o MFA, desativar o MFA e configurar o MFA a partir de GUI, API REST, PowerShell e SCCLI.

Configurar o AD FS como OAuth/OIDC

- Configurar o AD FS usando o assistente GUI do Windows*
  1. Navegue até **Painel do Gestor do servidor** > **Ferramentas** > **Gestão ADFS**.
  2. Navegue até **ADFS** > **grupos de aplicativos**.
     a. Clique com o botão direito do rato em **grupos de aplicações**.
     b. Selecione **Adicionar grupo de aplicativos** e digite **Nome do aplicativo**.
     c. Selecione **aplicação de servidor**.
     d. Clique em **seguinte**.
  3. Copiar **Identificador do cliente**.

     Esta é a ID do cliente. .. Adicionar URL de retorno de chamada (URL do servidor SnapCenter) em URL de redirecionamento. .. Clique em **seguinte**.

  4. Selecione **Generate shared secret** (gerar segredo partilhado).

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

  5. Na página **Summary**, clique em **Next**.
     a. Na página **Complete**, clique em **Close**.
  6. Clique com o botão direito no recém-adicionado **Application Group** e selecione **Properties**.
  7. Selecione **Adicionar aplicativo** nas Propriedades do aplicativo.
  8. Clique em **Adicionar aplicativo**.

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

  9. Na página Configurar API da Web, digite o URL do servidor SnapCenter e o identificador do cliente criados na etapa anterior na seção Identificador.

a. Clique em **Add**.

b. Clique em **seguinte**.

10. Na página **escolha Política de Controle de Acesso**, selecione a política de controle com base em sua exigência (por exemplo, permitir todos e exigir MFA) e clique em **Avançar**.
11. Na página **Configurar permissão de aplicativo**, por padrão openid é selecionado como um escopo, clique em **Avançar**.
12. Na página **Summary**, clique em **Next**.

    Na página **Complete**, clique em **Close**.

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

    A reivindicação 'aud' ou audiência 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 servidor SnapCenter) e o identificador do cliente foram adicionados corretamente.

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

16. Abra a ferramenta **AD FS Management** localizada no menu **Tools** no canto superior direito do Gerenciador de servidores.
    a. Selecione a pasta **grupos de aplicativos** na barra lateral esquerda.
    b. Selecione a API Web e clique em **edit**.
    c. Ir para a guia regras de transformação de emissão
17. Clique em **Adicionar regra**.
    a. Selecione **Enviar atributos LDAP como reclamações** no menu suspenso modelo de regra de reclamação.
    b. Clique em **seguinte**.
18. Introduza o nome **regra de reclamação**.
    a. Selecione **ative Directory** no menu suspenso Attribute store.
    b. Selecione **User-Principal-Name** no menu suspenso **LDAP Attribute** e **UPN** no menu suspenso o*utgoing Claim Type*.
    c. Clique em **Finish**.

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 reivindicações usando comandos do PowerShell. Esses comandos estão disponíveis em formato de script automatizado. Para obter mais informações, consulte o artigo da KB>.

1. Crie o novo grupo de aplicativos no AD FS usando o seguinte comamnd.

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

`ClientRoleIdentifier` nome do seu grupo de aplicações

`redirectURL` URL válido para redirecionamento após autorização

2. Crie o aplicativo AD FS Server 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 a partir da saída dos seguintes comandos porque, ele é mostrado 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 Transform rules.

```
$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 o tempo de expiração do token de acesso

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

Sobre esta tarefa

- Um token de acesso pode ser usado apenas para uma combinação específica de usuário, cliente e recurso. Os tokens de acesso não podem ser revogados e são válidos até sua expiração.
- Por padrão, o tempo de expiração de um token de acesso é de 60 minutos. Este tempo de expiração mínimo é suficiente e dimensionado. Você deve fornecer valor suficiente para evitar qualquer trabalho crítico contínuo dos negócios.

Passo

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

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

Obtenha o token portador do AD FS

Você deve preencher os parâmetros abaixo mencionados em qualquer cliente REST (como Postman) e ele solicita 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 portador.

A validade do token portador é configurável a partir do servidor AD FS por aplicativo e o período de validade padrão é de 60 minutos.

Campo	Valor
Tipo de concessão	Código de autorização
URL de retorno de chamada	Insira o URL base do aplicativo se você não tiver um URL de retorno de chamada.
URL de autenticação	[adfs-domain-name]/adfs/oauth2/autorize
Acesse o URL do token	[adfs-domain-name]/adfs/oauth2/token
ID do cliente	Introduza a ID de cliente do AD FS

Segredo do cliente	Insira o segredo do cliente do AD FS
Âmbito de aplicação	OpenID
Autenticação do cliente	Enviar como cabeçalho AUTH básico
Recurso	Na guia **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 servidor SnapCenter usando PowerShell, SCCLI e API REST

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

Autenticação de CLI de MFA do SnapCenter

No PowerShell e 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>]
```

Depois que o cmdlet acima é executado, uma sessão é criada para que o respetivo usuário execute outros cmdlets SnapCenter.

Autenticação da API REST do SnapCenter MFA

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

Fluxo de trabalho da API REST 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 (API REST do SnapCenter) para executar qualquer operação.

Passos

Para autenticar através do AD FS MFA

1. Configure o CLIENTE REST para chamar o endpoint do AD FS para obter o token de acesso.

Quando você pressiona o botão para obter um token de acesso para um aplicativo, você será redirecionado para a página SSO do AD FS, onde você deve fornecer suas credenciais do AD e autenticar com 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 de domínio ou domínio/usuário.

2. Na caixa de texto Senha, digite sua senha.
3. Clique em **Log in**.
4. Na seção **Opções de login**, selecione uma opção de autenticação e autentique (dependendo da configuração).
   - Push: Aprove a notificação de envio que é enviada para o telefone.
   - Código QR: Use o aplicativo móvel AUTH Point para digitalizar o código QR e, em seguida, digite o código de verificação mostrado no aplicativo
   - Senha de uso único: Digite a senha de uso único do token.
5. Após a autenticação bem-sucedida, um pop-up será aberto que contém o Access, ID e Atualizar Token.

   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 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.

Ative ou desative a funcionalidade SnapCenter MFA para API REST, CLI e GUI

GUI

Passos

1. Inicie sessão no servidor SnapCenter como Administrador do SnapCenter.
2. Clique em **Configurações** > **Configurações globais** > **Configurações MultiFactorAuthentication(MFA)**
3. Selecione a interface (GUI/RST API/CLI) para ativar ou desativar o login MFA.
   - Interface do PowerShell*

Passos

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

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

   O parâmetro PATH especifica a localização do arquivo xml de metadados MFA do AD FS.

Habilita o MFA para GUI do SnapCenter, API REST, PowerShell e SCCLI configurados com 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.

SCCLI Interface

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 POST para ativar MFA para GUI, API REST, PowerShell e SCCLI.

Parâmetro	Valor
URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Post
Solicitar corpo	"IsGuiMFAEnabled": False, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSConfigFilePath": "C: ADFS_metadata.abc.xml"
Corpo de resposta	"IGuiMFAEnabled": False, "ADFSConfigFilePath": NULL, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "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/multifactorauthentication
Método HTTP	Obter
Corpo de resposta	"IGuiMFAEnabled": False, "ADFSConfigFilePath": NULL, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com"

Informações sobre direitos autorais

Informações sobre marcas comerciais