Prepare-se para instalar o servidor SnapCenter

SnapCenter Software 4.7

NetApp
April 02, 2025

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
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 .
Contagem mínima de CPU	4 núcleos

Item	Requisitos
RAM mínima	8 GB O pool de buffers do MySQL Server usa 20% do total de RAM.
Espaço mínimo no disco rígido para o software e logs do servidor SnapCenter	4 GB Se você tiver o repositório SnapCenter na mesma unidade em que o servidor SnapCenter está instalado, então é recomendável ter 10 GB.
Espaço mínimo no disco rígido para o repositório SnapCenter	6 GB OBSERVAÇÃO: Se você tiver o servidor SnapCenter na mesma unidade em que o repositório SnapCenter está instalado, então é recomendável ter 10 GB.
Pacotes de software necessários	• Microsoft .NET Framework 4.7.2 ou posterior • Windows Management Framework (WMF) 4,0 ou posterior • PowerShell 4,0 ou posterior Para obter informações sobre solução de problemas .NET, consulte, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet." Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp" consulte .

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 8.3.0 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.

  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 .

Navegadores suportados

O software SnapCenter pode ser usado em vários navegadores.

- Chrome

  Se você estiver usando o V66, talvez não inicie a GUI do SnapCenter.

- Internet Explorer

  SnapCenter UI não carrega corretamente se você estiver usando IE 10 ou versões anteriores. Você deve atualizar para o IE 11.

  - Somente a segurança de nível padrão é suportada.

    Fazer alterações nas configurações de segurança do Internet Explorer resulta em problemas significativos de exibição do navegador.

  - A exibição de compatibilidade do Internet Explorer deve ser desativada.
- Microsoft Edge

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

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."

Tipo de porta	Porta predefinida
Porta MySQL	3306 (HTTPS), bidirecional 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"
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.
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."

Tipo de porta	Porta predefinida
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-ins personalizados 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.
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."

Tipo de porta	Porta predefinida
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 e AFF A licença padrão da SnapCenter é uma licença baseada em controlador e está incluída como parte do pacote premium. 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 ou AFF, poderá obter uma licença de avaliação do pacote Premium entrando em Contato com o representante de vendas. 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.

Licença	Quando necessário
Baseado em capacidade padrão da SnapCenter	Necessário com ONTAP Select e Cloud Volumes ONTAP Se você é um cliente do Cloud Volumes ONTAP ou do ONTAP Select, precisa adquirir uma licença baseada em capacidade por TB com base nos dados gerenciados pelo SnapCenter. Por padrão, o SnapCenter envia uma licença de teste baseada em capacidade padrão SnapCenter de 90 dias e 100 TB incorporada. Para outros detalhes, entre em Contato com o representante de vendas.
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.
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.

Licença	Quando necessário
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.

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

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.

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.

Ativar autenticação multifator (MFA)

Para habilitar a funcionalidade MFA, você deve executar algumas etapas no servidor do Serviço de Federação do ative Directory (AD FS) e no servidor SnapCenter.

O que você vai precisar

- O Serviço de Federação do ative Directory do Windows (AD FS) deve estar ativo e em execução no respetivo domínio.
- Você deve ter qualquer 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 serão interrompidas 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 .

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. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

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 o cmdlet *Set-SmMultiFactorAuthentication -enable -Path*.

   O parâmetro PATH especifica a localização do arquivo xml de metadados MFA do AD FS, que foi copiado para o servidor SnapCenter na etapa 3.

8. (Opcional) Verifique o status e as configurações do MFA usando o cmdlet *Get-SmMultiFactorAuthentication*.
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 e acesse a política de controle conforme necessário e clique em **Next**.
    e. Defina 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 ' Nome de exibição da parte dependente >' -SigningCertificateRevocationCheck None

    Set-AdfsRelyingPartyTrust -TARGETNAME ' Nome de exibição da parte dependente >' -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.

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

Depois de terminar

Depois de ativar, atualizar ou desativar as configurações de MFA no SnapCenter, feche todas as guias do navegador e reabra um navegador para fazer login novamente. Isto irá limpar os cookies de sessão existentes ou ativos.

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.localização do arquivo xml de metadados ADFS MFA>

Depois de terminar

Depois de ativar, atualizar ou desativar as configurações de MFA no SnapCenter, feche todas as guias do navegador e reabra um navegador para fazer login novamente. Isto irá limpar os cookies de sessão existentes ou ativos.

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).

       Consulte "Ativar a autenticação multifator"

Depois de terminar

Depois de ativar, atualizar ou desativar as configurações de MFA no SnapCenter, feche todas as guias do navegador e reabra um navegador para fazer login novamente. Isto irá limpar os cookies de sessão existentes ou ativos.

Desativar a autenticação multifator (MFA)

Desative o MFA e limpe os arquivos de configuração que foram criados quando o MFA foi habilitado usando o cmdlet *Set-SmMultiFactorAuthentication -Disable*.

Depois de terminar

Depois de ativar, atualizar ou desativar as configurações de MFA no SnapCenter, feche todas as guias do navegador e reabra um navegador para fazer login novamente. Isto irá limpar os cookies de sessão existentes ou ativos.

Informações sobre direitos autorais

Informações sobre marcas comerciais