



Usando logon único (SSO) para StorageGRID

StorageGRID

NetApp
March 10, 2025

Índice

Usando logon único (SSO) para StorageGRID	1
Como o single sign-on funciona	1
Iniciar sessão quando o SSO está ativado	1
Terminar sessão quando o SSO está ativado	3
Requisitos para o uso de logon único	3
Requisitos do provedor de identidade	3
Requisitos de certificado do servidor	4
Configurando logon único	4
Confirmar que usuários federados podem entrar	5
Usando o modo sandbox	6
Criando confianças de parte confiáveis no AD FS	9
Testando confianças de parte de confiança	15
Ativar o início de sessão único	16
Desativação do logon único	17
Desativando e rehabilitando temporariamente o logon único para um nó de administração	18

Usando logon único (SSO) para StorageGRID

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0). Quando o SSO está ativado, todos os usuários devem ser autenticados por um provedor de identidade externo antes que possam acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade ou a API de Gerenciamento de Locatário. Os utilizadores locais não podem iniciar sessão no StorageGRID.

- ["Como o single sign-on funciona"](#)
- ["Requisitos para o uso de logon único"](#)
- ["Configurando logon único"](#)

Como o single sign-on funciona

Antes de ativar o SSO (logon único), verifique como os processos de login e logout do StorageGRID são afetados quando o SSO está ativado.

Iniciar sessão quando o SSO está ativado

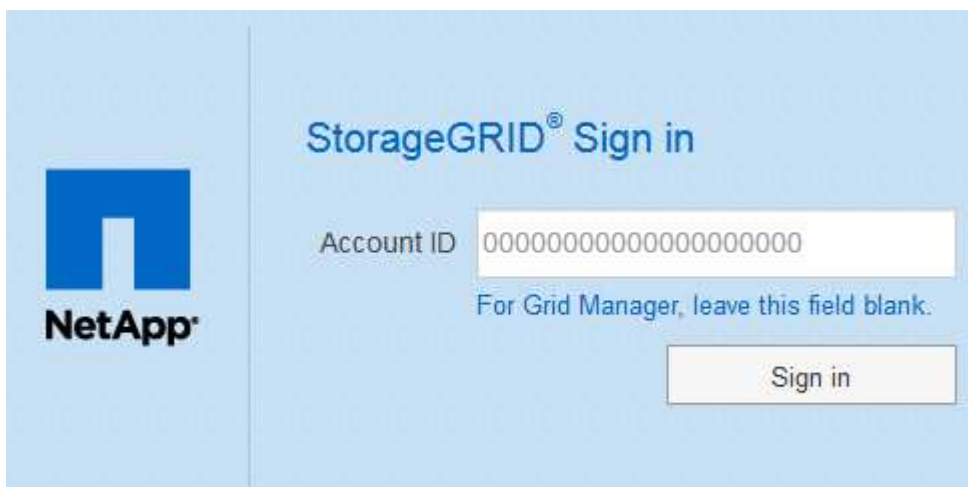
Quando o SSO está ativado e você entra no StorageGRID, você é redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

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

É apresentada a página de início de sessão do StorageGRID.

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



- Se você acessou anteriormente o Gerenciador de Grade ou o Gerente do Locatário, será solicitado que você selecione uma conta recente ou insira um ID de conta:

The image shows the StorageGRID Sign in interface. On the left is the NetApp logo. The main area has the title "StorageGRID® Sign in". Below the title, there is a "Recent" dropdown menu with "S3 tenant" selected. Below that is an "Account ID" text input field containing "27469746059057031822". A note below the field says "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.

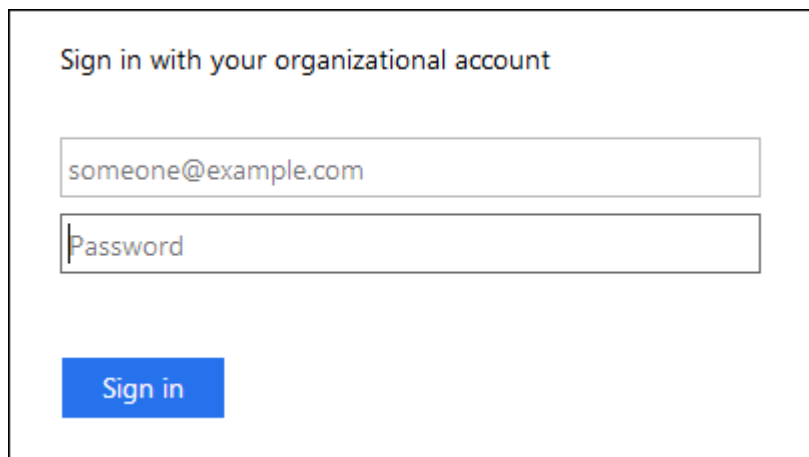
A página de login do StorageGRID não é exibida quando você insere o URL completo de uma conta de locatário (ou seja, um nome de domínio totalmente qualificado ou endereço IP seguido de `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO da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

2. Indique se deseja acessar o Gerenciador de Grade ou o Gerenciador de Locatário:

- Para acessar o Gerenciador de Grade, deixe o campo **ID de conta** em branco, digite **0** como ID de conta ou selecione **Gerenciador de Grade** se ele aparecer na lista de contas recentes.
- Para acessar o Gerenciador do Locatário, insira o ID da conta do locatário de 20 dígitos ou selecione um locatário pelo nome se ele aparecer na lista de contas recentes.

3. Clique em **entrar**

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

The image shows a sample SSO login form. It has the heading "Sign in with your organizational account". Below the heading are two input fields: the first contains "someone@example.com" and the second is labeled "Password". At the bottom left of the form is a blue "Sign in" button.

4. Faça login com suas credenciais SSO.

Se suas credenciais 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 que tenha permissão de acesso adequada, você será conectado ao Gerenciador de Grade ou ao Gerente do locatário, dependendo da

conta selecionada.

5. Opcionalmente, acesse outros nós de administração ou acesse o Gerenciador de grade ou o Gerenciador de locatário, se você tiver permissões adequadas.

Você não precisa reinserir suas credenciais SSO.

Terminar sessão quando o SSO está ativado

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

Passos

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

É apresentada a página de início de sessão do StorageGRID. A lista suspensa **Recent Accounts** (Contas recentes) é atualizada para incluir o **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 logado fora de...
Grid Manager em um ou mais nós de administração	Grid Manager em qualquer nó de administração	Grid Manager em todos os nós de administração
Gerenciador de locatários em um ou mais nós de administração	Gerente de locatário em qualquer nó de administrador	Gerenciador de locatários em todos os nós de administração
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Apenas o Grid Manager. Você também deve sair do Gerenciador do Locatário 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 para o uso de logon único

Antes de ativar o logon único (SSO) para um sistema StorageGRID, revise os requisitos nesta seção.



O logon único (SSO) não está disponível nas portas do Gerenciador de Grade restrito ou do Gerenciador de locatário. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Requisitos do provedor de identidade

O provedor de identidade (IDP) para SSO deve atender aos seguintes requisitos:

- Uma das seguintes versões do Active Directory Federation Service (AD FS):
 - AD FS 4,0, incluído no Windows Server 2016



O Windows Server 2016 deve estar usando o ["Atualização do KB3201845"](#), ou superior.

- AD FS 3,0, incluído na atualização do Windows Server 2012 R2 ou superior.
- Transport Layer Security (TLS) 1,2 ou 1,3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Requisitos de certificado do servidor

O StorageGRID usa um certificado de servidor de interface de gerenciamento em cada nó de administrador para proteger o acesso ao Gerenciador de grade, ao Gerenciador de locatário, à API de gerenciamento de grade e à API de gerenciamento de locatário. Quando você configura as confianças de parte confiáveis SSO para o StorageGRID no AD FS, você usa o certificado do servidor como o certificado de assinatura para solicitações do StorageGRID para o AD FS.

Se você ainda não tiver instalado um certificado de servidor personalizado para a interface de gerenciamento, você deve fazê-lo 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 dependentes do StorageGRID.



O uso do certificado de servidor padrão de um nó Admin na confiança de parte dependente do AD FS não é recomendado. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de poder iniciar sessão no nó recuperado, tem de atualizar a confiança da parte dependente no AD FS com o novo certificado.

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

Informações relacionadas

["Controlar o acesso através de firewalls"](#)

["Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"](#)

Configurando logon único

Quando o logon único (SSO) está ativado, os usuários só podem acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de gerenciamento de grade ou a API de gerenciamento de locatário se suas credenciais forem autorizadas usando o processo de login SSO implementado pela sua organização.

- ["Confirmar que usuários federados podem entrar"](#)
- ["Usando o modo sandbox"](#)
- ["Criando confianças de parte confiáveis no AD FS"](#)
- ["Testando confianças de parte de confiança"](#)

- ["Ativar o início de sessão único"](#)
- ["Desativação do logon único"](#)
- ["Desativando e rehabilitando temporariamente o logon único para um nó de administração"](#)

Confirmar que usuários federados podem entrar

Antes de ativar o logon único (SSO), você deve confirmar que pelo menos um usuário federado pode entrar no Gerenciador de Grade e entrar no Gerenciador de locatários para quaisquer contas de locatário existentes.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você está usando o Active Directory como fonte de identidade federada e o AD FS como provedor de identidade.

["Requisitos para o uso de logon único"](#)

Passos

1. Se houver contas de inquilino existentes, confirme que nenhum dos inquilinos está usando sua própria fonte de identidade.



Quando você ativa o SSO, uma fonte de identidade configurada no Gerenciador de locatário é substituída pela origem de identidade configurada no Gerenciador de Grade. Os usuários pertencentes à fonte de identidade do locatário não poderão mais entrar a menos que tenham uma conta com a fonte de identidade do Gerenciador de Grade.

- a. Inicie sessão no Gestor do Locatário para cada conta de inquilino.
 - b. Selecione **Access Control > Identity Federation**.
 - c. Confirme se a caixa de verificação **Ativar Federação de identidade** não está selecionada.
 - d. Se estiver, confirme se os grupos federados que possam estar em uso para essa conta de locatário não são mais necessários, desmarque a caixa de seleção e clique em **Salvar**.
2. Confirme se um usuário federado pode acessar o Gerenciador de Grade:
 - a. No Gerenciador de Grade, selecione **Configuração > Controle de Acesso > grupos de administradores**.
 - b. Certifique-se de que pelo menos um grupo federado tenha sido importado da origem de identidade do Active Directory e de que tenha sido atribuída a permissão de acesso raiz.
 - c. Terminar sessão.
 - d. Confirme que você pode fazer login novamente no Gerenciador de Grade como um usuário no grupo federado.
 3. Se houver contas de locatário existentes, confirme se um usuário federado que tenha permissão de acesso root pode entrar:
 - a. No Gerenciador de Grade, selecione **tenants**.
 - b. Selecione a conta de locatário e clique em **Editar conta**.

- c. Se a caixa de seleção **usa origem de identidade própria** estiver selecionada, desmarque a caixa e clique em **Salvar**.

Edit Tenant Account

Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional)

A página Contas do locatário é exibida.

- Selecione a conta de locatário, clique em **entrar** e faça login na conta de locatário como usuário raiz local.
- No Gerenciador do Locatário, clique em **Controle de Acesso > grupos**.
- Certifique-se de que pelo menos um grupo federado do Gerenciador de Grade recebeu a permissão de acesso raiz para esse locatário.
- Terminar sessão.
- Confirme que você pode fazer login novamente no locatário como um usuário no grupo federado.

Informações relacionadas

["Requisitos para o uso de logon único"](#)

["Gerenciando grupos de administradores"](#)

["Use uma conta de locatário"](#)

Usando o modo sandbox

Você pode usar o modo sandbox para configurar e testar as confianças de parte dependentes dos Serviços de Federação do Active Directory (AD FS) antes de aplicar o logon único (SSO) para usuários do StorageGRID. Depois que o SSO estiver ativado, você poderá reativar o modo sandbox para configurar ou testar novos e existentes trusts de terceiros. A reativação do modo sandbox desativa temporariamente o SSO para usuários do StorageGRID.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Quando o SSO está ativado e um usuário tenta entrar em um nó de administrador, o StorageGRID envia uma solicitação de autenticação para o AD FS. Por sua vez, o AD FS envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autorização foi bem-sucedida. Para solicitações bem-sucedidas, a resposta inclui um identificador universal exclusivo (UUID) para o usuário.

Para permitir que o StorageGRID (o provedor de serviços) e o AD FS (o provedor de identidade) se comuniquem com segurança sobre solicitações de autenticação de usuário, você deve configurar determinadas configurações no StorageGRID. Em seguida, você deve usar o AD FS para criar uma confiança de parte confiável para cada nó Admin. Finalmente, você deve retornar ao StorageGRID para ativar o SSO.

O modo Sandbox facilita a execução desta configuração de back-and-forth e testar todas as suas configurações antes de ativar o SSO.



O uso do modo sandbox é altamente recomendado, mas não é estritamente necessário. Se você estiver preparado para criar confianças de parte dependentes do AD FS imediatamente após configurar o SSO no StorageGRID e não precisar testar os processos de SSO e logout único (SLO) para cada nó de administrador, clique em **habilitado**, insira as configurações do StorageGRID, crie uma confiança de parte confiável para cada nó de administrador no AD FS e clique em **Salvar** para ativar o SSO.

Passos

1. Selecione **Configuração > Controle de Acesso > Início de sessão único**.

A página Single Sign-On (Início de sessão único) é exibida, com a opção **Disabled** selecionada.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Save



Se as opções de Status SSO não forem exibidas, confirme se você configurou o ative Directory como a origem de identidade federada. Consulte ""requisitos para utilizar o início de sessão único.""

2. Selecione a opção **Sandbox Mode**.

As configurações Provedor de identidade e parte dependente aparecem. Na seção Provedor de identidade, o campo **tipo de serviço** é somente leitura. Ele mostra o tipo de serviço de federação de identidade que você está usando (por exemplo, ative Directory).

3. Na seção Provedor de identidade:

- a. Insira o nome do Serviço de Federação, exatamente como aparece no AD FS.



Para localizar o Nome do Serviço de Federação, vá para Windows Server Manager. Selecione **Ferramentas > Gerenciamento do AD FS**. No menu Ação, selecione **Editar Propriedades do Serviço de Federação**. O Nome do Serviço de Federação é apresentado no segundo campo.

b. Especifique se deseja usar a Segurança da camada de Transporte (TLS) para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta a solicitações StorageGRID.

- **Use o 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 essa configuração, copie e cole o certificado na caixa de texto **certificado CA**.

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

4. Na seção parte dependente, especifique o identificador de parte dependente que você usará para nós de administrador do StorageGRID quando você configurar confianças de parte dependentes.

- Por exemplo, se sua grade tiver apenas um nó Admin e você não antecipar a adição de mais nós Admin no futuro, digite `SG` ou `StorageGRID`.
- Se sua grade incluir mais de um nó Admin, inclua a cadeia `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que inclui um identificador de parte confiável para cada nó Admin, com base no nome do host do nó. Observação: Você deve criar uma confiança de parte confiável para cada nó de administrador em seu sistema StorageGRID. Ter uma confiança de parte confiável para cada nó de administração garante que os usuários possam entrar e sair com segurança de qualquer nó de administração.

5. Clique em **Salvar**.

- Uma marca de verificação verde aparece no botão **Save** durante alguns segundos.



- O aviso de confirmação do modo Sandbox aparece, confirmando que o modo sandbox está agora ativado. Você pode usar esse modo enquanto usa o AD FS para configurar uma confiança de parte confiável para cada nó Admin e testar os processos de login único (SSO) e logout único (SLO).

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

Informações relacionadas

["Requisitos para o uso de logon único"](#)

Criando confianças de parte confiáveis no AD FS

Você deve usar os Serviços de Federação do Active Directory (AD FS) para criar uma confiança de parte confiável para cada nó de administração em seu sistema. Você pode criar trusts confiáveis de parte usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Criando uma confiança de parte confiável usando o Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais trusts de parte confiáveis.

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.



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

- Você tem experiência em criar confiança de parte confiável 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.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver

usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No menu Iniciar do Windows, clique com o botão direito do Mouse no 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_Identifer*, insira o Identificador de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão único. Por exemplo, SG-DC1-ADM1.
- Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

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 > confiar em parts**.

É apresentada a lista de confianças de partes dependentes.

5. Adicione uma Política de Controle de Acesso à confiança da entidade dependente recém-criada:

- a. Localize a confiança de quem confia que você acabou de criar.
- b. Clique com o botão direito do rato na fidedignidade e selecione **Editar política de controle de acesso**.
- c. Selecione uma política de controlo de acesso.
- d. Clique em **Apply** e clique em **OK**

6. Adicione uma Política de emissão de reclamação à recém-criada confiança da parte dependente:

- a. Localize a confiança de quem confia que você acabou de criar.
- b. Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.
- c. Clique em **Adicionar regra**.
- d. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.
- e. Na página Configurar regra, insira um nome de exibição para essa regra.

Por exemplo, **ObjectGUID to Name ID**.

- f. Para o Attribute Store, selecione **ative Directory**.
- g. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
- h. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
- i. Clique em **Finish** e clique em **OK**.

7. Confirme se os metadados foram importados com sucesso.
 - a. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.
 - b. Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** estão preenchidos.

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

8. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.
9. Quando terminar, regresse ao StorageGRID e "[teste todos os trusts de confiança](#)" confirme que estão configurados corretamente.

Criando uma confiança de parte confiável importando metadados de federação

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

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.



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

- Você tem experiência em criar confiança de parte confiável 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.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No Gerenciador do Windows Server, clique em **Ferramentas** e selecione **Gerenciamento do AD FS**.
2. Em ações, clique em **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e clique em **Iniciar**.
4. Selecione **Importar dados sobre a parte dependente publicada on-line ou em uma rede local**.
5. Em **Endereço de metadados de 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*, introduza o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

6. Conclua o assistente confiar na parte confiável, salve a confiança da parte confiável e feche o assistente.



Ao inserir o nome de exibição, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. Por exemplo, SG-DC1-ADM1.

7. Adicionar uma regra de reclamação:

- Clique com o botão direito do rato na confiança e selecione **Editar política de emissão de reclamação**.
- Clique em **Adicionar regra**:
- Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.
- Na página Configurar regra, insira um nome de exibição para essa regra.

Por exemplo, **ObjectGUID to Name ID**.

- Para o Attribute Store, selecione **ative Directory**.
- Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
- Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
- Clique em **Finish** e clique em **OK**.

8. Confirme se os metadados foram importados com sucesso.

- Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.
- Confirme se os campos nas guias **Endpoints**, **Identificadores** e **assinatura** estão preenchidos.

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

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

10. Quando terminar, regresse ao StorageGRID e "[teste todos os trusts de confiança](#)" confirme que estão configurados corretamente.

Criando uma confiança de parte confiável manualmente

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

O que você vai precisar

- Você configurou o SSO no StorageGRID e sabe o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de parte confiável para cada nó de administrador no seu sistema.



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

- Você tem o certificado personalizado que foi carregado para a interface de gerenciamento do

StorageGRID ou sabe como fazer login em um nó de administrador a partir do shell de comando.

- Você tem experiência em criar confiança de parte confiável 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.

Sobre esta tarefa

Estas instruções aplicam-se ao AD FS 4,0, que está incluído no Windows Server 2016. Se você estiver usando o AD FS 3,0, que está incluído no Windows 2012 R2, você notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se tiver dúvidas.

Passos

1. No Gerenciador do Windows Server, clique em **Ferramentas** e selecione **Gerenciamento do AD FS**.
2. Em ações, clique em **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e clique em **Iniciar**.
4. Selecione **Digite os dados sobre a parte confiável manualmente** e clique em **Avançar**.
5. Conclua o assistente confiança da parte dependente:

- a. Introduza um nome de apresentação para este nó de administração.

Para obter consistência, use o Identificador de parte confiável para o nó Admin, exatamente como ele aparece na página de logon único no Gerenciador de Grade. 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 o URL do endpoint do serviço SAML para o nó Admin:

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

Para *Admin_Node_FQDN*, introduza o nome de domínio totalmente qualificado para o nó Admin. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que você deve atualizar ou recriar essa confiança de parte confiável se esse endereço IP mudar alguma vez.)

- e. Na página Configurar Identificadores, especifique o Identificador da parte de dependência para o mesmo nó de administração:

```
Admin_Node_Identifier
```

Para *Admin_Node_Identifier*, insira o Identificador de parte dependente para o nó Admin, exatamente como aparece na página Início de sessão 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 reclamação é exibida.



Se a caixa de diálogo não for exibida, clique com o botão direito do Mouse no Trust e selecione **Editar política de emissão de reclamação**.

6. Para iniciar o assistente de regra de reclamação, clique em **Adicionar regra**:

- a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e clique em **Avançar**.
- b. Na página Configurar regra, insira um nome de exibição para essa regra.

Por exemplo, **ObjectGUID to Name ID**.

- c. Para o Attribute Store, selecione **active Directory**.
 - d. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
 - e. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
 - f. Clique em **Finish** e clique em **OK**.
7. Clique com o botão direito do rato na confiança da parte dependente para abrir as suas propriedades.
 8. Na guia **Endpoints**, configure o endpoint para logout único (SLO):

- a. Clique em **Add SAML**.
- b. Selecione **Endpoint Type > SAML Logout**.
- c. Selecione **Binding > Redirect**.
- d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste nó Admin:

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

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

- a. Clique em **OK**.
9. Na guia **assinatura**, especifique o certificado de assinatura para essa confiança de parte confiável:
 - a. Adicione o certificado personalizado:
 - Se tiver o certificado de gestão personalizado que carregou no StorageGRID, selecione esse certificado.
 - Se você não tiver o certificado personalizado, faça login no Admin Node, vá para `/var/local/mgmt-api` o diretório do Admin Node e adicione o `custom-server.crt` arquivo de certificado.

Observação: usando o certificado padrão do Admin Node (`server.crt`) não é recomendado. Se o nó Admin falhar, o certificado padrão será regenerado quando você recuperar o nó e você precisará atualizar a confiança da parte confiável.
 - b. Clique em **Apply** e clique em **OK**.

As propriedades da parte dependente são salvas e fechadas.

10. Repita essas etapas para configurar uma confiança de parte confiável para todos os nós de administração no sistema StorageGRID.
11. Quando terminar, regresse ao StorageGRID e "**teste todos os trusts de confiança**" confirme que estão configurados corretamente.

Testando confianças de parte de confiança

Antes de aplicar o uso de logon único (SSO) para StorageGRID, confirme se o logon único e o logout único (SLO) estão configurados corretamente. Se você criou uma confiança de parte confiável para cada nó Admin, confirme que você pode usar SSO e SLO para cada nó Admin.

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você configurou uma ou mais confianças de parte confiáveis no AD FS.

Passos

1. Selecione **Configuração > Controle de Acesso > Início de sessão único**.

A página Single Sign-On (Início de sessão único) é exibida, com a opção **Sandbox Mode** selecionada.

2. Nas instruções para o modo sandbox, localize o link para a página de logon do provedor de identidade.

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

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. Clique no link ou copie e cole o URL em um navegador para acessar a página de logon do provedor de identidade.
4. Para confirmar que você pode usar o SSO para entrar no StorageGRID, selecione **entrar em um dos seguintes sites**, selecione o identificador de parte confiável para seu nó de administrador principal e clique em **entrar**.

You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

Você é solicitado a digitar seu nome de usuário e senha.

5. Introduza o seu nome de utilizador federado e a palavra-passe.
 - Se as operações de login e logout 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, será exibida uma mensagem de erro. Corrija o problema, limpe os cookies do navegador e tente novamente.
6. Repita as etapas anteriores para confirmar que você pode entrar em qualquer outro nó Admin.

Se todas as operações de login e logout SSO forem bem-sucedidas, você estará pronto para ativar o SSO.

Ativar o início de sessão único

Depois de usar o modo sandbox para testar todas as suas trusts de terceiros dependentes do StorageGRID, você está pronto para ativar o logon único (SSO).

O que você vai precisar

- Você deve ter importado pelo menos um grupo federado da origem da identidade e atribuído permissões de gerenciamento de acesso raiz ao grupo. Você deve confirmar que pelo menos um usuário federado tem permissão de acesso root ao Gerenciador de Grade e ao Gerente do locatário para quaisquer contas de locatário existentes.
- Você deve ter testado todas as confianças de parte que dependem usando o modo sandbox.

Passos

1. Selecione **Configuração > Controle de Acesso > Início de sessão único**.

A página Single Sign-On (Início de sessão único) aparece com **Sandbox Mode** selecionado.

2. Altere o Status SSO para **Enabled**.
3. Clique em **Salvar**.

É apresentada uma mensagem de aviso.

Warning

Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Reveja o aviso e clique em **OK**.

O início de sessão único está agora ativado.



Todos os usuários devem usar o SSO para acessar o Gerenciador de Grade, o Gerenciador de Tenant, a API de gerenciamento de grade e a API de gerenciamento de locatário. Os usuários locais não podem mais acessar o StorageGRID.

Desativação do logon único

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

O que você vai precisar

- Você deve estar conectado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

Passos

1. Selecione **Configuração > Controle de Acesso > Início de sessão único**.

É apresentada a página Single Sign-on (Início de sessão único).

2. Selecione a opção **Disabled** (Desativado).
3. Clique em **Salvar**.

É apresentada uma mensagem de aviso indicando que os utilizadores locais poderão iniciar sessão.

Warning

Disable single sign-on

After you disable SSO or switch to sandbox mode, local users will be able to sign in. Are you sure you want to proceed?

Cancel

OK

4. Clique em **OK**.

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

Desativando e rehabilitando temporariamente o logon único para um nó de administração

Talvez você não consiga entrar no Gerenciador de Grade se o sistema de logon único (SSO) estiver inativo. Nesse caso, você pode desativar e reativar temporariamente o SSO para um nó de administrador. Para desativar e reativar o SSO, você deve acessar o shell de comando do nó.

O que você vai precisar

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber a senha para o usuário raiz local.

Sobre esta tarefa

Depois de desativar o SSO para um nó Admin, você pode entrar no Gerenciador de Grade como o usuário raiz local. Para proteger seu sistema StorageGRID, você deve usar o shell de comando do nó para reativar o SSO no nó Admin assim que você sair.



A desativação do SSO para um nó Admin não afeta as configurações de SSO para quaisquer outros nós Admin na grade. A caixa de seleção **Ativar SSO** na página de logon único no Gerenciador de Grade permanece selecionada e todas as configurações SSO existentes são mantidas, a menos que você as atualize.

Passos

1. Faça login em um nó Admin:
 - a. Introduza o seguinte comando: `ssh admin@Admin_Node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

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

Uma mensagem indica que o comando se aplica somente a esse nó Admin.

3. Confirme que você deseja desativar o SSO.

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

4. Em um navegador da Web, acesse o Gerenciador de Grade no mesmo nó Admin.

A página de login do Gerenciador de Grade agora é exibida porque o SSO foi desativado.

5. Inicie sessão com a raiz do nome de utilizador e a palavra-passe do utilizador raiz local.

6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração SSO:

- a. Selecione **Configuração > Controle de Acesso > Início de sessão único**.
- b. Altere as configurações de SSO incorretas ou desatualizadas.
- c. Clique em **Salvar**.

Clicar em **Salvar** na página de logon único reativa automaticamente o SSO para toda a grade.

7. Se você desativou o SSO temporariamente porque precisava acessar o Gerenciador de Grade por algum outro motivo:

- a. Execute qualquer tarefa ou tarefas que você precisa executar.
- b. Clique em **Sair** e feche o Gerenciador de Grade.
- c. Reative o SSO no nó Admin. Você pode executar uma das seguintes etapas:

- Execute o seguinte comando: `enable-saml`

Uma mensagem indica que o comando se aplica somente a esse nó Admin.

Confirme se você deseja ativar o SSO.

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

- Reinicie o nó da grade: `reboot`

8. A partir de um navegador da Web, acesse o Gerenciador de Grade a partir do mesmo nó Admin.

9. Confirme se a página de login do StorageGRID é exibida e que você deve inserir suas credenciais SSO para acessar o Gerenciador de Grade.

Informações relacionadas

["Configurando logon único"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.