Use o logon único (SSO)

StorageGRID software

NetApp
December 03, 2025

Índice

Use o logon único (SSO)

Configurar logon único

Quando o logon único (SSO) estiver habilitado, os usuários só poderão acessar o Grid Manager, o Tenant Manager, a Grid Management API ou a Tenant Management API se suas credenciais forem autorizadas usando o processo de logon SSO implementado pela sua organização. Usuários locais não podem fazer login no StorageGRID.

Como funciona o logon único

O sistema StorageGRID oferece suporte ao logon único (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0).

Antes de habilitar o logon único (SSO), revise como os processos de login e logout do StorageGRID são afetados quando o SSO está habilitado.

Sign in quando o SSO estiver habilitado

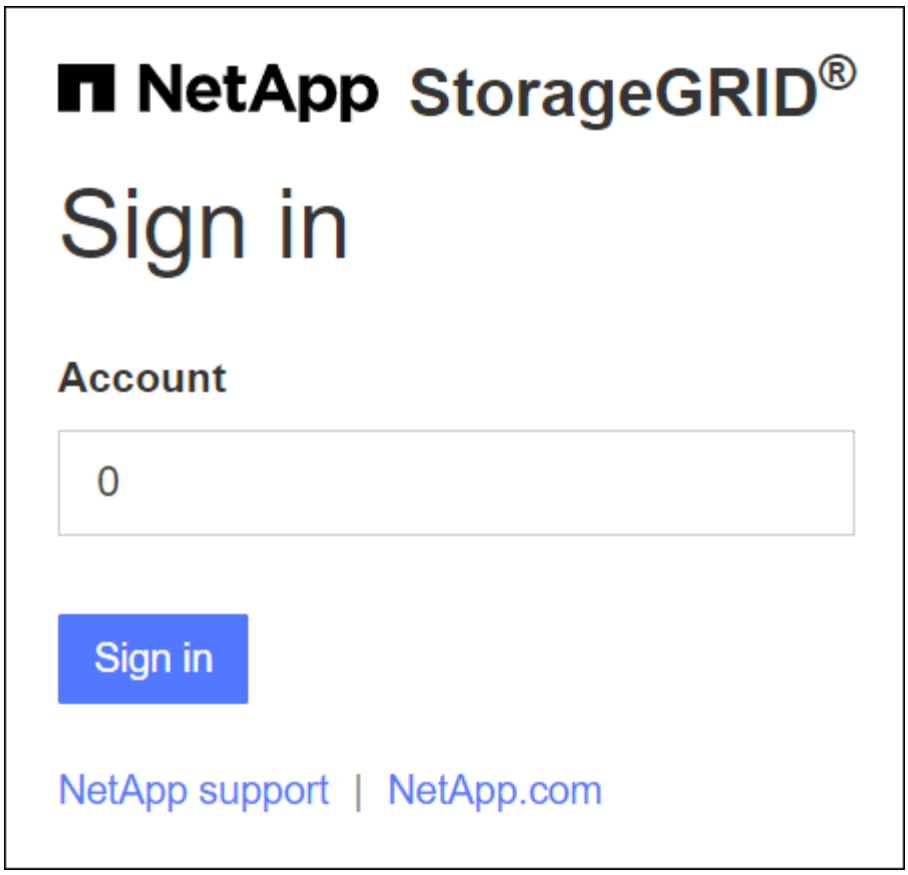
Quando o SSO estiver habilitado e você fizer login no StorageGRID, você será redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

1. Insira o nome de domínio totalmente qualificado ou o endereço IP de qualquer nó de administração do StorageGRID em um navegador da web.

   A página de Sign in do StorageGRID é exibida.

   - Se esta for a primeira vez que você acessa a URL neste navegador, será solicitado um ID de conta:

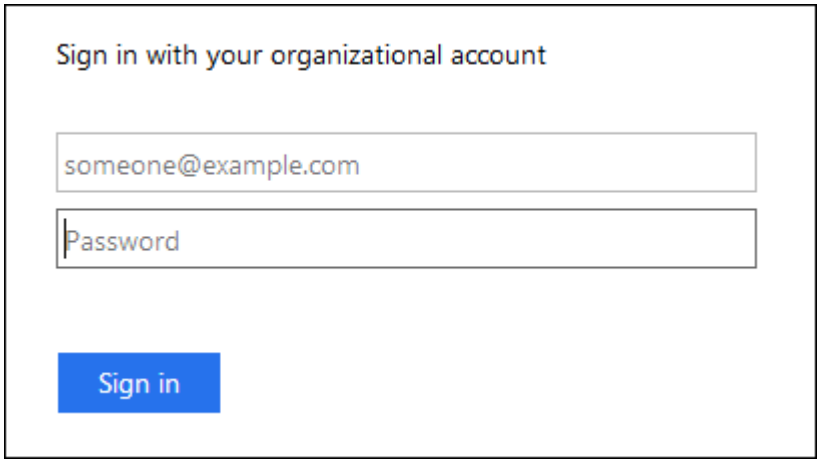


- Se você já acessou o Grid Manager ou o Tenant Manager, será solicitado que você selecione uma conta recente ou insira um ID de conta:

A página de Sign in do StorageGRID não é exibida quando você insere o URL completo de uma conta de locatário (ou seja, um nome de domínio totalmente qualificado ou endereço IP seguido por `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO da sua organização, onde poderáfaça login com suas credenciais SSO .

2. Indique se deseja acessar o Grid Manager ou o Tenant Manager:
   - Para acessar o Grid Manager, deixe o campo **ID da conta** em branco, digite **0** como ID da conta ou selecione **Grid Manager** se ele aparecer na lista de contas recentes.
   - Para acessar o Gerenciador de Inquilinos, insira o ID da conta do inquilino de 20 dígitos ou selecione um inquilino pelo nome se ele aparecer na lista de contas recentes.
3. Selecione * Sign in*

   O StorageGRID redireciona você para a página de login SSO da sua organização. Por exemplo:



4. Sign in com suas credenciais de SSO.

   Se suas credenciais de SSO estiverem corretas:

   a. O provedor de identidade (IdP) fornece uma resposta de autenticação ao StorageGRID.
   b. O StorageGRID valida a resposta de autenticação.
   c. Se a resposta for válida e você pertencer a um grupo federado com permissões de acesso ao StorageGRID , você será conectado ao Grid Manager ou ao Tenant Manager, dependendo da conta selecionada.

   Se a conta de serviço estiver inacessível, você ainda poderá fazer login, desde que seja um usuário existente que pertença a um grupo federado com permissões de acesso ao StorageGRID .

5. Opcionalmente, acesse outros nós de administração ou acesse o Grid Manager ou o Tenant Manager, se você tiver permissões adequadas.

   Você não precisa inserir novamente suas credenciais de SSO.

Sair quando o SSO estiver habilitado

Quando o SSO está habilitado para o StorageGRID, o que acontece quando você sai depende do que você está conectado e de onde você está saindo.

Passos

1. Localize o link **Sair** no canto superior direito da interface do usuário.
2. Selecione **Sair**.

   A página de Sign in do StorageGRID é exibida. O menu suspenso **Contas recentes** foi atualizado para incluir **Grid Manager** ou o nome do locatário, para que você possa acessar essas interfaces de usuário mais rapidamente no futuro.

Se você estiver conectado a…	E você sai de…	Você está desconectado de…
Gerenciador de grade em um ou mais nós de administração	Gerenciador de grade em qualquer nó de administração	Gerenciador de grade em todos os nós de administração **Observação:** Se você usar o Azure para SSO, poderá levar alguns minutos para sair de todos os nós de administração.
Gerenciador de locatários em um ou mais nós administrativos	Gerenciador de inquilinos em qualquer nó de administração	Gerenciador de inquilinos em todos os nós administrativos
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Somente o Grid Manager. Você também deve sair do Gerenciador de Locatários para sair do SSO.

A tabela resume o que acontece quando você sai se estiver usando uma única sessão do navegador. Se você estiver conectado ao StorageGRID em várias sessões do navegador, será necessário sair de todas as sessões do navegador separadamente.

Requisitos e considerações para logon único

Antes de habilitar o logon único (SSO) para um sistema StorageGRID , revise os requisitos e considerações.

Requisitos do provedor de identidade

O StorageGRID oferece suporte aos seguintes provedores de identidade SSO (IdP):

- Serviço de Federação do Active Directory (AD FS)
- Diretório Ativo do Azure (Azure AD)
- PingFederate

Você deve configurar a federação de identidade para seu sistema StorageGRID antes de poder configurar um provedor de identidade SSO. O tipo de serviço LDAP que você usa para federação de identidade controla qual

tipo de SSO você pode implementar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Diretório ativo	• Diretório ativo • Azul • PingFederate
Azul	Azul

Requisitos do AD FS

Você pode usar qualquer uma das seguintes versões do AD FS:

- AD FS do Windows Server 2022
- AD FS do Windows Server 2019
- AD FS do Windows Server 2016

> O Windows Server 2016 deve estar usando o "Atualização KB3201845" , ou superior.

Requisitos adicionais

- Segurança da Camada de Transporte (TLS) 1.2 ou 1.3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Considerações sobre o Azure

Se você usar o Azure como o tipo de SSO e os usuários tiverem nomes principais de usuário que não usam o sAMAccountName como prefixo, poderão ocorrer problemas de login se o StorageGRID perder sua conexão com o servidor LDAP. Para permitir que os usuários efetuem login, você deve restaurar a conexão com o servidor LDAP.

Requisitos de certificado do servidor

Por padrão, o StorageGRID usa um certificado de interface de gerenciamento em cada nó de administração para proteger o acesso ao Grid Manager, ao Tenant Manager, à Grid Management API e à Tenant Management API. Ao configurar relações de confiança de terceira parte confiável (AD FS), aplicativos empresariais (Azure) ou conexões de provedor de serviços (PingFederate) para o StorageGRID, você usa o certificado do servidor como o certificado de assinatura para solicitações do StorageGRID .

Se você ainda não o fez"configurou um certificado personalizado para a interface de gerenciamento" , você deve fazer isso agora. Quando você instala um certificado de servidor personalizado, ele é usado para todos os nós de administração e você pode usá-lo em todos os trusts de terceiros confiáveis do StorageGRID , aplicativos empresariais ou conexões SP .

> Não é recomendado usar o certificado de servidor padrão de um nó de administração em uma conexão de confiança de terceira parte, aplicativo empresarial ou SP . Se o nó falhar e você recuperá-lo, um novo certificado de servidor padrão será gerado. Antes de poder fazer login no nó recuperado, você deve atualizar a confiança da parte confiável, o aplicativo empresarial ou a conexão SP com o novo certificado.

Você pode acessar o certificado do servidor de um nó de administração efetuando login no shell de comando do nó e indo para `/var/local/mgmt-api` diretório. Um certificado de servidor personalizado é denominado `custom-server.crt` . O certificado do servidor padrão do nó é denominado `server.crt` .

Requisitos portuários

O logon único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único. Ver "Controle de acesso em firewall externo" .

Confirme se os usuários federados podem fazer login

Antes de habilitar o logon único (SSO), você deve confirmar se pelo menos um usuário federado pode fazer login no Grid Manager e no Tenant Manager para qualquer conta de locatário existente.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .
- Você já configurou a federação de identidade.

Passos

1. Se houver contas de locatários existentes, confirme se nenhum deles está usando sua própria fonte de identidade.

   Quando você habilita o SSO, uma fonte de identidade configurada no Tenant Manager é substituída pela fonte de identidade configurada no Grid Manager. Os usuários pertencentes à fonte de identidade do locatário não poderão mais fazer login, a menos que tenham uma conta com a fonte de identidade do Grid Manager.

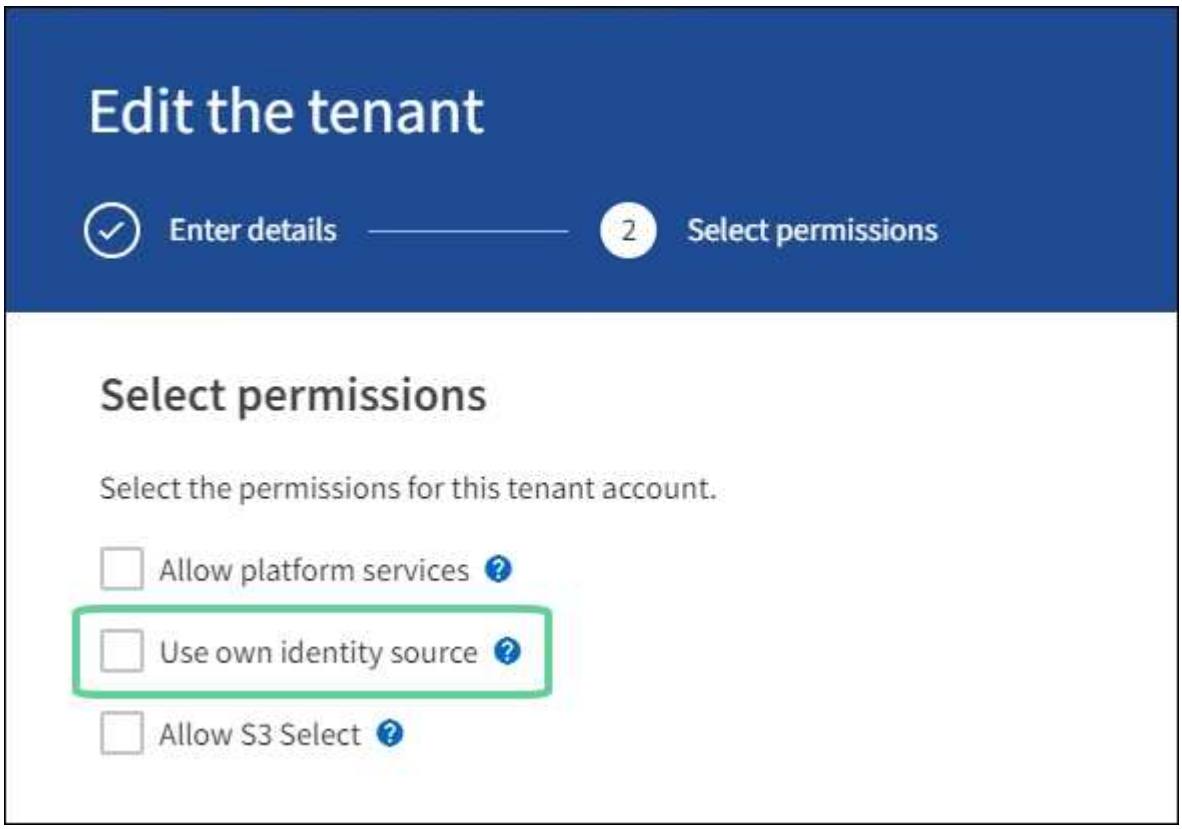
   a. Sign in no Gerenciador de Inquilinos para cada conta de inquilino.
   b. Selecione **GERENCIAMENTO DE ACESSO** > **Federação de identidade**.
   c. Confirme se a caixa de seleção **Ativar federação de identidade** não está marcada.
   d. Se for o caso, confirme se quaisquer grupos federados que possam estar em uso para esta conta de locatário não são mais necessários, desmarque a caixa de seleção e selecione **Salvar**.

2. Confirme se um usuário federado pode acessar o Grid Manager:
   a. No Grid Manager, selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Grupos de administradores**.
   b. Certifique-se de que pelo menos um grupo federado tenha sido importado da fonte de identidade do Active Directory e que tenha recebido a permissão de acesso Root.
   c. Sair.
   d. Confirme se você pode fazer login novamente no Grid Manager como um usuário no grupo federado.
3. Se houver contas de locatário existentes, confirme se um usuário federado com permissão de acesso Root pode fazer login:
   a. No Grid Manager, selecione **LOCATÁRIOS**.

b. Selecione a conta do locatário e selecione **Ações** > **Editar**.

c. Na guia Inserir detalhes, selecione **Continuar**.

d. Se a caixa de seleção **Usar fonte de identidade própria** estiver marcada, desmarque a caixa e selecione **Salvar**.



A página do inquilino é exibida.

a. Selecione a conta do locatário, selecione * Sign in* e entre na conta do locatário como usuário root local.

b. No Gerenciador de inquilinos, selecione **GERENCIAMENTO DE ACESSO** > **Grupos**.

c. Certifique-se de que pelo menos um grupo federado do Grid Manager tenha recebido a permissão de acesso Root para este locatário.

d. Sair.

e. Confirme se você pode fazer login novamente no locatário como um usuário no grupo federado.

Informações relacionadas

- "Requisitos e considerações para logon único"
- "Gerenciar grupos de administradores"
- "Use uma conta de inquilino"

Usar o modo sandbox

Você pode usar o modo sandbox para configurar e testar o logon único (SSO) antes de habilitá-lo para todos os usuários do StorageGRID . Após o SSO ser habilitado, você pode retornar ao modo sandbox sempre que precisar alterar ou testar novamente a

configuração.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .
- Você configurou a federação de identidade para seu sistema StorageGRID .
- Para a federação de identidade **tipo de serviço LDAP**, você selecionou Active Directory ou Azure, com base no provedor de identidade SSO que planeja usar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Diretório ativo	• Diretório ativo • Azul • PingFederate
Azul	Azul

Sobre esta tarefa

Quando o SSO está habilitado e um usuário tenta fazer login em um nó de administração, o StorageGRID envia uma solicitação de autenticação ao provedor de identidade do SSO. Por sua vez, o provedor de identidade SSO envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autenticação foi bem-sucedida. Para solicitações bem-sucedidas:

- A resposta do Active Directory ou PingFederate inclui um identificador universalmente exclusivo (UUID) para o usuário.
- A resposta do Azure inclui um Nome Principal do Usuário (UPN).

Para permitir que o StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre solicitações de autenticação do usuário, você deve configurar determinadas configurações no StorageGRID. Em seguida, você deve usar o software do provedor de identidade SSO para criar uma parte confiável (AD FS), aplicativo empresarial (Azure) ou provedor de serviços (PingFederate) para cada nó de administração. Por fim, você deve retornar ao StorageGRID para habilitar o SSO.

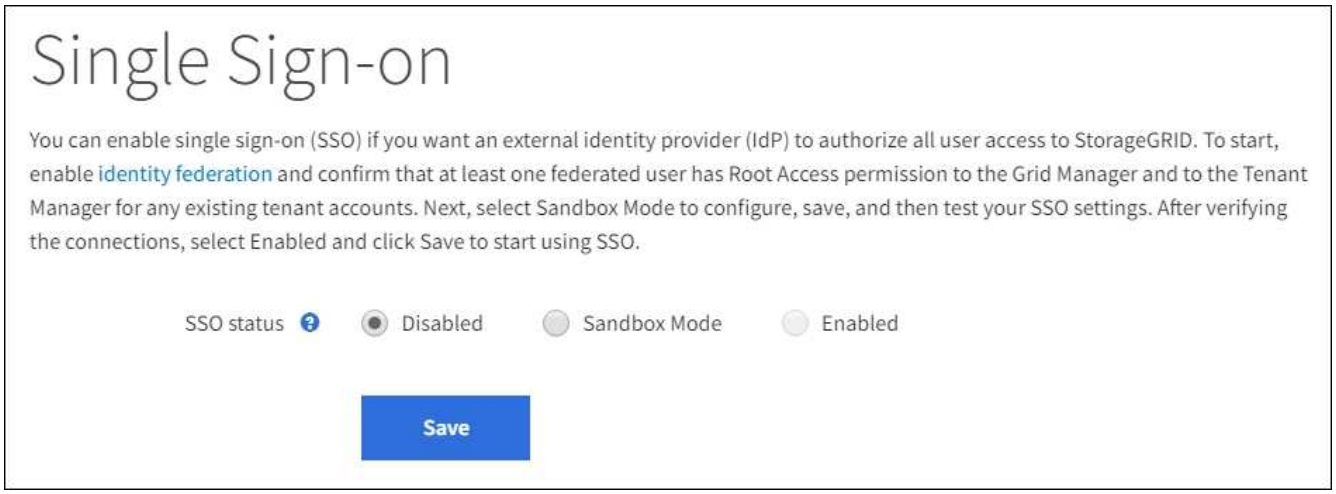
O modo sandbox facilita a execução dessa configuração de ida e volta e o teste de todas as suas configurações antes de habilitar o SSO. Quando você usa o modo sandbox, os usuários não conseguem fazer login usando SSO.

Acessar o modo sandbox

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.

   A página de logon único é exibida, com a opção **Desativado** selecionada.



Se as opções de Status do SSO não aparecerem, confirme se você configurou o provedor de identidade como a fonte de identidade federada. Ver "Requisitos e considerações para logon único" .

2. Selecione **Modo Sandbox**.

   A seção Provedor de Identidade é exibida.

Insira os detalhes do provedor de identidade

Passos

1. Selecione o **tipo de SSO** na lista suspensa.
2. Preencha os campos na seção Provedor de identidade com base no tipo de SSO selecionado.

Diretório ativo

a. Insira o **Nome do serviço de federação** para o provedor de identidade, exatamente como ele aparece no Serviço de Federação do Active Directory (AD FS).

> Para localizar o nome do serviço de federação, acesse o Gerenciador do Windows Server. Selecione **Ferramentas** > **Gerenciamento do AD FS**. No menu Ação, selecione **Editar propriedades do serviço de federação**. O nome do serviço da federação é mostrado no segundo campo.

b. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de SSO em resposta às solicitações do StorageGRID .

- **Usar certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, imediatamente"reinicie o serviço mgmt-api nos nós de administração" e testar um SSO bem-sucedido no Grid Manager.

c. Na seção Parte Confiável, especifique o **Identificador da parte confiável** para StorageGRID. Este valor controla o nome que você usa para cada parte confiável no AD FS.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera uma tabela que mostra o identificador da parte confiável para cada nó de administração no seu sistema, com base no nome do host do nó.

> Você deve criar uma parte confiável para cada nó de administração no seu sistema StorageGRID . Ter uma parte confiável para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

d. Selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.

Azul

a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de SSO em resposta às solicitações do

StorageGRID .

- **Usar certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, imediatamente"reinicie o serviço mgmt-api nos nós de administração" e testar um SSO bem-sucedido no Grid Manager.

b. Na seção Aplicativo Corporativo, especifique o **Nome do aplicativo corporativo** para StorageGRID. Este valor controla o nome que você usa para cada aplicativo empresarial no Azure AD.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera uma tabela que mostra um nome de aplicativo corporativo para cada nó de administração no seu sistema, com base no nome do host do nó.

> Você deve criar um aplicativo corporativo para cada nó de administração no seu sistema StorageGRID . Ter um aplicativo corporativo para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

c. Siga os passos em"Crie aplicativos corporativos no Azure AD" para criar um aplicativo corporativo para cada nó administrativo listado na tabela.

d. No Azure AD, copie a URL de metadados da federação para cada aplicativo empresarial. Em seguida, cole esta URL no campo **URL de metadados da federação** correspondente no StorageGRID.

e. Depois de copiar e colar uma URL de metadados de federação para todos os nós de administração, selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.

PingFederate

a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de SSO em resposta às solicitações do StorageGRID .

- **Usar certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.

- **Usar certificado CA personalizado**: Use um certificado CA personalizado para proteger a conexão.

  Se você selecionar esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

- **Não use TLS**: Não use um certificado TLS para proteger a conexão.

> Se você alterar o certificado da CA, imediatamente"reinicie o serviço mgmt-api nos nós de administração" e testar um SSO bem-sucedido no Grid Manager.

b. Na seção Provedor de serviços (SP), especifique o * ID de conexão do SP * para StorageGRID. Este valor controla o nome que você usa para cada conexão SP no PingFederate.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera uma tabela que mostra o ID de conexão do SP para cada nó de administração no seu sistema, com base no nome do host do nó.

> Você deve criar uma conexão SP para cada nó de administração no seu sistema StorageGRID . Ter uma conexão SP para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

c. Especifique a URL de metadados da federação para cada nó administrativo no campo **URL de metadados da federação**.

Use o seguinte formato:

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

d. Selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.

Configurar trusts de terceira parte confiável, aplicativos corporativos ou conexões SP

Quando a configuração é salva, o aviso de confirmação do modo Sandbox é exibido. Este aviso confirma que o modo sandbox agora está ativado e fornece instruções gerais.

O StorageGRID pode permanecer no modo sandbox pelo tempo que for necessário. No entanto, quando o

Modo Sandbox é selecionado na página de logon único, o SSO é desabilitado para todos os usuários do StorageGRID . Somente usuários locais podem fazer login.

Siga estas etapas para configurar confianças de partes confiáveis (Active Directory), aplicativos empresariais completos (Azure) ou configurar conexões SP (PingFederate).

Diretório ativo

Passos

1. Acesse os Serviços de Federação do Active Directory (AD FS).
2. Crie um ou mais trusts de parte confiável para o StorageGRID, usando cada identificador de parte confiável mostrado na tabela na página de logon único do StorageGRID .

   Você deve criar uma confiança para cada nó administrativo mostrado na tabela.

   Para obter instruções, acesse"Criar relações de confiança de terceira parte confiável no AD FS" .

Azul

Passos

1. Na página de logon único do nó de administração no qual você está conectado no momento, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração na sua grade, repita estas etapas:
   a. Sign in no nó.
   b. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Acesse o Portal do Azure.
4. Siga os passos em"Crie aplicativos corporativos no Azure AD" para carregar o arquivo de metadados SAML para cada nó de administração em seu aplicativo empresarial do Azure correspondente.

PingFederate

Passos

1. Na página de logon único do nó de administração no qual você está conectado no momento, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração na sua grade, repita estas etapas:
   a. Sign in no nó.
   b. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   c. Baixe e salve os metadados SAML para esse nó.
3. Acesse PingFederate.
4. "Crie uma ou mais conexões de provedor de serviços (SP) para StorageGRID" . Use o ID de conexão SP para cada nó de administração (mostrado na tabela na página de logon único do StorageGRID) e os metadados SAML que você baixou para esse nó de administração.

   Você deve criar uma conexão SP para cada nó de administração mostrado na tabela.

Testar conexões SSO

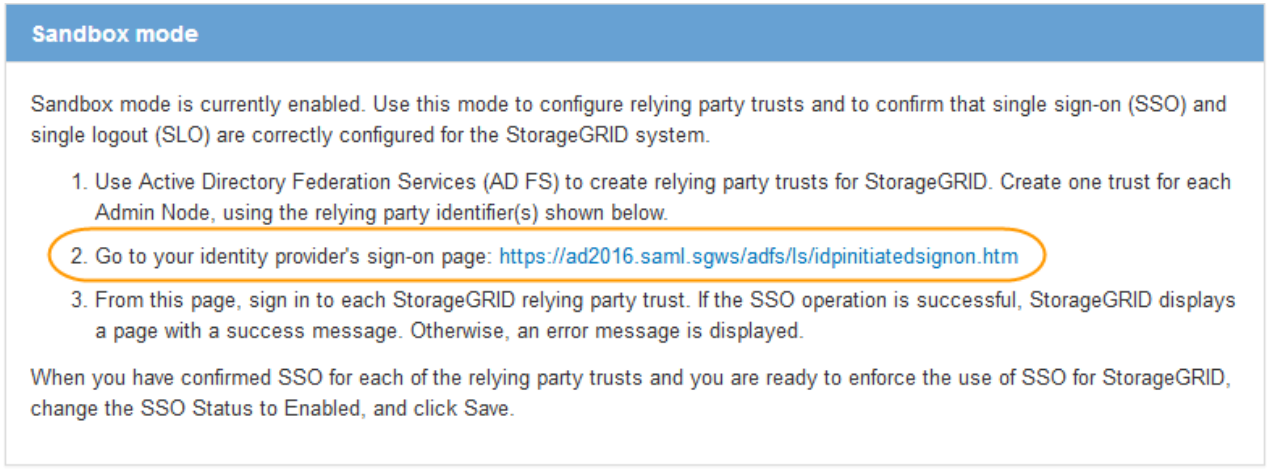
Antes de impor o uso do logon único para todo o seu sistema StorageGRID , você deve confirmar se o logon único e o logout único estão configurados corretamente para cada nó de administração.

Diretório ativo

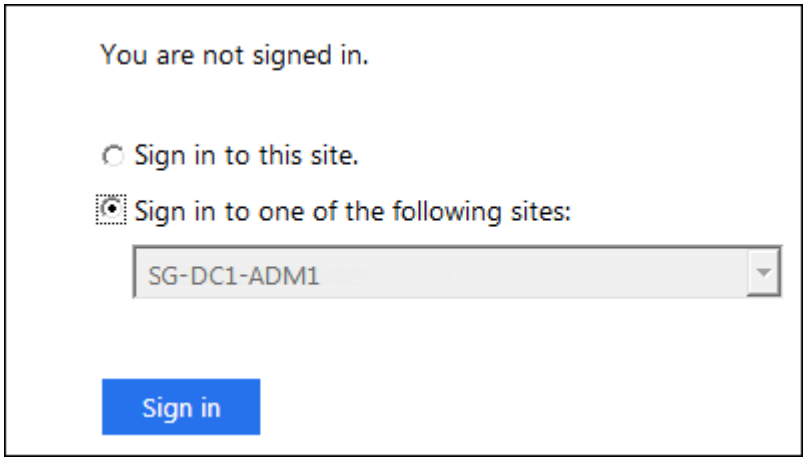
Passos

1. Na página de logon único do StorageGRID , localize o link na mensagem do modo Sandbox.

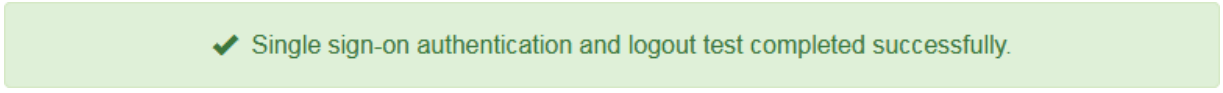
   O URL é derivado do valor inserido no campo **Nome do serviço da federação**.



2. Selecione o link ou copie e cole o URL em um navegador para acessar a página de login do seu provedor de identidade.
3. Para confirmar que você pode usar o SSO para fazer login no StorageGRID, selecione * Sign in em um dos seguintes sites*, selecione o identificador de parte confiável para seu nó de administração principal e selecione * Sign in*.



4. Digite seu nome de usuário e senha federados.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.



   - Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
5. Repita essas etapas para verificar a conexão SSO para cada nó de administração na sua grade.

Azul

Passos

1. Acesse a página de logon único no portal do Azure.
2. Selecione **Testar este aplicativo**.
3. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

     ✔ Single sign-on authentication and logout test completed successfully.

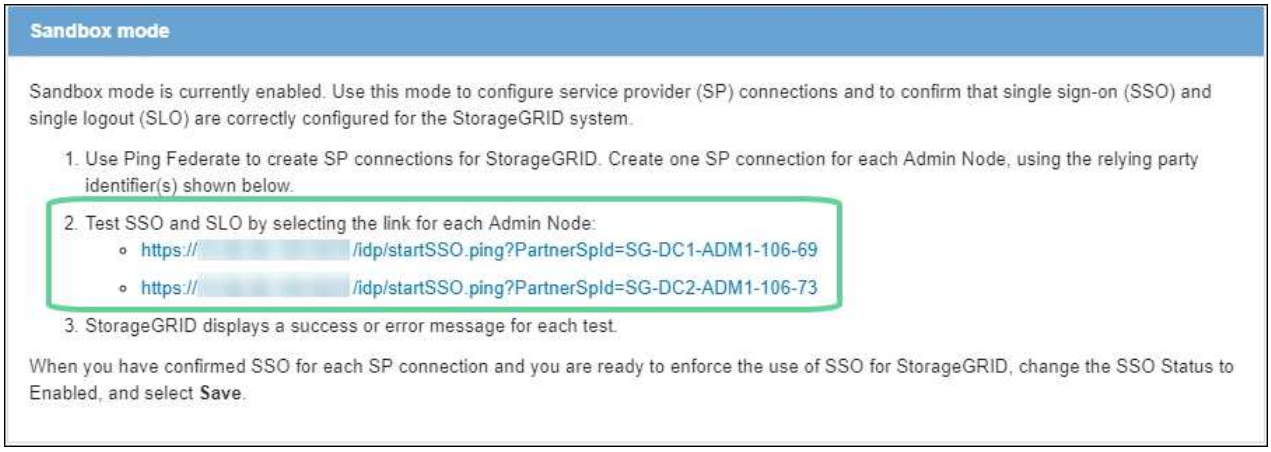
   - Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
4. Repita essas etapas para verificar a conexão SSO para cada nó de administração na sua grade.

PingFederate

Passos

1. Na página de logon único do StorageGRID , selecione o primeiro link na mensagem do modo Sandbox.

   Selecione e teste um link por vez.

2. Insira as credenciais de um usuário federado.
   - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
3. Selecione o próximo link para verificar a conexão SSO para cada nó de administração na sua grade.

   Se você vir uma mensagem de Página expirada, selecione o botão **Voltar** no seu navegador e reenvie suas credenciais.

Habilitar logon único

Depois de confirmar que você pode usar o SSO para fazer login em cada nó de administração, você pode habilitar o SSO para todo o seu sistema StorageGRID .

> Quando o SSO estiver habilitado, todos os usuários deverão usar o SSO para acessar o Grid Manager, o Tenant Manager, a Grid Management API e a Tenant Management API. Usuários locais não podem mais acessar o StorageGRID.

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
2. Altere o status do SSO para **Habilitado**.
3. Selecione **Salvar**.
4. Revise a mensagem de aviso e selecione **OK**.

   O logon único agora está habilitado.

> Se você estiver usando o Portal do Azure e acessar o StorageGRID do mesmo computador que usa para acessar o Azure, certifique-se de que o usuário do Portal do Azure também seja um usuário autorizado do StorageGRID (um usuário em um grupo federado que foi importado para o StorageGRID) ou saia do Portal do Azure antes de tentar entrar no StorageGRID.

Criar relações de confiança de terceira parte confiável no AD FS

Você deve usar os Serviços de Federação do Active Directory (AD FS) para criar uma parte confiável para cada nó de administração no seu sistema. Você pode criar trusts de terceira parte confiável usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **AD FS** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "Usar o modo sandbox" .
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador da parte confiável para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de administração na página de logon único do StorageGRID .

  > Você deve criar uma parte confiável para cada nó de administração no seu sistema StorageGRID . Ter uma parte confiável para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

- Você tem experiência na criação de relações de confiança de partes confiáveis no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in Gerenciamento do AD FS e pertence ao grupo Administradores.
- Se você estiver criando a confiança da parte confiável manualmente, terá o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID ou saberá como fazer login em um nó de administração a partir do shell de comando.

Sobre esta tarefa

Estas instruções se aplicam ao AD FS do Windows Server 2016. Se você estiver usando uma versão diferente do AD FS, notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Crie uma confiança de terceira parte confiável usando o Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais relações de confiança de terceira parte confiável.

Passos

1. No menu Iniciar do Windows, selecione com o botão direito do mouse o ícone do PowerShell e selecione **Executar como Administrador**.
2. No prompt de comando do PowerShell, digite o seguinte comando:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Para *Admin_Node_Identifier* , insira o Identificador da Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único. Por exemplo, `SG-DC1-ADM1` .
   - Para *Admin_Node_FQDN* , insira o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)
3. No Gerenciador do Windows Server, selecione **Ferramentas** > **Gerenciamento do AD FS**.

   A ferramenta de gerenciamento do AD FS é exibida.
4. Selecione **AD FS** > **Relying Party Trusts**.

   A lista de trusts de partes confiáveis é exibida.
5. Adicione uma Política de Controle de Acesso à confiança da parte confiável recém-criada:
   a. Localize a parte confiável que você acabou de criar.
   b. Clique com o botão direito do mouse no trust e selecione **Editar Política de Controle de Acesso**.
   c. Selecione uma Política de Controle de Acesso.
   d. Selecione **Aplicar** e selecione **OK**
6. Adicione uma Política de Emissão de Reivindicações ao Trust de Parte Confiável recém-criado:
   a. Localize a parte confiável que você acabou de criar.
   b. Clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.
   c. Selecione **Adicionar regra**.
   d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como declarações** na lista e selecione **Avançar**.
   e. Na página Configurar regra, insira um nome de exibição para esta regra.

      Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

f. Para o Attribute Store, selecione **Active Directory**.

g. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.

h. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** na lista suspensa.

i. Selecione **Concluir** e selecione **OK**.

7. Confirme se os metadados foram importados com sucesso.

a. Clique com o botão direito do mouse na parte confiável para abrir suas propriedades.

b. Confirme se os campos nas guias **Endpoints**, **Identifiers** e **Signature** estão preenchidos.

Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou insira os valores manualmente.

8. Repita essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .

9. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver"Usar o modo Sandbox" para obter instruções.

Crie uma parte confiável importando metadados da federação

Você pode importar os valores para cada parte confiável acessando os metadados SAML para cada nó de administração.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.

2. Em Ações, selecione **Adicionar confiança de terceira parte confiável**.

3. Na página de boas-vindas, escolha **Reivindicações cientes** e selecione **Iniciar**.

4. Selecione **Importar dados sobre a parte confiável publicados on-line ou em uma rede local**.

5. Em **Endereço de metadados da federação (nome do host ou URL)**, digite o local dos metadados SAML para este nó de administração:

`https://Admin_Node_FQDN/api/saml-metadata`

Para *`Admin_Node_FQDN`* , insira o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

6. Conclua o assistente de Relying Party Trust, salve o trust da parte confiável e feche o assistente.

Ao inserir o nome de exibição, use o Identificador de Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único no Grid Manager. Por exemplo, `SG-DC1-ADM1` .

7. Adicione uma regra de reivindicação:

a. Clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.

b. Selecione **Adicionar regra**:

c. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como declarações** na lista e selecione **Avançar**.

d. Na página Configurar regra, insira um nome de exibição para esta regra.

   Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

e. Para o Attribute Store, selecione **Active Directory**.

f. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.

g. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** na lista suspensa.

h. Selecione **Concluir** e selecione **OK**.

8. Confirme se os metadados foram importados com sucesso.

   a. Clique com o botão direito do mouse na parte confiável para abrir suas propriedades.

   b. Confirme se os campos nas guias **Endpoints**, **Identifiers** e **Signature** estão preenchidos.

      Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou insira os valores manualmente.

9. Repita essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .

10. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver"Usar o modo Sandbox" para obter instruções.

Crie uma parte confiável manualmente

Se você optar por não importar os dados para as partes confiáveis, poderá inserir os valores manualmente.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.
2. Em Ações, selecione **Adicionar confiança de terceira parte confiável**.
3. Na página de boas-vindas, escolha **Reivindicações cientes** e selecione **Iniciar**.
4. Selecione **Inserir dados sobre a parte confiável manualmente** e selecione **Avançar**.
5. Conclua o assistente Relying Party Trust:

   a. Insira um nome de exibição para este nó de administração.

      Para consistência, use o Identificador de Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único no Grid Manager. Por exemplo, `SG-DC1-ADM1` .

   b. Ignore a etapa para configurar um certificado de criptografia de token opcional.

   c. Na página Configurar URL, marque a caixa de seleção **Ativar suporte para o protocolo SAML 2.0 WebSSO**.

   d. Digite a URL do ponto de extremidade do serviço SAML para o nó de administração:

`https://Admin_Node_FQDN/api/saml-response`

Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado para o nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

e. Na página Configurar Identificadores, especifique o Identificador de Parte Confiável para o mesmo Nó de Administração:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, insira o Identificador da Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único. Por exemplo, `SG-DC1-ADM1`.

f. Revise as configurações, salve a confiança da parte confiável e feche o assistente.

A caixa de diálogo Editar política de emissão de reivindicações é exibida.

> Se a caixa de diálogo não aparecer, clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.

6. Para iniciar o assistente de Regra de Reivindicação, selecione **Adicionar regra**:
   a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como declarações** na lista e selecione **Avançar**.
   b. Na página Configurar regra, insira um nome de exibição para esta regra.

      Por exemplo, **ObjectGUID para ID de nome** ou **UPN para ID de nome**.

   c. Para o Attribute Store, selecione **Active Directory**.
   d. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
   e. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** na lista suspensa.
   f. Selecione **Concluir** e selecione **OK**.
7. Clique com o botão direito do mouse na parte confiável para abrir suas propriedades.
8. Na guia **Endpoints**, configure o endpoint para logout único (SLO):
   a. Selecione **Adicionar SAML**.
   b. Selecione **Tipo de endpoint** > **Logout SAML**.
   c. Selecione **Vinculação** > **Redirecionamento**.
   d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste nó de administração:

      `https://Admin_Node_FQDN/api/saml-logout`

Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado do nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

a. Selecione **OK**.

9. Na aba **Assinatura**, especifique o certificado de assinatura para esta parte confiável:
   a. Adicione o certificado personalizado:
      - Se você tiver o certificado de gerenciamento personalizado que carregou no StorageGRID, selecione esse certificado.
      - Se você não tiver o certificado personalizado, faça login no nó de administração, vá para `/var/local/mgmt-api` diretório do nó de administração e adicione o `custom-server.crt` arquivo de certificado.

> Usando o certificado padrão do nó de administração(`server.crt`) não é recomendado. Se o nó de administração falhar, o certificado padrão será regenerado quando você recuperar o nó, e você precisará atualizar a confiança da parte confiável.

   b. Selecione **Aplicar** e selecione **OK**.

      As propriedades da Parte Confiável são salvas e fechadas.

10. Repita essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .
11. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver"Usar o modo sandbox" para obter instruções.

Crie aplicativos corporativos no Azure AD

Use o Azure AD para criar um aplicativo empresarial para cada nó de administração no seu sistema.

Antes de começar

- Você começou a configurar o logon único para o StorageGRID e selecionou **Azure** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "Usar o modo sandbox" .
- Você tem o **Nome do aplicativo corporativo** para cada nó de administração no seu sistema. Você pode copiar esses valores da tabela de detalhes do nó de administração na página de logon único do StorageGRID .

> Você deve criar um aplicativo corporativo para cada nó de administração no seu sistema StorageGRID . Ter um aplicativo corporativo para cada nó administrativo garante que os usuários possam entrar e sair com segurança de qualquer nó administrativo.

- Você tem experiência na criação de aplicativos corporativos no Azure Active Directory.
- Você tem uma conta do Azure com uma assinatura ativa.
- Você tem uma das seguintes funções na conta do Azure: Administrador global, Administrador de aplicativos em nuvem, Administrador de aplicativos ou proprietário da entidade de serviço.

Acessar o Azure AD

Passos

1. Faça login no "Portal do Azure" .
2. Navegar para "Diretório Ativo do Azure" .
3. Selecione "Aplicações empresariais" .

Crie aplicativos corporativos e salve a configuração do StorageGRID SSO

Para salvar a configuração de SSO do Azure no StorageGRID, você deve usar o Azure para criar um aplicativo empresarial para cada nó de administração. Você copiará as URLs de metadados da federação do Azure e as colará nos campos **URL de metadados da federação** correspondentes na página de logon único do StorageGRID .

Passos

1. Repita as etapas a seguir para cada nó de administração.
   a. No painel Aplicativos empresariais do Azure, selecione **Novo aplicativo**.
   b. Selecione **Criar seu próprio aplicativo**.
   c. Para o nome, insira o **Nome do aplicativo corporativo** que você copiou da tabela de detalhes do nó de administração na página de logon único do StorageGRID .
   d. Deixe o botão de opção **Integrar qualquer outro aplicativo que você não encontrar na galeria (Não galeria)** selecionado.
   e. Selecione **Criar**.
   f. Selecione o link **Começar** em **2. Configure a caixa de logon único** ou selecione o link **Logon único** na margem esquerda.
   g. Selecione a caixa **SAML**.
   h. Copie o **App Federation Metadata URL**, que você pode encontrar em **Step 3 SAML Signing Certificate**.
   i. Acesse a página de logon único do StorageGRID e cole a URL no campo **URL de metadados da federação** que corresponde ao **Nome do aplicativo corporativo** que você usou.
2. Depois de colar uma URL de metadados de federação para cada nó de administração e fazer todas as outras alterações necessárias na configuração do SSO, selecione **Salvar** na página de logon único do StorageGRID .

Baixe metadados SAML para cada nó de administração

Depois que a configuração do SSO for salva, você poderá baixar um arquivo de metadados SAML para cada nó de administração no seu sistema StorageGRID .

Passos

1. Repita essas etapas para cada nó de administração.
   a. Sign in no StorageGRID a partir do nó de administração.
   b. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   c. Selecione o botão para baixar os metadados SAML para esse nó de administração.
   d. Salve o arquivo que você carregará no Azure AD.

Carregar metadados SAML para cada aplicativo empresarial

Depois de baixar um arquivo de metadados SAML para cada nó de administração do StorageGRID , execute as seguintes etapas no Azure AD:

Passos

1. Retorne ao Portal do Azure.
2. Repita estas etapas para cada aplicativo corporativo:

   > Talvez seja necessário atualizar a página de aplicativos corporativos para ver os aplicativos adicionados anteriormente na lista.

   a. Acesse a página Propriedades do aplicativo empresarial.
   b. Defina **Atribuição necessária** como **Não** (a menos que você queira configurar as atribuições separadamente).
   c. Acesse a página de login único.
   d. Conclua a configuração SAML.
   e. Selecione o botão **Carregar arquivo de metadados** e selecione o arquivo de metadados SAML que você baixou para o nó de administração correspondente.
   f. Após o carregamento do arquivo, selecione **Salvar** e depois selecione **X** para fechar o painel. Você retornará à página Configurar logon único com SAML.
3. Siga os passos em"Usar o modo sandbox" para testar cada aplicação.

Criar conexões de provedor de serviços (SP) no PingFederate

Use o PingFederate para criar uma conexão de provedor de serviços (SP) para cada nó de administração no seu sistema. Para acelerar o processo, você importará os metadados SAML do StorageGRID.

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **Ping Federate** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "Usar o modo sandbox" .
- Você tem o * ID de conexão SP * para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de administração na página de logon único do StorageGRID .
- Você baixou os **metadados SAML** para cada nó de administração no seu sistema.
- Você tem experiência na criação de conexões SP no PingFederate Server.
- Você tem ohttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["Guia de Referência do Administrador"^] para o servidor PingFederate. A documentação do PingFederate fornece instruções e explicações detalhadas passo a passo.
- Você tem o"Permissão de administrador" para o servidor PingFederate.

Sobre esta tarefa

Estas instruções resumem como configurar o PingFederate Server versão 10.3 como um provedor de SSO para o StorageGRID. Se você estiver usando outra versão do PingFederate, talvez seja necessário adaptar estas instruções. Consulte a documentação do PingFederate Server para obter instruções detalhadas para sua versão.

Pré-requisitos completos no PingFederate

Antes de criar as conexões SP que você usará para o StorageGRID, você deve concluir as tarefas de pré-requisito no PingFederate. Você usará informações desses pré-requisitos ao configurar as conexões SP .

Criar armazenamento de dados

Se ainda não o fez, crie um armazenamento de dados para conectar o PingFederate ao servidor LDAP do AD FS. Use os valores que você usou quando"configurando federação de identidade" em StorageGRID.

- **Tipo**: Diretório (LDAP)
- **Tipo LDAP**: Active Directory
- **Nome do atributo binário**: insira **objectGUID** na guia Atributos binários do LDAP exatamente como mostrado.

Criar validador de credenciais de senha

Caso ainda não tenha feito isso, crie um validador de credenciais de senha.

- **Tipo**: LDAP Nome de usuário Senha Validador de credenciais
- **Armazenamento de dados**: Selecione o armazenamento de dados que você criou.
- **Base de pesquisa**: insira informações do LDAP (por exemplo, DC=saml,DC=sgws).
- **Filtro de pesquisa**: sAMAccountName=${username}
- **Escopo**: Subárvore

Criar instância do adaptador IdP

Se ainda não o fez, crie uma instância do adaptador IdP.

Passos

1. Vá para **Autenticação** > **Integração** > **Adaptadores IdP**.
2. Selecione **Criar nova instância**.
3. Na guia Tipo, selecione **Adaptador IdP de formulário HTML**.
4. Na guia Adaptador IdP, selecione **Adicionar uma nova linha para 'Validadores de credenciais'**.
5. Selecione ovalidador de credenciais de senha você criou.
6. Na guia Atributos do adaptador, selecione o atributo **nome de usuário** para **Pseudônimo**.
7. Selecione **Salvar**.

Criar ou importar certificado de assinatura

Caso ainda não tenha feito isso, crie ou importe o certificado de assinatura.

Passos

1. Vá para **Segurança** > **Chaves e Certificados de Assinatura e Descriptografia**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP no PingFederate

Ao criar uma conexão SP no PingFederate, você importa os metadados SAML baixados do StorageGRID para o nó de administração. O arquivo de metadados contém muitos dos valores específicos que você precisa.

> Você deve criar uma conexão SP para cada nó de administração no seu sistema StorageGRID , para que os usuários possam entrar e sair com segurança de qualquer nó. Use estas instruções para criar a primeira conexão SP . Então vá paraCriar conexões SP adicionais para criar quaisquer conexões adicionais que você precisar.

Escolha o tipo de conexão SP

Passos

1. Vá para **Aplicativos** > **Integração** > *Conexões SP *.
2. Selecione **Criar conexão**.
3. Selecione **Não usar um modelo para esta conexão**.
4. Selecione **Perfis SSO do navegador** e **SAML 2.0** como o protocolo.

Importar metadados SP

Passos

1. Na guia Importar metadados, selecione **Arquivo**.
2. Escolha o arquivo de metadados SAML que você baixou da página de logon único do StorageGRID para o nó de administração.
3. Revise o Resumo de Metadados e as informações fornecidas na guia Informações Gerais.

   O ID da entidade do parceiro e o nome da conexão são definidos como o ID da conexão do StorageGRID SP . (por exemplo, 10.96.105.200-DC1-ADM1-105-200). O URL base é o IP do nó de administração do StorageGRID .

4. Selecione **Avançar**.

Configurar SSO do navegador IdP

Passos

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia Perfis SAML, selecione as opções * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selecione **Avançar**.
4. Na aba Assertion Lifetime, não faça alterações.
5. Na guia Criação de Asserção, selecione **Configurar Criação de Asserção**.
   a. Na guia Mapeamento de Identidade, selecione **Padrão**.
   b. Na guia Contrato de Atributo, use **SAML_SUBJECT** como Contrato de Atributo e o formato de nome não especificado que foi importado.

6. Para estender o contrato, selecione **Excluir** para remover o `urn:oid` , que não é usado.

Instância do adaptador de mapa

Passos

1. Na guia Mapeamento de fonte de autenticação, selecione **Mapear nova instância do adaptador**.
2. Na guia Instância do adaptador, selecione oinstância do adaptador você criou.
3. Na guia Método de mapeamento, selecione **Recuperar atributos adicionais de um armazenamento de dados**.
4. Na guia Origem do atributo e pesquisa de usuário, selecione **Adicionar origem do atributo**.
5. Na guia Armazenamento de dados, forneça uma descrição e selecione oarmazenamento de dados você adicionou.
6. Na guia Pesquisa de diretório LDAP:
   - Insira o **DN base**, que deve corresponder exatamente ao valor inserido no StorageGRID para o servidor LDAP.
   - Para o Escopo de pesquisa, selecione **Subárvore**.
   - Para a classe de objeto raiz, procure e adicione um destes atributos: **objectGUID** ou **userPrincipalName**.
7. Na guia Tipos de codificação de atributo binário LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia Filtro LDAP, digite **sAMAccountName=${username}**.
9. Na guia Cumprimento de contrato de atributo, selecione **LDAP (atributo)** no menu suspenso Origem e selecione **objectGUID** ou **userPrincipalName** no menu suspenso Valor.
10. Revise e salve a origem do atributo.
11. Na guia Fonte do atributo Failsave, selecione **Abortar a transação SSO**.
12. Revise o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configurar as definições do protocolo

Passos

1. Na guia * Conexão SP * > * SSO do navegador * > * Configurações do protocolo *, selecione * Definir configurações do protocolo *.
2. Na guia URL do serviço de consumidor de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para vinculação e `/api/saml-response` para URL do ponto de extremidade).
3. Na guia URLs do serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para vinculação e `/api/saml-logout` para URL do ponto de extremidade.
4. Na guia Ligações SAML permitidas, desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são necessários.
5. Na guia Política de Assinatura, deixe as caixas de seleção **Exigir que as solicitações de autenticação sejam assinadas** e **Sempre assinar declaração** marcadas.
6. Na guia Política de Criptografia, selecione **Nenhum**.
7. Revise o resumo e selecione **Concluído** para salvar as configurações do protocolo.

8. Revise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

Passos

1. Na guia Conexão SP , selecione **Credenciais**.
2. Na guia Credenciais, selecione **Configurar credenciais**.
3. Selecione ocertificado de assinatura que você criou ou importou.
4. Selecione **Avançar** para ir para **Gerenciar configurações de verificação de assinatura**.
   a. Na guia Modelo de confiança, selecione **Não ancorado**.
   b. Na guia Certificado de verificação de assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID .
5. Revise as telas de resumo e selecione **Salvar** para salvar a conexão SP .

Criar conexões SP adicionais

Você pode copiar a primeira conexão SP para criar as conexões SP necessárias para cada nó de administração na sua grade. Você carrega novos metadados para cada cópia.

> As conexões SP para diferentes nós administrativos usam configurações idênticas, com exceção do ID da entidade do parceiro, URL base, ID da conexão, nome da conexão, verificação de assinatura e URL de resposta do SLO.

Passos

1. Selecione **Ação** > **Copiar** para criar uma cópia da conexão SP inicial para cada nó de administração adicional.
2. Insira o ID da conexão e o nome da conexão para a cópia e selecione **Salvar**.
3. Selecione o arquivo de metadados correspondente ao nó de administração:
   a. Selecione **Ação** > **Atualizar com metadados**.
   b. Selecione **Escolher arquivo** e carregue os metadados.
   c. Selecione **Avançar**.
   d. Selecione **Salvar**.
4. Resolva o erro devido ao atributo não utilizado:
   a. Selecione a nova conexão.
   b. Selecione **Configurar SSO do navegador > Configurar criação de asserção > Contrato de atributo**.
   c. Exclua a entrada para **urn:oid**.
   d. Selecione **Salvar**.

Desativar logon único

Você pode desabilitar o logon único (SSO) se não quiser mais usar essa funcionalidade. Você deve desabilitar o logon único antes de poder desabilitar a federação de identidades.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem"permissões de acesso específicas" .

Passos

1. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.

   A página de logon único é exibida.

2. Selecione a opção **Desativado**.
3. Selecione **Salvar**.

   Uma mensagem de aviso aparece indicando que usuários locais agora poderão fazer login.

4. Selecione **OK**.

   Na próxima vez que você fizer login no StorageGRID , a página de Sign in do StorageGRID será exibida e você deverá inserir o nome de usuário e a senha de um usuário local ou federado do StorageGRID .

Desabilitar temporariamente e reabilitar o logon único para um nó de administração

Talvez você não consiga fazer login no Grid Manager se o sistema de logon único (SSO) ficar inativo. Nesse caso, você pode desabilitar temporariamente e reabilitar o SSO para um nó de administração. Para desabilitar e reabilitar o SSO, você deve acessar o shell de comando do nó.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você tem o `Passwords.txt` arquivo.
- Você sabe a senha do usuário root local.

Sobre esta tarefa

Depois de desabilitar o SSO para um nó de administração, você pode entrar no Grid Manager como usuário root local. Para proteger seu sistema StorageGRID , você deve usar o shell de comando do nó para reativar o SSO no nó de administração assim que sair.

> Desabilitar o SSO para um nó administrativo não afeta as configurações de SSO para nenhum outro nó administrativo na grade. A caixa de seleção **Habilitar SSO** na página Login Único no Grid Manager permanece selecionada, e todas as configurações de SSO existentes são mantidas, a menos que você as atualize.

Passos

1. Efetue login em um nó de administração:
   a. Digite o seguinte comando: `ssh admin@Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`

d. Digite a senha listada no `Passwords.txt` arquivo.

   Quando você está logado como root, o prompt muda de `$` para `#` .

2. Execute o seguinte comando:`disable-saml`

   Uma mensagem indica que o comando se aplica somente a este nó de administração.

3. Confirme que você deseja desabilitar o SSO.

   Uma mensagem indica que o logon único está desabilitado no nó.

4. Em um navegador da Web, acesse o Grid Manager no mesmo nó de administração.

   A página de login do Grid Manager agora é exibida porque o SSO foi desabilitado.

5. Sign in com o nome de usuário root e a senha do usuário root local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração do SSO:
   a. Selecione **CONFIGURAÇÃO** > **Controle de acesso** > **Logon único**.
   b. Altere as configurações de SSO incorretas ou desatualizadas.
   c. Selecione **Salvar**.

      Selecionar **Salvar** na página Login Único reativa automaticamente o SSO para toda a grade.

7. Se você desativou o SSO temporariamente porque precisava acessar o Grid Manager por algum outro motivo:

   a. Execute qualquer tarefa ou tarefas que você precise executar.
   b. Selecione **Sair** e feche o Grid Manager.
   c. Reative o SSO no nó de administração. Você pode executar qualquer uma das seguintes etapas:

      - Execute o seguinte comando: `enable-saml`

        Uma mensagem indica que o comando se aplica somente a este nó de administração.

      Confirme que você deseja habilitar o SSO.

   Uma mensagem indica que o logon único está habilitado no nó.

      - Reinicie o nó da grade: `reboot`

8. Em um navegador da web, acesse o Grid Manager no mesmo nó de administração.
9. Confirme se a página de Sign in do StorageGRID aparece e se você deve inserir suas credenciais de SSO para acessar o Grid Manager.

Informações sobre direitos autorais

Informações sobre marcas comerciais