Administrar um sistema StorageGRID

StorageGRID

NetApp
October 03, 2025

Índice

Administrar um sistema StorageGRID

Use estas instruções para configurar e administrar um sistema StorageGRID.

Essas instruções descrevem como usar o Gerenciador de Grade para configurar grupos e usuários, criar contas de locatário para permitir que aplicativos clientes S3 e Swift armazenem e recuperem objetos, configurem e gerenciem redes StorageGRID, configurem AutoSupport, gerenciem configurações de nó e muito mais.

> As instruções para gerenciar objetos com regras e políticas de gerenciamento de ciclo de vida das informações (ILM) foram movidas para "Gerenciar objetos com ILM"o .

Estas instruções destinam-se ao pessoal técnico que irá configurar, administrar e dar suporte a um sistema StorageGRID depois de instalado.

O que você vai precisar

- Você tem uma compreensão geral do sistema StorageGRID.
- Você tem conhecimento bastante detalhado de shells de comando do Linux, rede e configuração e configuração de hardware do servidor.

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Você deve definir a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Iniciar sessão no Grid Manager

Você acessa a página de login do Gerenciador de Grade inserindo o nome de domínio totalmente qualificado (FQDN) ou o endereço IP de um nó Admin na barra de endereços de um navegador da Web compatível.

O que você vai precisar

- Tem de ter as suas credenciais de início de sessão.
- Você deve ter o URL para o Gerenciador de Grade.
- Você deve estar usando um navegador da Web compatível.
- Os cookies devem estar ativados no seu navegador.
- Você deve ter permissões de acesso específicas.

Sobre esta tarefa

Cada sistema StorageGRID inclui um nó de administração principal e qualquer número de nós de administração não primários. Você pode entrar no Gerenciador de Grade em qualquer nó de administrador para gerenciar o sistema StorageGRID. No entanto, os nós de administração não são exatamente os mesmos:

- Reconhecimentos de alarmes (sistema legado) feitos em um nó Admin não são copiados para outros nós Admin. Por esse motivo, as informações exibidas para alarmes podem não ter a mesma aparência em cada nó de administração.
- Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

Se os nós de administração estiverem incluídos em um grupo de alta disponibilidade (HA), você se conetará usando o endereço IP virtual do grupo de HA ou um nome de domínio totalmente qualificado que mapeia para o endereço IP virtual. O nó de administração principal deve ser selecionado como o principal preferido do grupo, de modo que, quando você acessa o Gerenciador de grade, você o acessa no nó de administração principal, a menos que o nó de administração principal não esteja disponível.

Passos

1. Inicie um navegador da Web compatível.
2. Na barra de endereços do navegador, insira o URL do Gerenciador de Grade:

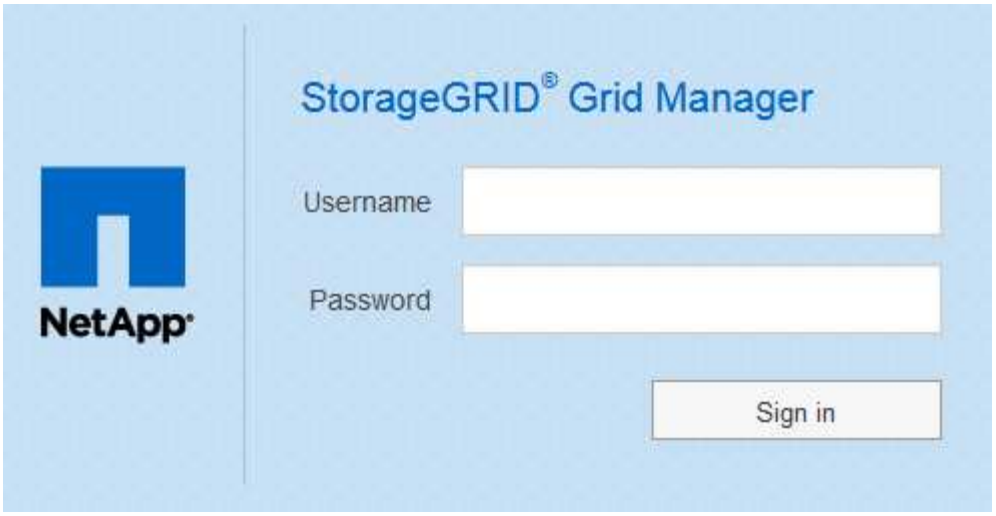
   `https://FQDN_or_Admin_Node_IP/`

   ```
   `_FQDN_or_Admin_Node_IP_`Onde está um nome de domínio totalmente
   qualificado ou o endereço IP de um nó Admin ou o endereço IP virtual de
   um grupo de HA de nós Admin.
   ```

   Se você precisar acessar o Gerenciador de Grade em uma porta diferente da porta padrão para HTTPS (443), digite o seguinte, onde *FQDN_or_Admin_Node_IP* é um nome de domínio totalmente qualificado ou endereço IP, e a porta é o número da porta:

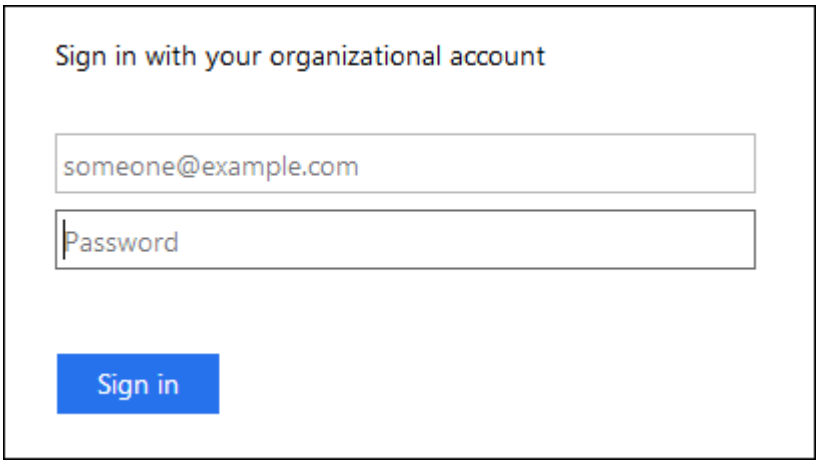
   `https://FQDN_or_Admin_Node_IP:port/`

3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Entre no Gerenciador de Grade:
   - Se o logon único (SSO) não estiver sendo usado para seu sistema StorageGRID:
     i. Insira seu nome de usuário e senha para o Gerenciador de Grade.
     ii. Clique em **entrar**.



- Se o SSO estiver ativado para o seu sistema StorageGRID e esta é a primeira vez que você acessou o URL neste navegador:
  i. Clique em **entrar**. Você pode deixar o campo ID da conta em branco.

  ii. Insira suas credenciais SSO padrão na página de login SSO da sua organização. Por exemplo:

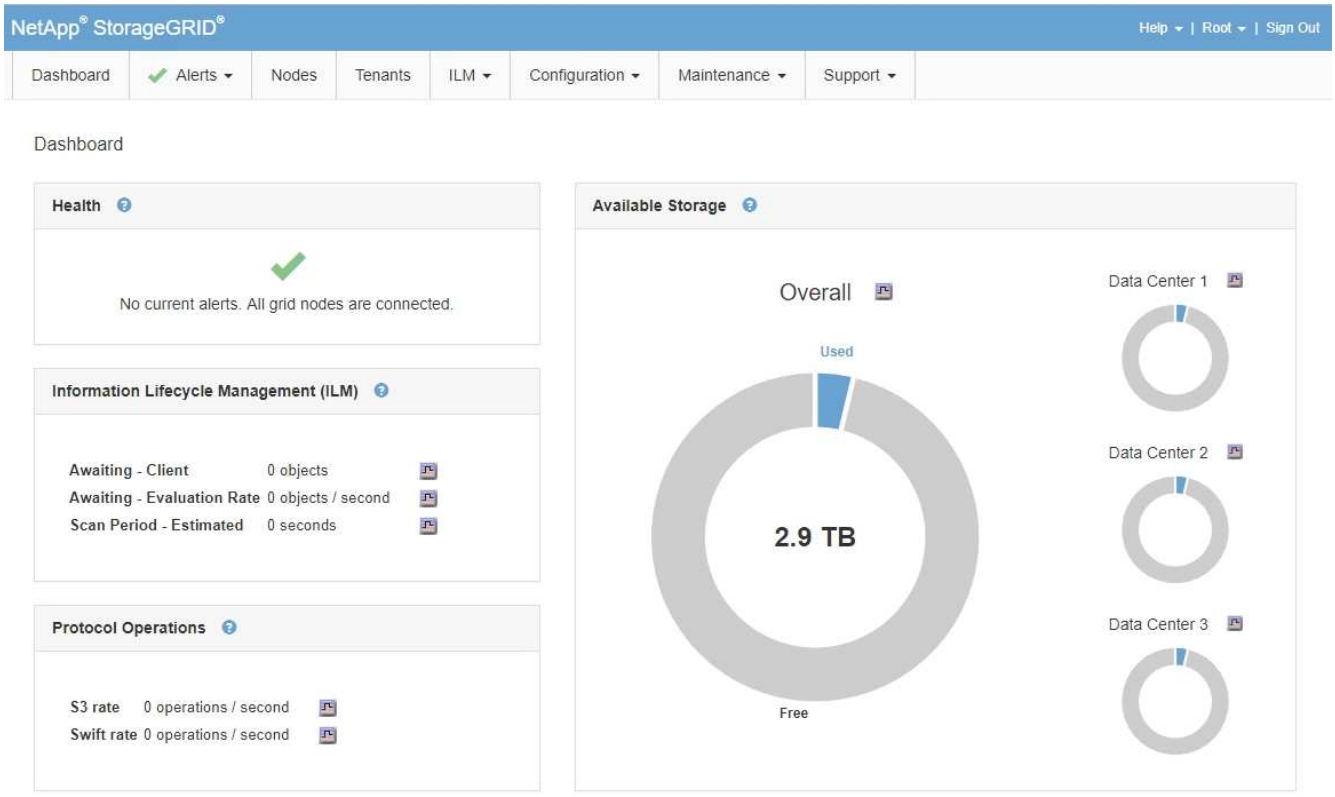


- Se o SSO estiver ativado para o seu sistema StorageGRID e você tiver acessado anteriormente o Gerenciador de Grade ou uma conta de locatário:

i. Faça um dos seguintes procedimentos:

- Digite **0** (o ID da conta do Gerenciador de Grade) e clique em **entrar**.
- Selecione **Gerenciador de Grade** se aparecer na lista de contas recentes e clique em **entrar**.

ii. Inicie sessão com as suas credenciais SSO padrão na página de início de sessão SSO da sua organização. Quando você estiver conetado, a página inicial do Gerenciador de Grade será exibida, que inclui o Painel de Controle. Para saber quais informações são fornecidas, consulte ""visualizando o Painel"" nas instruções para monitoramento e solução de problemas do StorageGRID.



5. Se você quiser entrar em outro nó de administração:

Opção	Passos
SSO não ativado	a. Na barra de endereços do navegador, insira o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração. Inclua o número da porta conforme necessário. b. Insira seu nome de usuário e senha para o Gerenciador de Grade. c. Clique em **entrar**.
SSO ativado	Na barra de endereços do navegador, insira o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração. Se você tiver feito login em um nó de administrador, poderá acessar outros nós de administrador sem ter que fazer login novamente. No entanto, se sua sessão SSO expirar, você será solicitado a fornecer suas credenciais novamente. **Observação:** SSO não está disponível na porta do Gerenciador de Grade restrito. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com logon único.

Informações relacionadas

"Requisitos do navegador da Web"

"Controlar o acesso através de firewalls"

"Configurando certificados de servidor"

"Configurando logon único"

"Gerenciando grupos de administradores"

"Gerenciamento de grupos de alta disponibilidade"

"Use uma conta de locatário"

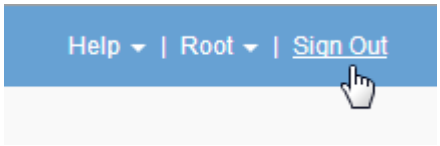
"Monitorizar Resolução de problemas"

Sair do Gerenciador de Grade

Quando terminar de trabalhar com o Gerenciador de Grade, você deve sair para garantir que usuários não autorizados não possam acessar o sistema StorageGRID. Fechar seu navegador pode não sair do sistema, com base nas configurações de cookies do navegador.

Passos

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



2. Clique em **Sair**.

Opção	Descrição
SSO não em uso	Você está desconetado do Admin Node. A página de login do Gerenciador de Grade é exibida. **Nota:** se você tiver feito login em mais de um nó Admin, você deve sair de cada nó.
SSO ativado	Você está desconetado de todos os nós de administrador que estava acessando. É apresentada a página de início de sessão do StorageGRID. **Grid Manager** está listado como padrão no menu suspenso **Recent Accounts** e o campo **Account ID** mostra 0. **Observação:** se o SSO estiver ativado e você também estiver conetado ao Gerenciador do Locatário, você também deverá sair da conta do locatário para sair do SSO.

Informações relacionadas

"Configurando logon único"

"Use uma conta de locatário"

Alterar a sua palavra-passe

Se você é um usuário local do Gerenciador de Grade, você pode alterar sua própria senha.

O que você vai precisar

Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Se você entrar no StorageGRID como um usuário federado ou se o logon único (SSO) estiver ativado, não será possível alterar sua senha no Gerenciador de Grade. Em vez disso, você deve alterar sua senha na fonte de identidade externa, por exemplo, ative Directory ou OpenLDAP.

Passos

1. No cabeçalho do Gerenciador de Grade, selecione ***your name*** **> alterar senha**.

2. Introduza a sua palavra-passe atual.
3. Introduza uma nova palavra-passe.

   Sua senha deve conter pelo menos 8 e não mais de 32 carateres. As senhas diferenciam maiúsculas de minúsculas.

4. Volte a introduzir a nova palavra-passe.
5. Clique em **Salvar**.

Alterando a senha de provisionamento

Use este procedimento para alterar a senha de provisionamento do StorageGRID. A frase-passe é necessária para procedimentos de recuperação, expansão e manutenção. A frase-passe também é necessária para fazer o download dos backups do pacote de recuperação que incluem as informações de topologia de grade e as chaves de criptografia para o sistema StorageGRID.

O que você vai precisar

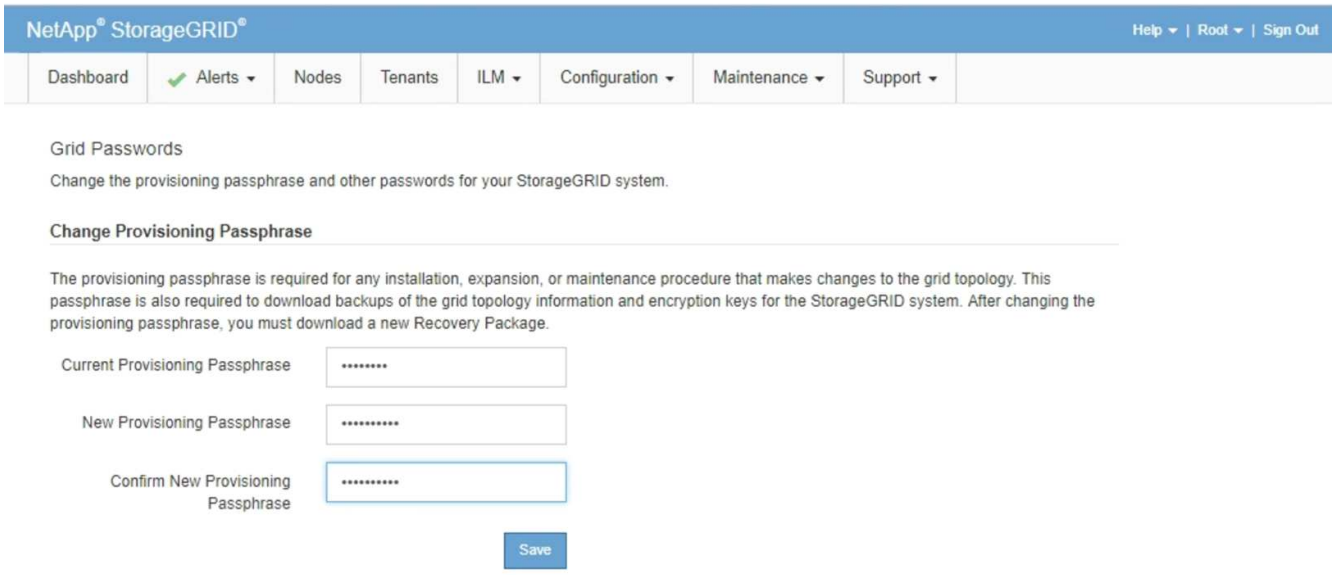
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento atual.

Sobre esta tarefa

A frase-passe de aprovisionamento é necessária para muitos procedimentos de instalação e manutenção e para transferir o pacote de recuperação. A senha de provisionamento não está listada no `Passwords.txt` arquivo. Certifique-se de documentar a senha de provisionamento e mantê-la em um local seguro e seguro.

Passos

1. Selecione **Configuração** > **Controle de Acesso** > **senhas de Grade**.



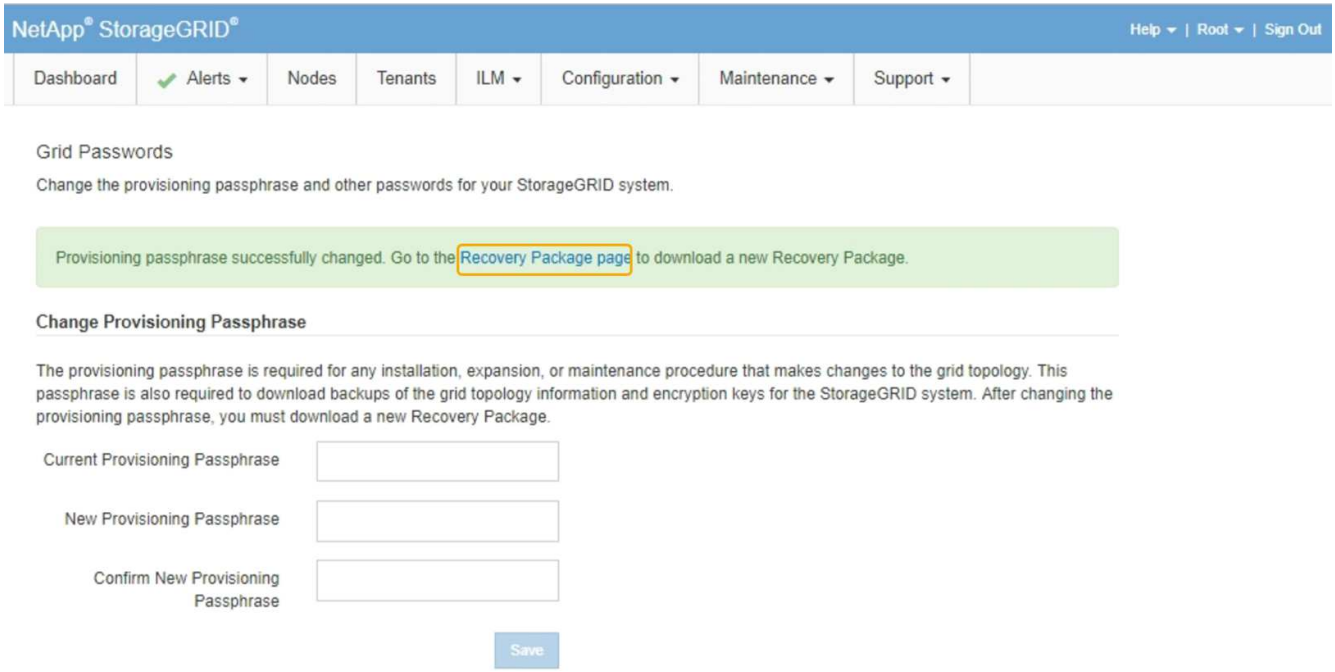
2. Introduza a sua frase-passe de aprovisionamento atual.

3. Introduza a nova frase-passe.a frase-passe tem de conter, no mínimo, 8 e não mais de 32 carateres. As senhas são sensíveis a maiúsculas e minúsculas.

> Armazene a nova senha de provisionamento em um local seguro. É necessário para procedimentos de instalação, expansão e manutenção.

4. Digite novamente a nova senha e clique em **Salvar**.

   O sistema exibe um banner verde de sucesso quando a alteração da senha de provisionamento estiver concluída. A mudança deve levar menos de um minuto.



5. Selecione o link **Pacote de recuperação** dentro do banner de sucesso.
6. Faça o download do novo Pacote de recuperação do Gerenciador de Grade. Selecione **Maintenance** > **Recovery Package** e insira a nova senha de provisionamento.

> Depois de alterar a senha de provisionamento, você deve baixar imediatamente um novo Pacote de recuperação. O arquivo do Pacote de recuperação permite restaurar o sistema se ocorrer uma falha.

Alterar o tempo limite da sessão do navegador

Você pode controlar se os usuários do Grid Manager e do Tenant Manager estão desconetados se estiverem inativos por mais de um determinado período de tempo.

O que você vai precisar

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

Sobre esta tarefa

O tempo limite de inatividade da GUI é predefinido para 900 segundos (15 minutos). Se a sessão do

navegador de um usuário não estiver ativa por esse período de tempo, a sessão expirará.

Conforme necessário, você pode aumentar ou diminuir o período de tempo limite definindo a opção de exibição tempo limite de inatividade da GUI.

Se o logon único (SSO) estiver ativado e a sessão do navegador do usuário expirar, o sistema se comportará como se o usuário clicasse em **Sair** manualmente. O usuário deve reinserir suas credenciais SSO para acessar o StorageGRID novamente.

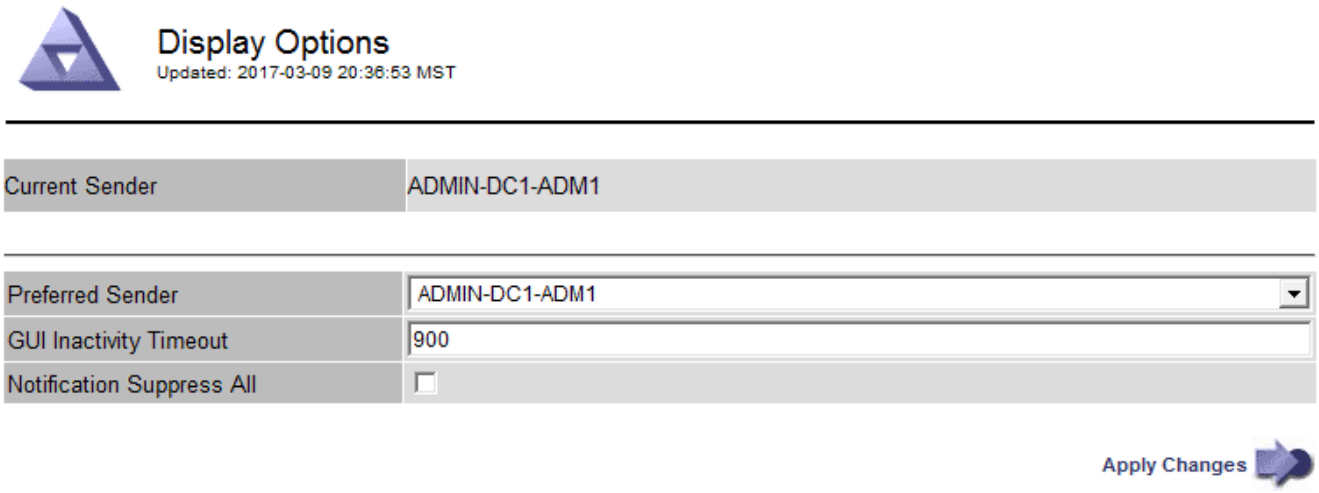
O tempo limite da sessão do usuário também pode ser controlado pelo seguinte:

- Um temporizador StorageGRID separado, não configurável, incluído para a segurança do sistema. Por padrão, o token de autenticação de cada usuário expira 16 horas após o login do usuário. Quando a autenticação de um usuário expira, esse usuário é automaticamente desconetado, mesmo que o valor do tempo limite de inatividade da GUI não tenha sido atingido. Para renovar o token, o usuário deve entrar novamente.
- Configurações de tempo limite para o provedor de identidade, supondo que o SSO esteja habilitado para o StorageGRID.

Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**.
2. Para **tempo limite de inatividade da GUI**, insira um período de tempo limite de 60 segundos ou mais.

   Defina este campo como 0 se não pretender utilizar esta funcionalidade. Os usuários são desconetados 16 horas após o início de sessão, quando seus tokens de autenticação expiram.



3. Clique em **aplicar alterações**.

   A nova configuração não afeta os usuários conetados atualmente. Os usuários devem entrar novamente ou atualizar seus navegadores para que a nova configuração de tempo limite entre em vigor.

Informações relacionadas

"Como o single sign-on funciona"

"Use uma conta de locatário"

Visualizar informações de licença do StorageGRID

Você pode visualizar as informações de licença do seu sistema StorageGRID, como a capacidade máxima de armazenamento da grade, sempre que necessário.

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

Sobre esta tarefa

Se houver um problema com a licença de software para este sistema StorageGRID, o painel Saúde no Painel inclui um ícone de Status da Licença e um link **Licença**. O número indica quantos problemas relacionados à licença existem.

Passo

Para visualizar a licença, execute um dos seguintes procedimentos:

- No painel Saúde do Painel, clique no ícone Status da Licença ou no link **Licença**. Este link aparece somente se houver um problema com a licença.
- Selecione **Manutenção** > **sistema** > **Licença**.

A Página de Licença é exibida e fornece as seguintes informações somente de leitura sobre a licença atual:

- ID do sistema StorageGRID, que é o número de identificação exclusivo para esta instalação do StorageGRID
- Número de série da licença
- Capacidade de armazenamento licenciada da rede
- Data de término da licença de software
- Data de término do contrato de serviço de suporte
- Conteúdo do arquivo de texto da licença

> Para as licenças emitidas antes do StorageGRID 10,3, a capacidade de armazenamento licenciada não está incluída no ficheiro de licença e é apresentada uma mensagem "consulte o Contrato de licença" em vez de um valor.

Atualizando informações de licença do StorageGRID

Você deve atualizar as informações de licença do seu sistema StorageGRID a qualquer momento que os termos de sua licença mudarem. Por exemplo, você deve atualizar as informações da licença se adquirir capacidade de armazenamento adicional para sua grade.

O que você vai precisar

- Você deve ter um novo arquivo de licença para aplicar ao seu sistema StorageGRID.
- Você deve ter permissões de acesso específicas.
- Você deve ter a senha de provisionamento.

Passos

1. Selecione **Manutenção** > **sistema** > **Licença**.
2. Introduza a frase-passe de aprovisionamento do seu sistema StorageGRID na caixa de texto **frase-passe de aprovisionamento**.
3. Clique em **Procurar**.
4. Na caixa de diálogo abrir, localize e selecione o novo arquivo de licença (`.txt`) e clique em **abrir**.

   O novo ficheiro de licença é validado e apresentado.

5. Clique em **Salvar**.

Usando a API de gerenciamento de grade

Você pode executar tarefas de gerenciamento do sistema usando a API REST do Grid Management em vez da interface de usuário do Grid Manager. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários, mais rapidamente.

A API de gerenciamento de grade usa a plataforma de API de código aberto Swagger. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores realizem operações em tempo real no StorageGRID com a API.

Recursos de nível superior

A API de gerenciamento de grade fornece os seguintes recursos de nível superior:

- `/grid`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, consulte as informações sobre como usar contas de locatário.
- `/private`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas. Essas APIs são destinadas apenas para uso interno e não são documentadas publicamente. Essas APIs também estão sujeitas a alterações sem aviso prévio.

Informações relacionadas

"Use uma conta de locatário"

"Prometheus: Noções básicas de consulta"

Operações da API Grid Management

A API Grid Management organiza as operações de API disponíveis nas seções a seguir.

- * Contas* — operações para gerenciar contas de inquilinos de armazenamento, incluindo a criação de novas contas e recuperação de uso de armazenamento para uma determinada conta.
- **Alarms** — operações para listar alarmes atuais (sistema legado) e retornar informações sobre a integridade da grade, incluindo os alertas atuais e um resumo dos estados de conexão do nó.
- **Alert-history** — operações em alertas resolvidos.
- **Alert-receivers** — operações em recetores de notificação de alerta (e-mail).
- **Alert-rules** — operações em regras de alerta.
- **Alert-silences** — operações em silêncios de alerta.
- **Alertas** — operações em alertas.
- **Audit** — operações para listar e atualizar a configuração da auditoria.
- **Auth** — operações para realizar autenticação de sessão do usuário.

  A API de gerenciamento de grade suporta o esquema de autenticação de token do portador. Para fazer login, você fornece um nome de usuário e senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com êxito, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("autorização: Portador *token*").

  > Se o logon único estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte "'autenticar na API se o logon único estiver ativado.'"

  Consulte ""proteção contra falsificação de solicitação entre sites"" para obter informações sobre como melhorar a segurança de autenticação.

- **Certificados de cliente** — operações para configurar certificados de cliente para que o StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **Config** — operações relacionadas à versão do produto e versões da API Grid Management. Você pode listar a versão de lançamento do produto e as principais versões da API de Gerenciamento de Grade suportadas por essa versão, e você pode desativar versões obsoletas da API.
- **Disabled-features** — operações para visualizar recursos que podem ter sido desativados.
- **dns-serviders** — operações para listar e alterar servidores DNS externos configurados.
- **Endpoint-domain-nanos** — operações para listar e alterar nomes de domínio de endpoint.
- **Codificação de apagamento** — operações em perfis de codificação de apagamento.
- **Expansão** — operações de expansão (nível de procedimento).
- **Expansion-nonos** — operações em expansão (nível de nó).
- **Expansão-sites** — operações em expansão (nível do site).
- **Grid-networks** — operações para listar e alterar a Grid Network List.

- * Grid-passwords* — operações para gerenciamento de senhas de grade.
- **Groups** — operações para gerenciar grupos de Administrador de Grade local e recuperar grupos de Administrador de Grade federados de um servidor LDAP externo.
- **Identity-source** — operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **ilm** — operações de gerenciamento do ciclo de vida da informação (ILM).
- **Licença** — operações para recuperar e atualizar a licença StorageGRID.
- **Logs** — operações para coletar e baixar arquivos de log.
- **Métricas** — operações em métricas do StorageGRID, incluindo consultas instantâneas de métricas em um único ponto no tempo e consultas de métricas de intervalo ao longo de um intervalo de tempo. A API Grid Management usa a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de back-end. Para obter informações sobre a construção de consultas Prometheus, consulte o site Prometheus.

> As métricas que `private` incluem em seus nomes são destinadas apenas para uso interno. Essas métricas estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

- **Node-health** — operações no status de integridade do nó.
- **ntp-serviders** — operações para listar ou atualizar servidores NTP (Network Time Protocol) externos.
- **Objects** — operações em objetos e metadados de objetos.
- **Recovery** — operações para o procedimento de recuperação.
- **Recovery-package** — operações para baixar o Recovery Package.
- **Regions** — operações para visualizar e criar regiões.
- **S3-object-lock** — operações em configurações globais de bloqueio de objetos S3D.
- **Server-certificate** — operações para visualizar e atualizar certificados de servidor do Grid Manager.
- **snmp** — operações na configuração SNMP atual.
- **Traffic-classes** — operações para políticas de classificação de tráfego.
- **Não confiável-cliente-rede** — operações na configuração de rede cliente não confiável.
- **Usuários** — operações para visualizar e gerenciar usuários do Grid Manager.

Emissão de solicitações de API

A interface do usuário Swagger fornece detalhes completos e documentação para cada operação da API.

O que você vai precisar

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

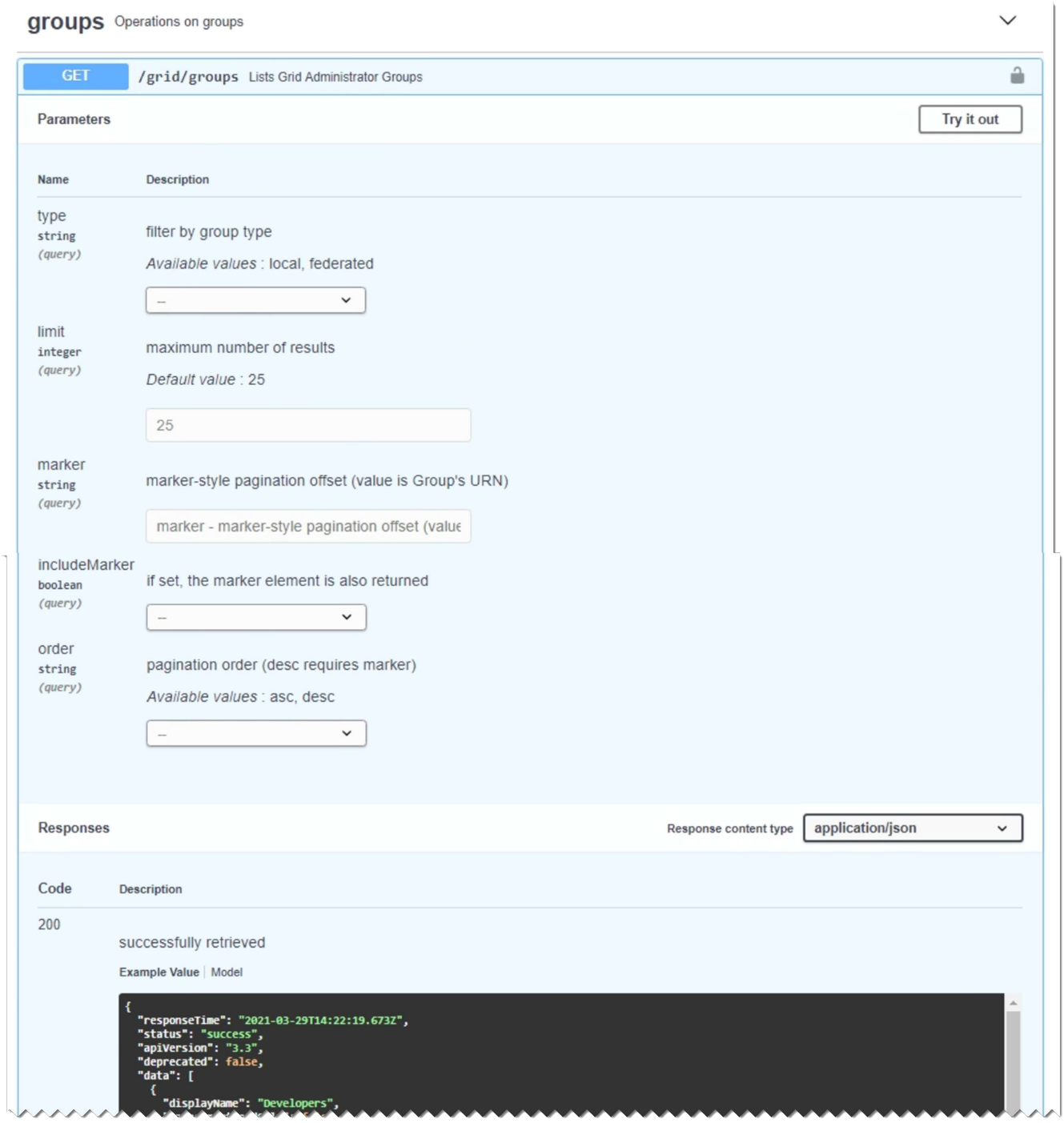
> Todas as operações de API que você executa usando a página da Web do API Docs são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

Passos

1. Selecione **Ajuda** > **Documentação da API** no cabeçalho do Grid Manager.
2. Selecione a operação desejada.

   Ao expandir uma operação de API, você pode ver as ações HTTP disponíveis, como GET, PUT, UPDATE e DELETE.

3. Selecione uma ação HTTP para ver os detalhes da solicitação, incluindo o URL do endpoint, uma lista de todos os parâmetros necessários ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.



4. Determine se a solicitação requer parâmetros adicionais, como um grupo ou ID de usuário. Em seguida, obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.

5. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode clicar em **modelo** para aprender os requisitos para cada campo.
6. Clique em **Experimente**.
7. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
8. Clique em **Executar**.
9. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Controle de versão da API Grid Management

A API de gerenciamento de grade usa o controle de versão para suportar atualizações sem interrupções.

Por exemplo, este URL de solicitação especifica a versão 3 da API.

`https://hostname_or_ip_address/api/v3/authorize`

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são ***not compatible*** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que ***are compatíveis*** com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades. O exemplo a seguir ilustra como a versão da API é carregada com base no tipo de alterações feitas.

Tipo de alteração para API	Versão antiga	Nova versão
Compatível com versões mais antigas	2,1	2,2
Não compatível com versões mais antigas	2,1	3,0

Quando você instala o software StorageGRID pela primeira vez, apenas a versão mais recente da API de gerenciamento de grade está ativada. No entanto, quando você atualiza para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.

> Você pode usar a API Grid Management para configurar as versões suportadas. Consulte a seção "config" da documentação da API Swagger para obter mais informações. Você deve desativar o suporte para a versão mais antiga depois de atualizar todos os clientes da API Grid Management para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True
- Um aviso obsoleto é adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Determinando quais versões de API são suportadas na versão atual

Use a seguinte solicitação de API para retornar uma lista das principais versões da API suportada:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especificando uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v3`) ou um cabeçalho (`Api-Version: 3`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Proteção contra falsificação de solicitação entre sites (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra StorageGRID usando tokens CSRF para melhorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes de API podem optar por ativá-lo quando fizerem login.

Um invasor que pode acionar uma solicitação para um site diferente (como um POST de formulário HTTP) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conetado.

O StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro específico DO corpo DO POST.

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição é `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando verdadeiro, um `GridCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes itens:

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido para o valor do cookie de token CSRF.
- Para endpoints que aceitam um corpo codificado por formulário: Um `csrfToken` parâmetro corpo de solicitação codificado por formulário.

Consulte a documentação da API on-line para obter exemplos e detalhes adicionais.

> As solicitações que têm um conjunto de cookies de token CSRF também irão aplicar o `"Content-Type: application/json"` cabeçalho para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

Usando a API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado para o seu sistema StorageGRID, você não poderá usar as solicitações padrão de autenticação API para fazer login e sair da API de gerenciamento de grade ou da API de gerenciamento de locatário.

Iniciar sessão na API se o início de sessão único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para obter um token de autenticação do AD FS válido para a API de Gerenciamento de Grade ou a API de Gerenciamento de locatário.

O que você vai precisar

- Você conhece o nome de usuário e a senha SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py` script Python, que está localizado no diretório arquivos de instalação do StorageGRID (`./rpms`para Linux ou CentOS, para Ubuntu ou Debian, `./debs` e `./vsphere` para VMware).

- Um exemplo de fluxo de trabalho de solicitações curl.

  O fluxo de trabalho curl pode ter um tempo limite se você o executar muito lentamente. Você pode ver o erro: Uma SubjectConfirmation válida não foi encontrada nesta resposta.

  > O fluxo de trabalho cURL de exemplo não protege a senha de ser vista por outros usuários.

Se você tiver um problema de codificação de URL, poderá ver o erro: Versão SAML não suportada.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
   - Use o `storagegrid-ssoauth.py` script Python. Avance para o passo 2.
   - Use solicitações curl. Avance para o passo 3.
2. Se você quiser usar o `storagegrid-ssoauth.py` script, passe o script para o interpretador Python e execute o script.

   Quando solicitado, insira valores para os seguintes argumentos:

   - O nome de usuário SSO
   - O domínio onde o StorageGRID está instalado
   - O endereço para StorageGRID
   - Se você quiser acessar a API de gerenciamento do locatário, insira o ID da conta do locatário. E

   ```
   python3 /tmp/storagegrid-ssoauth.py
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

3. Se você quiser usar solicitações curl, use o procedimento a seguir.

   a. Declare as variáveis necessárias para iniciar sessão.

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export SAMLDOMAIN='my-domain'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   export AD_FS_ADDRESS='adfs.example.com'
   ```

Para acessar a API de gerenciamento de grade, use 0 como `TENANTACCOUNTID`.

b. Para receber um URL de autenticação assinada, emita uma SOLICITAÇÃO POST para `/api/v3/authorize-saml`, e remova a codificação JSON adicional da resposta.

Este exemplo mostra uma SOLICITAÇÃO POST para um URL de autenticação assinada para `TENANTACCOUNTID`. Os resultados serão passados para Python -m json.tool para remover a codificação JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

A resposta para este exemplo inclui um URL assinado que é codificado por URL, mas não inclui a camada adicional de codificação JSON.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenha um URL completo que inclua o ID de solicitação do cliente do AD FS.

Uma opção é solicitar o formulário de login usando o URL da resposta anterior.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

A resposta inclui o ID de solicitação do cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salve o ID de solicitação do cliente da resposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envie suas credenciais para a ação de formulário da resposta anterior.

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=For
msAuthentication" --include
```

O AD FS retorna um redirecionamento 302, com informações adicionais nos cabeçalhos.

> Se a autenticação multifator (MFA) estiver ativada para seu sistema SSO, o post de formulário também conterá a segunda senha ou outras credenciais.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salve o `MSISAuth` cookie da resposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envie uma SOLICITAÇÃO GET para o local especificado com os cookies do POST de autenticação.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --cookie "MSISAuth=$MSISAuth" --include
```

Os cabeçalhos de resposta conterão informações de sessão do AD FS para uso posterior de logout e o corpo de resposta contém o SAMLResponse em um campo de formulário oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salve o `SAMLResponse` do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Usando o `SAMLResponse` , faça uma solicitação StorageGRID`/api/saml-response` para gerar um token de autenticação StorageGRID.

   Para `RelayState`, use o ID da conta do locatário ou use 0 se quiser entrar na API de gerenciamento de grade.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

A resposta inclui o token de autenticação.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salve o token de autenticação na resposta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Agora você pode usar `MYTOKEN` para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Sair da API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatário.

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID simplesmente fazendo logout da página de logout única da sua organização. Ou, você pode acionar o logout único (SLO) do StorageGRID, que requer um token válido do portador do StorageGRID.

Passos

1. Para gerar uma solicitação de logout assinada, passe `cookie "sso=true"` para a API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Um URL de logout é retornado:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Salve o URL de logout.

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para o StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

A resposta 302 é devolvida. O local de redirecionamento não é aplicável ao logout somente API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Exclua o token do portador do StorageGRID.

A exclusão do token portador do StorageGRID funciona da mesma forma que sem SSO. Se `cookie "sso=true"` não for fornecido, o usuário será desconetado do StorageGRID sem afetar o estado SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

Uma `204 No Content` resposta indica que o usuário está desconetado agora.

```
HTTP/1.1 204 No Content
```

Usando certificados de segurança do StorageGRID

Certificados de segurança são pequenos arquivos de dados usados para criar conexões seguras e confiáveis entre componentes do StorageGRID e entre componentes do StorageGRID e sistemas externos.

O StorageGRID usa dois tipos de certificados de segurança:

- **Certificados de servidor** são necessários quando você usa conexões HTTPS. Os certificados de servidor são usados para estabelecer conexões seguras entre clientes e servidores, autenticando a identidade de um servidor para seus clientes e fornecendo um caminho de comunicação seguro para os dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam uma identidade de cliente ou usuário no servidor, fornecendo autenticação mais segura do que senhas sozinhas. Os certificados de cliente não encriptam dados.

Quando um cliente se coneta ao servidor usando HTTPS, o servidor responde com o certificado do servidor, que contém uma chave pública. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

O StorageGRID funciona como o servidor para algumas conexões (como o endpoint do balanceador de carga) ou como o cliente para outras conexões (como o serviço de replicação do CloudMirror).

Uma autoridade de certificação externa (CA) pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. O StorageGRID também inclui uma autoridade de certificação (CA) integrada que gera certificados de CA internos durante a instalação do sistema. Esses certificados internos de CA são usados, por padrão, para proteger o tráfego interno do StorageGRID. Embora você possa usar os certificados de CA internos para um ambiente que não seja de produção, a prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa. Conexões não protegidas sem certificado também são suportadas, mas não são recomendadas.

- Os certificados de CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser os especificados para verificar conexões de servidor.
- Todos os certificados personalizados devem atender às diretrizes de fortalecimento do sistema para certificados de servidor.

  "Endurecimento do sistema"

- O StorageGRID oferece suporte ao agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados da CA).

> O StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todas as grades. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa em vez do certificado CA do sistema operacional.

Variantes dos tipos de certificado de servidor e cliente são implementadas de várias maneiras. Você deve ter todos os certificados necessários para sua configuração específica do StorageGRID prontos antes de configurar o sistema.

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado de cliente administrador	Cliente	Instalado em cada cliente, permitindo que o StorageGRID autentique o acesso de cliente externo. • Permite que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	**Configuração** > **Controle de Acesso** > **certificados de Cliente**	"Configurando certificados de cliente de administrador"
Certificado de federação de identidade	Servidor	Autentica a conexão entre o StorageGRID e um ative Directory externo, OpenLDAP ou Oracle Directory Server.usado para federação de identidade, o que permite que grupos de administradores e usuários sejam gerenciados por um sistema externo.	**Configuração** > **Controle de Acesso** > **Federação de identidade**	"Usando a federação de identidade"
Certificado de logon único (SSO)	Servidor	Autentica a conexão entre os Serviços de Federação do ative Directory (AD FS) e o StorageGRID que é usado para solicitações de logon único (SSO).	**Configuração** > **Controle de Acesso** > **Início de sessão único**	"Configurando logon único"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado de servidor de gerenciamento de chaves (KMS)	Servidor e cliente	Autentica a conexão entre o StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID.	**Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**	"Adicionar um servidor de gerenciamento de chaves (KMS)"
Certificado de notificação de alerta por e-mail	Servidor e cliente	Autentica a conexão entre um servidor de e-mail SMTP e o StorageGRID que é usado para notificações de alerta. • Se as comunicações com o servidor SMTP exigirem TLS (Transport Layer Security), você deverá especificar o certificado CA do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	**Alertas** > **Configuração de e-mail**	"Monitorizar Resolução de problemas"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado de ponto final do balanceador de carga	Servidor	Autentica a conexão entre clientes S3 ou Swift e o serviço StorageGRID Load Balancer em nós de gateway ou nós de administração. Você carrega ou gera um certificado do balanceador de carga quando configura um endpoint do balanceador de carga. Os aplicativos do cliente usam o certificado do balanceador de carga ao se conetar ao StorageGRID para salvar e recuperar dados do objeto. **Nota:** o certificado do balanceador de carga é o certificado mais utilizado durante a operação normal do StorageGRID.	**Configuração** > **Configurações de rede** > **pontos finais do Load Balancer**	• "Configuração dos pontos de extremidade do balanceador de carga" • Criando um ponto de extremidade do balanceador de carga para FabricPool "Configurar o StorageGRID para FabricPool"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado do servidor de interface de gerenciamento	Servidor	Autentica a conexão entre navegadores da Web cliente e a interface de gerenciamento do StorageGRID, permitindo que os usuários acessem o Gerenciador de Grade e o Gerenciador de locatário sem avisos de segurança. Este certificado também autentica as conexões da API de Gerenciamento de Grade e da API de Gerenciamento do locatário. Você pode usar o certificado de CA interno ou carregar um certificado personalizado.	**Configuração** > **Configurações de rede** > **certificados de servidor**	• "Configurando certificados de servidor" • "Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"
Certificado de endpoint do Cloud Storage Pool	Servidor	Autentica a conexão do pool de storage de nuvem do StorageGRID para um local de storage externo (como o storage S3 Glacier ou Microsoft Azure Blob). Um certificado diferente é necessário para cada tipo de provedor de nuvem.	**ILM** > **conjuntos de armazenamento**	"Gerenciar objetos com ILM"
Certificado de endpoint de serviços de plataforma	Servidor	Autentica a conexão do serviço da plataforma StorageGRID a um recurso de storage S3.	**Gerenciador do Locatário** > **ARMAZENAMENTO (S3)** > **terminais de serviços da plataforma**	"Use uma conta de locatário"

Certificado	Tipo de certificado	Descrição	Localização de navegação	Detalhes
Certificado do servidor de extremidade do serviço API do Object Storage	Servidor	Autentica conexões de cliente S3 ou Swift seguras ao serviço LDR (local Distribution Router) em um nó de armazenamento ou ao serviço CLB (descontinuado Connection Load Balancer) em um nó de gateway.	**Configuração** > **Configurações de rede** > **pontos finais do Load Balancer**	"Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB"

Exemplo 1: Serviço do Load Balancer

Neste exemplo, o StorageGRID atua como servidor.

1. Você configura um ponto de extremidade do balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.
2. Você configura uma conexão de cliente S3 ou Swift para o endpoint do balanceador de carga e carrega o mesmo certificado para o cliente.
3. Quando o cliente deseja salvar ou recuperar dados, ele se coneta ao endpoint do balanceador de carga usando HTTPS.
4. O StorageGRID responde com o certificado do servidor, que contém uma chave pública e com uma assinatura baseada na chave privada.
5. O cliente verifica esse certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados de objeto para o StorageGRID.

Exemplo 2: Servidor de gerenciamento de chaves externas (KMS)

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software servidor de gerenciamento de chaves externo, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado pela CA, um certificado de cliente público e a chave privada para o certificado de cliente.
2. Usando o Gerenciador de Grade, você configura um servidor KMS e carrega os certificados de servidor e cliente e a chave privada do cliente.
3. Quando um nó StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura com base na chave privada.
4. O servidor KMS valida a assinatura do certificado e decide que pode confiar no StorageGRID.
5. O servidor KMS responde usando a conexão validada.

Informações sobre direitos autorais

Informações sobre marcas comerciais