Prepare-se para instalar o servidor SnapCenter

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

Prepare-se para instalar o servidor SnapCenter

Requisitos de domínio e grupo de trabalho

O servidor SnapCenter pode ser instalado em sistemas que estejam em um domínio ou em um grupo de trabalho. O usuário usado para instalação deve ter Privileges de administrador na máquina no caso de grupo de trabalho e domínio.

Para instalar plug-ins do servidor SnapCenter e do SnapCenter em hosts Windows, você deve usar um dos seguintes:

- **Domínio ative Directory**

  Você deve usar um usuário de domínio com direitos de administrador local. O usuário do domínio deve ser membro do grupo Administrador local no host do Windows.

- **Grupos de trabalho**

  Você deve usar uma conta local que tenha direitos de administrador local.

Embora as trusts de domínio, florestas de vários domínios e trusts de vários domínios sejam suportados, os domínios de floresta cruzada não são suportados. A documentação da Microsoft sobre domínios e trusts do ative Directory contém mais informações.

Depois de instalar o servidor SnapCenter, você não deve alterar o domínio no qual o host SnapCenter está localizado. Se você remover o host do servidor SnapCenter do domínio em que estava quando o servidor SnapCenter foi instalado e tentar desinstalar o servidor SnapCenter, a operação de desinstalação falhará.

Requisitos de espaço e dimensionamento

Antes de instalar o servidor SnapCenter, você deve estar familiarizado com os requisitos de espaço e dimensionamento. Você também deve aplicar as atualizações de sistema e segurança disponíveis.

Item	Requisitos de host do Windows	Requisitos de host do Linux
Sistemas operacionais	Microsoft Windows Apenas as versões em inglês, alemão, japonês e chinês simplificado dos sistemas operacionais são suportadas. Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp"consulte .	• Red Hat Enterprise Linux (RHEL) 8 e 9 • SUSE Linux Enterprise Server (SLES) 15 Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp"consulte .

Item	Requisitos de host do Windows	Requisitos de host do Linux
Contagem mínima de CPU	4 núcleos	4 núcleos
RAM mínima	8 GB O pool de buffers do MySQL Server usa 20% do total de RAM.	8 GB
Espaço mínimo no disco rígido para o software e logs do servidor SnapCenter	7 GB Se você tiver o repositório SnapCenter na mesma unidade em que o servidor SnapCenter está instalado, então é recomendável ter 15 GB.	15 GB
Espaço mínimo no disco rígido para o repositório SnapCenter	8 GB OBSERVAÇÃO: Se você tiver o servidor SnapCenter na mesma unidade em que o repositório SnapCenter está instalado, então é recomendável ter 15 GB.	Não aplicável

Item	Requisitos de host do Windows	Requisitos de host do Linux
Pacotes de software necessários	• Microsoft .NET Framework 4.7.2 ou posterior • Pacote de Hospedagem ASP.NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell 7.4.2 ou posterior Para obter informações específicas de solução de problemas .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet" consulte .	• ASP.NET Core Runtime começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell 7.4.2 ou posterior • O nginx é um servidor web que pode ser usado como proxy reverso • PAM-devel PAM (Pluggable Authentication Modules) é uma ferramenta de segurança do sistema que permite que os administradores de sistema definam a política de autenticação sem ter que recompilar programas que fazem a autenticação.

Requisitos de host SAN

Se o seu host SnapCenter fizer parte de um ambiente FC/iSCSI, talvez seja necessário instalar software adicional no sistema para permitir o acesso ao storage ONTAP.

O SnapCenter não inclui Utilitários do anfitrião ou um DSM. Se o seu host SnapCenter fizer parte de um ambiente SAN, talvez seja necessário instalar e configurar o seguinte software:

- Utilitários do host

  Os Utilitários de host são compatíveis com FC e iSCSI e permitem que você use o MPIO em seus servidores Windows. Para obter informações, "Documentação dos utilitários do host"consulte .

- Microsoft DSM para Windows MPIO

  Este software funciona com drivers MPIO do Windows para gerenciar vários caminhos entre computadores host NetApp e Windows.

  É necessário um DSM para configurações de alta disponibilidade.

> Se estiver a utilizar o ONTAP DSM, deve migrar para o Microsoft DSM. Para obter mais informações, "Como migrar do ONTAP DSM para o Microsoft DSM"consulte .

Sistemas e aplicações de storage compatíveis

Você deve conhecer o sistema de storage compatível, as aplicações e os bancos de dados.

- O SnapCenter oferece suporte ao ONTAP 9.12.1 e posterior para proteger seus dados.
- O SnapCenter oferece suporte ao Amazon FSX for NetApp ONTAP para proteger seus dados da versão de patch do software SnapCenter 4,5 P1.

  Se você estiver usando o Amazon FSX for NetApp ONTAP, verifique se os plug-ins de host do servidor SnapCenter são atualizados para 4,5 P1 ou posterior para executar operações de proteção de dados.

  É compatível com NVMe (non-volátil Memory Express) em Transport Control Protocol (TCP).

  Para obter informações sobre o Amazon FSX for NetApp ONTAP, "Documentação do Amazon FSX para NetApp ONTAP" consulte .

- O SnapCenter oferece suporte à proteção de diferentes aplicativos e bancos de dados.

  Para obter informações detalhadas sobre os aplicativos e bancos de dados suportados, "Ferramenta de Matriz de interoperabilidade do NetApp" consulte .

- O SnapCenter 4,9 P1 e posterior oferece suporte à proteção de workloads Oracle e Microsoft SQL em ambientes de data center definido por software (SDDC) da Amazon Web Services (AWS).

  Para obter mais informações, "Proteja workloads Oracle e MS SQL usando o NetApp SnapCenter em ambientes AWS SDDC"consulte .

Navegadores suportados

O software SnapCenter pode ser usado em vários navegadores.

- Chrome versão 125 e posterior
- Microsoft Edge 110.0.1587.17 e posterior

Para obter as informações mais recentes sobre versões suportadas, consulte : "Ferramenta de Matriz de interoperabilidade do NetApp".

Requisitos de conexão e porta

Você deve garantir que os requisitos de conexões e portas sejam atendidos antes de instalar os plug-ins do servidor SnapCenter e do aplicativo ou do banco de dados.

- Os aplicativos não podem compartilhar uma porta.

  Cada porta deve ser dedicada ao aplicativo apropriado.

- Para portas personalizáveis, você pode selecionar uma porta personalizada durante a instalação se não quiser usar a porta padrão.

  Você pode alterar uma porta de plug-in após a instalação usando o assistente Modificar host.

- Para portas fixas, você deve aceitar o número de porta padrão.
- Firewalls
  - Firewalls, proxies ou outros dispositivos de rede não devem interferir nas conexões.

- Se você especificar uma porta personalizada ao instalar o SnapCenter, adicione uma regra de firewall no host do plug-in para essa porta para o Loader de plug-ins do SnapCenter.

A tabela a seguir lista as diferentes portas e seus valores padrão.

Tipo de porta	Porta predefinida
Porta SnapCenter	8146 (HTTPS), bidirecional, personalizável, como no URL *https://server:8146* Usado para comunicação entre o cliente SnapCenter (o usuário SnapCenter) e o servidor SnapCenter. Também usado para comunicação dos hosts de plug-in para o servidor SnapCenter. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Porta de comunicação SnapCenter SMCore	8145 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre o servidor SnapCenter e os hosts onde os plug-ins do SnapCenter estão instalados. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Porta de serviço do Agendador	8154 (HTTPS) Esta porta é usada para orquestrar os fluxos de trabalho do agendador do SnapCenter para todos os plug-ins gerenciados dentro do host do servidor SnapCenter de maneira centralizada. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Porto RabbitMQ	5672 (tcp) Esta é a porta padrão em que o RabbitMQ escuta e é usada para comunicação entre o serviço de Agendador e o SnapCenter.

Tipo de porta	Porta predefinida
Porta MySQL	3306 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre o SnapCenter e o banco de dados do repositório MySQL. Você pode criar conexões seguras do servidor SnapCenter para o servidor MySQL. "Saiba mais" Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Hosts de plug-in do Windows	135, 445 (TCP) Além das portas 135 e 445, o intervalo de portas dinâmico especificado pela Microsoft também deve estar aberto. As operações de instalação remota usam o serviço Windows Management Instrumentation (WMI), que procura dinamicamente esse intervalo de portas. Para obter informações sobre o intervalo de portas dinâmico suportado, consulte "Visão geral do serviço e requisitos de porta de rede para Windows" As portas são usadas para comunicação entre o servidor SnapCenter e o host no qual o plug-in está sendo instalado. Para enviar binários de pacotes de plug-in para hosts de plug-in do Windows, as portas devem estar abertas apenas no host de plug-in e podem ser fechadas após a instalação.
Hosts plug-in Linux ou AIX	22 (SSH) As portas são usadas para comunicação entre o servidor SnapCenter e o host onde o plug-in está sendo instalado. As portas são usadas pelo SnapCenter para copiar binários de pacotes de plug-in para hosts de plug-in Linux ou AIX e devem ser abertas ou excluídas do firewall ou iptables.

Tipo de porta	Porta predefinida
Pacote de plug-ins do SnapCenter para Windows, pacote de plug-ins do SnapCenter para Linux ou pacote de plug-ins do SnapCenter para AIX	8145 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre SMCore e hosts onde o pacote plug-ins está instalado. O caminho de comunicação também precisa ser aberto entre o LIF de gerenciamento da SVM e o servidor SnapCenter. Para personalizar a porta, consulte "Adicione hosts e instale o plug-in do SnapCenter para Microsoft Windows" ou "Adicione hosts e instale o pacote de plug-ins do SnapCenter para Linux ou AIX."
Plug-in SnapCenter para banco de dados Oracle	27216, personalizável A porta JDBC padrão é usada pelo plug-in para Oracle para conexão com o banco de dados Oracle. Para personalizar a porta, consulte "Adicione hosts e instale o pacote de plug-ins do SnapCenter para Linux ou AIX."
Plug-in do SnapCenter para banco de dados do Exchange	909, personalizável A porta NET.TCP padrão é usada pelo plug-in para Windows para conetar-se aos retornos de chamada do Exchange VSS. Para personalizar a porta, "Adicione hosts e instale o Plug-in para o Exchange"consulte .
Plug-ins compatíveis com NetApp para SnapCenter	9090 (HTTPS), fixo Esta é uma porta interna que é usada somente no host de plug-in personalizado; nenhuma exceção de firewall é necessária. A comunicação entre o servidor SnapCenter e plug-ins personalizados é roteada através da porta 8145.
Porta de comunicação do cluster ONTAP ou SVM	443 (HTTPS), bidirectional80 (HTTP), bidirecional A porta é usada pela sal (camada de abstração de storage) para comunicação entre o host que executa o servidor SnapCenter e o SVM. Atualmente, a porta também é usada pelo sal em hosts plug-in do SnapCenter para Windows para comunicação entre o host do plug-in do SnapCenter e o SVM.

Tipo de porta	Porta predefinida
Plug-in do SnapCenter para o banco de dados SAP HANA vCode Spell Checkerports	3instance_number13 ou 3instance_number15, HTTP ou HTTPS, bidirecional e personalizável Para um locatário único de contentor de banco de dados multitenant (MDC), o número da porta termina com 13; para não MDC, o número da porta termina com 15. Por exemplo, 32013 é o número da porta, por exemplo, 20 e 31015 é o número da porta, por exemplo, 10. Para personalizar a porta, consulte "Adicione hosts e instale pacotes plug-in em hosts remotos."
Porta de comunicação do controlador de domínio	Consulte a documentação da Microsoft para identificar as portas que devem ser abertas no firewall em um controlador de domínio para que a autenticação funcione corretamente. É necessário abrir as portas necessárias da Microsoft no controlador de domínio para que o servidor SnapCenter, os hosts Plug-in ou outro cliente Windows possam autenticar os usuários.

Para modificar os detalhes da porta, "Modificar hosts de plug-in"consulte .

Licenças SnapCenter

O SnapCenter requer várias licenças para habilitar a proteção de dados de aplicativos, bancos de dados, sistemas de arquivos e máquinas virtuais. O tipo de licenças do SnapCenter que você instala depende do ambiente de storage e dos recursos que deseja usar.

Licença	Quando necessário
Baseado em controladora padrão da SnapCenter	Necessário para FAS, AFF e All SAN Array (ASA) A licença padrão da SnapCenter é uma licença baseada em controlador e está incluída como parte do ONTAP One. Se você tiver a licença do SnapManager Suite, você também obtém o direito de licença padrão do SnapCenter. Se você quiser instalar o SnapCenter em uma base de avaliação com o storage FAS, AFF ou ASA, poderá obter uma licença de avaliação do ONTAP One entrando em Contato com o representante de vendas. Para obter informações sobre as licenças incluídas no ONTAP One, "Licenças incluídas no ONTAP One" consulte . O SnapCenter também é oferecido como parte do pacote de proteção de dados. Se você comprou o A400 ou posterior, você deve comprar o pacote de proteção de dados.
SnapMirror ou SnapVault	ONTAP A licença SnapMirror ou SnapVault é necessária se a replicação estiver ativada no SnapCenter.
SnapRestore	Necessário para restaurar e verificar backups. Em sistemas de storage primário • Necessário nos sistemas de destino do SnapVault para executar a verificação remota e restaurar a partir de um backup. • Necessário nos sistemas de destino SnapMirror para efetuar a verificação remota.
FlexClone	Necessário clonar bancos de dados e operações de verificação. Em sistemas de storage primário e secundário • Necessário nos sistemas de destino do SnapVault para criar clones a partir do backup do Vault secundário. • Necessário nos sistemas de destino do SnapMirror para criar clones do backup secundário do SnapMirror.

Licença	Quando necessário
Protocolos	• Licença iSCSI ou FC para LUNs • Licença CIFS para compartilhamentos SMB • Licença NFS para VMDKs do tipo NFS • Licença iSCSI ou FC para VMDKs do tipo VMFS Necessário nos sistemas de destino do SnapMirror para fornecer dados se um volume de origem não estiver disponível.
Licenças padrão da SnapCenter (opcional)	Destinos secundários É recomendado, mas não obrigatório, que você adicione licenças padrão do SnapCenter a destinos secundários. Se as licenças padrão do SnapCenter não estiverem habilitadas em destinos secundários, você não poderá usar o SnapCenter para fazer backup de recursos no destino secundário após executar uma operação de failover. No entanto, é necessária uma licença FlexClone em destinos secundários para executar operações de clonagem e verificação.

As licenças do SnapCenter Advanced e do SnapCenter nas File Services estão obsoletas e não estão mais disponíveis. A licença padrão e a licença baseada em capacidade não são mais necessárias para o Amazon FSX for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP e Azure NetApp Files.

Você deve instalar uma ou mais licenças do SnapCenter. Para obter informações sobre como adicionar licenças, "Adicione licenças padrão baseadas em controladora SnapCenter"consulte .

Licenças SMBR (Single Mailbox Recovery)

Se você estiver usando o plug-in do SnapCenter para gerenciar bancos de dados do Microsoft Exchange Server e a recuperação de caixa de correio única (SMBR), você precisará de licença adicional para SMBR, que precisa ser adquirida separadamente com base na caixa de correio do usuário.

A recuperação de caixa de correio única NetApp chegou ao fim da disponibilidade (EOA) em 12 de maio de 2023. Para obter mais informações, "CPC-00507"consulte . A NetApp continuará a oferecer suporte a clientes que adquiriram capacidade, manutenção e suporte da caixa de correio por meio de números de peça de marketing introduzidos em 24 de junho de 2020, durante o período do direito ao suporte.

O NetApp Single Mailbox Recovery é um produto parceiro fornecido pela Ontrack. O Ontrack PowerControls oferece recursos semelhantes aos da recuperação de caixa de correio única do NetApp. Os clientes podem adquirir novas licenças de software Ontrack PowerControls e renovações de manutenção e suporte Ontrack PowerControls do Ontrack (até licensingteam@ontrack.com) para recuperação granular da caixa de correio após a data EOA de 12 de maio de 2023.

Registe-se para aceder ao software SnapCenter

Você pode acessar o software SnapCenter se você é novo no Amazon FSX for NetApp ONTAP ou Azure NetApp Files e não tem uma conta NetApp existente.

Antes de começar

- Você deve ter acesso ao ID de e-mail corporativo.
- Se você usa o Azure NetApp Files, você deve ter o ID de assinatura do Azure.
- Se você estiver usando o Amazon FSX for NetApp ONTAP, você deve ter o ID do sistema de arquivos do seu sistema de arquivos FSX for ONTAP.

Sobre esta tarefa

Seu Registro está sujeito a validações de informações e pode levar até um dia para confirmar e atualizar a nova conta do site de suporte da NetApp (NSS) para acesso "completo" a partir do acesso "convidado".

Passos

1. Clique https://mysupport.netapp.com/site/user/registration para inscrição.
2. Insira seu ID de e-mail corporativo, preencha o captcha e aceite a política de privacidade do NetApp e clique em **Enviar**.
3. Autentique o Registro inserindo a OTP enviada para seu ID de e-mail e clique em **continuar**.
4. Na página de conclusão do registo, introduza os seguintes detalhes para concluir o registo.
   a. Selecione **Cliente NetApp / Usuário final**.
   b. No campo DE NÚMERO DE SÉRIE, insira um dos seguintes itens:
      - ID de subscrição do Azure se estiver a utilizar o Azure NetApp Files.
      - ID do sistema de arquivos se você estiver usando o Amazon FSX for NetApp ONTAP.

Você pode levantar um ticket em https://mysupport.netapp.com/site/help se você enfrentar qualquer problema durante o Registro ou para saber o status.

Métodos de autenticação para suas credenciais

As credenciais usam diferentes métodos de autenticação, dependendo do aplicativo ou do ambiente. As credenciais autenticam os usuários para que eles possam executar operações do SnapCenter. Você deve criar um conjunto de credenciais para a instalação de plug-ins e outro conjunto para operações de proteção de dados.

Autenticação do Windows

O método de autenticação do Windows é autenticado no ative Directory. Para autenticação do Windows, o ative Directory é configurado fora do SnapCenter. O SnapCenter se autentica sem configuração adicional. Você precisa de uma credencial do Windows para executar tarefas como adicionar hosts, instalar pacotes de plug-in e agendar tarefas.

Autenticação de domínio não confiável

O SnapCenter permite a criação de credenciais do Windows usando usuários e grupos pertencentes aos

domínios não confiáveis. Para que a autenticação seja bem-sucedida, você deve Registrar os domínios não confiáveis com o SnapCenter.

Autenticação local do grupo de trabalho

O SnapCenter permite a criação de credenciais do Windows com usuários e grupos de trabalho locais. A autenticação do Windows para usuários e grupos de grupos de trabalho locais não acontece no momento da criação de credenciais do Windows, mas é adiada até que o Registro do host e outras operações de host sejam executadas.

Autenticação do SQL Server

O método de autenticação SQL é autenticado em uma instância do SQL Server. Isso significa que uma instância do SQL Server deve ser descoberta no SnapCenter. Portanto, antes de adicionar uma credencial SQL, você deve adicionar um host, instalar pacotes de plug-in e atualizar recursos. Você precisa de autenticação do SQL Server para executar operações como agendamento no SQL Server ou descoberta de recursos.

Autenticação Linux

O método de autenticação Linux é autenticado em um host Linux. Você precisa de autenticação Linux durante a etapa inicial de adicionar o host Linux e instalar o pacote de plug-ins do SnapCenter remotamente a partir da GUI do SnapCenter.

Autenticação AIX

O método de autenticação AIX é autenticado em um host AIX. Você precisa de autenticação AIX durante a etapa inicial de adicionar o host AIX e instalar o pacote de plug-ins do SnapCenter para AIX remotamente a partir da GUI do SnapCenter.

Autenticação de banco de dados Oracle

O método de autenticação de banco de dados Oracle é autenticado em um banco de dados Oracle. Você precisa de uma autenticação de banco de dados Oracle para executar operações no banco de dados Oracle se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados. Portanto, antes de adicionar uma credencial de banco de dados Oracle, você deve criar um usuário Oracle no banco de dados Oracle com sysdba Privileges.

Autenticação Oracle ASM

O método de autenticação Oracle ASM é autenticado em uma instância do Oracle Automatic Storage Management (ASM). Se for necessário acessar a instância do Oracle ASM e se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados, você precisará de uma autenticação Oracle ASM. Portanto, antes de adicionar uma credencial Oracle ASM, você deve criar um usuário Oracle com sysasm Privileges na instância ASM.

Autenticação de catálogo RMAN

O método de autenticação de catálogo RMAN é autenticado no banco de dados de catálogo do Oracle Recovery Manager (RMAN). Se você configurou um mecanismo de catálogo externo e registrou seu banco de dados no banco de dados de catálogo, você precisa adicionar autenticação de catálogo RMAN.

Conexões e credenciais de storage

Antes de executar operações de proteção de dados, você deve configurar as conexões de armazenamento e adicionar as credenciais que o servidor SnapCenter e os plug-ins SnapCenter usarão.

- * Conexões de armazenamento*

  As conexões de armazenamento dão aos plug-ins do servidor SnapCenter e do SnapCenter acesso ao armazenamento do ONTAP. A configuração dessas conexões também envolve a configuração de recursos do AutoSupport e do sistema de Gerenciamento de Eventos (EMS).

- **Credenciais**

  - Administrador de domínio ou qualquer membro do grupo de administradores

    Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são:

    - *NetBIOS_username*
    - *Domain FQDN_username*
    - *upn*

  - Administrador local (apenas para grupos de trabalho)

    Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host.

  O formato válido para o campo Nome de usuário é: *Nome de usuário*

  - Credenciais para grupos de recursos individuais

    Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver Privileges de administrador completo, será necessário atribuir pelo menos o grupo de recursos e Privileges de backup ao nome de usuário.

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