# Administrar o StorageGRID

StorageGRID

NetApp
October 03, 2025

# Índice


Administrar o StorageGRID . . . 1
- Administrar um sistema StorageGRID . . . 1
  - Requisitos do navegador da Web . . . 1
  - Iniciar sessão no Grid Manager . . . 2
  - Sair do Gerenciador de Grade . . . 6
  - Alterar a sua palavra-passe . . . 7
  - Alterando a senha de provisionamento . . . 8
  - Alterar o tempo limite da sessão do navegador . . . 9
  - Visualizar informações de licença do StorageGRID . . . 10
  - Atualizando informações de licença do StorageGRID . . . 11
  - Usando a API de gerenciamento de grade . . . 12
  - Usando certificados de segurança do StorageGRID . . . 24
- Controlar o acesso do administrador ao StorageGRID . . . 31
  - Controlar o acesso através de firewalls . . . 31
  - Usando a federação de identidade . . . 32
  - Gerenciando grupos de administradores . . . 38
  - Gerenciamento de usuários locais . . . 47
  - Usando logon único (SSO) para StorageGRID . . . 49
  - Configurando certificados de cliente de administrador . . . 67
- Configurando servidores de gerenciamento de chaves . . . 76
  - O que é um servidor de gerenciamento de chaves (KMS)? . . . 76
  - Rever os métodos de encriptação StorageGRID . . . 76
  - Visão geral do KMS e da configuração do appliance . . . 79
  - Considerações e requisitos para usar um servidor de gerenciamento de chaves . . . 82
  - Considerações para alterar o KMS para um site . . . 85
  - Configurando o StorageGRID como um cliente no KMS . . . 88
  - Adicionar um servidor de gerenciamento de chaves (KMS) . . . 89
  - Visualizar detalhes do KMS . . . 97
  - Exibindo nós criptografados . . . 99
  - Editar um servidor de gerenciamento de chaves (KMS) . . . 101
  - Remover um servidor de gerenciamento de chaves (KMS) . . . 104
- Gerenciamento de locatários . . . 105
  - Quais são as contas de inquilino . . . 106
  - Criando e configurando contas de inquilino . . . 106
  - Configurando S3 locatários . . . 107
  - Configurando os locatários Swift . . . 107
  - Criando uma conta de locatário . . . 108
  - Alterando a senha do usuário raiz local de um locatário . . . 115
  - Editando uma conta de locatário . . . 117
  - Excluindo uma conta de locatário . . . 119
  - Gerenciamento de serviços de plataforma para contas de locatários do S3 . . . 120
- Configurando conexões de cliente S3 e Swift . . . 129
  - Resumo: Endereços IP e portas para conexões de clientes . . . 130

Gerenciamento do balanceamento de carga . . . 132
Gerenciando redes de clientes não confiáveis . . . 142
Gerenciamento de grupos de alta disponibilidade . . . 145
Configurando nomes de domínio de endpoint da API S3 . . . 157
Ativar HTTP para comunicações cliente . . . 159
Controlar quais operações do cliente são permitidas . . . 160
Gerenciamento de redes e conexões StorageGRID . . . 161
Diretrizes para redes StorageGRID . . . 161
Visualização de endereços IP . . . 162
Cifras suportadas para conexões TLS de saída . . . 163
Alteração da encriptação de transferência de rede . . . 164
Configurando certificados de servidor . . . 165
Configurando as configurações de proxy de armazenamento . . . 172
Configurando as configurações de proxy Admin . . . 174
Gerir políticas de classificação de tráfego . . . 175
Quais são os custos da ligação . . . 188
Configurando o AutoSupport . . . 190
Informações incluídas nas mensagens do AutoSupport . . . 191
Usando o Active IQ . . . 191
Aceder às definições do AutoSupport . . . 191
Protocolos para envio de mensagens AutoSupport . . . 192
Opções de AutoSupport . . . 192
Especificando o protocolo para mensagens AutoSupport . . . 193
Habilitando o AutoSupport sob demanda . . . 194
Desativar mensagens AutoSupport semanais . . . 195
Desativando mensagens AutoSupport acionadas por eventos . . . 196
Acionando manualmente uma mensagem AutoSupport . . . 197
Adicionar um destino AutoSupport adicional . . . 198
Envio de mensagens do e-Series AutoSupport através do StorageGRID . . . 200
Solução de problemas de mensagens do AutoSupport . . . 204
Gerenciando nós de storage . . . 206
O que é um nó de storage . . . 206
Gerenciando Opções de armazenamento . . . 210
Gerenciamento do storage de metadados de objetos . . . 215
Configuração de configurações globais para objetos armazenados . . . 223
Configurações do nó de storage . . . 225
Gerenciamento de nós de storage completos . . . 230
Gerenciando nós de administração . . . 230
O que é um nó Admin . . . 231
Usando vários nós de administração . . . 232
Identificando o nó de administração principal . . . 234
Selecionar um remetente preferido . . . 234
Exibindo status de notificação e filas . . . 235
Como os nós de administração mostram alarmes reconhecidos (sistema legado) . . . 236
Configurando o acesso de cliente de auditoria . . . 237

Gerenciando nós de arquivamento . . . 254
O que é um nó de arquivo . . . 255
Configurando conexões de nó de arquivo para armazenamento de arquivamento . . . 256
Definir alarmes personalizados para o nó de arquivo . . . 271
Integração do Tivoli Storage Manager . . . 271
Migração de dados para o StorageGRID . . . 278
Confirmar a capacidade do sistema StorageGRID . . . 279
Determinando a política de ILM para dados migrados . . . 279
Impacto da migração nas operações . . . 280
Agendamento da migração de dados . . . 280
Monitoramento da migração de dados . . . 280
Criação de notificações personalizadas para alarmes de migração . . . 281

# Administrar o StorageGRID

Saiba como configurar o sistema StorageGRID.

- "Administrar um sistema StorageGRID"
- "Controlar o acesso do administrador ao StorageGRID"
- "Configurando servidores de gerenciamento de chaves"
- "Gerenciamento de locatários"
- "Configurando conexões de cliente S3 e Swift"
- "Gerenciamento de redes e conexões StorageGRID"
- "Configurando o AutoSupport"
- "Gerenciando nós de storage"
- "Gerenciando nós de administração"
- "Gerenciando nós de arquivamento"
- "Migração de dados para o StorageGRID"

# 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 |

| Navegador da Web | Versão mínima suportada |
|---|---|
| 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:

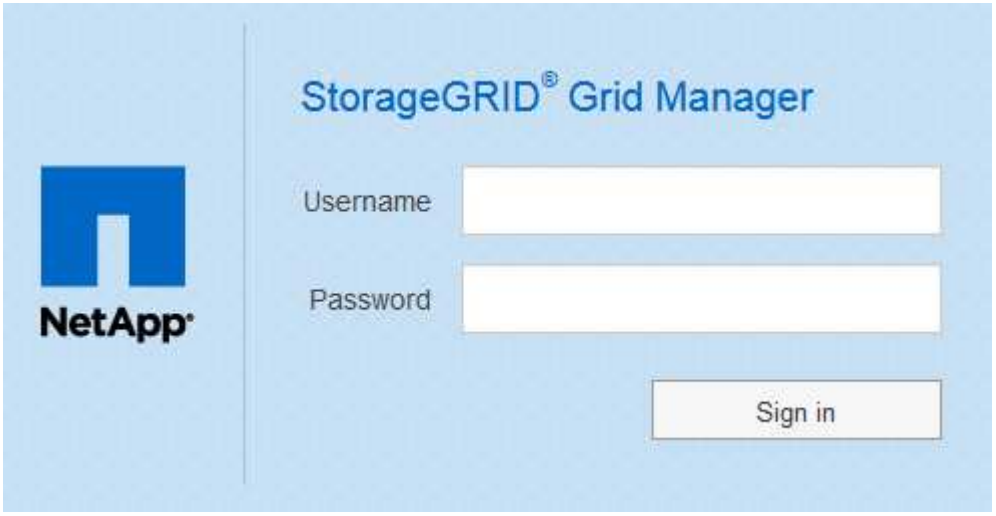
   `https://FQDN_or_Admin_Node_IP/`

`_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:

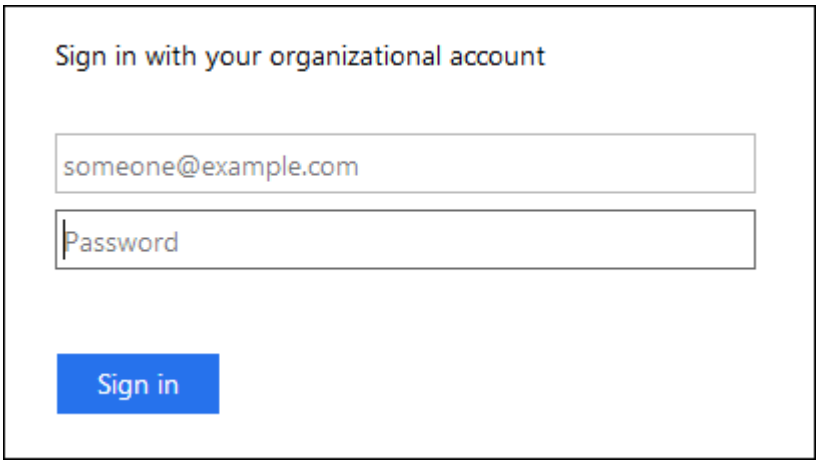
`https://FQDN_or_Admin_Node_IP:port/`

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:

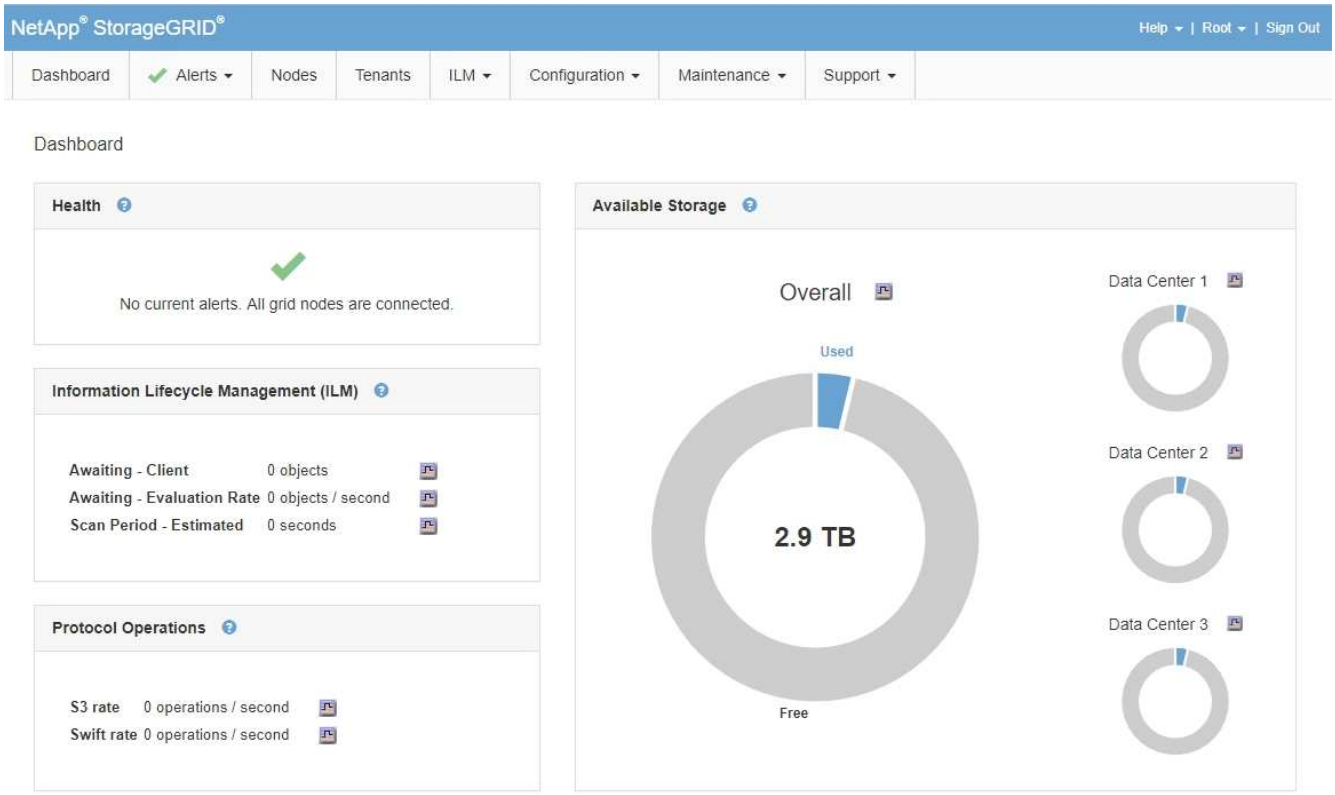



- Se o SSO estiver ativado para o seu sistema StorageGRID e você tiver acessado anteriormente o Gerenciador de Grade ou uma conta de locatário:

  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.<br>b. Insira seu nome de usuário e senha para o Gerenciador de Grade.<br>c. Clique em **entrar**. |

| Opção | Passos |
| --- | --- |
| SSO ativado | Na barra de endereços do navegador, insira o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração.<br><br>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.<br><br>**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"

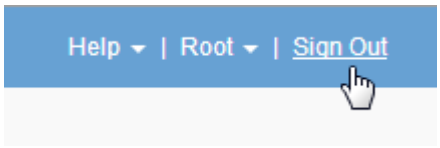
"Monitorizar Resolução de problemas"

## 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.<br><br>A página de login do Gerenciador de Grade é exibida.<br><br>**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.<br><br>**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**

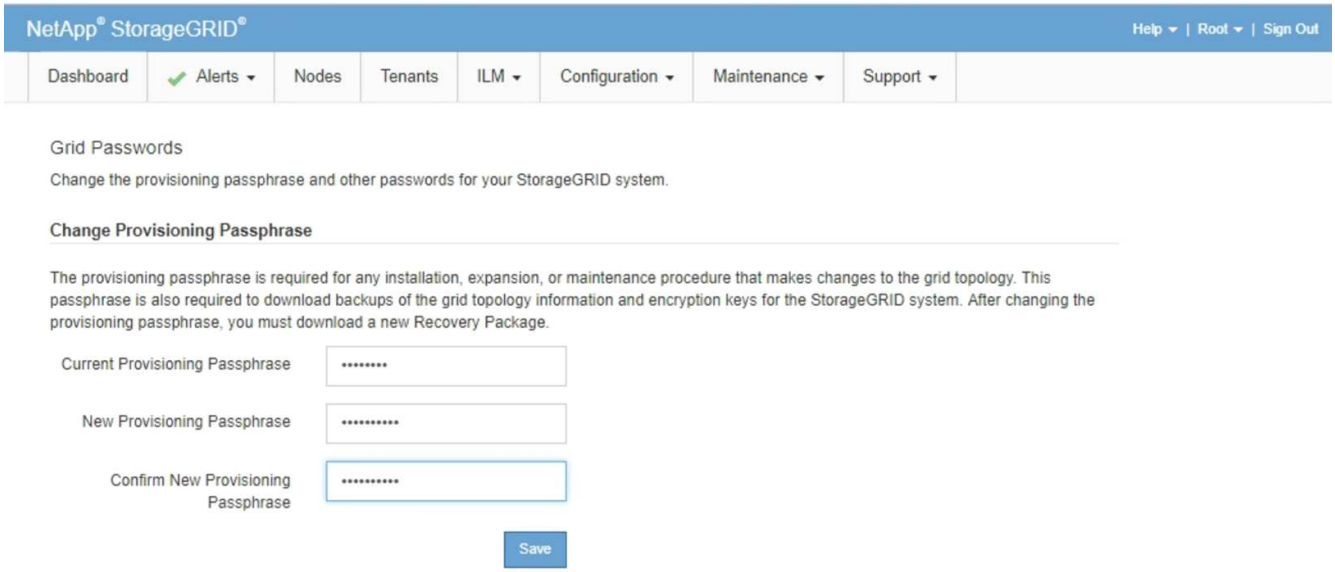
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de Manutenção ou Acesso root.
- Você deve ter a senha de provisionamento atual.

**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**.

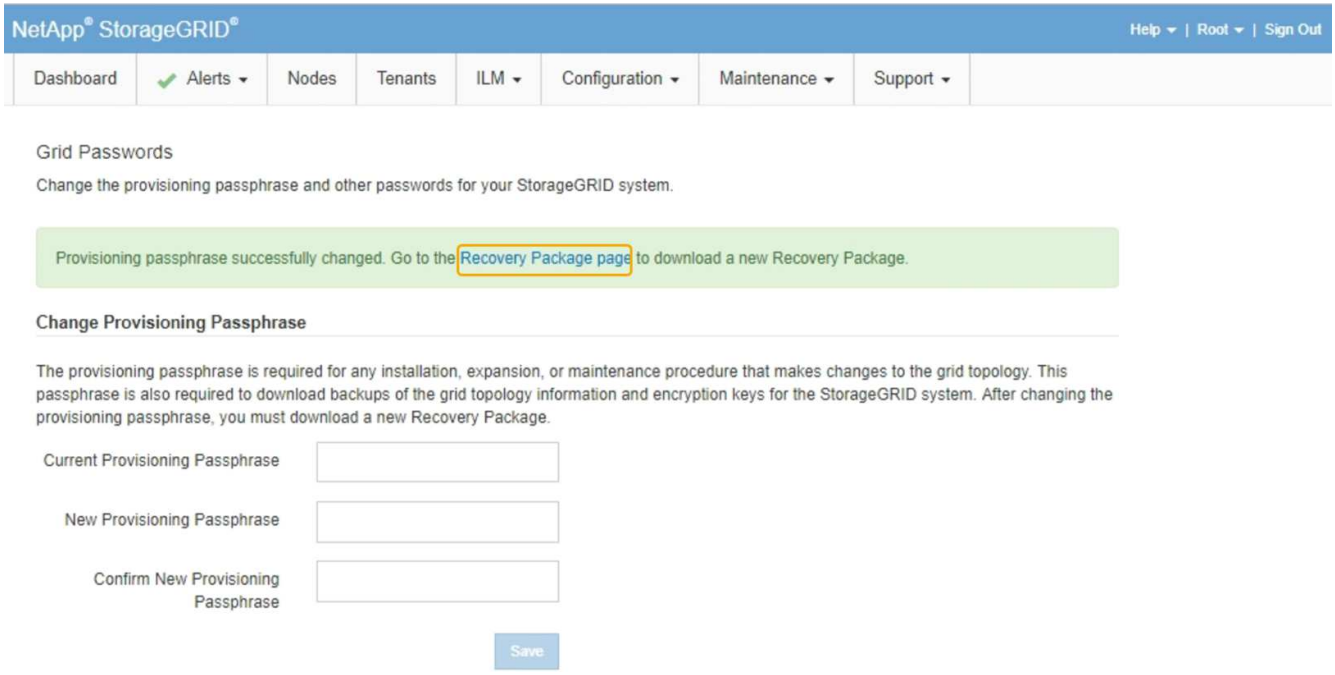



2. Introduza a sua frase-passe de aprovisionamento atual.
3. Introduza a nova frase-passe.a frase-passe tem de conter, no mínimo, 8 e não mais de 32 carateres. As senhas são sensíveis a maiúsculas e minúsculas.

> 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.

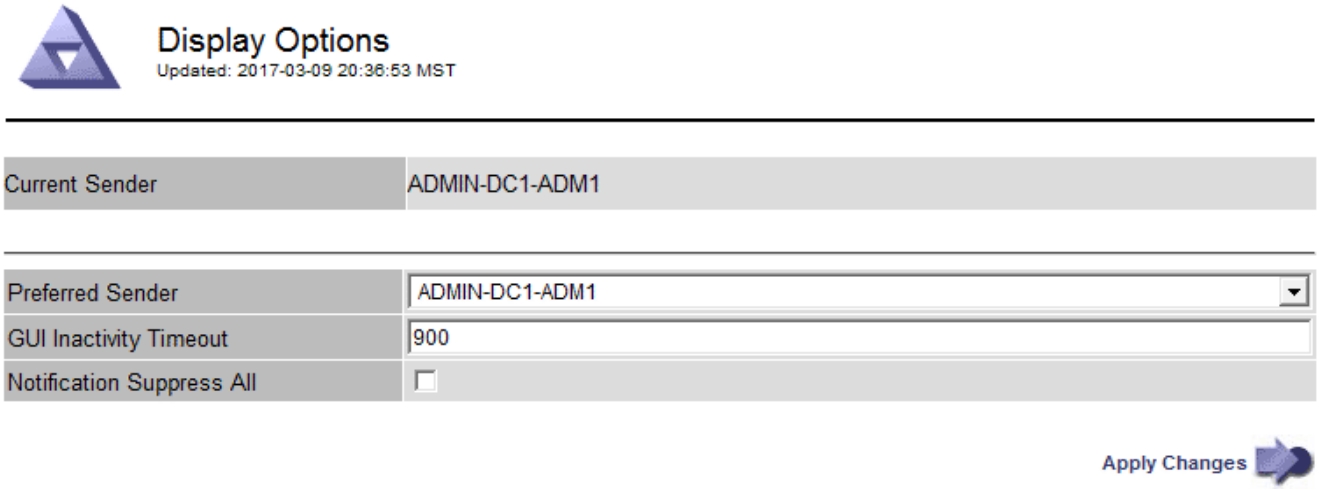
O tempo limite da sessão do usuário também pode ser controlado pelo seguinte:

- 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.

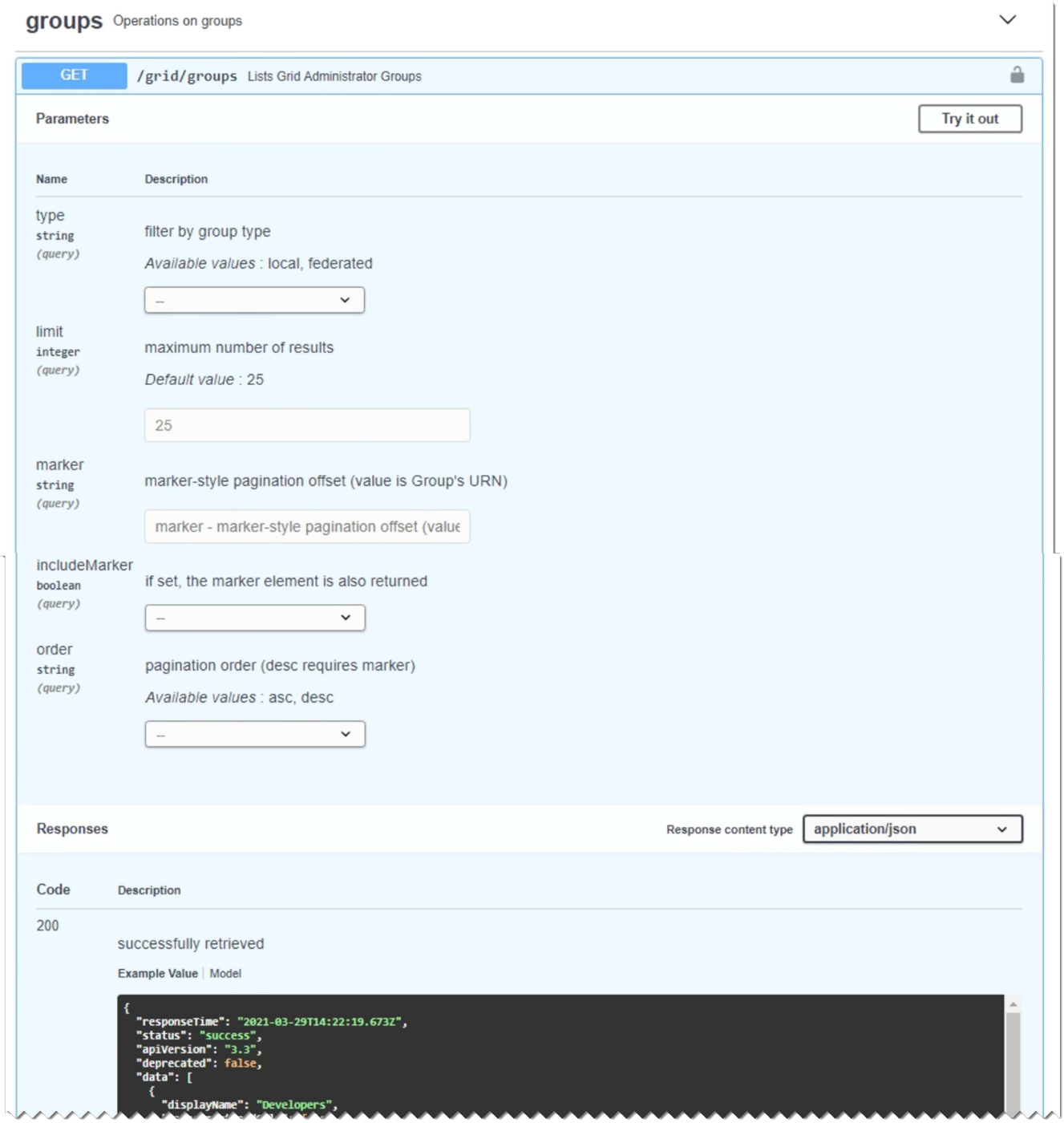
> Todas as operações de API que você executa usando a página da Web do API Docs são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

#### 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


   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.<br>• Permite que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus.<br>• 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.<br>• Se as comunicações com o servidor SMTP exigirem TLS (Transport Layer Security), você deverá especificar o certificado CA do servidor de e-mail.<br>• 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.<br><br>**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"<br>• Criando um ponto de extremidade do balanceador de carga para FabricPool<br><br>"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.<br><br>Este certificado também autentica as conexões da API de Gerenciamento de Grade e da API de Gerenciamento do locatário.<br><br>Você pode usar o certificado de CA interno ou carregar um certificado personalizado. | **Configuração** > **Configurações de rede** > **certificados de servidor** | • "Configurando certificados de servidor"<br>• "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.

# Controlar o acesso do administrador ao StorageGRID

Você pode controlar o acesso do administrador ao sistema StorageGRID abrindo ou fechando portas de firewall, gerenciando grupos de administração e usuários, configurando logon único (SSO) e fornecendo certificados de cliente para permitir acesso externo seguro às métricas do StorageGRID.

- "Controlar o acesso através de firewalls"
- "Usando a federação de identidade"
- "Gerenciando grupos de administradores"
- "Gerenciamento de usuários locais"
- "Usando logon único (SSO) para StorageGRID"
- "Configurando certificados de cliente de administrador"

## Controlar o acesso através de firewalls

Quando quiser controlar o acesso através de firewalls, abra ou feche portas específicas no firewall externo.

### Controlar o acesso no firewall externo

Você pode controlar o acesso às interfaces de usuário e APIs nos nós de administração do StorageGRID abrindo ou fechando portas específicas no firewall externo. Por exemplo, você pode evitar que os locatários sejam capazes de se conetar ao Gerenciador de Grade no firewall, além de usar outros métodos para controlar o acesso ao sistema.

| Porta | Descrição | Se a porta estiver aberta… |
|---|---|---|
| 443 | Porta HTTPS padrão para nós de administração | Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade, a API de gerenciamento de grade, o Gerenciador de locatário e a API de gerenciamento do locatário.<br><br>**Nota:** a porta 443 também é usada para algum tráfego interno. |
| 8443 | Porta restrita do Gerenciador de Grade em nós de administração | • Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade e a API de Gerenciamento de Grade usando HTTPS.<br>• Os navegadores da Web e os clientes da API de gerenciamento não podem acessar o Gerenciador do locatário ou a API de gerenciamento do locatário.<br>• As solicitações de conteúdo interno serão rejeitadas. |

| Porta | Descrição | Se a porta estiver aberta… |
| --- | --- | --- |
| 9443 | Porta restrita do Gerenciador de inquilinos em nós de administração | • Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador do locatário e a API de gerenciamento do locatário usando HTTPS.<br>• Navegadores da Web e clientes de API de gerenciamento não podem acessar o Gerenciador de Grade ou a API de Gerenciamento de Grade.<br>• As solicitações de conteúdo interno serão rejeitadas. |

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.

**Informações relacionadas**

"Iniciar sessão no Grid Manager"

"Criando uma conta de locatário se o StorageGRID não estiver usando SSO"

"Resumo: Endereços IP e portas para conexões de clientes"

"Gerenciando redes de clientes não confiáveis"

"Instale Ubuntu ou Debian"

"Instale o VMware"

"Instale o Red Hat Enterprise Linux ou CentOS"

## Usando a federação de identidade

O uso da federação de identidade torna a configuração de grupos e usuários mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares.

### Configurando a federação de identidade

Você pode configurar a federação de identidade se quiser que os grupos de administração e usuários sejam gerenciados em outro sistema, como ative Directory, OpenLDAP ou Oracle Directory Server.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Se você pretende ativar o logon único (SSO), você deve usar o ative Directory como a origem de identidade federada e o AD FS como o provedor de identidade. Consulte ""requisitos para utilizar o início de sessão único.""
- Você deve estar usando o ative Directory, OpenLDAP ou Oracle Directory Server como o provedor de identidade.

Se pretender utilizar um serviço LDAP v3 que não esteja listado, tem de contactar o suporte técnico.

- Se você pretende usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade deve estar usando TLS 1,2 ou 1,3.

**Sobre esta tarefa**

Você deve configurar uma origem de identidade para o Gerenciador de Grade se quiser importar os seguintes tipos de grupos federados:

- Grupos de administração. Os usuários nos grupos de administração podem entrar no Gerenciador de Grade e executar tarefas, com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários de locatários que não usam sua própria origem de identidade. Os usuários em grupos de inquilinos podem entrar no Gerenciador de inquilinos e executar tarefas, com base nas permissões atribuídas ao grupo no Gerenciador de inquilinos.

**Passos**

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.
2. Selecione **Ativar federação de identidade**.

   São apresentados os campos para configurar o servidor LDAP.

3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.

   Você pode selecionar **ative Directory**, **OpenLDAP** ou **Other**.

   Se selecionar **OpenLDAP**, tem de configurar o servidor OpenLDAP. Consulte as diretrizes para configurar um servidor OpenLDAP.

   Selecione **Other** para configurar valores para um servidor LDAP que use o Oracle Directory Server.

4. Se você selecionou **Other**, preencha os campos na seção atributos LDAP.
   - **Nome exclusivo do usuário**: O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `uid` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `uid`.
   - **UUID de usuário**: O nome do atributo que contém o identificador exclusivo permanente de um usuário LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.
   - **Group unique name**: O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente `sAMAccountName` ao ative Directory e `cn` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `cn`.
   - **Group UUID**: O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente `objectGUID` ao ative Directory e `entryUUID` ao OpenLDAP. Se estiver configurando o Oracle Directory Server, digite `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos no formato de 16 bytes ou string, onde os hífens são ignorados.

5. Na secção Configurar servidor LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias.
   - **Nome do host**: O nome do host do servidor ou endereço IP do servidor LDAP.
   - **Port**: A porta usada para se conetar ao servidor LDAP.

     A porta padrão para STARTTLS é 389 e a porta padrão para LDAPS é 636. No entanto, você pode usar qualquer porta desde que seu firewall esteja configurado corretamente.

   - **Nome de usuário**: O caminho completo do nome distinto (DN) para o usuário que se conetará ao servidor LDAP.

     No ative Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

     O usuário especificado deve ter permissão para listar grupos e usuários e para acessar os seguintes atributos:

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`
     - `cn`
     - `memberOf` ou `isMemberOf`

   - **Senha**: A senha associada ao nome de usuário.
   - **Group base DN**: O caminho completo do nome distinto (DN) para uma subárvore LDAP que você deseja pesquisar grupos. No exemplo do ative Directory (abaixo), todos os grupos cujo Nome distinto é relativo ao DN base (DC-StorageGRID,DC-com) podem ser usados como grupos federados.

     Os valores **Group unique name** devem ser exclusivos dentro do **Group base DN** a que pertencem.

   - **DN da base do usuário**: O caminho completo do nome distinto (DN) de uma subárvore LDAP que você deseja pesquisar por usuários.

     Os valores **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN base do usuário** a que pertencem.

6. Na seção **Transport Layer Security (TLS)**, selecione uma configuração de segurança.
   - **Use STARTTLS (recomendado)**: Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada.
   - **Use LDAPS**: A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Esta opção é suportada por razões de compatibilidade.
   - **Não use TLS**: O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido.

     O uso da opção **não usar TLS** não é suportado se o servidor do ative Directory forçar a assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

7. Se você selecionou STARTTLS ou LDAPS, escolha o certificado usado para proteger a conexão.

- **Use o certificado CA do sistema operacional**: Use o certificado CA padrão instalado no sistema operacional para proteger conexões.
- **Use certificado CA personalizado**: Use um certificado de segurança personalizado.

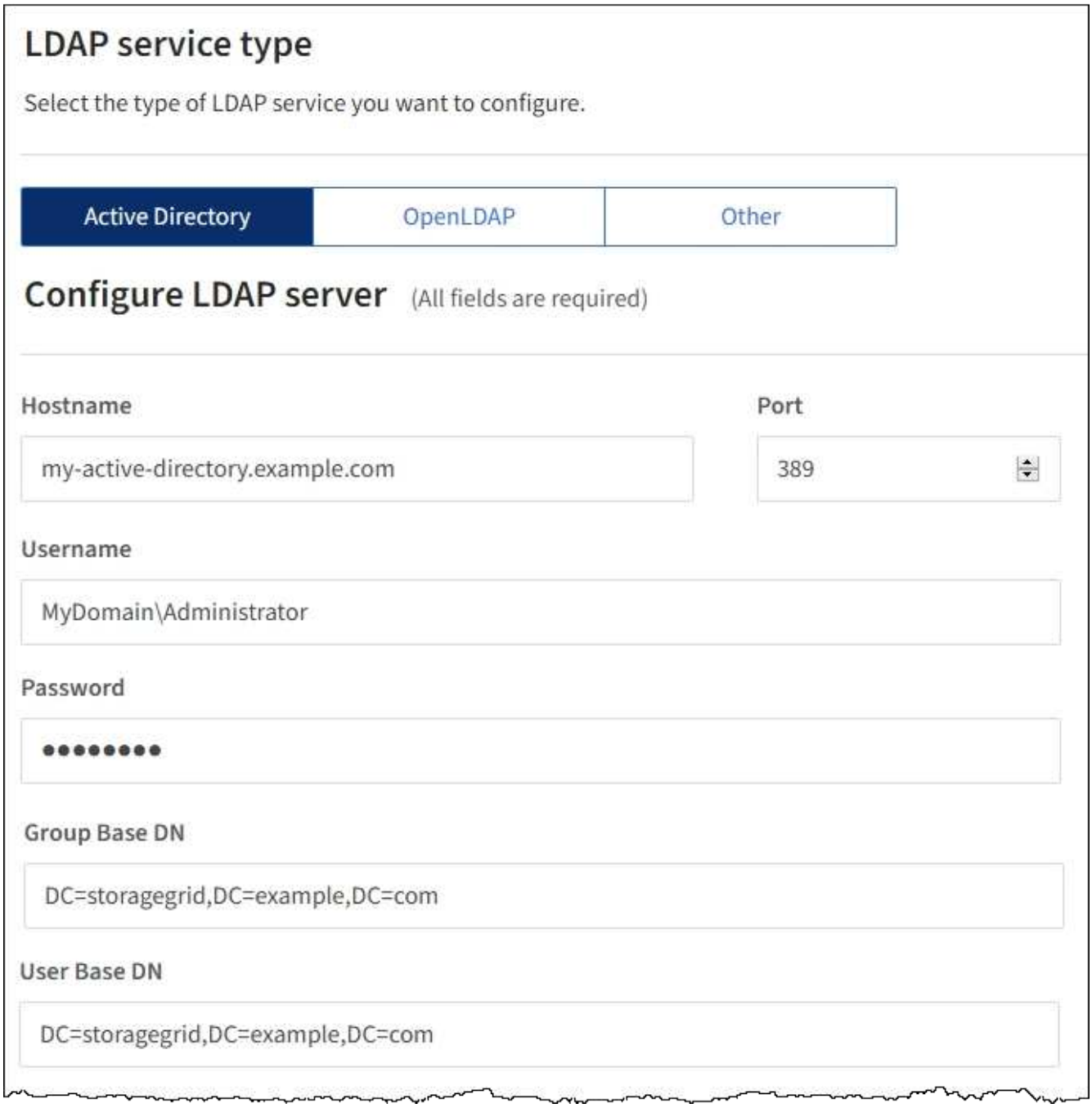
  Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto certificado da CA.

8. Opcionalmente, selecione **testar conexão** para validar suas configurações de conexão para o servidor LDAP.

   Uma mensagem de confirmação aparece no canto superior direito da página se a conexão for válida.

9. Se a conexão for válida, selecione **Salvar**.

   A captura de tela a seguir mostra valores de configuração de exemplo para um servidor LDAP que usa o ative Directory.




**Informações relacionadas**

"Cifras suportadas para conexões TLS de saída"

"Requisitos para o uso de logon único"

"Criando uma conta de locatário"

"Use uma conta de locatário"

#### Diretrizes para configurar um servidor OpenLDAP

Se você quiser usar um servidor OpenLDAP para federação de identidade, você deve configurar configurações específicas no servidor OpenLDAP.

### Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para manutenção de associação reversa em grupo no Guia do Administrador para OpenLDAP.

### Indexação

Você deve configurar os seguintes atributos OpenLDAP com as palavras-chave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Além disso, certifique-se de que os campos mencionados na ajuda do Nome de usuário sejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção da associação de grupo reverso no Guia do Administrador para OpenLDAP.

#### Informações relacionadas

"Documentação do OpenLDAP: Guia do administrador da versão 2,4"

### Forçando a sincronização com a fonte de identidade

O sistema StorageGRID sincroniza periodicamente grupos federados e usuários da origem da identidade. Você pode forçar o início da sincronização se quiser ativar ou restringir as permissões de usuário o mais rápido possível.

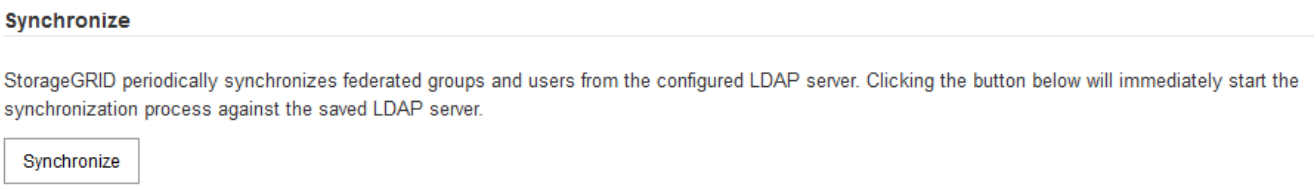
#### O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- A origem da identidade deve estar ativada.

#### Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.

   A página Federação de identidade é exibida. O botão **Sincronizar** está na parte inferior da página.

2. Clique em **Sincronizar**.

   Uma mensagem de confirmação indica que a sincronização foi iniciada com êxito. O processo de sincronização pode demorar algum tempo, dependendo do ambiente.

O alerta **Falha na sincronização da federação de identidade** é acionado se houver um problema na sincronização de grupos federados e usuários da origem da identidade.

### Desativando a federação de identidade

Você pode desativar temporariamente ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desativada, não há comunicação entre o StorageGRID e a fonte de identidade. No entanto, todas as configurações que você configurou são mantidas, permitindo que você reative facilmente a federação de identidade no futuro.

#### 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

Antes de desativar a federação de identidade, você deve estar ciente do seguinte:

- Os utilizadores federados não poderão iniciar sessão.
- Os usuários federados que estiverem conetados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a origem da identidade não ocorrerá e os alertas ou alarmes não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Ativar Federação de identidade** será desativada se o logon único (SSO) estiver definido como **ativado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade.

#### Passos

1. Selecione **Configuração** > **Controle de Acesso** > **Federação de identidade**.
2. Desmarque a caixa de seleção **Ativar Federação de identidade**.
3. Clique em **Salvar**.

#### Informações relacionadas

"Desativação do logon único"

## Gerenciando grupos de administradores

Você pode criar grupos de administração para gerenciar as permissões de segurança para um ou mais usuários de administração. Os usuários devem pertencer a um grupo para ter acesso ao sistema StorageGRID.

### Criando grupos de administração

Os grupos de administração permitem determinar quais usuários podem acessar quais recursos e operações no Gerenciador de Grade e na API de Gerenciamento de Grade.

#### O que você vai precisar

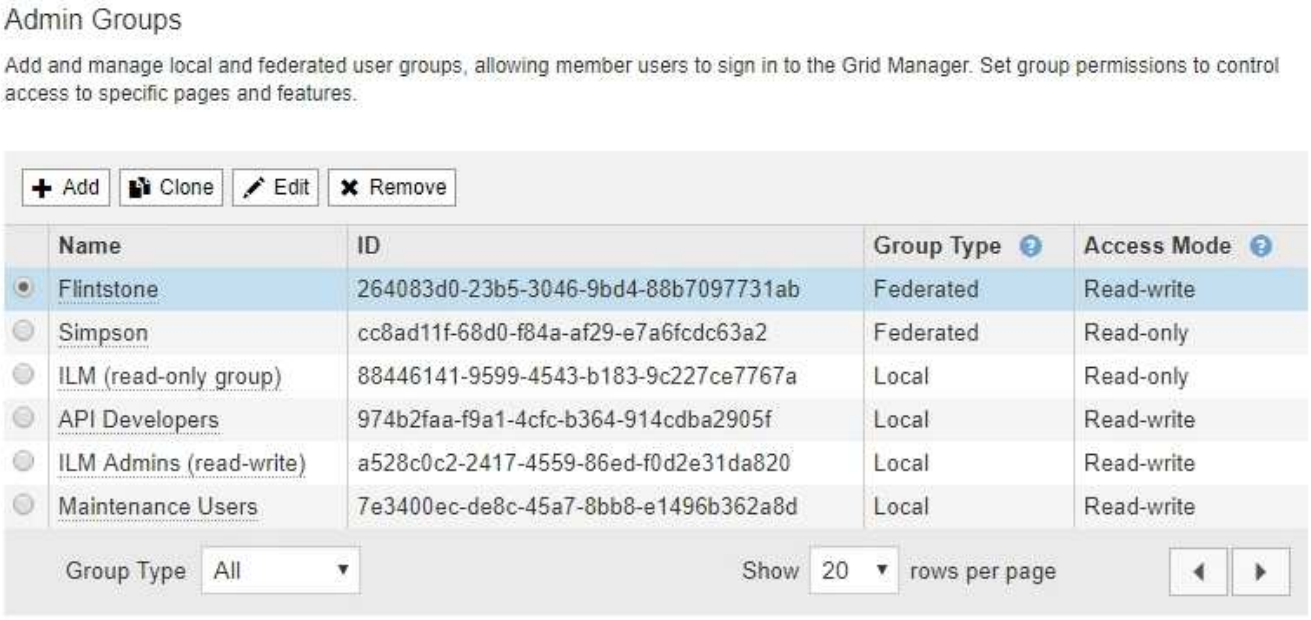
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

- Se você pretende importar um grupo federado, você deve ter a federação de identidade configurada e o grupo federado já deve existir na origem de identidade configurada.

**Passos**

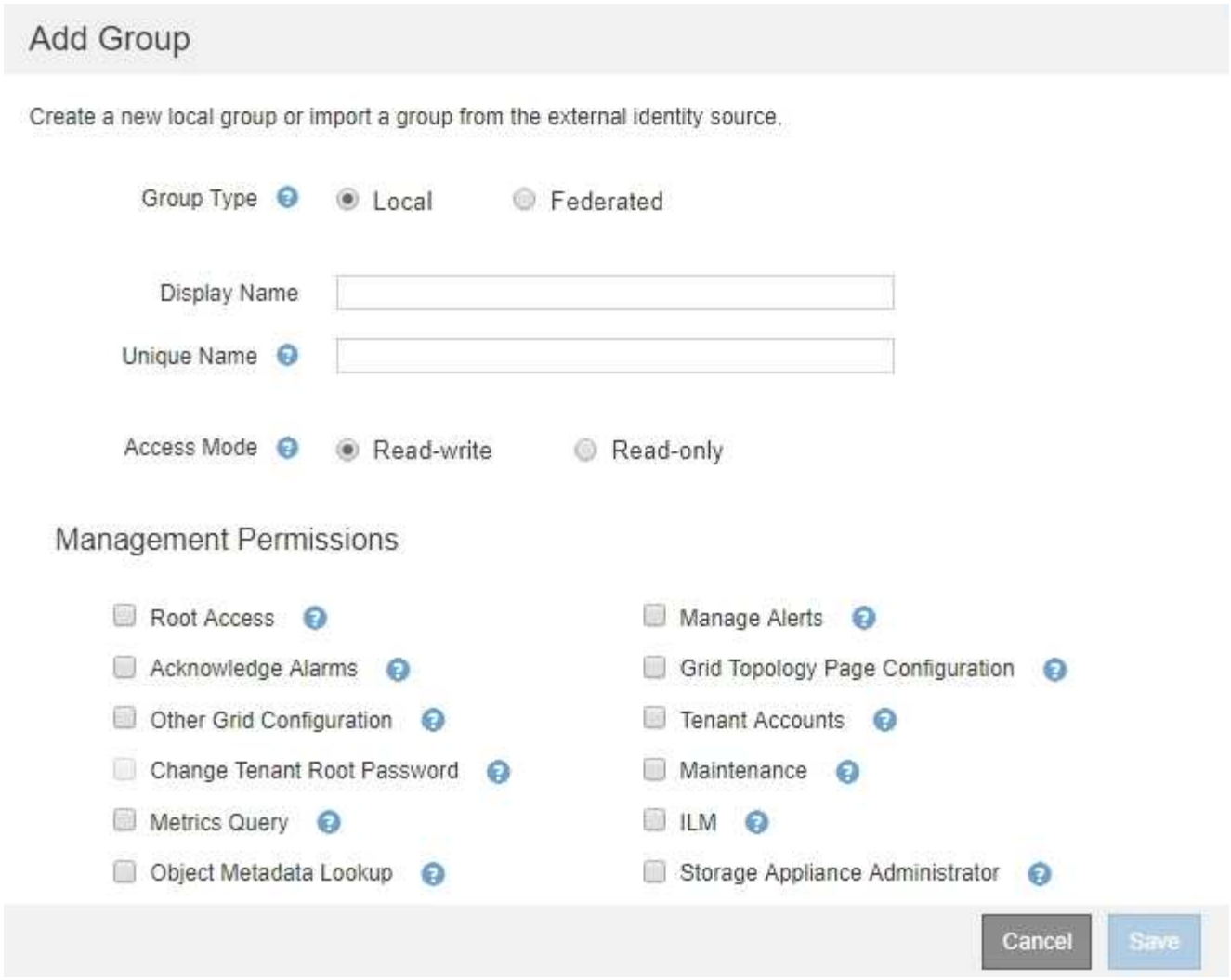
1. Selecione **Configuration** > **Access Control** > **Admin Groups**.

   A página grupos de administração é exibida e lista todos os grupos de administração existentes.




2. Selecione **Adicionar**.

   A caixa de diálogo Adicionar grupo é exibida.




3. Para tipo de grupo, selecione **local** se quiser criar um grupo que será usado somente no StorageGRID ou selecione **federado** se quiser importar um grupo da origem de identidade.
4. Se você selecionou **local**, digite um nome de exibição para o grupo. O nome de exibição é o nome que aparece no Gerenciador de Grade. Por exemplo, "'usuários de Manutenção'" ou "'Administradores de ILM.'"
5. Introduza um nome exclusivo para o grupo.
   - **Local**: Digite o nome exclusivo que você deseja. Por exemplo, "'Administradores ILM.'"
   - **Federated**: Insira o nome do grupo exatamente como ele aparece na origem de identidade configurada.
6. Para **modo de Acesso**, selecione se os usuários do grupo podem alterar as configurações e executar operações no Gerenciador de Grade e na API de Gerenciamento de Grade ou se eles só podem exibir configurações e recursos.
   - **Leitura-escrita** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade. Os usuários locais só de leitura podem alterar suas próprias senhas.

Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

7. Selecione uma ou mais permissões de gerenciamento.

   Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes ao grupo não poderão entrar no StorageGRID.

8. Selecione **Guardar**.

   O novo grupo é criado. Se este for um grupo local, agora você pode adicionar um ou mais usuários. Se este for um grupo federado, a fonte de identidade gerencia quais usuários pertencem ao grupo.

**Informações relacionadas**

"Gerenciamento de usuários locais"

### Permissões do grupo de administração

Ao criar grupos de usuários admin, você seleciona uma ou mais permissões para controlar o acesso a recursos específicos do Gerenciador de Grade. Em seguida, você pode atribuir cada usuário a um ou mais desses grupos de administração para determinar quais tarefas o usuário pode executar.

Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes a esse grupo não poderão entrar no Gerenciador de Grade.

Por padrão, qualquer usuário que pertença a um grupo que tenha pelo menos uma permissão pode executar as seguintes tarefas:

- Faça login no Gerenciador de Grade
- Veja o Dashboard
- Exibir as páginas de nós
- Monitore a topologia da grade
- Ver alertas atuais e resolvidos
- Visualizar alarmes atuais e históricos (sistema legado)
- Alterar sua própria senha (somente usuários locais)
- Visualize determinadas informações nas páginas Configuração e Manutenção

As seções a seguir descrevem as permissões que você pode atribuir ao criar ou editar um grupo de administradores. Qualquer funcionalidade não mencionada explicitamente requer a permissão de acesso root.

#### Acesso à raiz

Essa permissão fornece acesso a todos os recursos de administração de grade.

#### Gerenciar alertas

Essa permissão fornece acesso a opções de gerenciamento de alertas. Os usuários devem ter essa permissão para gerenciar silêncios, notificações de alerta e regras de alerta.

#### Reconhecer alarmes (sistema legado)

Esta permissão fornece acesso para reconhecer e responder a alarmes (sistema legado). Todos os usuários conetados podem visualizar alarmes atuais e históricos.

Se você quiser que um usuário monitore a topologia da grade e reconheça somente alarmes, você deve atribuir essa permissão.

#### Configuração da página de topologia da grelha

Esta permissão fornece acesso às seguintes opções de menu:

- Guias de configuração disponíveis nas páginas em **suporte** > **Ferramentas** > **topologia de grade**.
- **Redefinir contagens de eventos** na guia **nós** > **Eventos**.

#### Outra Configuração de Grade

Esta permissão fornece acesso a opções de configuração de grade adicionais.

> Para ver essas opções adicionais, os usuários também devem ter a permissão de Configuração de Página de topologia de Grade.

- **Alarmes** (sistema legado):
  - Alarmes globais
  - Configuração de e-mail legado
- **ILM**:
  - Pools de armazenamento
  - Classes de armazenamento
- **Configuração** > **Configurações de rede**
  - Custo da ligação
- **Configuração** > **Configurações do sistema**:
  - Opções de exibição
  - Opções de grelha
  - Opções de armazenamento
- **Configuração** > **Monitoramento**:
  - Eventos
- **Suporte**:
  - AutoSupport

#### Contas de inquilino

Esta permissão fornece acesso à página **tenants** > **Tenant Accounts**.

> A versão 1 da API Grid Management (que foi obsoleta) usa essa permissão para gerenciar políticas de grupo de locatários, redefinir senhas de administrador Swift e gerenciar chaves de acesso S3 do usuário raiz.

#### Altere a senha raiz do locatário

Essa permissão fornece acesso à opção **alterar senha de root** na página Contas de locatário, permitindo que você controle quem pode alterar a senha para o usuário raiz local do locatário. Os usuários que não têm essa permissão não podem ver a opção **alterar senha de root**.

> Você deve atribuir a permissão Contas do locatário ao grupo antes de poder atribuir essa permissão.

#### Manutenção

Esta permissão fornece acesso às seguintes opções de menu:

- **Configuração** > **Configurações do sistema**:
  - Nomes de domínio*
  - Certificados de servidor*
- **Configuração** > **Monitoramento**:
  - Auditoria*
- **Configuração** > **Controle de Acesso**:
  - Senhas de grade
- **Manutenção** > **tarefas de manutenção**
  - Descomissionar
  - Expansão
  - Recuperação
- **Manutenção** > **rede**:
  - Servidores DNS*
  - Rede de rede*
  - Servidores NTP*
- **Manutenção** > **sistema**:
  - Licença*
  - Pacote de recuperação
  - Atualização de software
- **Suporte** > **Ferramentas**:
  - Registos
- Os usuários que não têm a permissão Manutenção podem exibir, mas não editar, as páginas marcadas com um asterisco.

#### Consulta de métricas

Esta permissão fornece acesso à página **suporte** > **Ferramentas** > **métricas**. Essa permissão também fornece acesso a consultas de métricas personalizadas do Prometheus usando a seção **Metrics** da API Grid Management.

#### ILM

Esta permissão fornece acesso às seguintes opções de menu **ILM**:

- **Codificação de apagamento**
- **Regras**
- **Políticas**
- **Regiões**

> O acesso às opções de menu **ILM** > **Storage Pools** e **ILM** > **Storage grades** é controlado pelas outras permissões de Configuração de Grade e topologia de Grade Page Configuration.

#### Pesquisa de metadados de objetos

Esta permissão fornece acesso à opção de menu **ILM** > **Object Metadata Lookup**.

#### Administrador do dispositivo de armazenamento

Essa permissão fornece acesso ao Gerenciador de sistemas do e-Series SANtricity em dispositivos de storage por meio do Gerenciador de Grade.

#### Interação entre permissões e modo de acesso

Para todas as permissões, a configuração modo de acesso do grupo determina se os usuários podem alterar configurações e executar operações ou se eles podem exibir somente as configurações e recursos relacionados. Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

#### Desativando recursos da API de Gerenciamento de Grade

Você pode usar a API de gerenciamento de grade para desativar completamente certos recursos no sistema StorageGRID. Quando um recurso é desativado, ninguém pode receber permissões para executar as tarefas relacionadas a esse recurso.

**Sobre esta tarefa**

O sistema de funcionalidades desativadas permite-lhe impedir o acesso a determinadas funcionalidades no sistema StorageGRID. A desativação de um recurso é a única maneira de impedir que o usuário raiz ou os usuários que pertencem a grupos de administração com a permissão de acesso root possam usar esse recurso.

Para entender como essa funcionalidade pode ser útil, considere o seguinte cenário:

*A empresa A é um provedor de serviços que aluga a capacidade de armazenamento de seu sistema StorageGRID criando contas de inquilino. Para proteger a segurança dos objetos de seus arrendatários, a empresa A quer garantir que seus próprios funcionários nunca possam acessar qualquer conta de locatário depois que a conta tiver sido implantada.*

*A empresa A pode atingir esse objetivo usando o sistema Deactivate Features na API Grid Management. Ao desativar completamente o recurso **Change Tenant Root Password** no Gerenciador de Grade (tanto a UI quanto a API), a empresa A pode garantir que nenhum usuário Admin - incluindo o usuário root e usuários pertencentes a grupos com a permissão de acesso root - pode alterar a senha para o usuário root de qualquer conta de locatário.*

### Reativando as funcionalidades desativadas

Por padrão, você pode usar a API de Gerenciamento de Grade para reativar um recurso que foi desativado. No entanto, se você quiser impedir que os recursos desativados sejam reativados, você pode desativar o próprio recurso **activateFeatures**.

> O recurso **activateFeatures** não pode ser reativado. Se você decidir desativar esse recurso, esteja ciente de que você perderá permanentemente a capacidade de reativar quaisquer outros recursos desativados. Você deve entrar em Contato com o suporte técnico para restaurar qualquer funcionalidade perdida.

Para obter detalhes, consulte as instruções para a implementação de aplicativos cliente S3 ou Swift.

**Passos**

1. Acesse a documentação do Swagger para a API de gerenciamento de grade.
2. Localize o endpoint Deactivate Features
3. Para desativar um recurso, como **alterar senha de root do locatário**, envie um corpo para a API assim:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Quando a solicitação estiver concluída, o recurso alterar senha raiz do locatário é desativado. A permissão de gerenciamento de senha raiz do locatário de alteração não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário falhará com "'403 Forbidden.'"

4. Para reativar todos os recursos, envie um corpo para a API assim:

```
{ "grid": null }
```

Quando esta solicitação estiver concluída, todos os recursos, incluindo o recurso alterar senha de root do locatário, são reativados. A permissão de gerenciamento de senha de raiz do locatário de alteração agora aparece na interface do usuário e qualquer solicitação de API que tente alterar a senha de raiz de um locatário será bem-sucedida, assumindo que o usuário tenha a permissão de gerenciamento de senha de raiz do locatário ou altere a permissão de gerenciamento de senha de raiz do locatário.

> O exemplo anterior faz com que os recursos *All* desativados sejam reativados. Se outros recursos tiverem sido desativados que devem permanecer desativados, você deverá especificá-los explicitamente na SOLICITAÇÃO PUT. Por exemplo, para reativar o recurso alterar senha de raiz do locatário e continuar a desativar o recurso de reconhecimento de alarme, envie esta SOLICITAÇÃO DE COMPRA:

```
{ "grid": { "alarmAcknowledgment": true } }
```

**Informações relacionadas**

"Usando a API de gerenciamento de grade"

### Modificando um grupo de administração

Você pode modificar um grupo de administração para alterar as permissões associadas ao grupo. Para grupos de administração locais, também é possível atualizar o nome de exibição.

**O que você vai precisar**

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

**Passos**

1. Selecione **Configuration** > **Access Control** > **Admin Groups**.
2. Selecione o grupo.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Editar**.
4. Opcionalmente, para grupos locais, digite o nome do grupo que aparecerá para os usuários, por exemplo, "'usuários de Manutenção.'"

   Não é possível alterar o nome exclusivo, que é o nome do grupo interno.

5. Opcionalmente, altere o modo de acesso do grupo.
   - **Leitura-escrita** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
   - **Somente leitura**: Os usuários só podem visualizar configurações e recursos. Eles não podem fazer alterações ou executar quaisquer operações no Gerenciador de Grade ou na API de Gerenciamento de Grade. Os usuários locais só de leitura podem alterar suas próprias senhas.

   > Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

6. Opcionalmente, adicione ou remova permissões de grupo.

   Consulte informações sobre as permissões do grupo de administração.

7. Selecione **Guardar**.

**Informações relacionadas**

Permissões do grupo de administração

### Eliminar um grupo de administração

Você pode excluir um grupo de administração quando quiser remover o grupo do sistema e remover todas as permissões associadas ao grupo. A exclusão de um grupo de administração remove quaisquer usuários de administrador do grupo, mas não exclui os usuários de administrador.

**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**

Quando você exclui um grupo, os usuários atribuídos a esse grupo perderão todos os Privileges de Acesso ao Gerenciador de Grade, a menos que sejam concedidos Privileges por um grupo diferente.

**Passos**

1. Selecione **Configuration** > **Access Control** > **Admin Groups**.
2. Selecione o nome do grupo.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Selecione **Remover**.
4. Selecione **OK**.

## Gerenciamento de usuários locais

Você pode criar usuários locais e atribuí-los a grupos de administração locais para determinar quais recursos do Gerenciador de Grade esses usuários podem acessar.

O Gerenciador de Grade inclui um usuário local predefinido, chamado "root". Embora você possa adicionar e remover usuários locais, não é possível remover o usuário root.

Se o logon único (SSO) tiver sido ativado, os usuários locais não poderão fazer login no StorageGRID.

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

### Criando um usuário local

Se tiver criado grupos de administração locais, pode criar um ou mais utilizadores locais e atribuir cada utilizador a um ou mais grupos. As permissões do grupo controlam quais recursos do Gerenciador de Grade o usuário pode acessar.

**Sobre esta tarefa**

Você só pode criar usuários locais e só pode atribuir esses usuários a grupos de administração locais. Usuários federados e grupos federados são gerenciados usando a fonte de identidade externa.

**Passos**

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Clique em **criar**.
3. Introduza o nome de apresentação do utilizador, o nome exclusivo e a palavra-passe.
4. Atribua o usuário a um ou mais grupos que governam as permissões de acesso.

   A lista de nomes de grupos é gerada a partir da tabela grupos.

5. Clique em **Salvar**.

**Informações relacionadas**

"Gerenciando grupos de administradores"

### Modificando a conta de um usuário local

Você pode modificar a conta de um usuário de administrador local para atualizar o nome de exibição do usuário ou a associação de grupo. Você também pode impedir temporariamente que um usuário acesse o sistema.

**Sobre esta tarefa**

Só pode editar utilizadores locais. Os detalhes do usuário federados são sincronizados automaticamente com a fonte de identidade externa.

**Passos**

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Selecione o utilizador que pretende editar.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Editar**.
4. Opcionalmente, faça alterações no nome ou na associação ao grupo.
5. Opcionalmente, para impedir que o usuário acesse o sistema temporariamente, marque **Negar acesso**.
6. Clique em **Salvar**.

   As novas configurações são aplicadas da próxima vez que o usuário sair e, em seguida, voltar a entrar no Gerenciador de Grade.

### Eliminar a conta de um utilizador local

Você pode excluir contas de usuários locais que não precisam mais de acesso ao Gerenciador de Grade.

**Passos**

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Selecione o utilizador local que pretende eliminar.

   Não é possível eliminar o utilizador local raiz predefinido.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **Remover**.
4. Clique em **OK**.

### Alterar a palavra-passe de um utilizador local

Os usuários locais podem alterar suas próprias senhas usando a opção **alterar senha** no banner do Gerenciador de Grade. Além disso, os usuários que têm acesso à página usuários administradores podem

alterar senhas para outros usuários locais.

**Sobre esta tarefa**

Você pode alterar senhas apenas para usuários locais. Os usuários federados devem alterar suas próprias senhas na fonte de identidade externa.

**Passos**

1. Selecione **Configuration** > **Access Control** > **Admin Users**.
2. Na página usuários, selecione o usuário.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Em seguida, você pode usar o recurso Localizar do navegador para procurar um item específico nas linhas exibidas atualmente.

3. Clique em **alterar senha**.
4. Introduza e confirme a palavra-passe e clique em **Guardar**.

## 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.

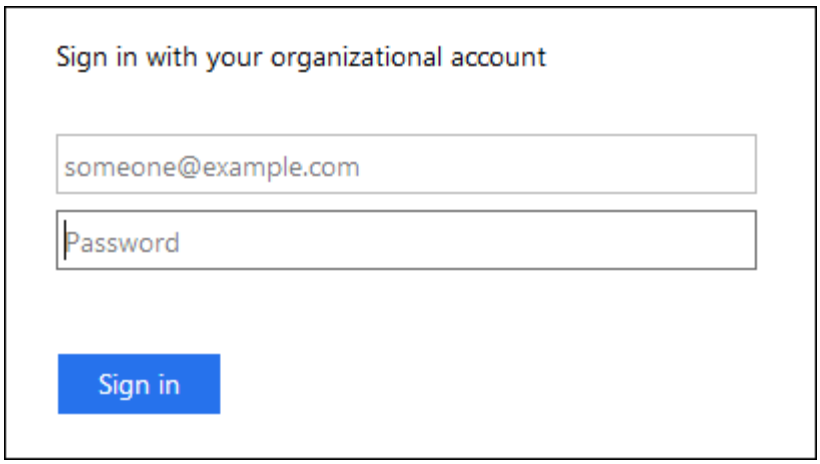
   - Se esta for a primeira vez que você acessou o URL neste navegador, será solicitado um ID de conta:


- 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:


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:




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 conetado 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 conetado 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 conetado 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 |

| Se você estiver conetado a… | E você sai de… | Você está logado fora de… |
| --- | --- | --- |
| 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 conetado 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 ative 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 conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você está usando o ative Directory como fonte de identidade federada e o AD FS como provedor de identidade.

  "Requisitos para o uso de logon único"

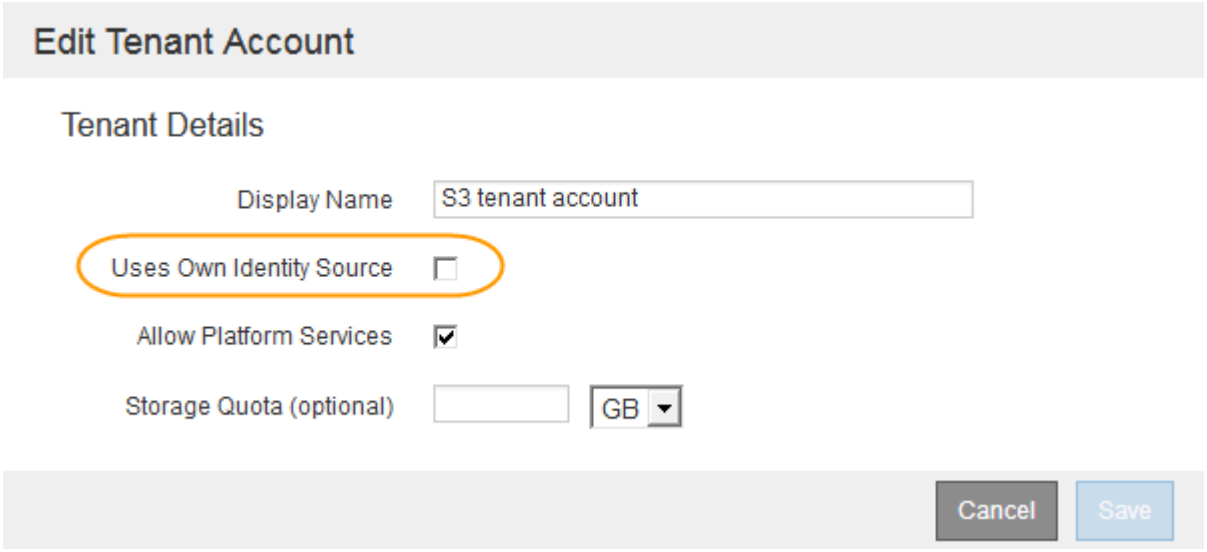
**Passos**

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 ative 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**.




   A página Contas do locatário é exibida.
   a. Selecione a conta de locatário, clique em **entrar** e faça login na conta de locatário como usuário raiz local.
   b. No Gerenciador do Locatário, clique em **Controle de Acesso** > **grupos**.
   c. Certifique-se de que pelo menos um grupo federado do Gerenciador de Grade recebeu a permissão de acesso raiz para esse locatário.
   d. Terminar sessão.
   e. 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 ative 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 conetado 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.

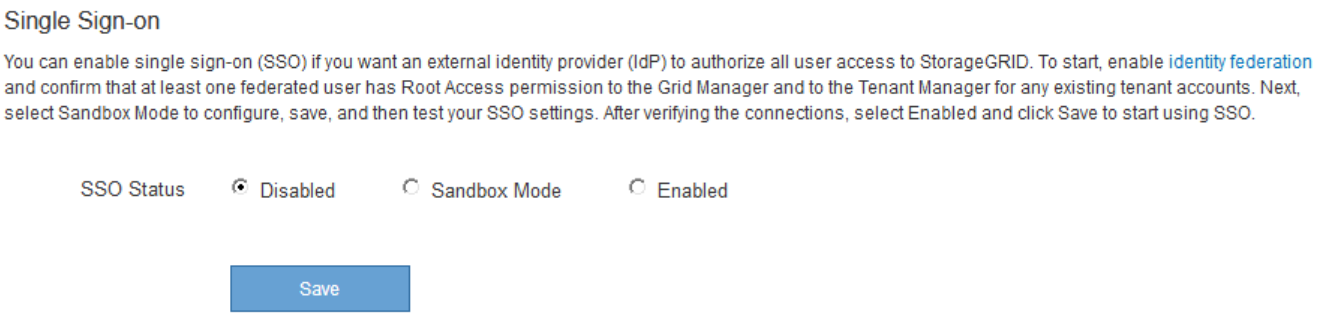
O modo Sandbox facilita a execução desta configuração de back-and-forth e testar todas as suas configurações antes de ativar o SSO.

> 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.




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.

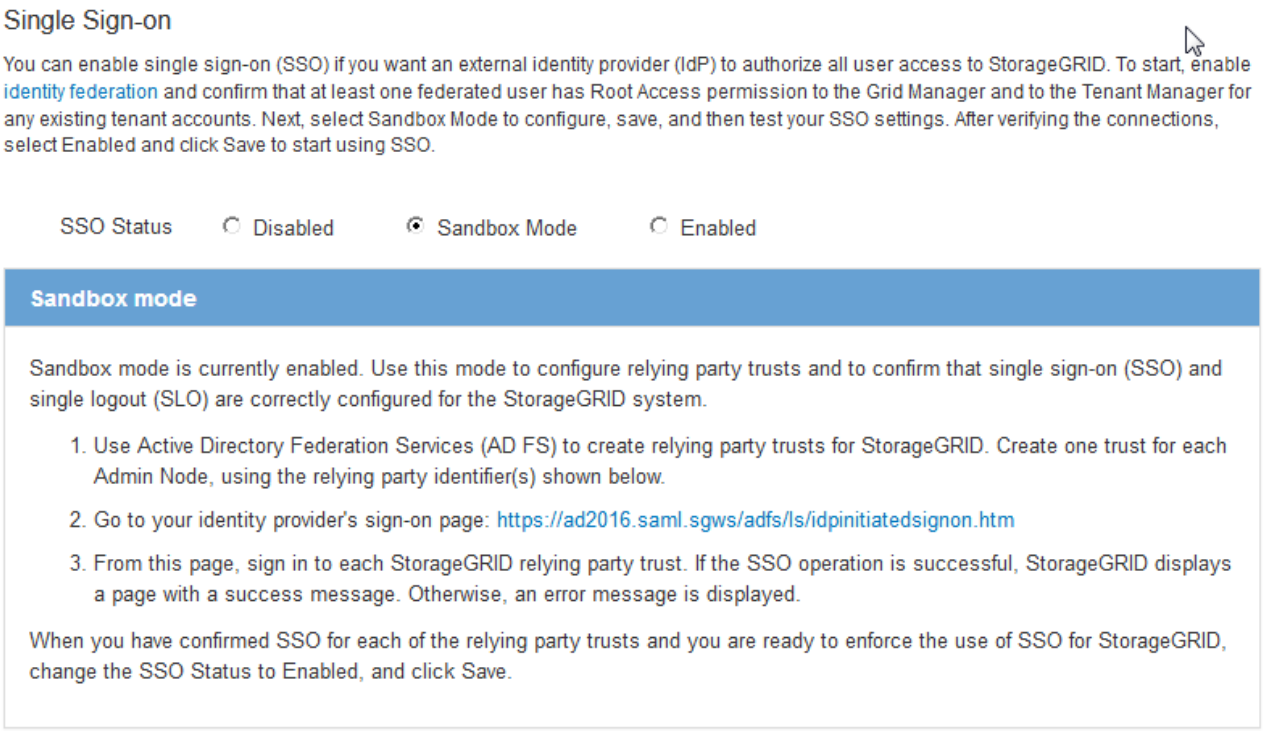
4. Na seção parte dependente, especifique o identificador de parte dependente que você usará para nós de administrador do StorageGRID quando você configurar confianças de parte dependentes.

   - 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).

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

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

   e. Para o Attribute Store, selecione **ative Directory**.
   f. Na coluna LDAP Attribute da tabela Mapping, digite **objectGUID**.
   g. Na coluna Outgoing Claim Type (tipo de reclamação de saída) da tabela Mapeamento, selecione **Name ID** (ID do nome) na lista suspensa.
   h. Clique em **Finish** e clique em **OK**.
8. 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.

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 **ative 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 conetado 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.

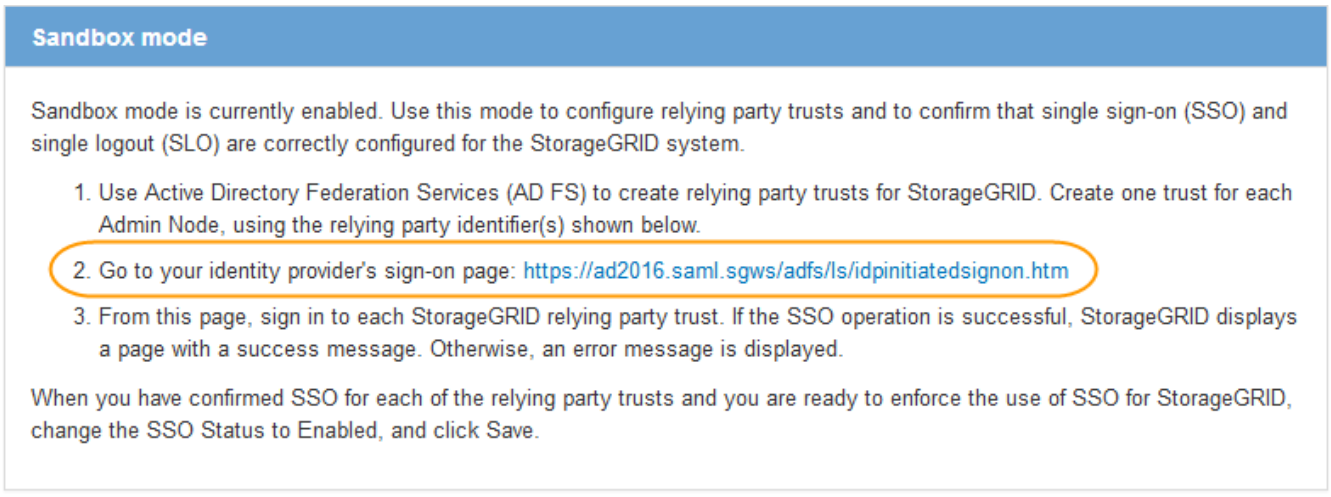
**Passos**

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.

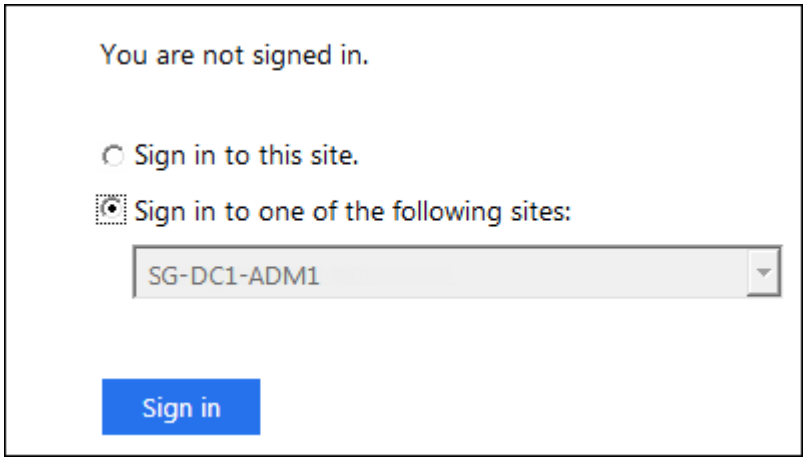
2. Nas instruções para o modo sandbox, localize o link para a página de logon do provedor de identidade.

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




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**.




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.

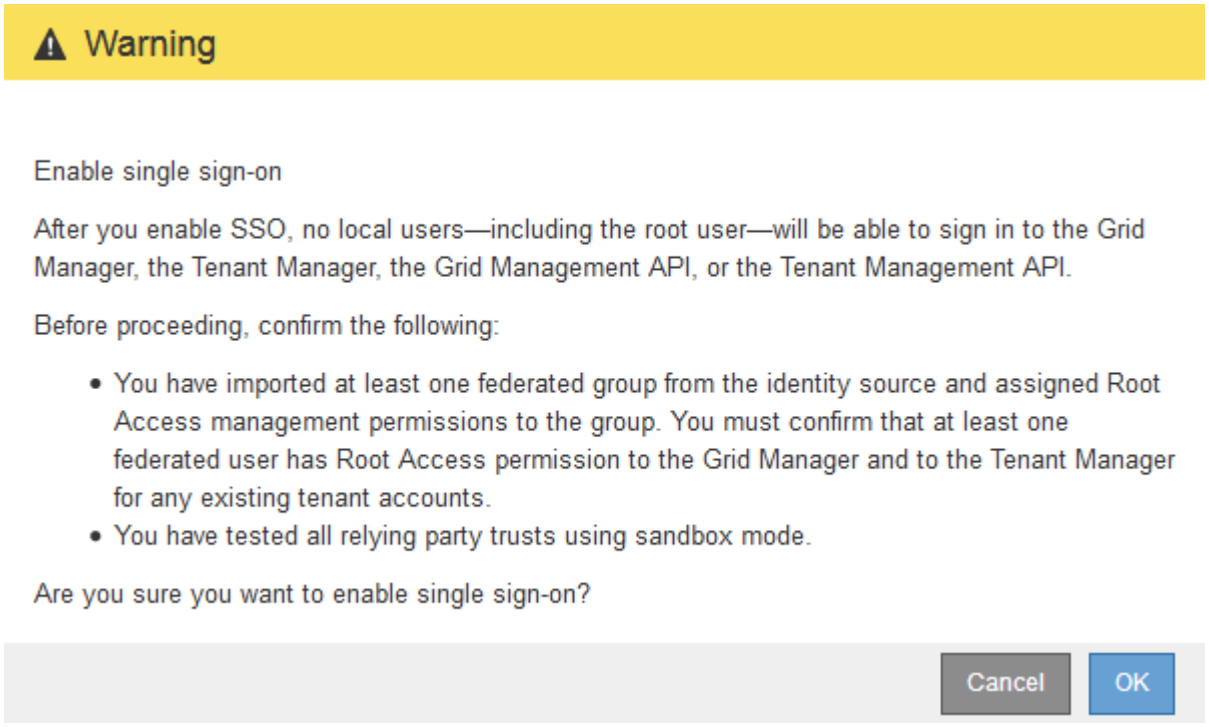
**Passos**

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.




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

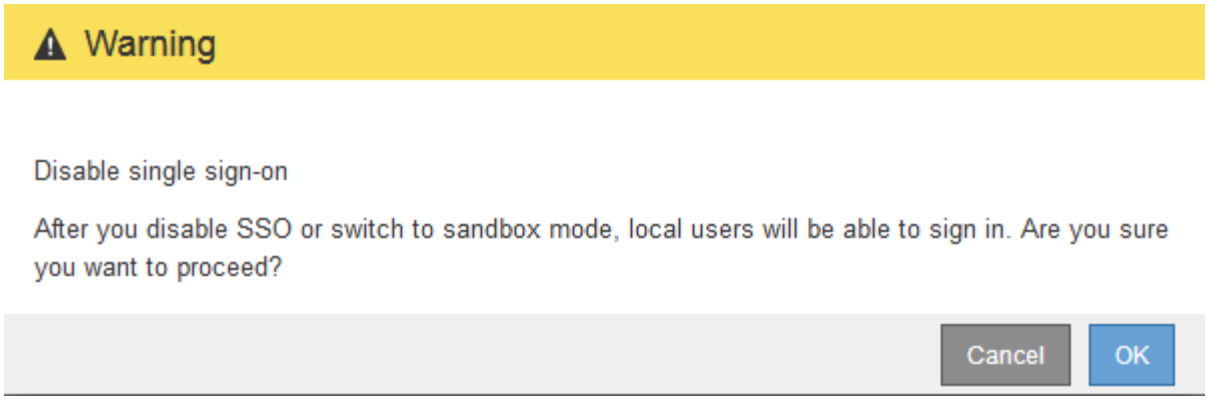
**Passos**

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.




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"

## Configurando certificados de cliente de administrador

Você pode usar certificados de cliente para permitir que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. Os certificados de cliente fornecem uma maneira segura de usar ferramentas externas para monitorar o StorageGRID.

Se você precisar acessar o StorageGRID usando uma ferramenta de monitoramento externa, você deve carregar ou gerar um certificado de cliente usando o Gerenciador de Grade e copiar as informações do certificado para a ferramenta externa.

### Adicionando certificados de cliente administrador

Para adicionar um certificado de cliente, você pode fornecer seu próprio certificado ou gerar um usando o Gerenciador de Grade.

**O que você vai precisar**

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve saber o endereço IP ou o nome de domínio do nó Admin.
- Você deve ter configurado o certificado do servidor de interface de gerenciamento do StorageGRID e ter o pacote de CA correspondente
- Se você quiser carregar seu próprio certificado, a chave pública e a chave privada do certificado devem estar disponíveis no computador local.

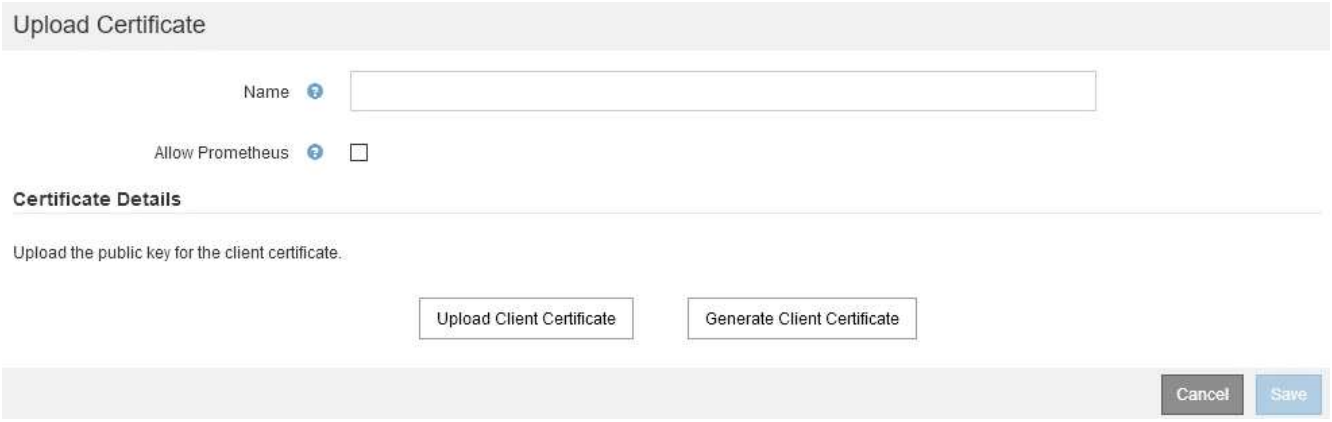
**Passos**

1. No Gerenciador de Grade, selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

   A página certificados de cliente é exibida.


2. Selecione **Adicionar**.

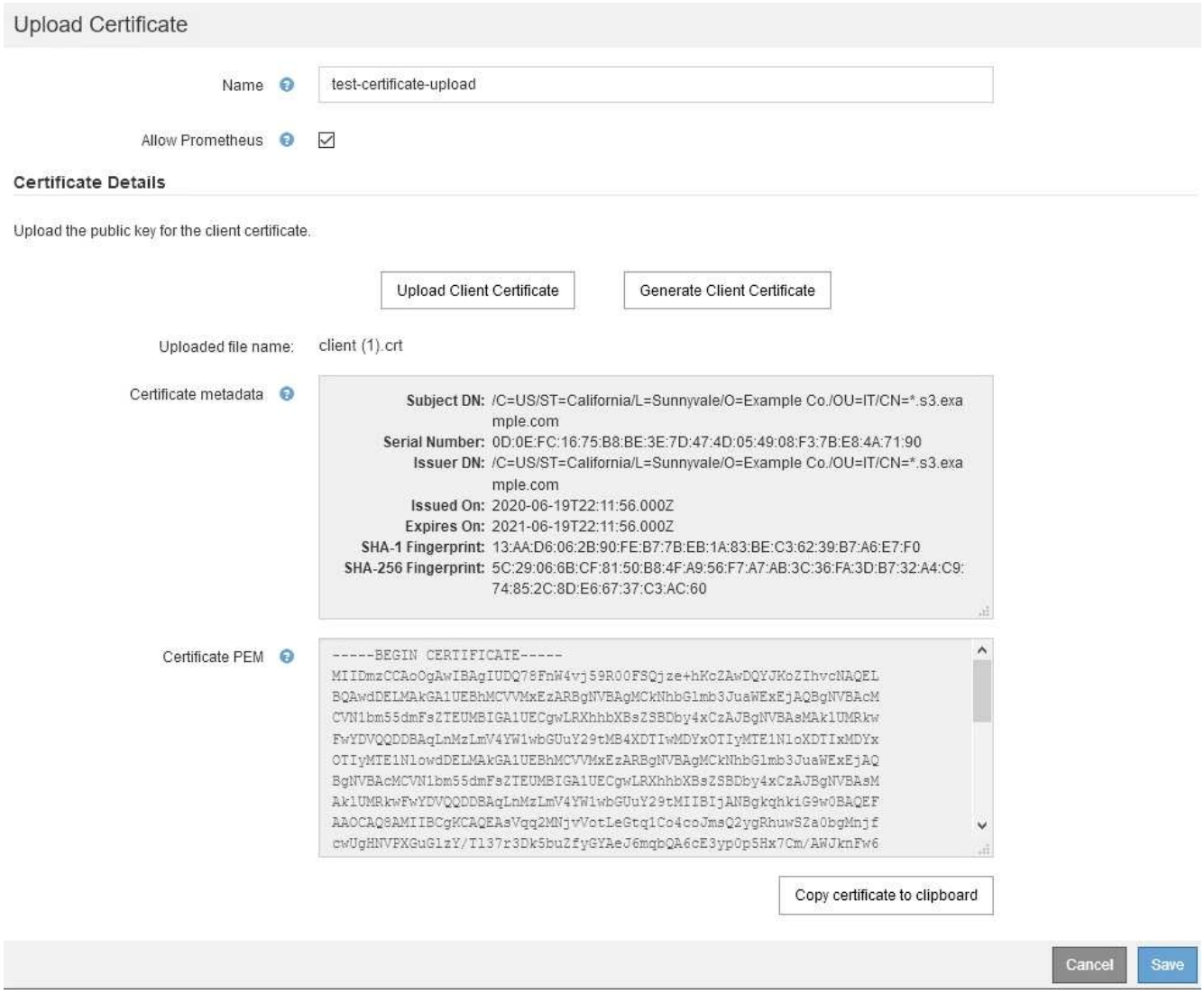
   A página carregar certificado é exibida.




3. Digite um nome entre 1 e 32 carateres para o certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, marque a caixa de seleção **Allow Prometheus**.

5. Carregar ou gerar um certificado:
   a. Para carregar um certificado, vá aqui.
   b. Para gerar um certificado, vá aqui.
6. para carregar um certificado:
   a. Selecione **carregar certificado de cliente**.
   b. Procure a chave pública do certificado.

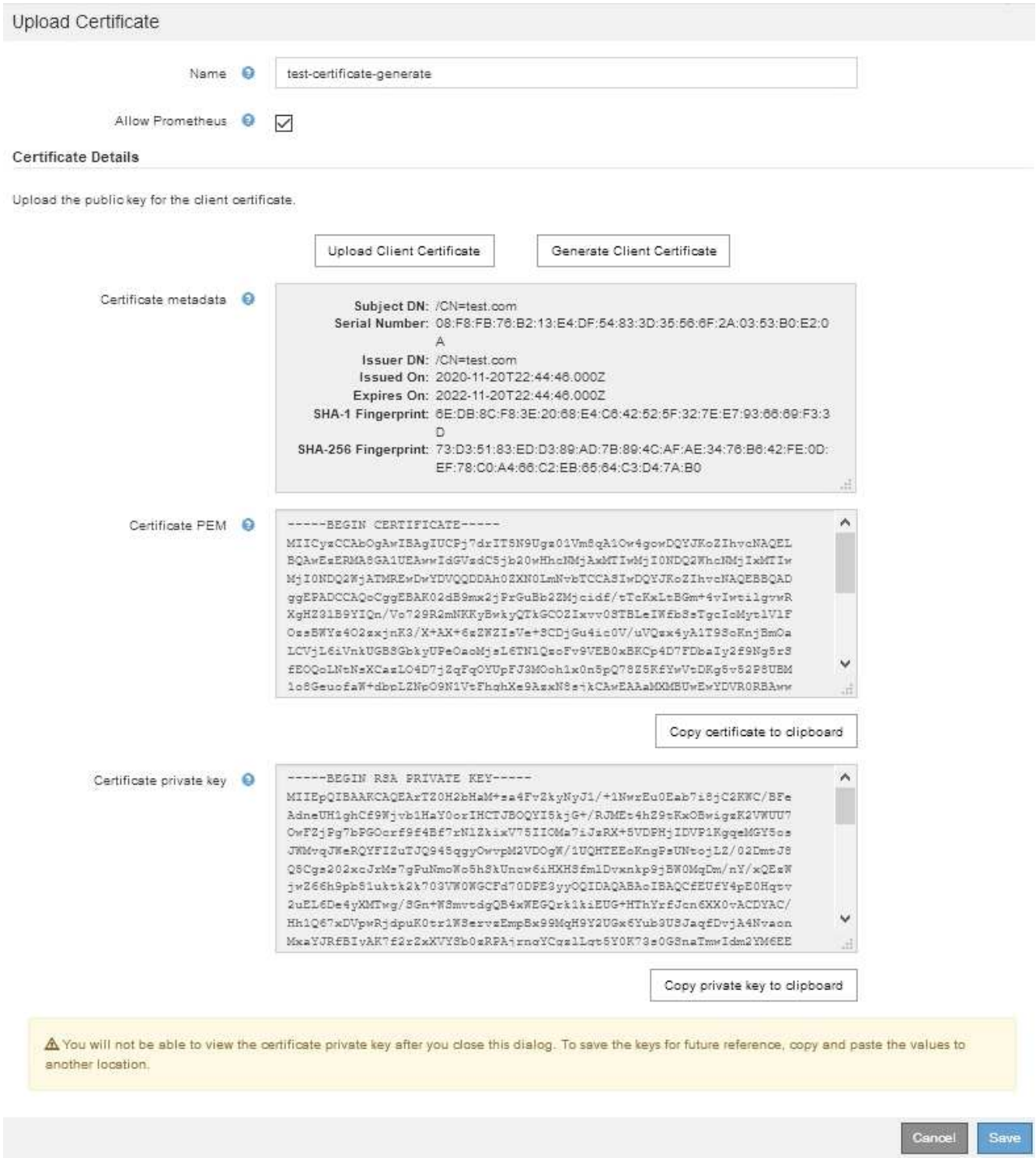
      Depois de carregar a chave pública para o certificado, os campos **metadados do certificado** e **PEM** do certificado são preenchidos.




   a. Selecione **Copiar certificado para a área de transferência** e cole o certificado na ferramenta de monitoramento externa.
   b. Use uma ferramenta de edição para copiar e colar a chave privada na sua ferramenta de monitoramento externo.
   c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.
7. para gerar um certificado:

a. Selecione **Generate Client Certificate**.
b. Introduza o nome de domínio ou o endereço IP do nó de administração.
c. Opcionalmente, insira um assunto X,509, também chamado de Nome distinto (DN), para identificar o administrador que possui o certificado.
d. Opcionalmente, selecione o número de dias em que o certificado é válido. O padrão é de 730 dias.
e. Selecione **Generate**.

   Os campos **metadados do certificado**, **PEM** do certificado e **chave privada do certificado** são preenchidos.




a. Selecione **Copiar certificado para a área de transferência** e cole o certificado na ferramenta de monitoramento externa.

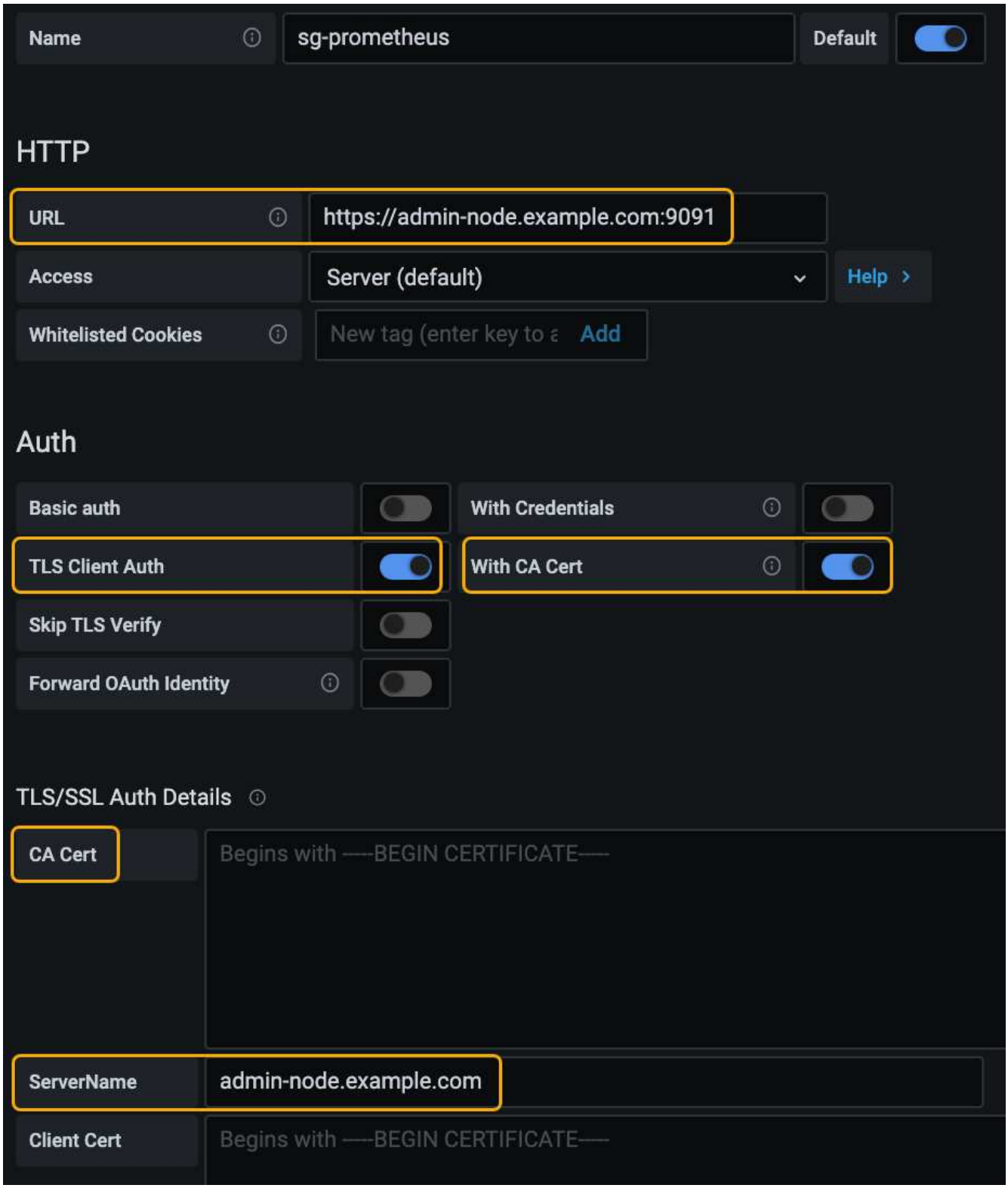
b. Selecione **Copie a chave privada para a área de transferência** e cole a chave na ferramenta de monitoramento externa.

> Não será possível visualizar a chave privada depois de fechar a caixa de diálogo. Copie a chave para um local seguro.

c. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.

8. Configure as seguintes configurações em sua ferramenta de monitoramento externo, como Grafana.

   Um exemplo de Grafana é mostrado na seguinte captura de tela:




   a. **Nome**: Insira um nome para a conexão.

      O StorageGRID não requer essas informações, mas você deve fornecer um nome para testar a conexão.

b. **URL**: Insira o nome de domínio ou o endereço IP do nó Admin. Especifique HTTPS e porta 9091.

   Por exemplo: `https://admin-node.example.com:9091`

c. Ative **TLS Client Authorization** e **with CA Cert**.

d. Copie e cole o certificado do servidor de interface de gerenciamento ou o pacote CA para **CA Cert** em Detalhes de autenticação TLS/SSL.

e. **ServerName**: Insira o nome de domínio do nó Admin.

   O nome do servidor deve corresponder ao nome de domínio como aparece no certificado do servidor de interface de gerenciamento.

f. Salve e teste o certificado e a chave privada que você copiou do StorageGRID ou de um arquivo local.

   Agora você pode acessar as métricas Prometheus do StorageGRID com sua ferramenta de monitoramento externo.

Para obter informações sobre as métricas, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

**Informações relacionadas**

"Usando certificados de segurança do StorageGRID"

"Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário"

"Monitorizar Resolução de problemas"

### Editando certificados de cliente do administrador

Você pode editar um certificado para alterar seu nome, ativar ou desativar o acesso Prometheus ou carregar um novo certificado quando o atual expirar.

**O que você vai precisar**

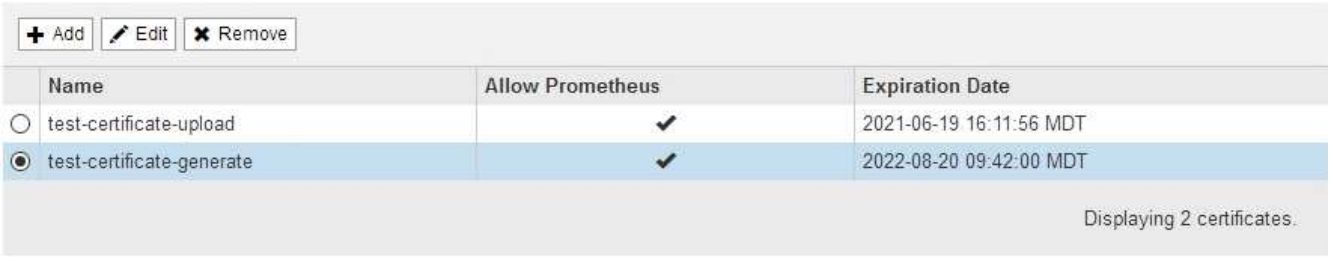
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve saber o endereço IP ou o nome de domínio do nó Admin.
- Se você quiser carregar um novo certificado e uma chave privada, eles devem estar disponíveis no computador local.

**Passos**

1. Selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

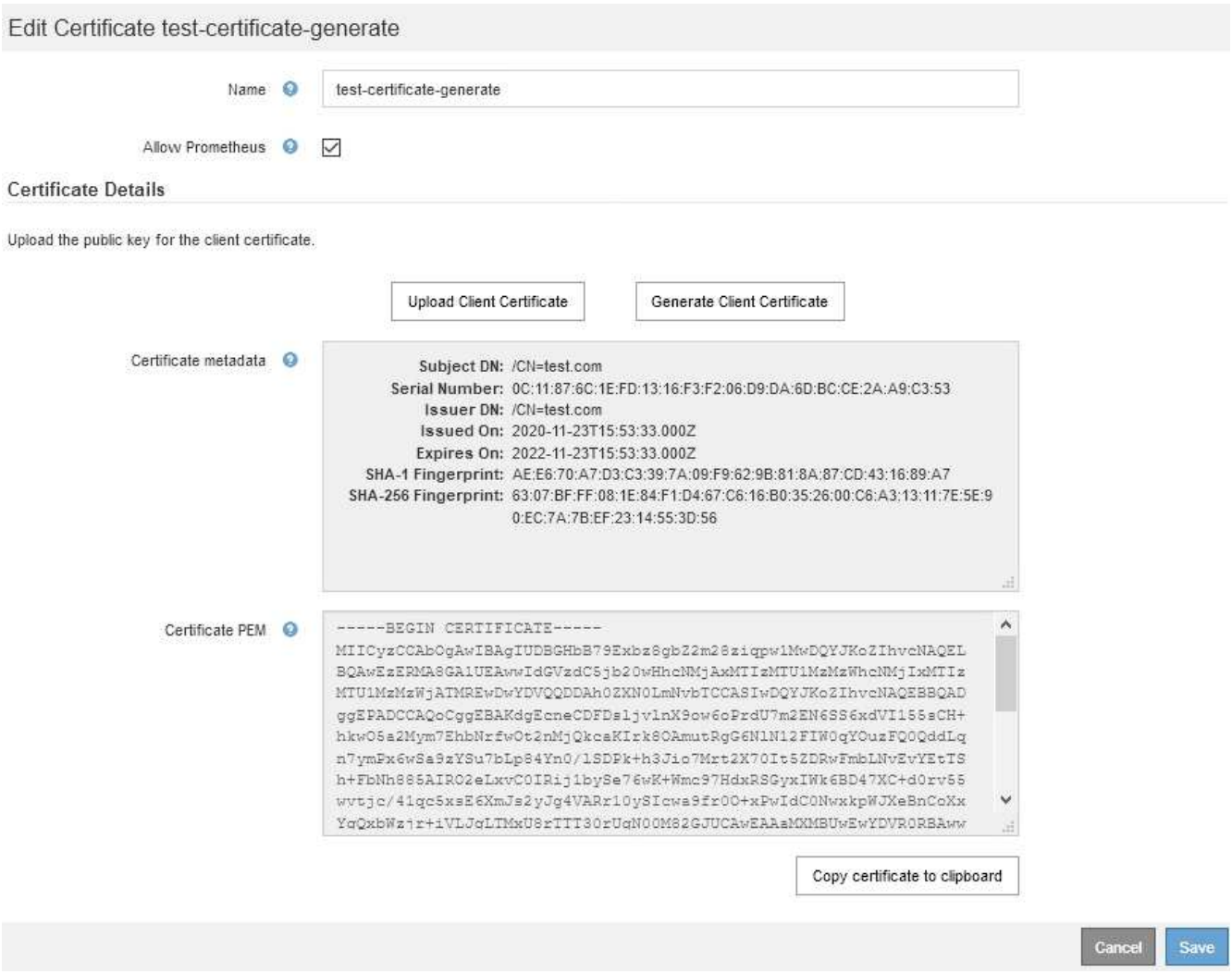
   A página certificados de cliente é exibida. Os certificados existentes são listados.

   As datas de expiração do certificado são listadas na tabela. Se um certificado expirar em breve ou já estiver expirado, uma mensagem será exibida na tabela e um alerta será acionado.




2. Selecione o botão de opção à esquerda do certificado que deseja editar.
3. Selecione **Editar**.

   A caixa de diálogo Editar certificado é exibida.




4. Faça as alterações desejadas no certificado.
5. Selecione **Salvar** para salvar o certificado no Gerenciador de Grade.
6. Se você carregou um novo certificado:
   a. Selecione **Copiar certificado para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.
   b. Use uma ferramenta de edição para copiar e colar a nova chave privada na sua ferramenta de monitoramento externo.

c. Salve e teste o certificado e a chave privada em sua ferramenta de monitoramento externa.

7. Se você gerou um novo certificado:
   a. Selecione **Copiar certificado para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.
   b. Selecione **Copiar chave privada para a área de transferência** para colar o certificado em sua ferramenta de monitoramento externa.

      Não será possível visualizar ou copiar a chave privada depois de fechar a caixa de diálogo. Copie a chave para um local seguro.

   c. Salve e teste o certificado e a chave privada em sua ferramenta de monitoramento externa.

### Removendo certificados de cliente de administrador

Se você não precisar mais de um certificado, você pode removê-lo.

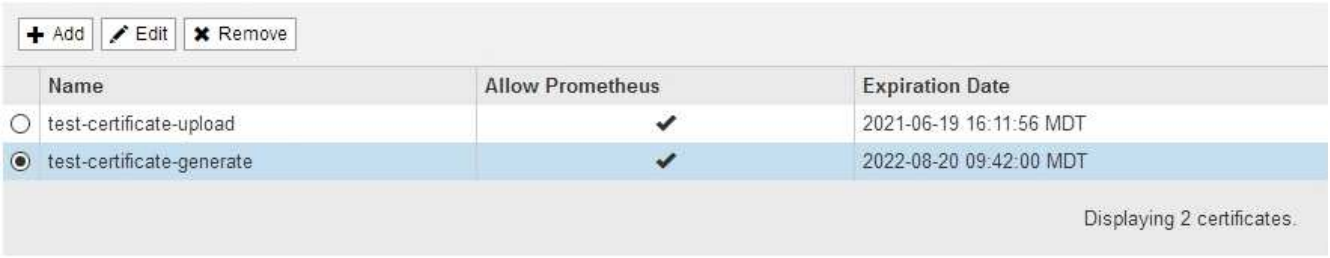
**O que você vai precisar**

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

**Passos**

1. Selecione **Configuração** > **Controle de Acesso** > **certificados de Cliente**.

   A página certificados de cliente é exibida. Os certificados existentes são listados.




2. Selecione o botão de opção à esquerda do certificado que deseja remover.
3. Selecione **Remover**.

   É apresentada uma caixa de diálogo de confirmação.


4. Selecione **OK**.

O certificado é removido.

# Configurando servidores de gerenciamento de chaves

Você pode configurar um ou mais servidores de gerenciamento de chaves externos (KMS) para proteger os dados em nós de dispositivo especialmente configurados.

## O que é um servidor de gerenciamento de chaves (KMS)?

Um servidor de gerenciamento de chaves (KMS) é um sistema externo de terceiros que fornece chaves de criptografia para nós de dispositivos StorageGRID no site associado do StorageGRID usando o Protocolo de interoperabilidade de Gerenciamento de chaves (KMIP).

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó de dispositivo StorageGRID que tenha a configuração **criptografia de nó** ativada durante a instalação. O uso de servidores de gerenciamento de chaves com esses nós de dispositivo permite que você proteja seus dados mesmo que um dispositivo seja removido do data center. Depois que os volumes do dispositivo são criptografados, você não pode acessar nenhum dado no dispositivo, a menos que o nó possa se comunicar com o KMS.

> ⓘ O StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar os nós do dispositivo. Se você pretende usar um servidor de gerenciamento de chaves externo para proteger dados do StorageGRID, você deve entender como configurar esse servidor e entender como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo dessas instruções. Se precisar de ajuda, consulte a documentação do servidor de gerenciamento de chaves ou entre em Contato com o suporte técnico.

## Rever os métodos de encriptação StorageGRID

O StorageGRID fornece várias opções para criptografar dados. Você deve analisar os métodos disponíveis para determinar quais métodos atendem aos requisitos de proteção de dados.

A tabela fornece um resumo de alto nível dos métodos de criptografia disponíveis no StorageGRID.

| Opção de criptografia | Como funciona | Aplica-se a |
| --- | --- | --- |
| Servidor de gerenciamento de chaves (KMS) no Grid Manager | Configure um servidor de gerenciamento de chaves para o site StorageGRID (**Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**) e habilite a criptografia de nó para o dispositivo. Em seguida, um nó de dispositivo se coneta ao KMS para solicitar uma chave de criptografia de chave (KEK). Essa chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume. | Nós de dispositivo que têm **Node Encryption** ativado durante a instalação. Todos os dados no dispositivo são protegidos contra perda física ou remoção do data center. Pode ser usado com alguns dispositivos de armazenamento e serviços StorageGRID. |
| Conduza a segurança no Gerenciador de sistemas do SANtricity | Se o recurso Segurança da unidade estiver habilitado para um dispositivo de armazenamento, você poderá usar o Gerenciador de sistema do SANtricity para criar e gerenciar a chave de segurança. A chave é necessária para aceder aos dados nas unidades seguras. | Dispositivos de storage com unidades Full Disk Encryption (FDE) ou unidades FIPS (Federal Information Processing Standard). Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de armazenamento ou com qualquer dispositivo de serviço.<br><br>"SG6000 dispositivos de armazenamento"<br><br>"SG5700 dispositivos de armazenamento"<br><br>"SG5600 dispositivos de armazenamento" |
| Opção de grade de criptografia de objetos armazenados | A opção **Stored Object Encryption** pode ser ativada no Grid Manager (**Configuration** > **System Settings** > **Grid Options**). Quando ativado, todos os novos objetos que não são criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão. | Dados de objeto S3 e Swift recém-ingeridos.os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.<br><br>"Configurando a criptografia de objeto armazenado" |

| Opção de criptografia | Como funciona | Aplica-se a |
| --- | --- | --- |
| Criptografia de bucket do S3 | Você emite uma solicitação de criptografia PUT Bucket para habilitar a criptografia para o bucket. Todos os novos objetos que não são criptografados no nível do objeto são criptografados durante a ingestão. | Apenas dados de objetos S3 recém-ingeridos.a encriptação tem de ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.<br><br>"Use S3" |
| Criptografia do lado do servidor de objetos S3 (SSE) | Você emite uma solicitação S3 para armazenar um objeto e incluir o `x-amz-server-side-encryption` cabeçalho da solicitação. | Somente dados de objeto S3 recém-ingeridos.a criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.<br><br>StorageGRID gerencia as chaves.<br><br>"Use S3" |
| Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C) | Você emite uma solicitação S3 para armazenar um objeto e incluir três cabeçalhos de solicitação.<br><br>• `x-amz-server-side-encryption-customer-algorithm`<br>• `x-amz-server-side-encryption-customer-key`<br>• `x-amz-server-side-encryption-customer-key-MD5` | Somente dados de objeto S3 recém-ingeridos.a criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.<br><br>As chaves são gerenciadas fora do StorageGRID.<br><br>"Use S3" |
| Criptografia de volume externo ou datastore | Você usa um método de criptografia fora do StorageGRID para criptografar um volume ou armazenamento de dados inteiro, se sua plataforma de implantação o suportar. | Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou datastore seja criptografado.<br><br>Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados. |

| Opção de criptografia | Como funciona | Aplica-se a |
| --- | --- | --- |
| Criptografia de objetos fora do StorageGRID | Você usa um método de criptografia fora do StorageGRID para criptografar dados e metadados de objetos antes que eles sejam ingeridos no StorageGRID. | Somente dados e metadados de objetos (os dados de configuração do sistema não são criptografados).<br><br>Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.<br><br>"Amazon Simple Storage Service - Guia do desenvolvedor: Protegendo dados usando criptografia do lado do cliente" |

**Usando vários métodos de criptografia**

Dependendo dos seus requisitos, você pode usar mais de um método de criptografia de cada vez. Por exemplo:

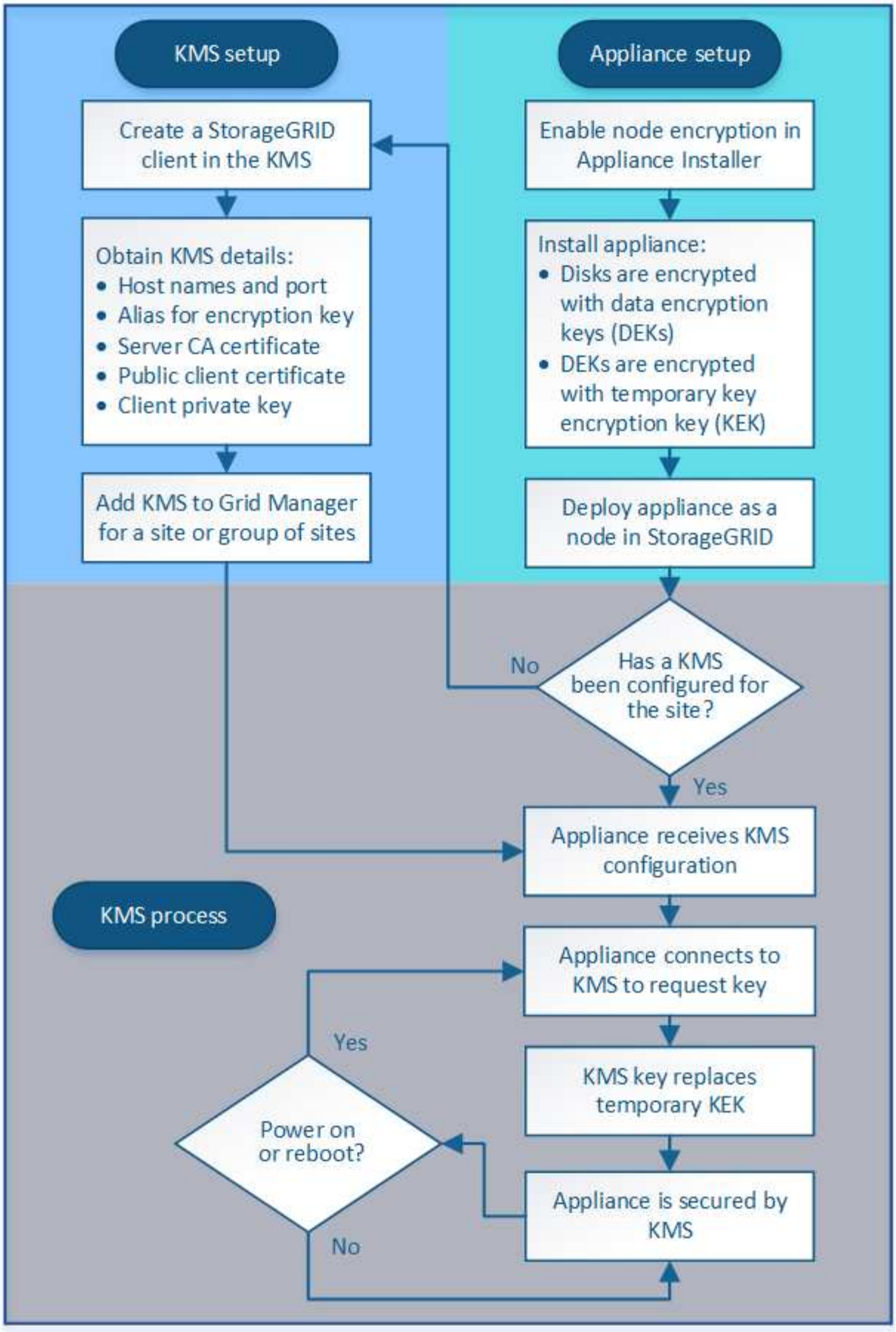
- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança da unidade no Gerenciador de sistema do SANtricity para "criptografar" os dados nas unidades de autocriptografia nos mesmos dispositivos.
- Você pode usar um KMS para proteger dados nos nós do dispositivo e também usar a opção de grade criptografia de objetos armazenados para criptografar todos os objetos quando eles são ingeridos.

Se apenas uma pequena parte de seus objetos exigir criptografia, considere controlar a criptografia no intervalo ou no nível de objeto individual. Ativar vários níveis de criptografia tem um custo de desempenho adicional.

## Visão geral do KMS e da configuração do appliance

Antes de usar um servidor de gerenciamento de chaves (KMS) para proteger dados do StorageGRID nos nós do dispositivo, você deve concluir duas tarefas de configuração: Configurar um ou mais servidores KMS e habilitar a criptografia de nós para os nós do dispositivo. Quando essas duas tarefas de configuração são concluídas, o processo de gerenciamento de chaves ocorre automaticamente.

O fluxograma mostra as etapas de alto nível para usar um KMS para proteger os dados do StorageGRID em nós do dispositivo.




O fluxograma mostra a configuração do KMS e a configuração do appliance ocorrendo em paralelo; no

entanto, você pode configurar os servidores de gerenciamento de chaves antes ou depois de habilitar a criptografia de nó para novos nós de dispositivo, com base em seus requisitos.

### Configurando o servidor de gerenciamento de chaves (KMS)

A configuração de um servidor de gerenciamento de chaves inclui as seguintes etapas de alto nível.

| Passo | Consulte |
|---|---|
| Acesse o software KMS e adicione um cliente para StorageGRID a cada cluster KMS ou KMS. | "Configurando o StorageGRID como um cliente no KMS" |
| Obtenha as informações necessárias para o cliente StorageGRID no KMS. | "Configurando o StorageGRID como um cliente no KMS" |
| Adicione o KMS ao Gerenciador de Grade, atribua-o a um único site ou a um grupo padrão de sites, carregue os certificados necessários e salve a configuração do KMS. | "Adicionar um servidor de gerenciamento de chaves (KMS)" |

### Configurar o aparelho

A configuração de um nó de dispositivo para uso do KMS inclui os seguintes passos de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o Instalador de dispositivos StorageGRID para ativar a configuração **criptografia de nó** para o dispositivo.

   > Não é possível ativar a configuração **criptografia de nó** depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm criptografia de nó ativada.

2. Execute o Instalador de dispositivos StorageGRID. Durante a instalação, uma chave de criptografia de dados aleatórios (DEK) é atribuída a cada volume de dispositivo, da seguinte forma:
   - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco LUKS (Unified Key Setup) do Linux no sistema operacional do dispositivo e não podem ser alteradas.
   - Cada DEK individual é criptografado por uma chave mestra de criptografia (KEK). O KEK inicial é uma chave temporária que criptografa os DEKs até que o dispositivo possa se conetar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

Para obter detalhes, consulte o seguinte:

- "Aparelhos de serviços SG100 SG1000"
- "SG6000 dispositivos de armazenamento"
- "SG5700 dispositivos de armazenamento"
- "SG5600 dispositivos de armazenamento"

#### Processo de criptografia de gerenciamento de chaves (ocorre automaticamente)

A criptografia de gerenciamento de chaves inclui as seguintes etapas de alto nível que são executadas automaticamente.

1. Quando você instala um dispositivo que tem criptografia de nó ativada na grade, o StorageGRID determina se existe uma configuração de KMS para o site que contém o novo nó.
   - Se um KMS já tiver sido configurado para o site, o appliance receberá a configuração do KMS.
   - Se um KMS ainda não tiver sido configurado para o site, os dados no appliance continuarão a ser criptografados pelo KEK temporário até que você configure um KMS para o site e o appliance receba a configuração do KMS.
2. O dispositivo usa a configuração KMS para se conetar ao KMS e solicitar uma chave de criptografia.
3. O KMS envia uma chave de criptografia para o dispositivo. A nova chave do KMS substitui o KEK temporário e agora é usada para criptografar e descriptografar os DEKs para os volumes do dispositivo.

   > Todos os dados existentes antes do nó de dispositivo criptografado se conetarem ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do dispositivo não devem ser considerados protegidos contra a remoção do data center até que a chave temporária seja substituída pela chave de criptografia KMS.

4. Se o aparelho estiver ligado ou reinicializado, ele se reconeta ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não pode sobreviver a uma perda de energia ou a uma reinicialização.

## Considerações e requisitos para usar um servidor de gerenciamento de chaves

Antes de configurar um servidor de gerenciamento de chaves externo (KMS), você deve entender as considerações e os requisitos.

#### Quais são os requisitos do KMIP?

O StorageGRID é compatível com KMIP versão 1,4.

"Especificação do protocolo de interoperabilidade de gerenciamento de chaves versão 1,4"

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID é compatível com as seguintes cifras TLS v1,2 para KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Você deve garantir que cada nó de dispositivo que usa criptografia de nó tenha acesso de rede ao cluster KMS ou KMS configurado para o site.

As configurações do firewall de rede devem permitir que cada nó do dispositivo se comunique através da porta usada para comunicações KMIP (Key Management Interoperability Protocol). A porta KMIP padrão é 5696.

#### Quais aparelhos são suportados?

Você pode usar um servidor de gerenciamento de chaves (KMS) para gerenciar chaves de criptografia para qualquer dispositivo StorageGRID em sua grade que tenha a configuração **criptografia de nó** ativada. Esta definição só pode ser ativada durante a fase de configuração de hardware da instalação do dispositivo

utilizando o Instalador de dispositivos StorageGRID.

> Não é possível ativar a criptografia de nó depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não têm a criptografia de nó ativada.

Você pode usar o KMS configurado para os seguintes dispositivos e nós de dispositivo StorageGRID:

| Aparelho | Tipo de nó |
|---|---|
| Dispositivo de serviços SG1000 | Nó de administração ou nó de gateway |
| Dispositivo de serviços SG100 | Nó de administração ou nó de gateway |
| SG6000 dispositivo de armazenamento | Nó de storage |
| SG5700 dispositivo de armazenamento | Nó de storage |
| SG5600 dispositivo de armazenamento | Nó de storage |

Você não pode usar o KMS configurado para nós baseados em software (não-dispositivo), incluindo o seguinte:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados em contentores do Docker em hosts Linux

Os nós implantados nessas outras plataformas podem usar criptografia fora do StorageGRID no armazenamento de dados ou no nível de disco.

### Quando devo configurar servidores de gerenciamento de chaves?

Para uma nova instalação, você normalmente deve configurar um ou mais servidores de gerenciamento de chaves no Gerenciador de Grade antes de criar locatários. Essa ordem garante que os nós sejam protegidos antes que quaisquer dados de objeto sejam armazenados neles.

Você pode configurar os servidores de gerenciamento de chaves no Gerenciador de Grade antes ou depois de instalar os nós do dispositivo.

### Quantos servidores de gerenciamento de chaves eu preciso?

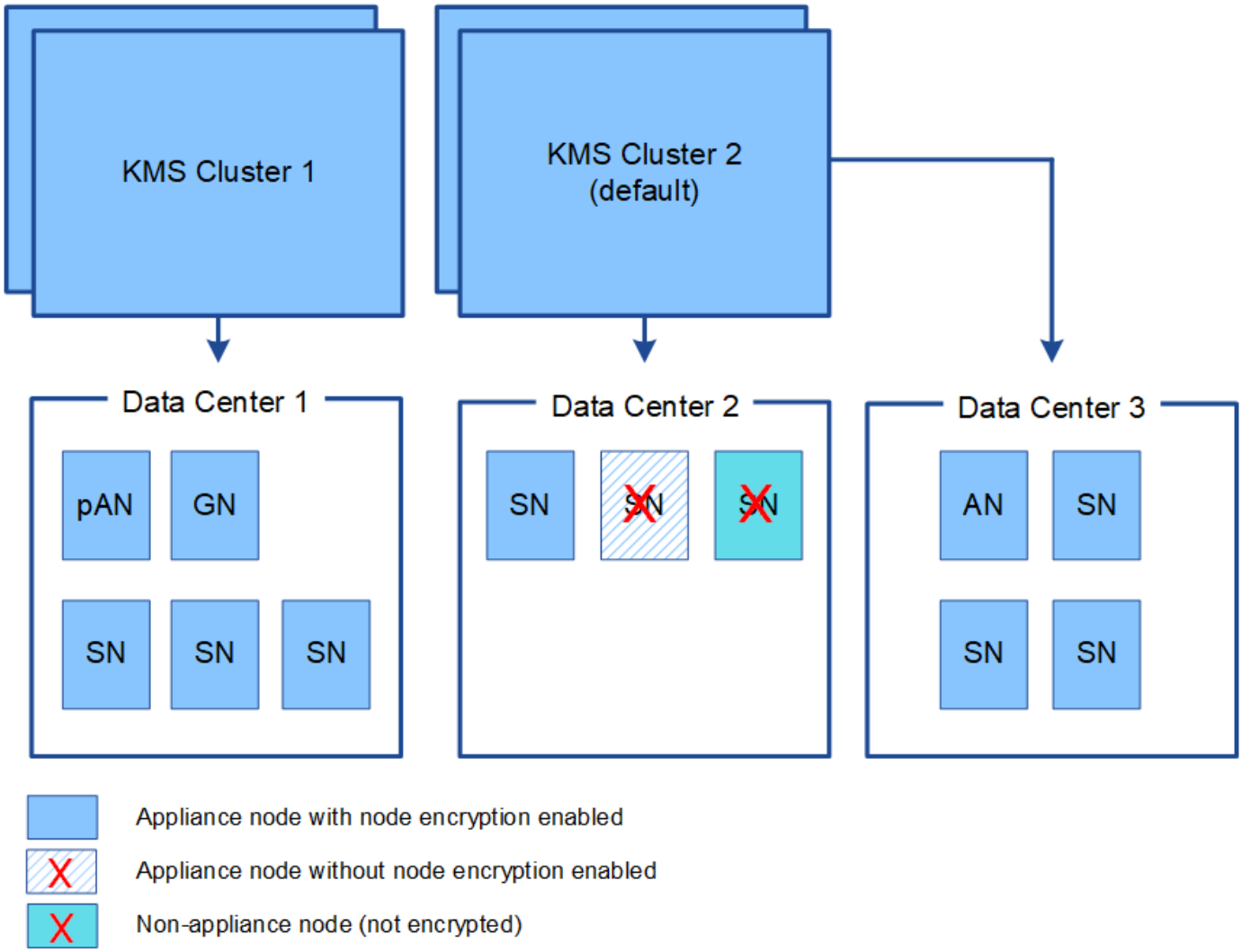
Você pode configurar um ou mais servidores de gerenciamento de chaves externos para fornecer chaves de criptografia aos nós do dispositivo em seu sistema StorageGRID. Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único local ou em um grupo de sites.

O StorageGRID é compatível com o uso de clusters KMS. Cada cluster KMS contém vários servidores de gerenciamento de chaves replicados que compartilham configurações e chaves de criptografia. O uso de clusters KMS para gerenciamento de chaves é recomendado porque melhora os recursos de failover de uma configuração de alta disponibilidade.

Por exemplo, suponha que seu sistema StorageGRID tenha três locais de data center. Você pode configurar um cluster KMS para fornecer uma chave para todos os nós do dispositivo no Data Center 1 e um segundo cluster KMS para fornecer uma chave para todos os nós do dispositivo em todos os outros locais. Ao adicionar

o segundo cluster KMS, você pode configurar um KMS padrão para o Data Center 2 e o Data Center 3.

Observe que você não pode usar um KMS para nós que não sejam do dispositivo ou para nenhum nó de dispositivo que não tenha a configuração **criptografia do nó** ativada durante a instalação.




**O que acontece quando uma chave é girada?**

Como prática recomendada de segurança, você deve girar periodicamente a chave de criptografia usada por cada KMS configurado.

Ao girar a chave de criptografia, use o software KMS para girar da última versão usada da chave para uma nova versão da mesma chave. Não rode para uma chave totalmente diferente.

> Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS no Gerenciador de Grade. Em vez disso, gire a chave atualizando a versão da chave no software KMS. Use o mesmo alias de chave para novas chaves que foi usado para chaves anteriores. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.

Quando a nova versão da chave estiver disponível:

- Ele é distribuído automaticamente para os nós de dispositivos criptografados no site ou sites associados ao KMS. A distribuição deve ocorrer dentro de uma hora de quando a chave é girada.
- Se o nó do dispositivo criptografado estiver offline quando a nova versão da chave for distribuída, o nó receberá a nova chave assim que for reinicializada.
- Se a nova versão de chave não puder ser usada para criptografar volumes de appliance por qualquer motivo, o alerta **rotação da chave de criptografia KMS falhou** será acionado para o nó do appliance. Talvez seja necessário entrar em Contato com o suporte técnico para obter ajuda na resolução desse alerta.

**Posso reutilizar um nó de appliance depois que ele foi criptografado?**

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID, primeiro será necessário desativar o nó da grade para mover dados de objeto para outro nó. Em seguida, você pode usar o Instalador de dispositivos StorageGRID para limpar a configuração do KMS. A limpeza da configuração KMS desativa a configuração **criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração KMS para o site StorageGRID.

> Sem acesso à chave de criptografia KMS, todos os dados que permanecem no dispositivo não podem mais ser acessados e ficam permanentemente bloqueados.

"Aparelhos de serviços SG100 SG1000"

"SG6000 dispositivos de armazenamento"

"SG5700 dispositivos de armazenamento"

"SG5600 dispositivos de armazenamento"

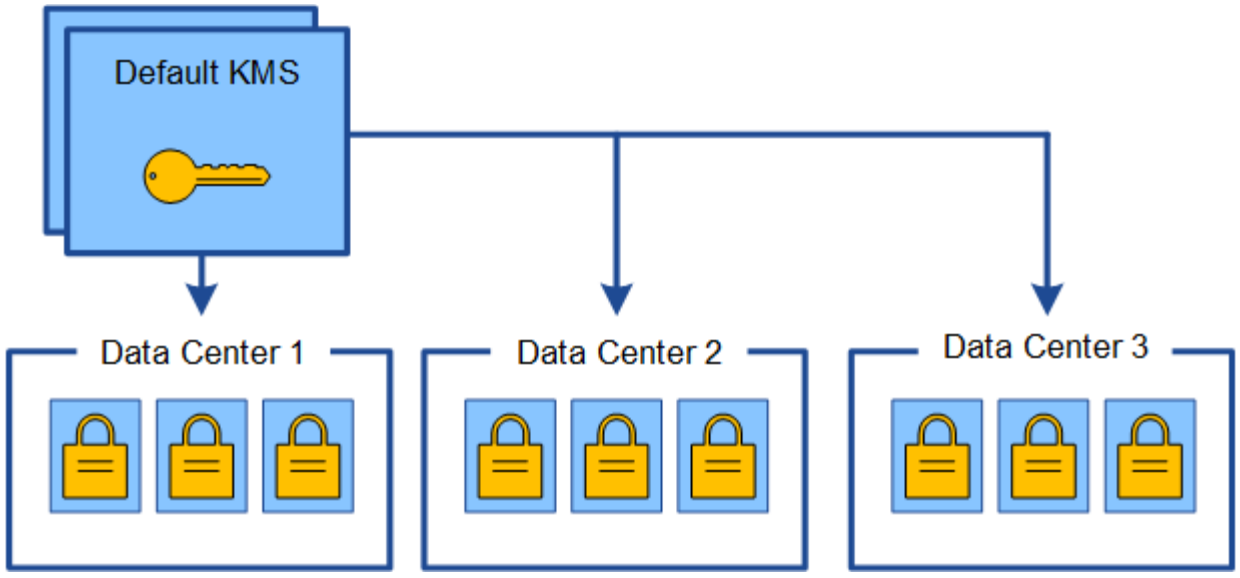
## Considerações para alterar o KMS para um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único local ou em um grupo de sites. Se você precisar alterar qual KMS é usado para um site, talvez seja necessário copiar a chave de criptografia de um KMS para outro.

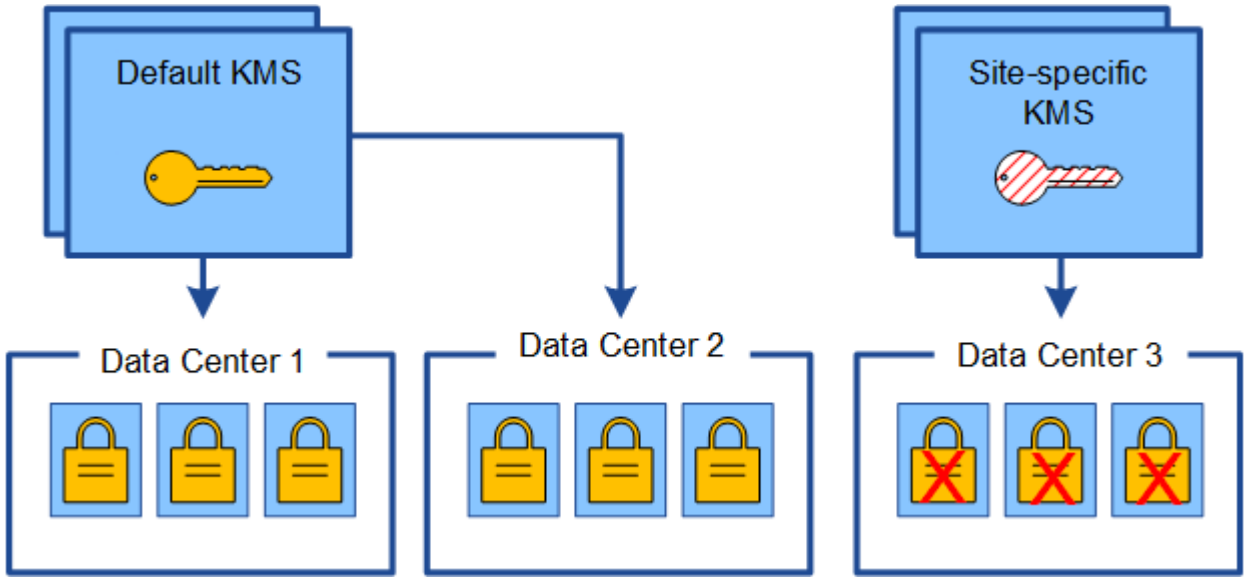
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS. Você deve garantir que o KMS tenha a chave correta para descriptografar os nós de dispositivo criptografado no local.

Por exemplo:

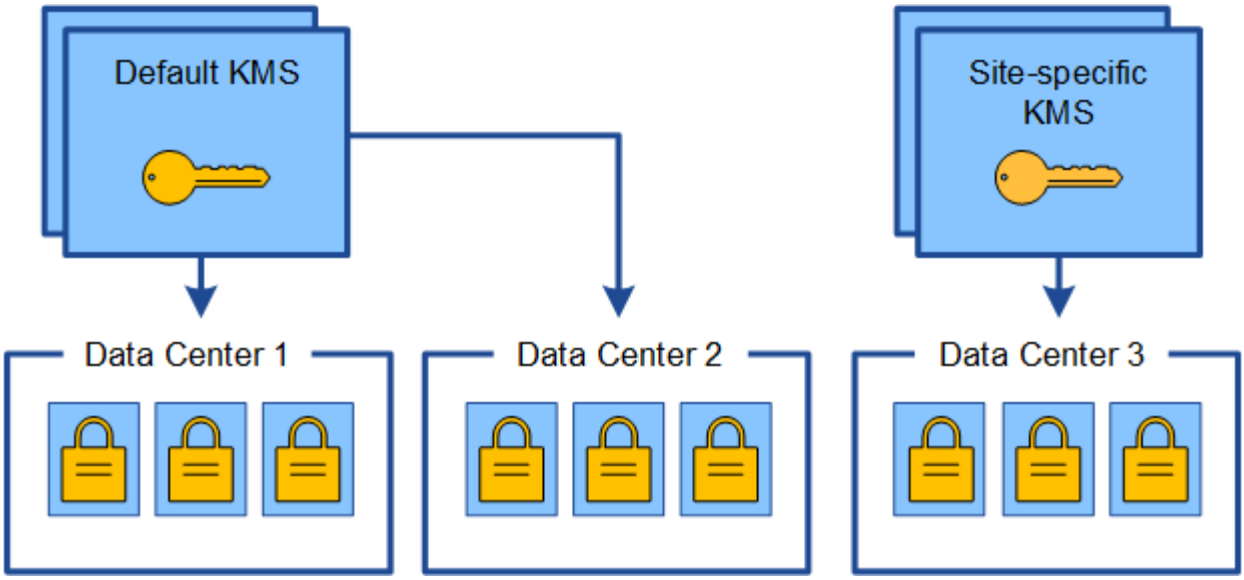
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar os nós do dispositivo em todos os locais. Esta mesma chave também deve ser usada para descriptografar esses aparelhos.




3. Você decide adicionar um KMS específico para um site (Data Center 3 na figura). No entanto, como os nós do appliance já estão criptografados, um erro de validação ocorre quando você tenta salvar a configuração para o KMS específico do site. O erro ocorre porque o KMS específico do site não tem a chave correta para descriptografar os nós nesse site.




4. Para resolver o problema, copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. (Tecnicamente, você copia a chave original para uma nova chave com o mesmo alias. A chave original torna-se uma versão anterior da nova chave.) O KMS específico do local agora tem a chave correta para descriptografar os nós do appliance no Data Center 3, para que ele possa ser salvo no StorageGRID.




**Casos de uso para alterar qual KMS é usado para um site**

A tabela resume as etapas necessárias para os casos mais comuns para alterar o KMS de um site.

| Caso de uso para alterar o KMS de um site | Passos necessários |
|---|---|
| Você tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como KMS padrão. | Edite o KMS específico do site. No campo **gerencia chaves para**, selecione **Sites não gerenciados por outro KMS (KMS padrão)**. O KMS específico do site agora será usado como o KMS padrão. Ele se aplicará a quaisquer sites que não tenham um KMS dedicado.<br><br>"Editar um servidor de gerenciamento de chaves (KMS)" |
| Você tem um KMS padrão e adiciona um novo site em uma expansão. Você não deseja usar o KMS padrão para o novo site. | 1. Se os nós de appliance no novo site já tiverem sido criptografados pelo KMS padrão, use o software KMS para copiar a versão atual da chave de criptografia do KMS padrão para um novo KMS.<br>2. Usando o Gerenciador de Grade, adicione o novo KMS e selecione o site.<br><br>"Adicionar um servidor de gerenciamento de chaves (KMS)" |

| Caso de uso para alterar o KMS de um site | Passos necessários |
| --- | --- |
| Você quer que o KMS para um site use um servidor diferente. | 1. Se os nós do dispositivo no local já tiverem sido criptografados pelo KMS existente, use o software KMS para copiar a versão atual da chave de criptografia do KMS existente para o novo KMS.<br>2. Usando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome de host ou endereço IP.<br><br>"Adicionar um servidor de gerenciamento de chaves (KMS)" |

## Configurando o StorageGRID como um cliente no KMS

Você deve configurar o StorageGRID como um cliente para cada servidor de gerenciamento de chaves externo ou cluster KMS antes de poder adicionar o KMS ao StorageGRID.

**Sobre esta tarefa**

Estas instruções aplicam-se ao Thales CipherTrust Manager k170v, versões 2,0, 2,1 e 2,2. Se tiver dúvidas sobre o uso de um servidor de gerenciamento de chaves diferente com o StorageGRID, entre em Contato com o suporte técnico.

"Thales CipherTrust Manager"

**Passos**

1. A partir do software KMS, crie um cliente StorageGRID para cada cluster KMS ou KMS que você pretende usar.

   Cada KMS gerencia uma única chave de criptografia para os nós do StorageGRID Appliances em um único local ou em um grupo de sites.

2. A partir do software KMS, crie uma chave de criptografia AES para cada cluster KMS ou KMS.

   A chave de criptografia precisa ser exportável.

3. Registre as seguintes informações para cada cluster KMS ou KMS.

   Você precisa dessas informações quando você adiciona o KMS ao StorageGRID.

   - Nome do host ou endereço IP para cada servidor.
   - Porta KMIP usada pelo KMS.
   - Alias de chave para a chave de criptografia no KMS.

   > ⓘ A chave de criptografia já deve existir no KMS. O StorageGRID não cria nem gerencia chaves KMS.

4. Para cada cluster KMS ou KMS, obtenha um certificado de servidor assinado por uma autoridade de certificação (CA) ou um pacote de certificados que contém cada um dos arquivos de certificado CA

codificados em PEM, concatenados em ordem de cadeia de certificados.

O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

- O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM).
- O campo Nome alternativo do assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou o endereço IP ao qual o StorageGRID se conetará.

> Ao configurar o KMS no StorageGRID, você deve inserir os mesmos FQDNs ou endereços IP no campo **Nome do host**.

- O certificado do servidor deve corresponder ao certificado usado pela interface KMIP do KMS, que normalmente usa a porta 5696.

5. Obtenha o certificado de cliente público emitido para o StorageGRID pelo KMS externo e a chave privada para o certificado de cliente.

   O certificado de cliente permite que o StorageGRID se autentique no KMS.

## Adicionar um servidor de gerenciamento de chaves (KMS)

Você usa o assistente do servidor de gerenciamento de chaves do StorageGRID para adicionar cada cluster KMS ou KMS.

**O que você vai precisar**

- Tem de ter revisto a "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você deve ter "Configurado o StorageGRID como um cliente no KMS", e você deve ter as informações necessárias para cada cluster KMS ou KMS
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

**Sobre esta tarefa**

Se possível, configure qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. Se você criar o KMS padrão primeiro, todos os dispositivos criptografados por nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site mais tarde, primeiro copie a versão atual da chave de criptografia do KMS padrão para o novo KMS.

"Considerações para alterar o KMS para um site"

**Passos**

1. "Passo 1: Insira os detalhes do KMS"
2. "Passo 2: Carregar certificado de servidor"
3. "Passo 3: Faça o upload de certificados de cliente"

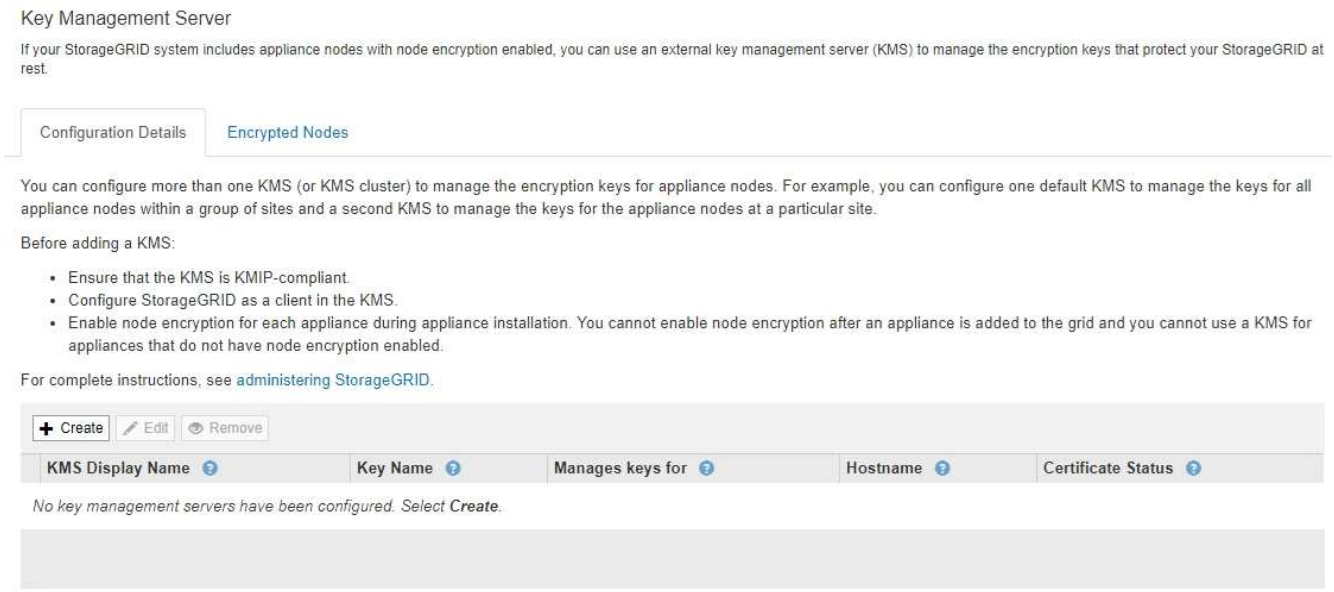
**Passo 1: Insira os detalhes do KMS**

Na Etapa 1 (Inserir detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves, você fornece detalhes sobre o cluster KMS ou KMS.

**Passos**

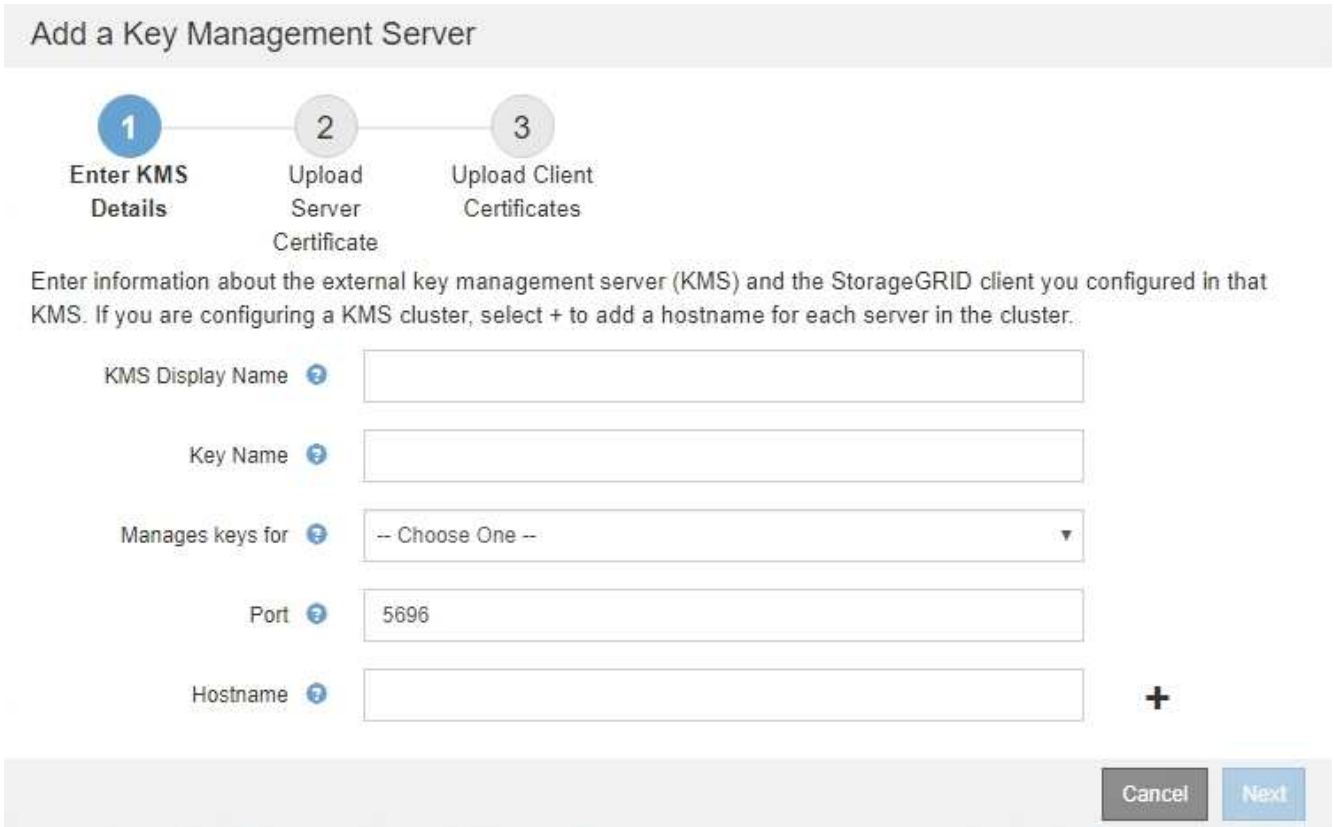
1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida com a guia Configuration Details (Detalhes da configuração) selecionada.




2. Selecione **criar**.

   O passo 1 (Digite os detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves é exibido.



3. Insira as seguintes informações para o KMS e o cliente StorageGRID que você configurou nesse KMS.

| Campo | Descrição |
| --- | --- |
| Nome de exibição de KMS | Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres. |
| Nome da chave | O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres. |
| Gere as chaves para | O site StorageGRID que será associado a este KMS. Se possível, você deve configurar qualquer servidor de gerenciamento de chaves específico do site antes de configurar um KMS padrão que se aplica a todos os sites não gerenciados por outro KMS.<br>• Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um local específico.<br>• Selecione **Sites não gerenciados por outro KMS (KMS padrão)** para configurar um KMS padrão que se aplicará a quaisquer sites que não tenham um KMS dedicado e a quaisquer sites que você adicionar em expansões subsequentes.<br>**Nota:** Um erro de validação ocorrerá quando você salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas você não forneceu a versão atual da chave de criptografia original para o novo KMS. |
| Porta | A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP. |
| Nome do anfitrião | O nome de domínio ou endereço IP totalmente qualificado para o KMS.<br>**Observação:** o campo SAN do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar ao KMS ou a todos os servidores em um cluster KMS. |

4. Se você estiver usando um cluster KMS, selecione o sinal de mais ➕para adicionar um nome de host para cada servidor no cluster.
5. Selecione **seguinte**.

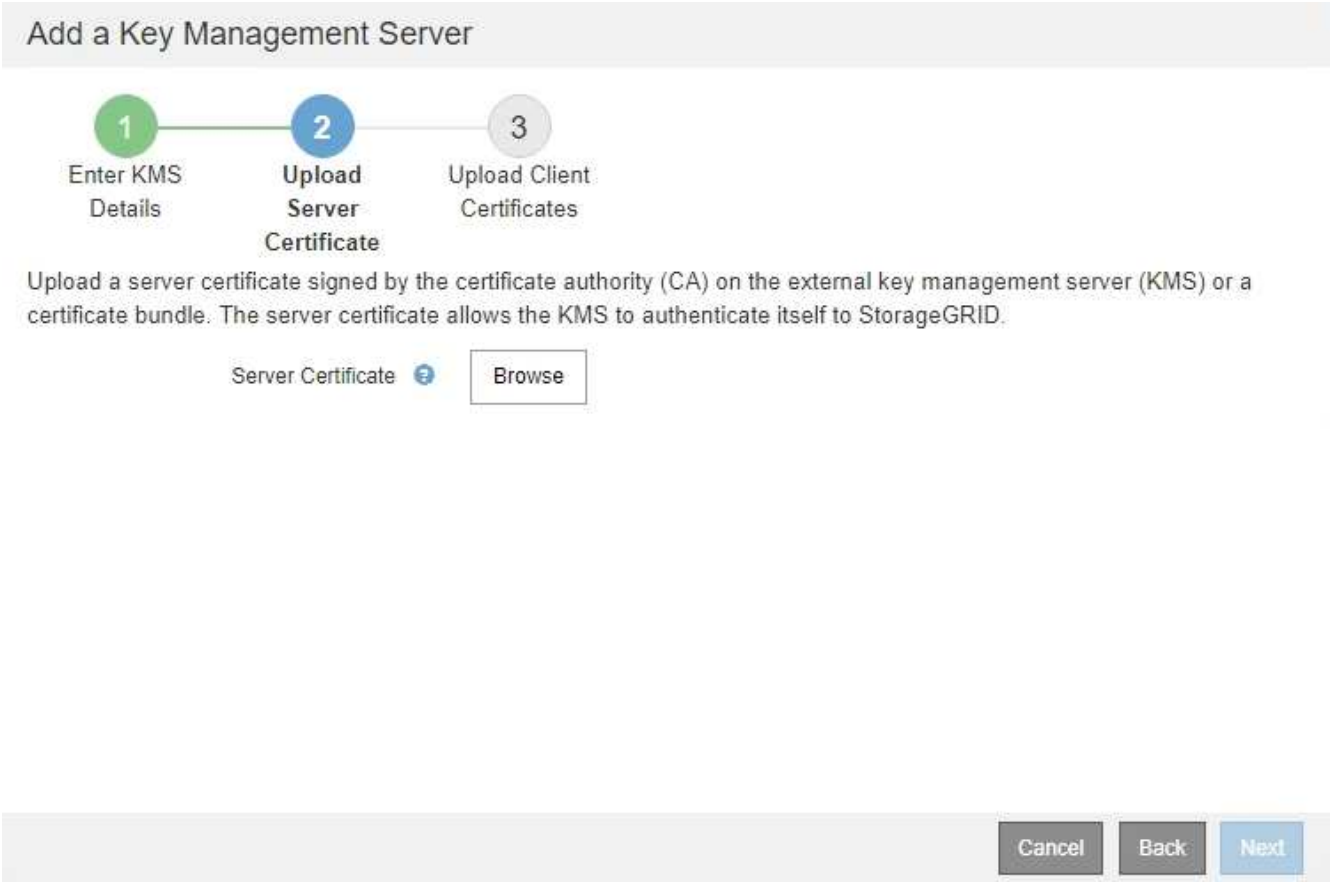
A etapa 2 (carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

### Passo 2: Carregar certificado de servidor

Na Etapa 2 (carregar certificado do servidor) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado do servidor (ou pacote de certificados) para o KMS. O certificado do servidor permite que o KMS externo se autentique no StorageGRID.

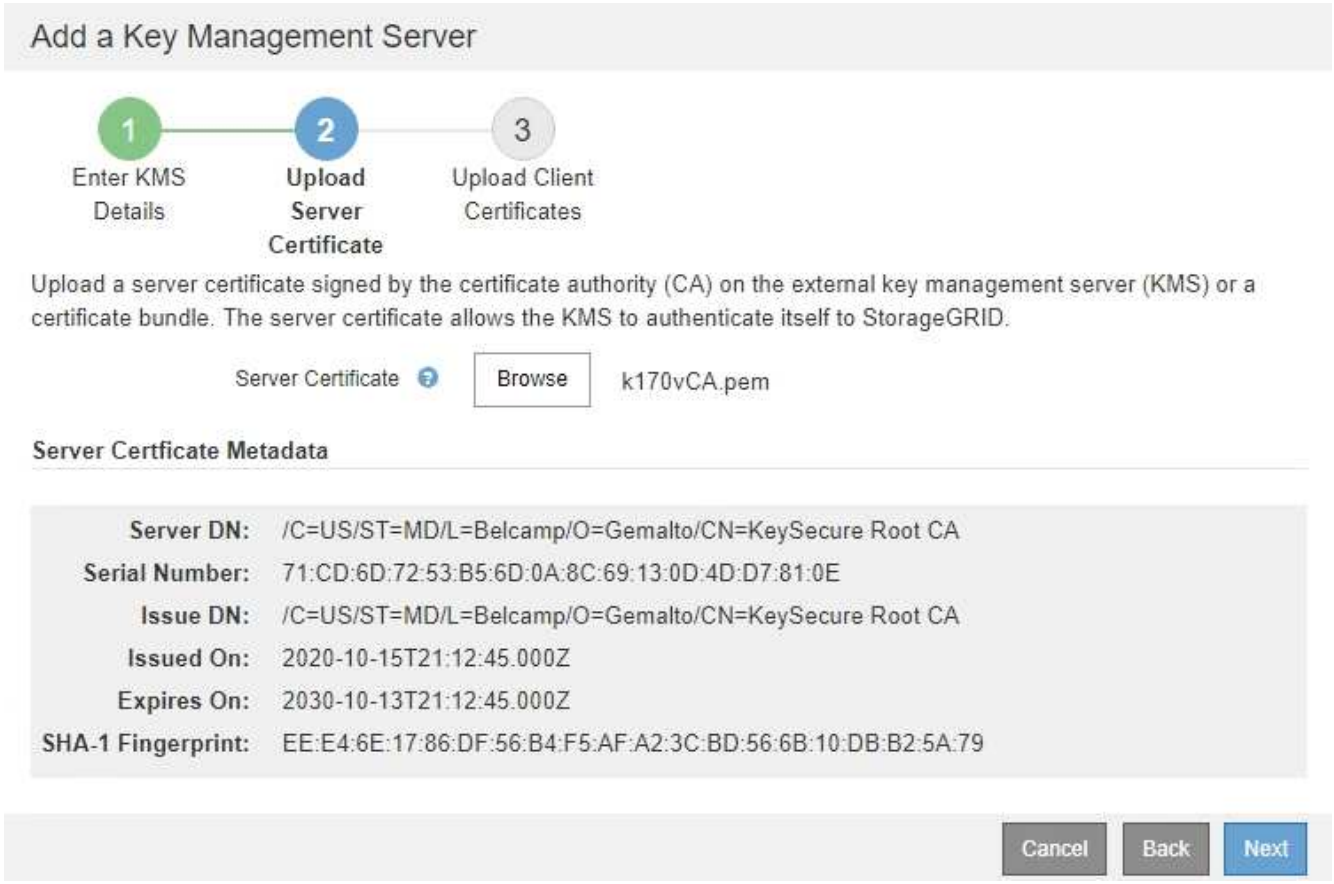
**Passos**

1. A partir de **passo 2 (carregar certificado do servidor)**, navegue até a localização do certificado ou pacote de certificados do servidor guardado.




2. Carregue o ficheiro de certificado.

   Os metadados do certificado do servidor são exibidos.




Se você carregou um pacote de certificados, os metadados de cada certificado serão exibidos em sua própria guia.

3. Selecione **seguinte**.

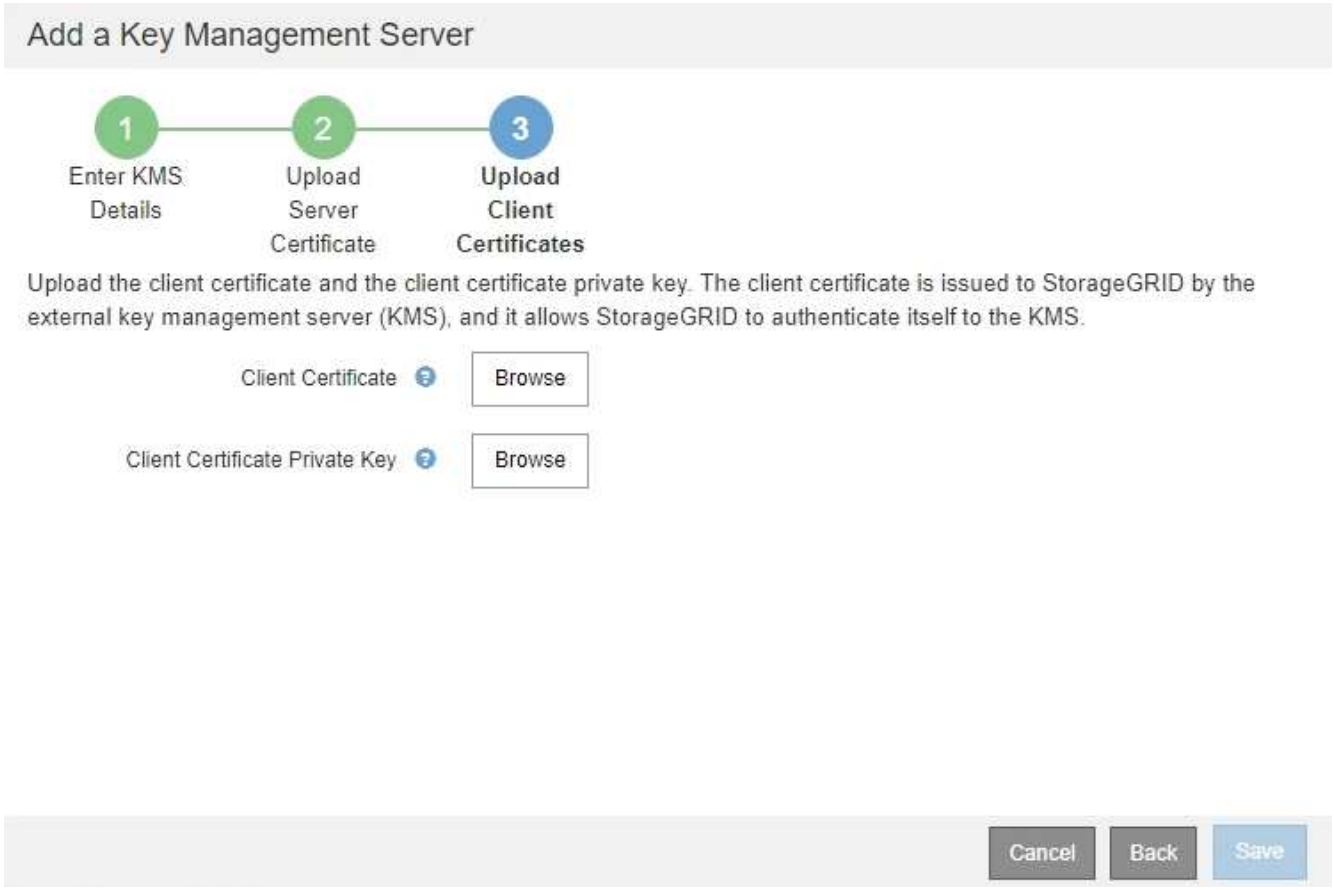
   A etapa 3 (carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves é exibida.

### Passo 3: Faça o upload de certificados de cliente

Na Etapa 3 (carregar certificados de cliente) do assistente Adicionar um servidor de gerenciamento de chaves, você carrega o certificado de cliente e a chave privada do certificado de cliente. O certificado de cliente permite que o StorageGRID se autentique no KMS.

#### Passos

1. A partir do **passo 3 (carregar certificados de cliente)**, navegue até a localização do certificado de cliente.

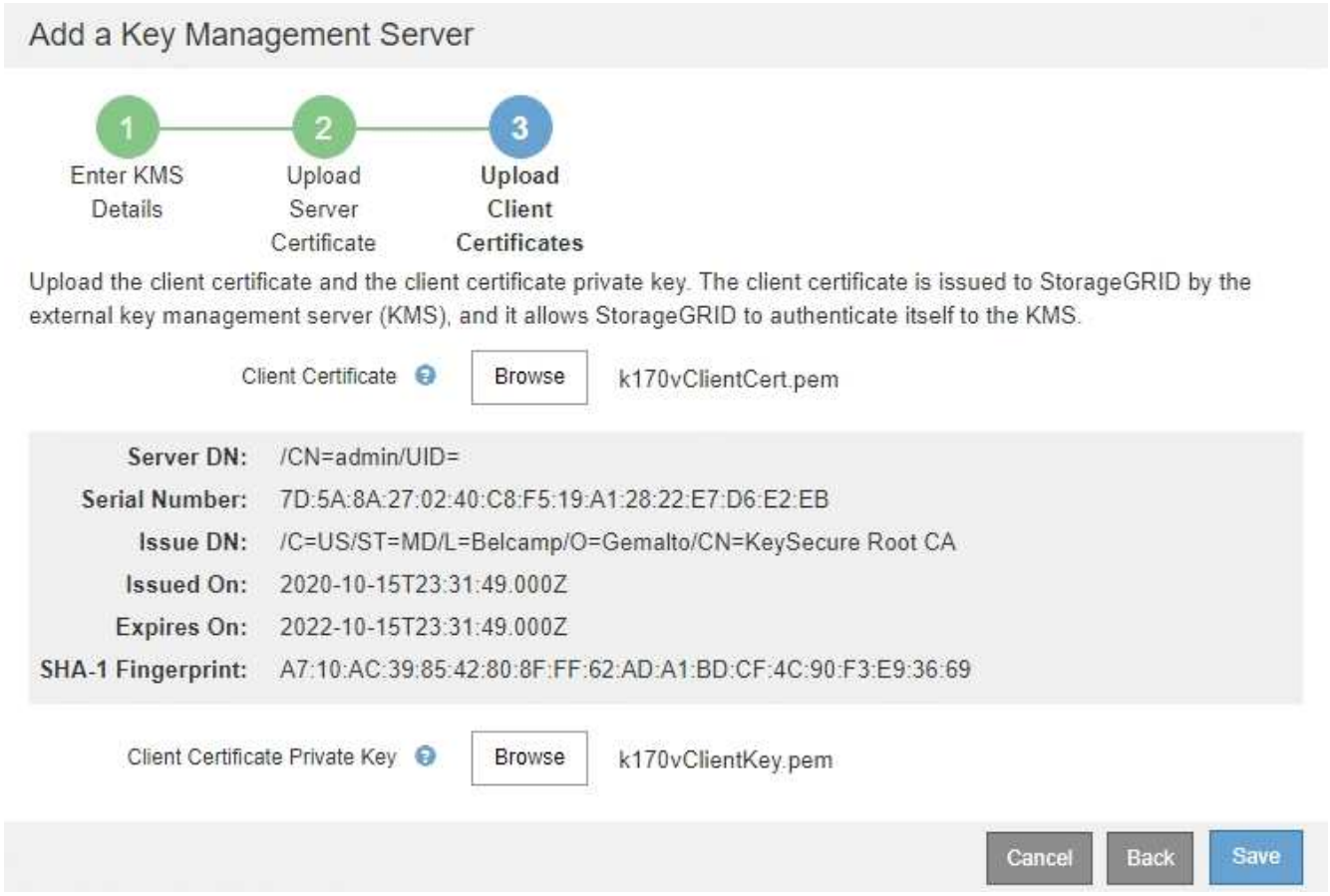



2. Carregue o ficheiro de certificado do cliente.

   Os metadados do certificado do cliente são exibidos.

3. Navegue até a localização da chave privada para o certificado do cliente.
4. Carregue o ficheiro de chave privada.

   Os metadados do certificado de cliente e da chave privada do certificado de cliente são exibidos.




5. Selecione **Guardar**.

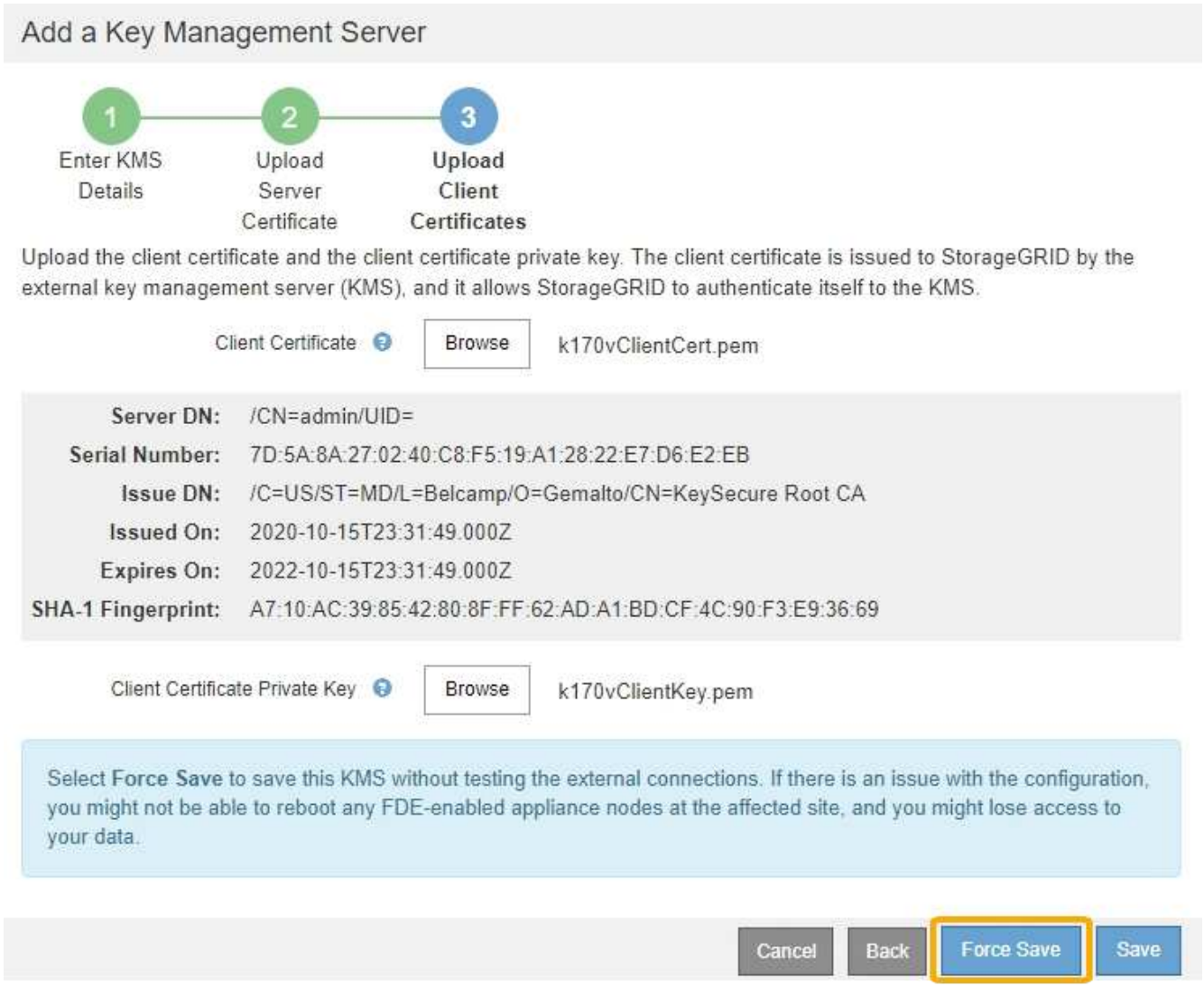
   As conexões entre o servidor de gerenciamento de chaves e os nós do dispositivo são testadas. Se todas as conexões forem válidas e a chave correta for encontrada no KMS, o novo servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

   > Imediatamente após adicionar um KMS, o status do certificado na página Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status atual.

6. Se uma mensagem de erro for exibida quando você selecionar **Salvar**, revise os detalhes da mensagem e selecione **OK**.

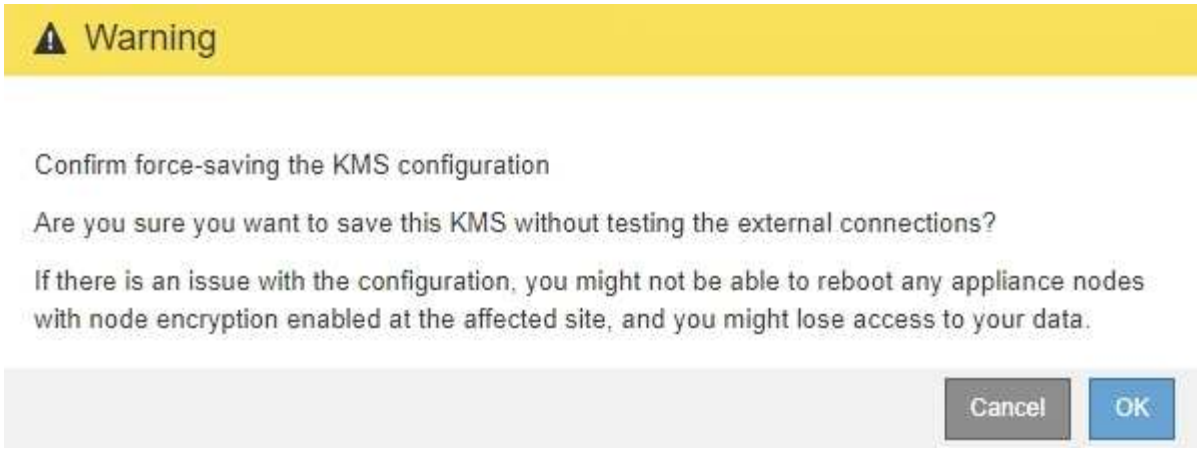
   Por exemplo, você pode receber um erro de entidade 422: Não processável se um teste de conexão falhar.

7. Se você precisar salvar a configuração atual sem testar a conexão externa, selecione **Force Save**.




Selecionar **Force Save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.




A configuração do KMS é salva, mas a conexão com o KMS não é testada.

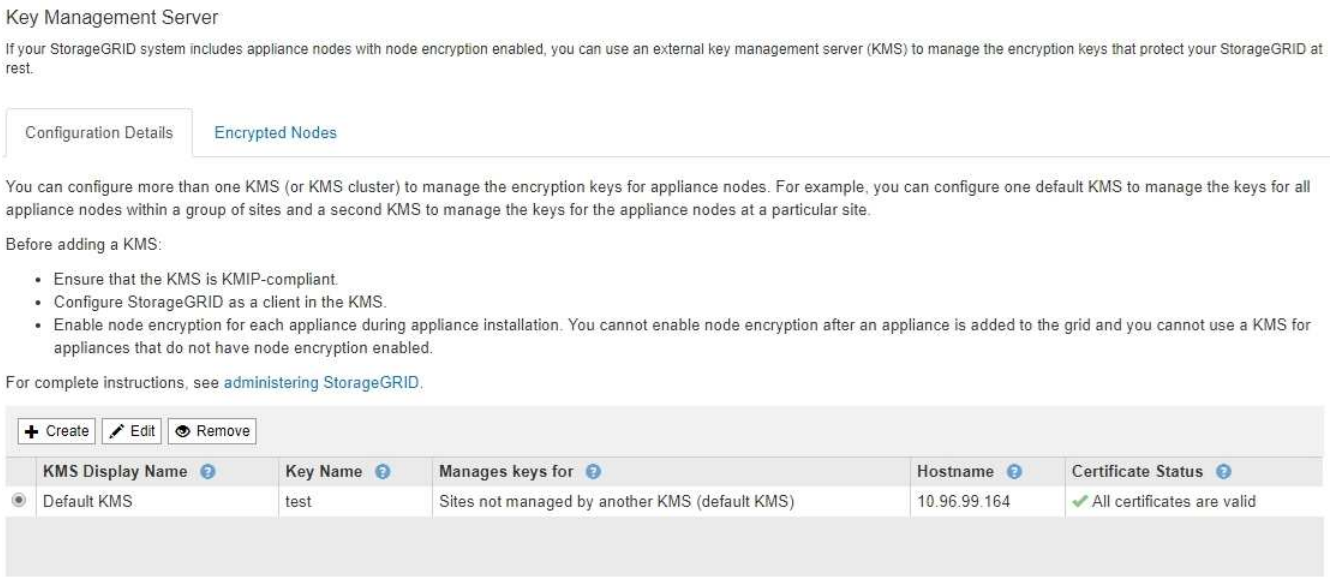
## Visualizar detalhes do KMS

Você pode exibir informações sobre cada servidor de gerenciamento de chaves (KMS) em seu sistema StorageGRID, incluindo o status atual do servidor e dos certificados de cliente.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves configurados.




2. Reveja as informações na tabela para cada KMS.

| Campo | Descrição |
| --- | --- |
| Nome de exibição de KMS | O nome descritivo do KMS. |

| Campo | Descrição |
| --- | --- |
| Nome da chave | O alias de chave para o cliente StorageGRID no KMS. |
| Gere as chaves para | O site StorageGRID associado ao KMS.<br><br>Este campo exibe o nome de um site StorageGRID específico ou **sites não gerenciados por outro KMS (KMS padrão).** |
| Nome do anfitrião | O nome de domínio totalmente qualificado ou endereço IP do KMS.<br><br>Se houver um cluster de dois servidores de gerenciamento de chaves, o nome de domínio totalmente qualificado ou o endereço IP de ambos os servidores serão listados. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o nome de domínio totalmente qualificado ou o endereço IP do primeiro KMS são listados juntamente com o número de servidores de gerenciamento de chaves adicionais no cluster.<br><br>Por exemplo: `10.10.10.10 and 10.10.10.11` Ou `10.10.10.10 and 2 others`.<br><br>Para exibir todos os nomes de host em um cluster, selecione um KMS e, em seguida, selecione **Editar**. |
| Estado do certificado | Estado atual do certificado do servidor, do certificado da CA opcional e do certificado do cliente: Válido, expirado, próximo da expiração ou desconhecido.<br><br>**Nota:** pode demorar StorageGRID até 30 minutos para obter atualizações do status do certificado. Você deve atualizar o navegador da Web para ver os valores atuais. |

3. Se o Status do certificado for desconhecido, aguarde até 30 minutos e, em seguida, atualize o navegador da Web.

> Imediatamente após adicionar um KMS, o status do certificado na página Key Management Server (servidor de gerenciamento de chaves) aparece como desconhecido. Pode demorar StorageGRID até 30 minutos para obter o status real de cada certificado. Você deve atualizar o navegador da Web para ver o status real.

4. Se a coluna Status do certificado indicar que um certificado expirou ou está prestes a expirar, solucione o problema o mais rápido possível.

   Consulte as ações recomendadas para os alertas **expiração do certificado KMS CA**, **expiração do**

**certificado do cliente KMS** e **expiração do certificado do servidor KMS** nas instruções para monitoramento e solução de problemas do StorageGRID.

> Você deve resolver quaisquer problemas de certificado o mais rápido possível para manter o acesso aos dados.

**Informações relacionadas**

"Monitorizar Resolução de problemas"

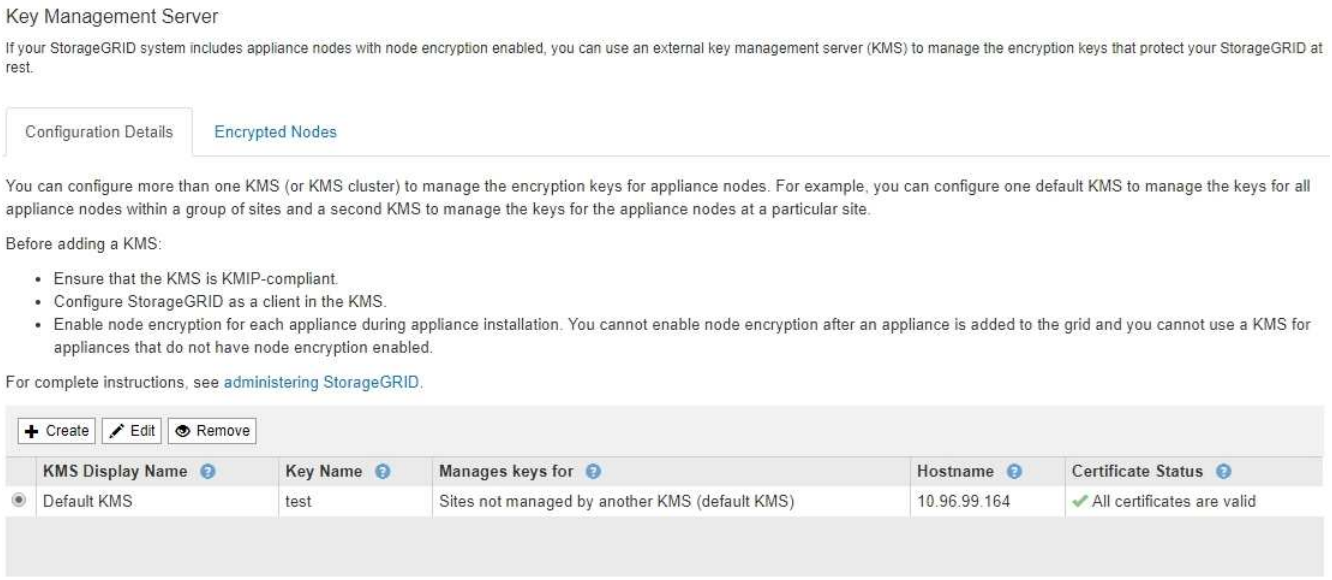
## Exibindo nós criptografados

Você pode exibir informações sobre os nós do dispositivo no seu sistema StorageGRID que têm a configuração **criptografia de nó** ativada.

**Passos**

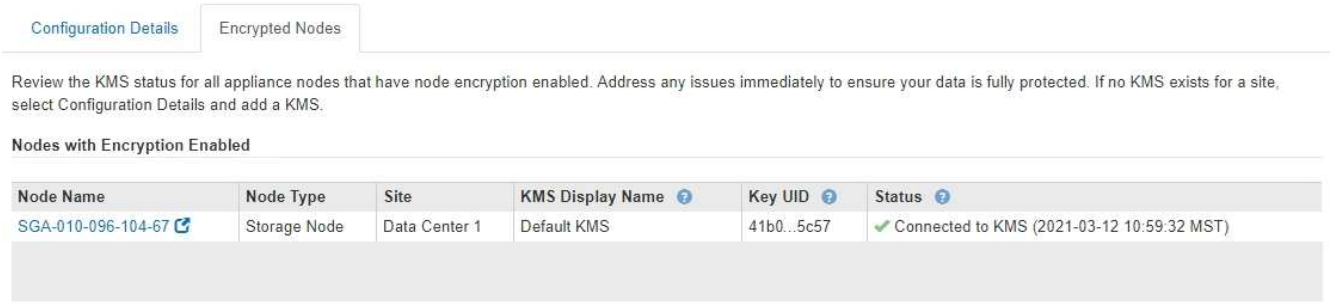
1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram configurados.




2. Na parte superior da página, selecione a guia **nós criptografados**.


   A guia nós criptografados lista os nós do dispositivo no sistema StorageGRID que têm a configuração **criptografia de nó** ativada.




3. Revise as informações na tabela para cada nó de dispositivo.

| Coluna | Descrição |
|---|---|
| Nome do nó | O nome do nó do dispositivo. |
| Tipo nó | O tipo de nó: Storage, Admin ou Gateway. |
| Local | O nome do site do StorageGRID onde o nó está instalado. |
| Nome de exibição de KMS | O nome descritivo do KMS usado para o nó.<br><br>Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS.<br><br>"Adicionar um servidor de gerenciamento de chaves (KMS)" |
| UID da chave | O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do dispositivo. Para exibir um UID de chave inteiro, passe o cursor sobre a célula.<br><br>Um traço (--) indica que a chave UID é desconhecida, possivelmente por causa de um problema de conexão entre o nó do aparelho e o KMS. |
| Estado | O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conetado, o carimbo de data/hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações de configuração do KMS.<br><br>**Observação:** você deve atualizar seu navegador para ver os novos valores. |

4. Se a coluna Status indicar um problema KMS, solucione o problema imediatamente.

   Durante as operações normais de KMS, o status será **conectado ao KMS**. Se um nó for desconetado da grade, o estado de conexão do nó é mostrado (administrativamente para baixo ou desconhecido).

   Outras mensagens de status correspondem a alertas StorageGRID com os mesmos nomes:

   - Falha ao carregar a configuração DE KMS

- Erro de conetividade DE KMS
- Nome da chave de encriptação KMS não encontrado
- Falha na rotação da chave de CRIPTOGRAFIA KMS
- A chave KMS falhou ao desencriptar um volume de aparelho
- O KMS não está configurado consulte as ações recomendadas para esses alertas nas instruções para monitoramento e solução de problemas do StorageGRID.

> Você deve resolver quaisquer problemas imediatamente para garantir que seus dados estejam totalmente protegidos.

**Informações relacionadas**

"Monitorizar Resolução de problemas"

## Editar um servidor de gerenciamento de chaves (KMS)

Talvez seja necessário editar a configuração de um servidor de gerenciamento de chaves, por exemplo, se um certificado estiver prestes a expirar.

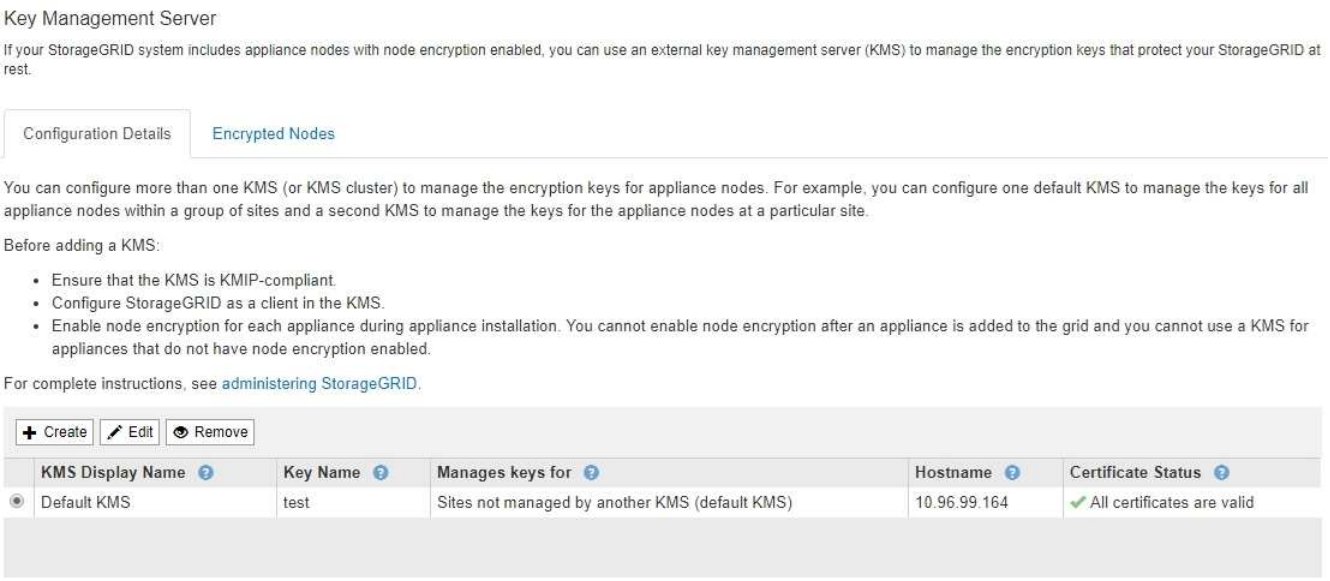
**O que você vai precisar**

- Tem de ter revisto a "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Se pretende atualizar o local selecionado para um KMS, tem de ter revisto o "Considerações para alterar o KMS para um site".
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.



2. Selecione o KMS que deseja editar e selecione **Editar**.
3. Opcionalmente, atualize os detalhes em **Etapa 1 (Inserir detalhes do KMS)** do assistente Editar um servidor de gerenciamento de chaves.

| Campo | Descrição |
| --- | --- |
| Nome de exibição de KMS | Um nome descritivo para ajudá-lo a identificar este KMS. Deve ter entre 1 e 64 carateres. |
| Nome da chave | O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 carateres.<br><br>Você só precisa editar o nome da chave em casos raros. Por exemplo, você deve editar o nome da chave se o alias for renomeado no KMS ou se todas as versões da chave anterior tiverem sido copiadas para o histórico de versões do novo alias.<br><br>Nunca tente girar uma chave alterando o nome da chave (alias) para o KMS. Em vez disso, gire a chave atualizando a versão da chave no software KMS. O StorageGRID requer que todas as versões de chave usadas anteriormente (bem como quaisquer versões futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias de chave para um KMS configurado, o StorageGRID pode não conseguir descriptografar seus dados.<br><br>"Considerações e requisitos para usar um servidor de gerenciamento de chaves" |
| Gere as chaves para | Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, opcionalmente selecione **Sites não gerenciados por outro KMS (KMS padrão)**. Esta seleção converte um KMS específico do site para o KMS padrão, que se aplicará a todos os sites que não têm um KMS dedicado e a quaisquer sites adicionados em uma expansão.<br><br>**Observação:** se você estiver editando um KMS específico do site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não poderá selecionar um site específico. |
| Porta | A porta que o servidor KMS usa para comunicações KMIP (Key Management Interoperability Protocol). O padrão é 5696, que é a porta padrão KMIP. |

| Campo | Descrição |
| --- | --- |
| Nome do anfitrião | O nome de domínio ou endereço IP totalmente qualificado para o KMS.<br><br>**Observação:** o campo SAN do certificado do servidor deve incluir o FQDN ou o endereço IP que você inserir aqui. Caso contrário, o StorageGRID não poderá se conetar ao KMS ou a todos os servidores em um cluster KMS. |

4. Se você estiver configurando um cluster KMS, selecione o sinal de mais ➕para adicionar um nome de host para cada servidor no cluster.
5. Selecione **seguinte**.

   A etapa 2 (carregar certificado do servidor) do assistente Editar um servidor de gerenciamento de chaves é exibida.

6. Se precisar substituir o certificado do servidor, selecione **Procurar** e carregue o novo arquivo.
7. Selecione **seguinte**.

   A etapa 3 (carregar certificados de cliente) do assistente Editar um servidor de gerenciamento de chaves é exibida.

8. Se precisar substituir o certificado de cliente e a chave privada do certificado de cliente, selecione **Procurar** e carregue os novos arquivos.
9. Selecione **Guardar**.

   As conexões entre o servidor de gerenciamento de chaves e todos os nós de dispositivos criptografados por nós nos locais afetados são testadas. Se todas as conexões de nó forem válidas e a chave correta for encontrada no KMS, o servidor de gerenciamento de chaves será adicionado à tabela na página servidor de gerenciamento de chaves.

10. Se for apresentada uma mensagem de erro, reveja os detalhes da mensagem e selecione **OK**.

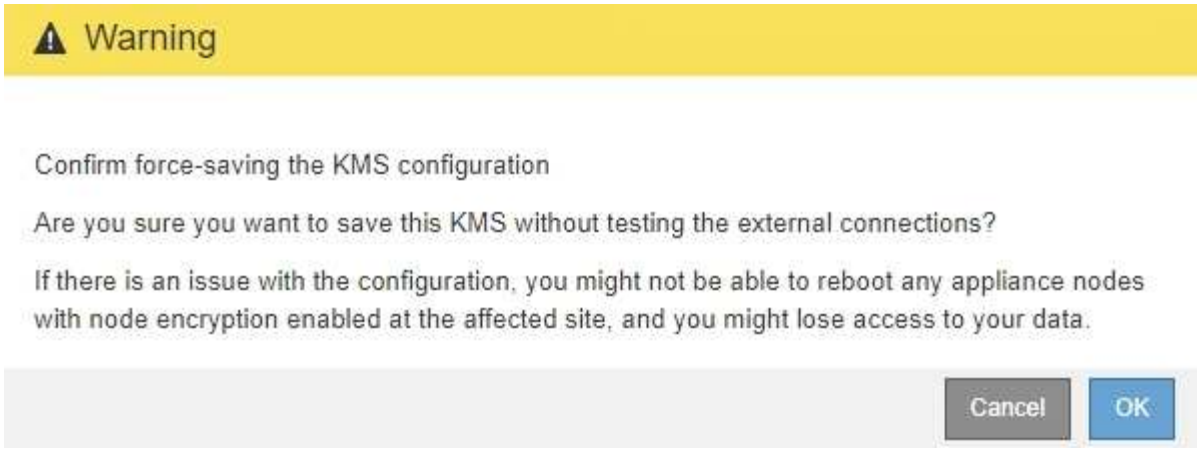
    Por exemplo, você pode receber um erro de entidade 422: Não processável se o site selecionado para este KMS já for gerenciado por outro KMS, ou se um teste de conexão falhou.

11. Se você precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Force Save**.

    > ⓘ Selecionar **Force Save** salva a configuração do KMS, mas não testa a conexão externa de cada dispositivo para esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós de dispositivo que têm a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

    A configuração do KMS é salva.

12. Reveja o aviso de confirmação e selecione **OK** se tiver a certeza de que pretende forçar a gravação da configuração.




A configuração do KMS é salva, mas a conexão com o KMS não é testada.

## Remover um servidor de gerenciamento de chaves (KMS)

Em alguns casos, você pode querer remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se você tiver desativado o site.

**O que você vai precisar**

- Tem de ter revisto a "considerações e requisitos para usar um servidor de gerenciamento de chaves".
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

**Sobre esta tarefa**

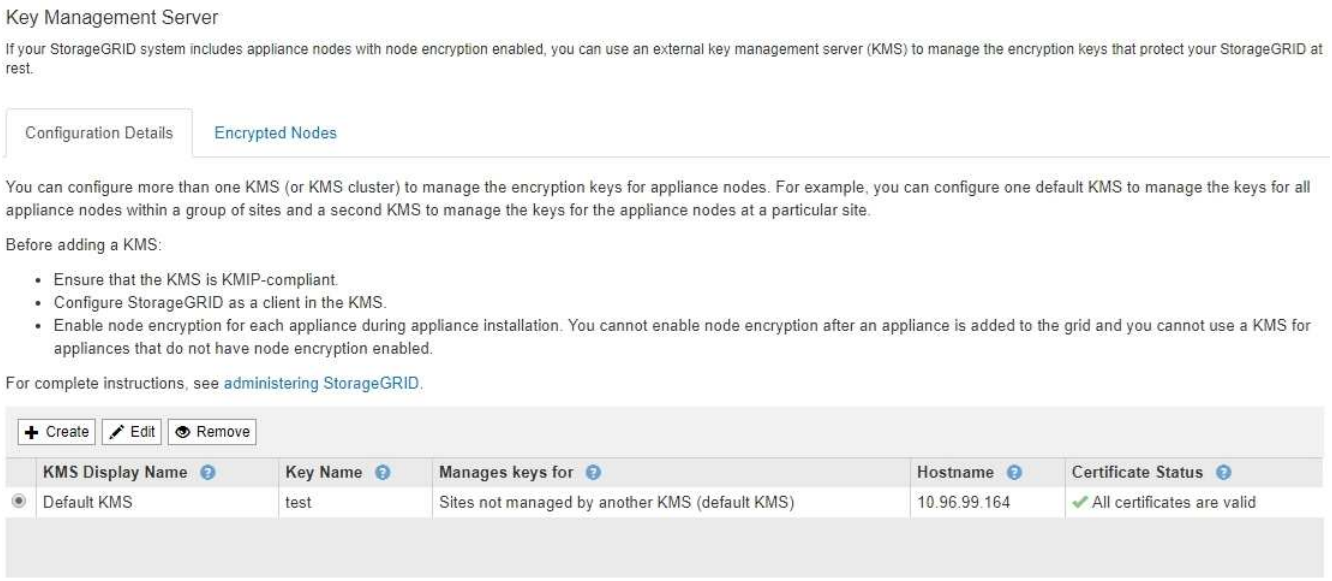
Você pode remover um KMS nestes casos:

- Você pode remover um KMS específico do site se o site tiver sido desativado ou se o site não incluir nós de dispositivo com criptografia de nó ativada.
- Você pode remover o KMS padrão se um KMS específico do site já existir para cada site que tenha nós de dispositivo com criptografia de nó ativada.

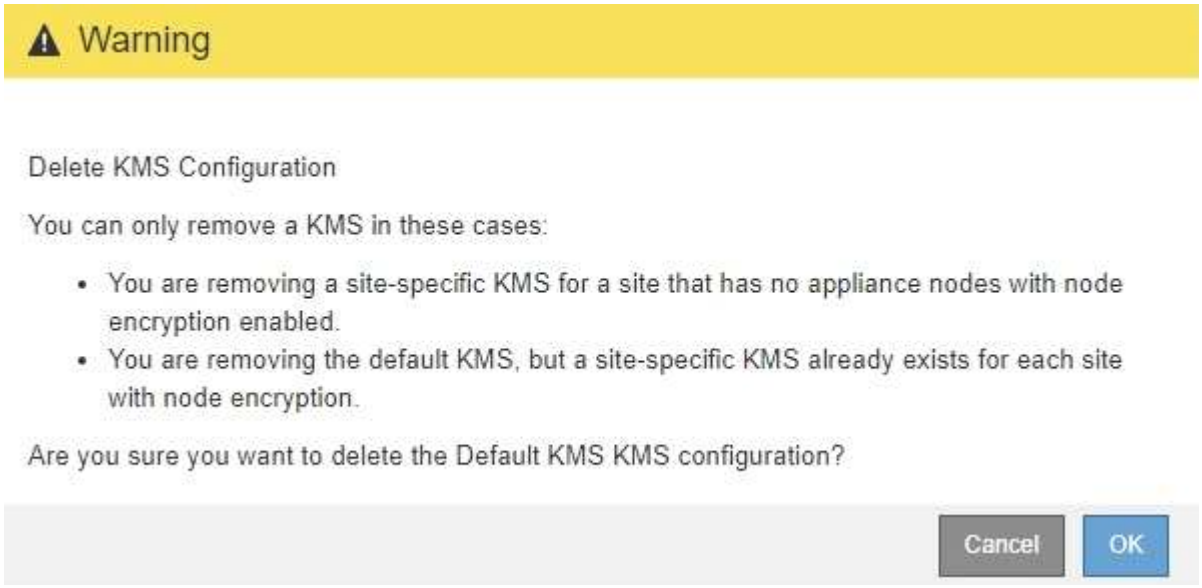
**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **servidor de gerenciamento de chaves**.

   A página Key Management Server (servidor de gerenciamento de chaves) é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.




2. Selecione o botão de opção para o KMS que deseja remover e selecione **Remover**.
3. Reveja as considerações na caixa de diálogo de aviso.




4. Selecione **OK**.

   A configuração do KMS é removida.

# Gerenciamento de locatários

Como administrador de grade, você cria e gerencia as contas de locatário que os clientes S3 e Swift usam para armazenar e recuperar objetos, monitorar o uso do armazenamento e gerenciar as ações que os clientes podem executar usando seu sistema StorageGRID.

## Quais são as contas de inquilino

As contas de locatário permitem que aplicativos clientes que usam a API REST do Simple Storage Service (S3) ou a API REST Swift armazenem e recuperem objetos no StorageGRID.

Cada conta de locatário suporta o uso de um único protocolo, que você especifica quando você cria a conta. Para armazenar e recuperar objetos em um sistema StorageGRID com ambos os protocolos, você deve criar duas contas de locatário: Uma para buckets e objetos do S3 e outra para contentores e objetos do Swift. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários autorizados, buckets ou containers e objetos.

Opcionalmente, você pode criar contas de locatário adicionais se quiser segregar os objetos armazenados em seu sistema por diferentes entidades. Por exemplo, você pode configurar várias contas de locatário em qualquer um desses casos de uso:

- * Caso de uso corporativo:* se você estiver administrando um sistema StorageGRID em um aplicativo corporativo, talvez queira separar o armazenamento de objetos da grade pelos diferentes departamentos da sua organização. Nesse caso, você pode criar contas de inquilino para o departamento de marketing, o departamento de suporte ao cliente, o departamento de recursos humanos e assim por diante.

  > Se você usar o protocolo cliente S3, você pode simplesmente usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa usar contas de locatário. Consulte as instruções para implementar aplicativos cliente S3 para obter mais informações.

- * Caso de uso do provedor de serviços:* se você estiver administrando um sistema StorageGRID como provedor de serviços, você pode segregar o armazenamento de objetos da grade pelas diferentes entidades que alugarão o armazenamento em sua grade. Neste caso, você criaria contas de inquilino para a empresa A, empresa B, empresa C e assim por diante.

## Criando e configurando contas de inquilino

Ao criar uma conta de locatário, você especifica as seguintes informações:

- Nome de exibição da conta de locatário.
- Qual protocolo de cliente será usado pela conta de locatário (S3 ou Swift).
- Para contas de locatário do S3: Se a conta de locatário tem permissão para usar serviços de plataforma com buckets do S3. Se você permitir que as contas de inquilino usem serviços de plataforma, você deve garantir que a grade esteja configurada para suportar seu uso. Consulte ""Gerenciando serviços de plataforma.""
- Opcionalmente, uma cota de armazenamento para a conta de locatário - o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos do locatário. Se a cota for excedida, o locatário não poderá criar novos objetos.

  > A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco).

- Se a federação de identidade estiver ativada para o sistema StorageGRID, qual grupo federado tem permissão de acesso root para configurar a conta de locatário.
- Se o logon único (SSO) não estiver em uso para o sistema StorageGRID, se a conta do locatário usará sua própria origem de identidade ou compartilhará a origem de identidade da grade e a senha inicial para o usuário raiz local do locatário.

Depois que uma conta de locatário for criada, você poderá executar as seguintes tarefas:

- **Gerenciar serviços de plataforma para a grade**: Se você habilitar serviços de plataforma para contas de locatários, certifique-se de entender como as mensagens de serviços de plataforma são entregues e os requisitos de rede que o uso de serviços de plataforma coloca na implantação do StorageGRID.
- **Monitorar o uso de armazenamento de uma conta de locatário**: Depois que os locatários começam a usar suas contas, você pode usar o Grid Manager para monitorar quanto armazenamento cada locatário consome.

  Se você tiver definido cotas para locatários, poderá ativar o alerta **uso alto da cota do locatário** para determinar se os locatários estão consumindo suas cotas. Se ativado, esse alerta é acionado quando um locatário usou 90% de sua cota. Para obter mais informações, consulte a referência de alertas nas instruções para monitoramento e solução de problemas do StorageGRID.

- **Configurar operações do cliente**: Você pode configurar se alguns tipos de operações do cliente são proibidos.

## Configurando S3 locatários

Depois que uma conta de locatário do S3 for criada, os usuários do locatário poderão acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Gerenciando chaves de acesso S3
- Criação e gerenciamento de buckets do S3
- Monitoramento do uso do storage
- Usando serviços de plataforma (se ativado)

> Os usuários de locatários do S3 podem criar e gerenciar chaves de acesso do S3 e buckets com o Gerenciador de locatários, mas devem usar um aplicativo cliente do S3 para obter e gerenciar objetos.

## Configurando os locatários Swift

Depois que uma conta de locatário Swift for criada, o usuário raiz do locatário poderá acessar o Gerenciador do locatário para executar tarefas como as seguintes:

- Configurando a federação de identidade (a menos que a origem de identidade seja compartilhada com a grade) e criando grupos e usuários locais
- Monitoramento do uso do storage

> Os usuários Swift devem ter a permissão de acesso root para acessar o Gerenciador do locatário. No entanto, a permissão de acesso root não permite que os usuários se autentiquem na API REST do Swift para criar contentores e ingerir objetos. Os usuários devem ter a permissão Swift Administrator para se autenticar na API Swift REST.

**Informações relacionadas**

"Use uma conta de locatário"

## Criando uma conta de locatário

Você deve criar pelo menos uma conta de locatário para controlar o acesso ao storage no sistema StorageGRID.

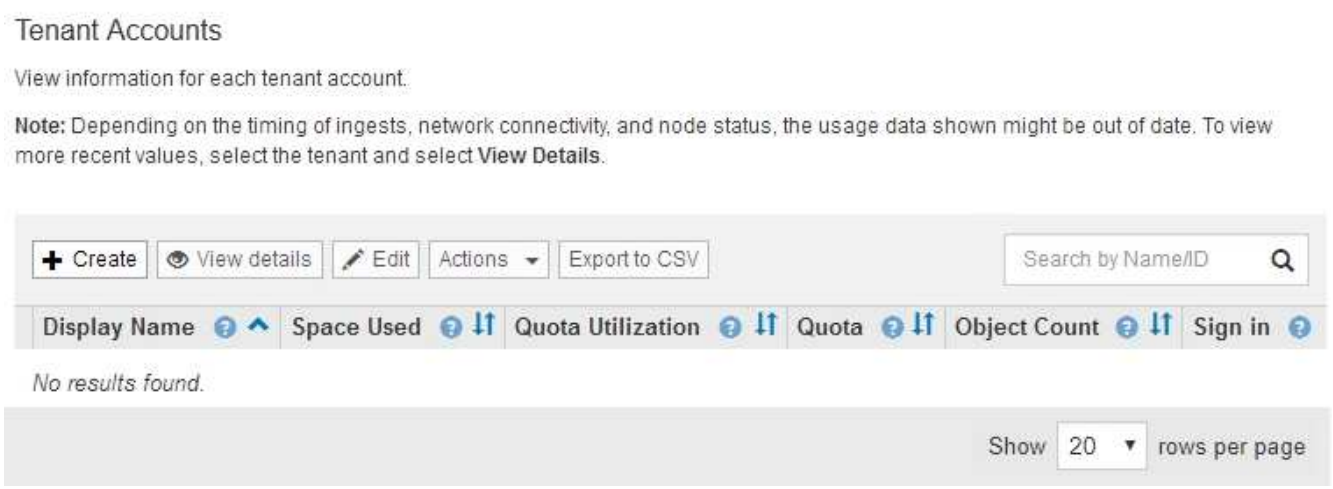
**O que você vai precisar**

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

**Passos**

1. Selecione **tenants**.

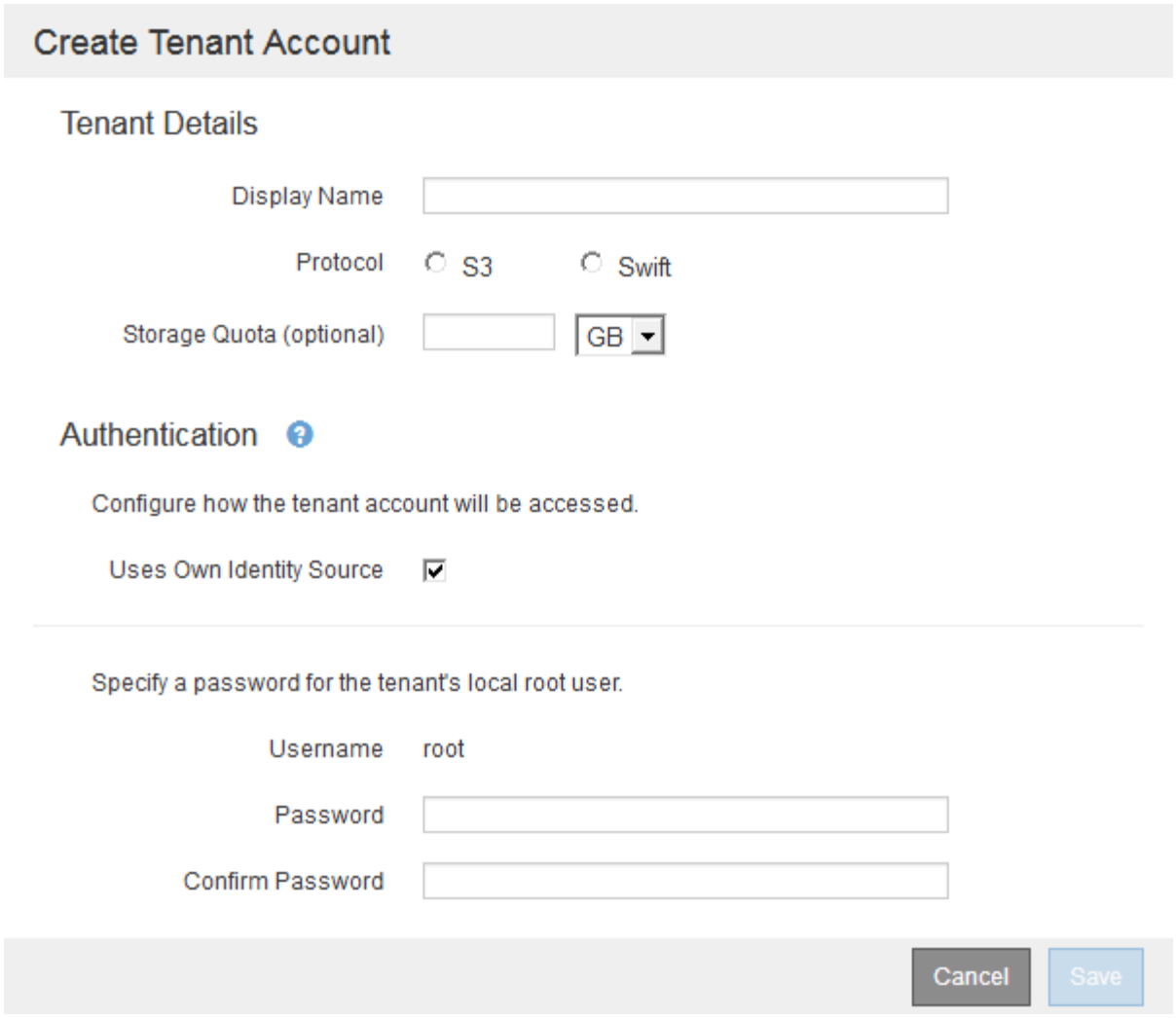
   A página Contas do locatário é exibida e lista todas as contas de locatário existentes.



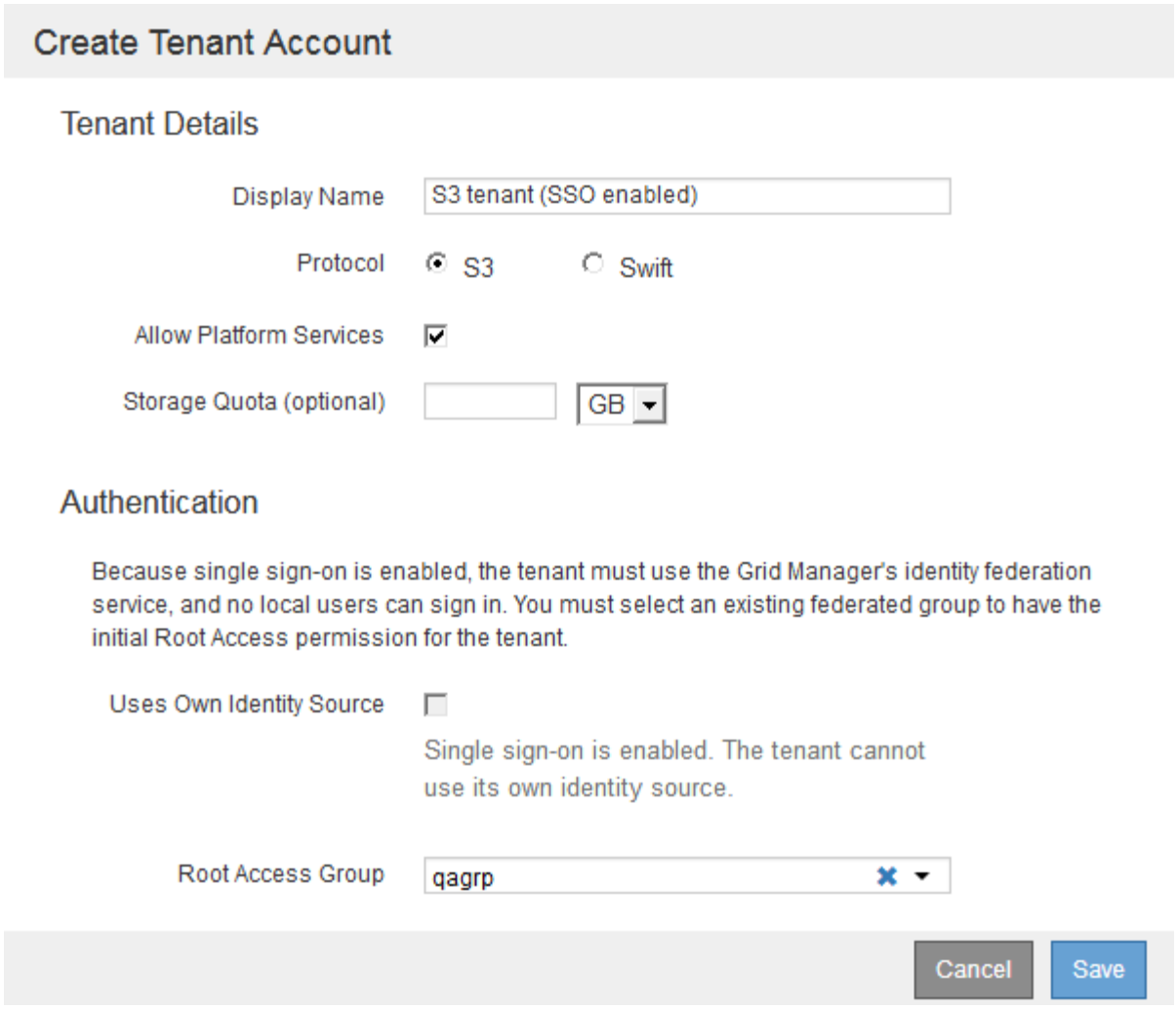

2. Selecione **criar**.

   A página criar conta de locatário é exibida. Os campos incluídos na página dependem se o logon único (SSO) foi ativado para o sistema StorageGRID.

   - Se o SSO não estiver sendo usado, a página criar conta do locatário será assim.




◦ Se o SSO estiver ativado, a página criar conta do locatário será assim.




**Informações relacionadas**

"Usando a federação de identidade"

"Configurando logon único"

### Criando uma conta de locatário se o StorageGRID não estiver usando SSO

Quando você cria uma conta de locatário, você especifica um nome, um protocolo de cliente e, opcionalmente, uma cota de armazenamento. Se o StorageGRID não estiver usando logon único (SSO), você também deve especificar se a conta de locatário usará sua própria origem de identidade e configurar a senha inicial para o usuário raiz local do locatário.

**Sobre esta tarefa**

Se a conta de locatário usar a origem de identidade configurada para o Gerenciador de Grade e você quiser conceder permissão de acesso raiz para a conta de locatário a um grupo federado, você deve ter importado esse grupo federado para o Gerenciador de Grade. Você não precisa atribuir nenhuma permissão do Gerenciador de Grade a esse grupo de administradores. Consulte as instruções para "gerenciando grupos de administradores".

**Passos**

1. Na caixa de texto **Nome de exibição**, insira um nome de exibição para essa conta de locatário.

   Os nomes de exibição não precisam ser exclusivos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.

2. Selecione o protocolo de cliente que será usado por esta conta de locatário, seja **S3** ou **Swift**.
3. Para contas de locatário do S3, mantenha a caixa de seleção **permitir Serviços de Plataforma** selecionada, a menos que você não queira que esse locatário use serviços de plataforma para buckets do S3.

   Se os serviços de plataforma estiverem ativados, um locatário poderá usar recursos, como a replicação do CloudMirror, que acessam serviços externos. Talvez você queira desativar o uso desses recursos para limitar a quantidade de largura de banda da rede ou outros recursos que um locatário consome. Consulte ""Gerenciando serviços de plataforma.""

4. Na caixa de texto **cota de armazenamento**, insira opcionalmente o número máximo de gigabytes, terabytes ou petabytes que você deseja disponibilizar para os objetos desse locatário. Em seguida, selecione as unidades na lista suspensa.

   Deixe esse campo em branco se você quiser que esse locatário tenha uma cota ilimitada.

   A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco). As cópias ILM e a codificação de apagamento não contribuem para a quantidade de cota usada. Se a cota for excedida, a conta de locatário não poderá criar novos objetos.

   Para monitorar o uso de armazenamento de cada conta de locatário, selecione **uso**. As contas de locatário também podem monitorar seu próprio uso de storage no Dashboard no Gerenciador do locatário ou com a API de gerenciamento do locatário. Observe que os valores de uso de storage de um locatário podem ficar desatualizados se os nós forem isolados de outros nós na grade. Os totais serão atualizados quando a conetividade de rede for restaurada.

5. Se o locatário gerenciar seus próprios grupos e usuários, siga estas etapas.
   a. Marque a caixa de seleção **usa a própria fonte de identidade** (padrão).

      Se esta caixa de verificação estiver selecionada e pretender utilizar a federação de identidade para grupos de inquilinos e utilizadores, o inquilino tem de configurar a sua própria origem de identidade. Consulte as instruções para usar contas de locatário.

   b. Especifique uma senha para o usuário raiz local do locatário.
6. Se o locatário usar os grupos e usuários configurados para o Gerenciador de Grade, siga estas etapas.
   a. Desmarque a caixa de seleção **usa a própria fonte de identidade**.
   b. Faça um ou ambos os procedimentos a seguir:
      - No campo Grupo de Acesso raiz, selecione um grupo federado existente no Gerenciador de Grade que deve ter a permissão de acesso raiz inicial para o locatário.

        Se você tiver permissões adequadas, os grupos federados existentes do Gerenciador de Grade serão listados quando você clicar no campo. Caso contrário, introduza o nome exclusivo do grupo.

- Especifique uma senha para o usuário raiz local do locatário.

7. Clique em **Salvar**.

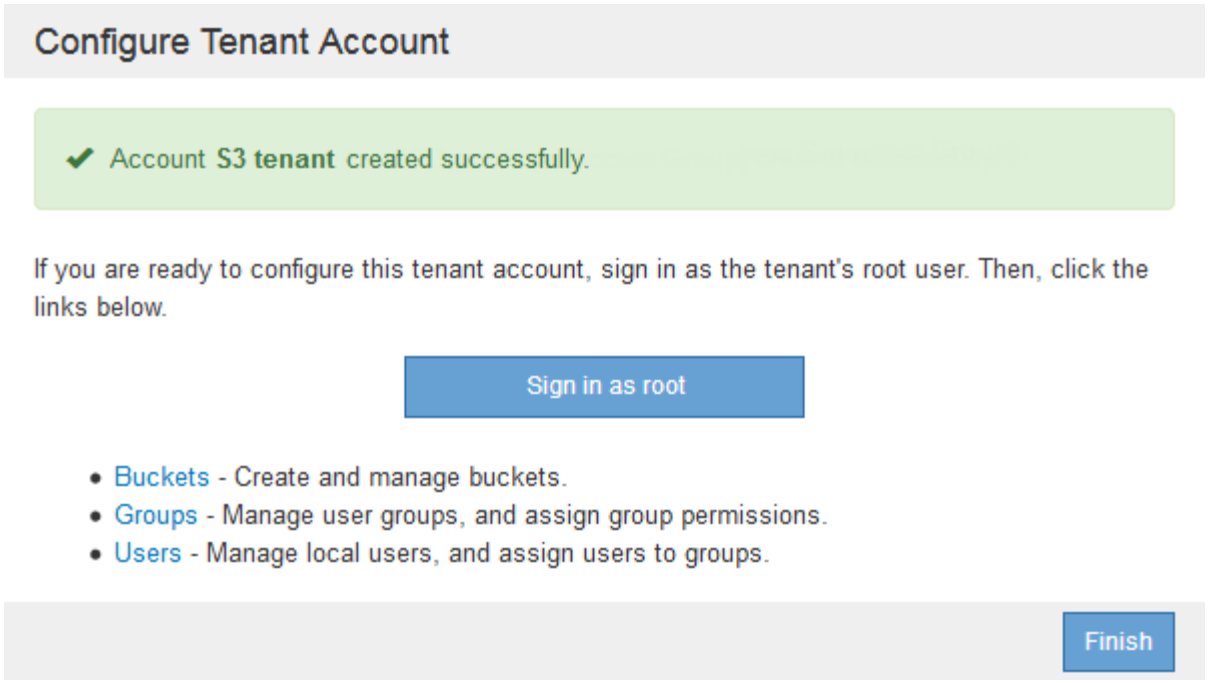
   A conta de locatário é criada.

8. Opcionalmente, acesse o novo locatário. Caso contrário, vá para a etapa acessando o locatário mais tardede .

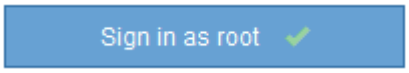
| Se você é… | Faça isso… |
| --- | --- |
| Acessando o Gerenciador de Grade em uma porta restrita | Clique em **restrito** para saber mais sobre como acessar essa conta de locatário.<br><br>O URL do Gerenciador do Locatário tem este formato:<br><br>`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/`<br><br>• *`FQDN_or_Admin_Node_IP`* É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador<br>• *`port`* é a porta somente locatário<br>• *`20-digit-account-id`* É o ID exclusivo da conta do locatário |
| Acessando o Gerenciador de Grade na porta 443, mas você não definiu uma senha para o usuário raiz local | Clique em **entrar** e insira as credenciais de um usuário no grupo federado de acesso root. |
| Acessando o Gerenciador de Grade na porta 443 e você define uma senha para o usuário raiz local | Vá para a próxima etapa para faça login como root. |

9. Faça login no locatário como root:

   a. Na caixa de diálogo Configurar conta de locatário, clique no botão **entrar como root**.




Uma marca de seleção verde aparece no botão, indicando que você agora está conetado à conta de locatário como usuário raiz.




a. Clique nos links para configurar a conta de locatário.

   Cada link abre a página correspondente no Gerenciador do Locatário. Para concluir a página, consulte as instruções para usar contas de locatário.

b. Clique em **Finish**.

10. para acessar o locatário mais tarde:

| Se você estiver usando… | Faça um destes… |
|---|---|
| Porta 443 | • No Gerenciador de Grade, selecione **tenants** e clique em **Sign in** à direita do nome do locatário.<br>• Insira o URL do locatário em um navegador da Web:<br>`https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/`<br>◦ *FQDN_or_Admin_Node_IP* É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador<br>◦ *20-digit-account-id* É o ID exclusivo da conta do locatário |

| Se você estiver usando… | Faça um destes… |
| --- | --- |
| Uma porta restrita | • No Gerenciador de Grade, selecione **tenants** e clique em **Restricted**.<br>• Insira o URL do locatário em um navegador da Web:<br>`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id`<br>◦ *FQDN_or_Admin_Node_IP* É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador<br>◦ *port* é a porta restrita somente para locatário<br>◦ *20-digit-account-id* É o ID exclusivo da conta do locatário |

**Informações relacionadas**

"Controlar o acesso através de firewalls"

"Gerenciamento de serviços de plataforma para contas de locatários do S3"

"Use uma conta de locatário"

### Criando uma conta de locatário se o SSO estiver habilitado

Quando você cria uma conta de locatário, você especifica um nome, um protocolo de cliente e, opcionalmente, uma cota de armazenamento. Se o logon único (SSO) estiver ativado para o StorageGRID, você também especificará qual grupo federado tem permissão de acesso root para configurar a conta de locatário.

**Passos**

1. Na caixa de texto **Nome de exibição**, insira um nome de exibição para essa conta de locatário.

   Os nomes de exibição não precisam ser exclusivos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.

2. Selecione o protocolo de cliente que será usado por esta conta de locatário, seja **S3** ou **Swift**.
3. Para contas de locatário do S3, mantenha a caixa de seleção **permitir Serviços de Plataforma** selecionada, a menos que você não queira que esse locatário use serviços de plataforma para buckets do S3.

   Se os serviços de plataforma estiverem ativados, um locatário poderá usar recursos, como a replicação do CloudMirror, que acessam serviços externos. Talvez você queira desativar o uso desses recursos para limitar a quantidade de largura de banda da rede ou outros recursos que um locatário consome. Consulte ""Gerenciando serviços de plataforma.""

4. Na caixa de texto **cota de armazenamento**, insira opcionalmente o número máximo de gigabytes, terabytes ou petabytes que você deseja disponibilizar para os objetos desse locatário. Em seguida, selecione as unidades na lista suspensa.

Deixe esse campo em branco se você quiser que esse locatário tenha uma cota ilimitada.

> A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco). As cópias ILM e a codificação de apagamento não contribuem para a quantidade de cota usada. Se a cota for excedida, a conta de locatário não poderá criar novos objetos.

> Para monitorar o uso de armazenamento de cada conta de locatário, selecione **uso**. As contas de locatário também podem monitorar seu próprio uso de storage no Dashboard no Gerenciador do locatário ou com a API de gerenciamento do locatário. Observe que os valores de uso de storage de um locatário podem ficar desatualizados se os nós forem isolados de outros nós na grade. Os totais serão atualizados quando a conetividade de rede for restaurada.

5. Observe que a caixa de seleção **usa a própria fonte de identidade** está desmarcada e desativada.

   Como o SSO está habilitado, o locatário deve usar a origem de identidade que foi configurada para o Gerenciador de Grade. Nenhum usuário local pode entrar.

6. No campo **Root Access Group**, selecione um grupo federado existente no Gerenciador de Grade para ter a permissão de acesso raiz inicial para o locatário.

   > Se você tiver permissões adequadas, os grupos federados existentes do Gerenciador de Grade serão listados quando você clicar no campo. Caso contrário, introduza o nome exclusivo do grupo.

7. Clique em **Salvar**.

   A conta de locatário é criada. A página Contas do locatário é exibida e inclui uma linha para o novo locatário.

8. Se você for um usuário no grupo de acesso root, opcionalmente clique no link **entrar** para que o novo locatário acesse imediatamente o Gerenciador de Locatário, onde você pode configurar o locatário. Caso contrário, forneça o URL do link **entrar** para o administrador da conta do locatário. (O URL de um locatário é o nome de domínio totalmente qualificado ou o endereço IP de qualquer nó Admin, seguido de `/?accountId=`*`20-digit-account-id`*.)

   > Uma mensagem de acesso negado será exibida se você clicar em **entrar**, mas você não pertencer ao grupo de acesso raiz da conta de locatário.

**Informações relacionadas**

"Configurando logon único"

"Gerenciamento de serviços de plataforma para contas de locatários do S3"

"Use uma conta de locatário"

## Alterando a senha do usuário raiz local de um locatário

Talvez seja necessário alterar a senha do usuário raiz local de um locatário se o usuário raiz estiver bloqueado para fora da conta.

**O que você vai precisar**

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

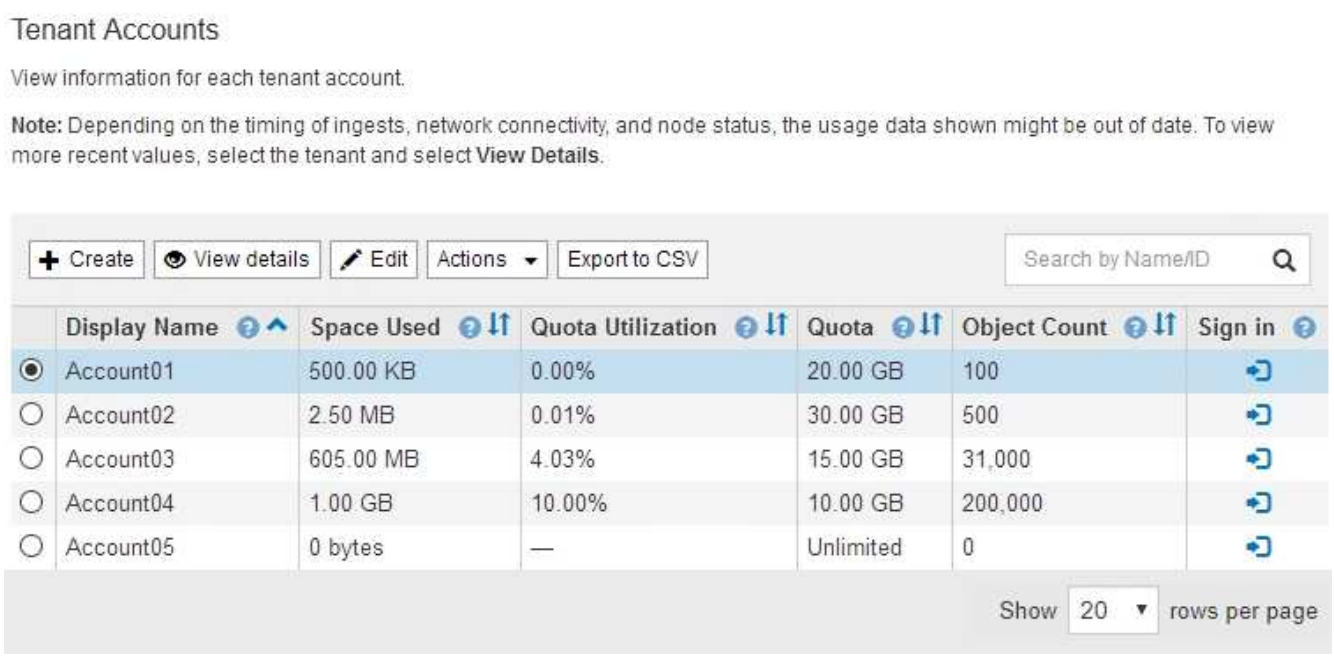
**Sobre esta tarefa**

Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, o usuário raiz local não poderá entrar na conta de locatário. Para executar tarefas de usuário raiz, os usuários devem pertencer a um grupo federado que tenha a permissão de acesso raiz para o locatário.

**Passos**

1. Selecione **tenants**.

   A página Contas do locatário é exibida e lista todas as contas de locatário existentes.

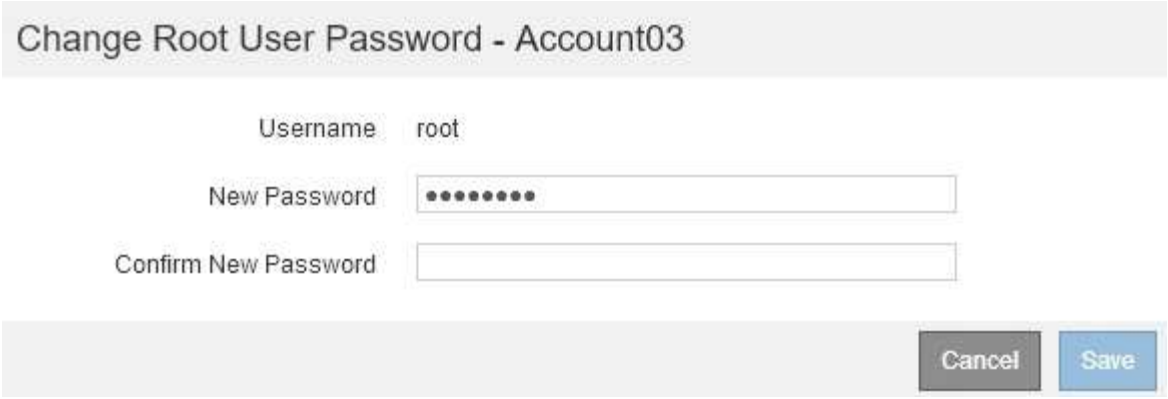



2. Selecione a conta de locatário que você deseja editar.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Use a caixa de pesquisa para procurar uma conta de locatário por nome de exibição ou ID de locatário.

   Os botões Ver Detalhes, Editar e ações ficam ativados.

3. Na lista suspensa **ações**, selecione **alterar senha de root**.




4. Introduza a nova palavra-passe para a conta de locatário.
5. Selecione **Guardar**.

**Informações relacionadas**

"Controlar o acesso do administrador ao StorageGRID"

## Editando uma conta de locatário

Você pode editar uma conta de locatário para alterar o nome de exibição, alterar a configuração de origem de identidade, permitir ou desativar serviços de plataforma ou inserir uma cota de armazenamento.

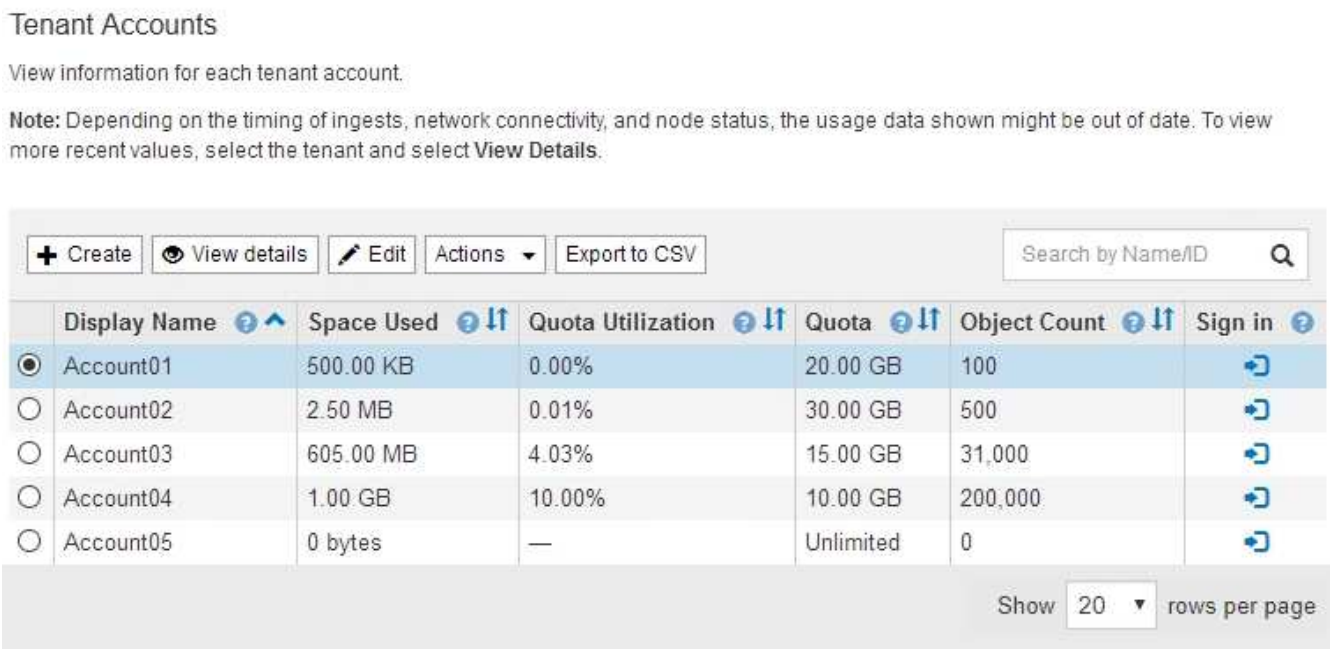
**O que você vai precisar**

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

**Passos**

1. Selecione **tenants**.

   A página Contas do locatário é exibida e lista todas as contas de locatário existentes.

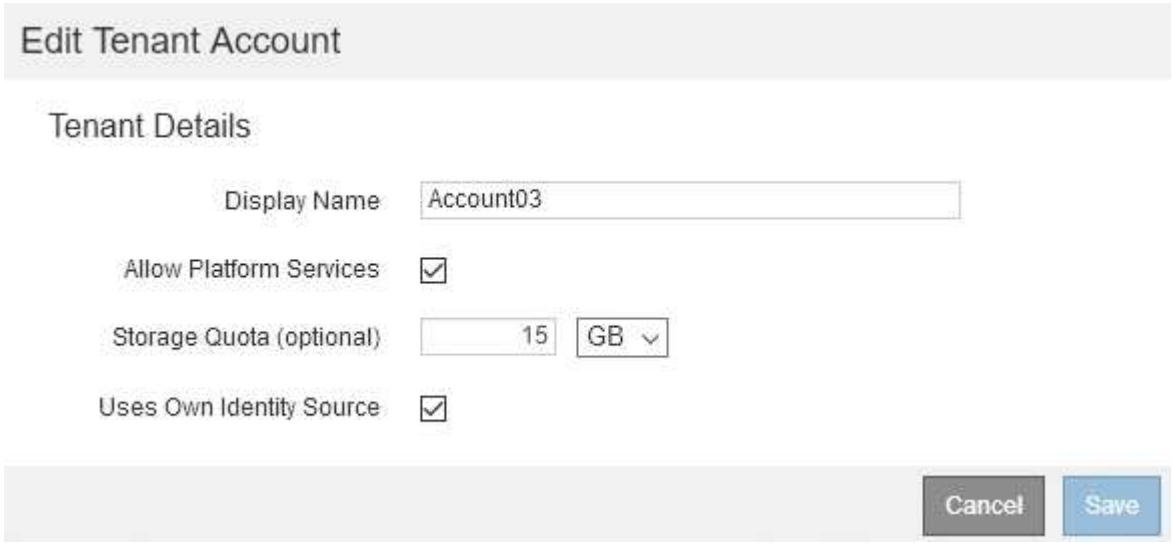


2. Selecione a conta de locatário que você deseja editar.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Use a caixa de pesquisa para procurar uma conta de locatário por nome de exibição ou ID de locatário.

3. Selecione **Editar**.

   A página Editar conta do locatário é exibida. Este exemplo é para uma grade que não usa logon único (SSO). Essa conta de locatário não configurou sua própria origem de identidade.




4. Altere os valores dos campos conforme necessário.
   a. Altere o nome de exibição dessa conta de locatário.
   b. Altere a configuração da caixa de seleção **permitir Serviços de Plataforma** para determinar se a conta de locatário pode usar serviços de plataforma para seus buckets do S3.

      Se você desabilitar os serviços de plataforma para um locatário que já os esteja usando, os serviços que eles configuraram para seus buckets do S3 deixarão de funcionar. Nenhuma mensagem de erro é enviada ao locatário. Por exemplo, se o locatário tiver configurado a replicação do CloudMirror para um bucket do S3, ele ainda poderá armazenar objetos no bucket, mas as cópias desses objetos não serão mais feitas no bucket externo do S3 configurado como um endpoint.

   c. Para **cota de armazenamento**, altere o número máximo de gigabytes, terabytes ou petabytes disponíveis para os objetos desse locatário ou deixe o campo em branco se desejar que esse locatário tenha uma cota ilimitada.

      A cota de armazenamento de um locatário representa uma quantidade lógica (tamanho do objeto), e não uma quantidade física (tamanho no disco). As cópias ILM e a codificação de apagamento não contribuem para a quantidade de cota usada.

Para monitorar o uso de armazenamento de cada conta de locatário, selecione **uso**. As contas de inquilino também podem monitorar seu próprio uso no Dashboard no Gerenciador do locatário ou com a API de gerenciamento do locatário. Observe que os valores de uso de storage de um locatário podem ficar desatualizados se os nós forem isolados de outros nós na grade. Os totais serão atualizados quando a conetividade de rede for restaurada.

d. Altere a configuração da caixa de seleção **usa a própria origem de identidade** para determinar se a conta de locatário usará sua própria origem de identidade ou a origem de identidade que foi configurada para o Gerenciador de Grade.

Se a caixa de verificação **usa a própria fonte de identidade** for:

- Desativado e verificado, o locatário já habilitou sua própria fonte de identidade. Um locatário deve desativar sua origem de identidade antes de poder usar a fonte de identidade que foi configurada para o Gerenciador de Grade.
- Desativado e desmarcado, SSO está ativado para o sistema StorageGRID. O locatário deve usar a fonte de identidade que foi configurada para o Gerenciador de Grade.

5. Selecione **Guardar**.

**Informações relacionadas**

"Gerenciamento de serviços de plataforma para contas de locatários do S3"

"Use uma conta de locatário"

## Excluindo uma conta de locatário

Você pode excluir uma conta de locatário se quiser remover permanentemente o acesso do locatário ao sistema.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter removido todos os buckets (S3), contentores (Swift) e objetos associados à conta de locatário.

**Passos**

1. Selecione **tenants**.
2. Selecione a conta de locatário que deseja excluir.

   Se o sistema incluir mais de 20 itens, você pode especificar quantas linhas são mostradas em cada página de uma vez. Use a caixa de pesquisa para procurar uma conta de locatário por nome de exibição ou ID de locatário.

3. Na lista suspensa **ações**, selecione **Remover**.
4. Selecione **OK**.

**Informações relacionadas**

"Controlar o acesso do administrador ao StorageGRID"

## Gerenciamento de serviços de plataforma para contas de locatários do S3

Se você ativar os serviços de plataforma para contas de locatário do S3, configure sua grade para que os locatários possam acessar os recursos externos necessários para usar esses serviços.

- "Quais são os serviços de plataforma"
- "Rede e portas para serviços de plataforma"
- "Entrega por local de mensagens de serviços de plataforma"
- "Solução de problemas de serviços da plataforma"

### Quais são os serviços de plataforma

Os serviços de plataforma incluem replicação do CloudMirror, notificações de eventos e o serviço de integração de pesquisa.

Esses serviços permitem que os locatários usem a seguinte funcionalidade com seus buckets do S3:

- **Replicação do CloudMirror**: O serviço de replicação do StorageGRID CloudMirror é usado para espelhar objetos específicos de um bucket do StorageGRID para um destino externo especificado.

  Por exemplo, você pode usar a replicação do CloudMirror para espelhar Registros específicos de clientes no Amazon S3 e aproveitar os serviços da AWS para realizar análises nos seus dados.

  > ⓘ A replicação do CloudMirror não é suportada se o bucket de origem tiver o S3 Object Lock ativado.

- **Notificações**: As notificações de eventos por bucket são usadas para enviar notificações sobre ações específicas executadas em objetos para um Amazon Simple Notification Service (SNS) externo especificado.

  Por exemplo, você pode configurar alertas para serem enviados aos administradores sobre cada objeto adicionado a um bucket, onde os objetos representam arquivos de log associados a um evento crítico do sistema.

  > ⓘ Embora a notificação de evento possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

- **Serviço de integração de pesquisa**: O serviço de integração de pesquisa é usado para enviar metadados de objetos S3 para um índice Elasticsearch especificado, onde os metadados podem ser pesquisados ou analisados usando o serviço externo.

  Por exemplo, você pode configurar seus buckets para enviar metadados de objeto S3 para um serviço Elasticsearch remoto. Você pode usar o Elasticsearch para realizar pesquisas entre buckets e realizar análises sofisticadas de padrões presentes nos metadados do objeto.

  > ⓘ Embora a integração do Elasticsearch possa ser configurada em um bucket com o bloqueio de objeto S3 ativado, os metadados do bloqueio de objeto S3 (incluindo o status reter até a data e retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Com os serviços de plataforma, os locatários têm a capacidade de usar recursos de storage externos, serviços de notificação e serviços de pesquisa ou análise com seus dados. Como o local de destino para serviços de plataforma geralmente é externo à implantação do StorageGRID, você deve decidir se deseja permitir que os locatários usem esses serviços. Se o fizer, você deverá habilitar o uso de serviços de plataforma quando criar ou editar contas de locatário. Você também deve configurar sua rede de modo que as mensagens de serviços de plataforma que os locatários geram possam chegar aos destinos deles.

#### Recomendações para o uso de serviços de plataforma

Antes de usar os serviços de plataforma, você deve estar ciente das seguintes recomendações:

- Você não deve usar mais de 100 locatários ativos com solicitações do S3 que exigem replicação, notificações e integração de pesquisa do CloudMirror. Ter mais de 100 inquilinos ativos ativos pode resultar em desempenho mais lento do cliente S3.
- Se um bucket do S3 no sistema StorageGRID tiver o controle de versão e a replicação do CloudMirror habilitado, você também deverá habilitar o controle de versão do bucket do S3 para o endpoint de destino. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no endpoint.

#### Informações relacionadas

"Use uma conta de locatário"

"Configurando as configurações de proxy de armazenamento"

"Monitorizar Resolução de problemas"

#### Rede e portas para serviços de plataforma

Se você permitir que um locatário do S3 use serviços de plataforma, você deve configurar a rede para a grade para garantir que as mensagens de serviços de plataforma possam ser entregues aos seus destinos.

Você pode ativar os serviços de plataforma para uma conta de locatário do S3 ao criar ou atualizar a conta de locatário. Se os serviços de plataforma estiverem ativados, o locatário poderá criar endpoints que servem como destino para replicação do CloudMirror, notificações de eventos ou mensagens de integração de pesquisa a partir de seus buckets do S3. Essas mensagens de serviços de plataforma são enviadas de nós de storage que executam o serviço ADC para os endpoints de destino.

Por exemplo, os locatários podem configurar os seguintes tipos de endpoints de destino:

- Um cluster Elasticsearch hospedado localmente
- Um aplicativo local compatível com o recebimento de mensagens do Simple Notification Service (SNS)
- Um bucket do S3 hospedado localmente na mesma ou em outra instância do StorageGRID
- Um endpoint externo, como um endpoint no Amazon Web Services.

Para garantir que as mensagens dos serviços da plataforma possam ser entregues, você deve configurar a rede ou as redes que contêm os nós de armazenamento ADC. Você deve garantir que as portas a seguir possam ser usadas para enviar mensagens de serviços de plataforma para os endpoints de destino.

Por padrão, as mensagens dos serviços da plataforma são enviadas nas seguintes portas:

- **80**: Para URIs de endpoint que começam com http
- **443**: Para URIs de endpoint que começam com https

Os locatários podem especificar uma porta diferente quando criam ou editam um endpoint.

> Se uma implantação do StorageGRID for usada como destino para a replicação do CloudMirror, as mensagens de replicação podem ser recebidas em uma porta diferente de 80 ou 443. Verifique se a porta que está sendo usada para S3 pela implantação do StorageGRID de destino está especificada no endpoint.

Se você usar um servidor proxy não transparente, também deverá configurar as configurações de proxy de armazenamento para permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

**Informações relacionadas**

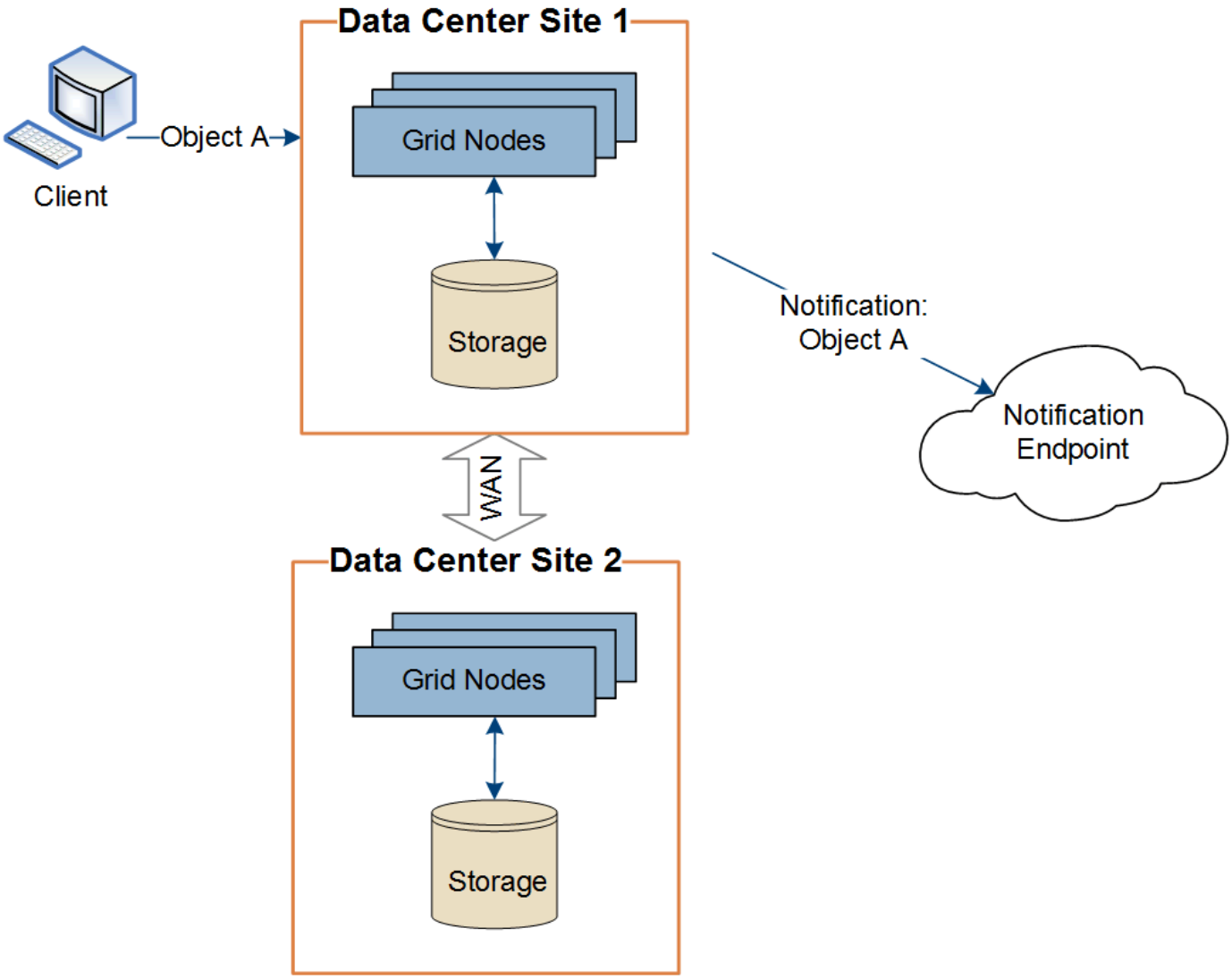
"Configurando as configurações de proxy de armazenamento"

"Use uma conta de locatário"

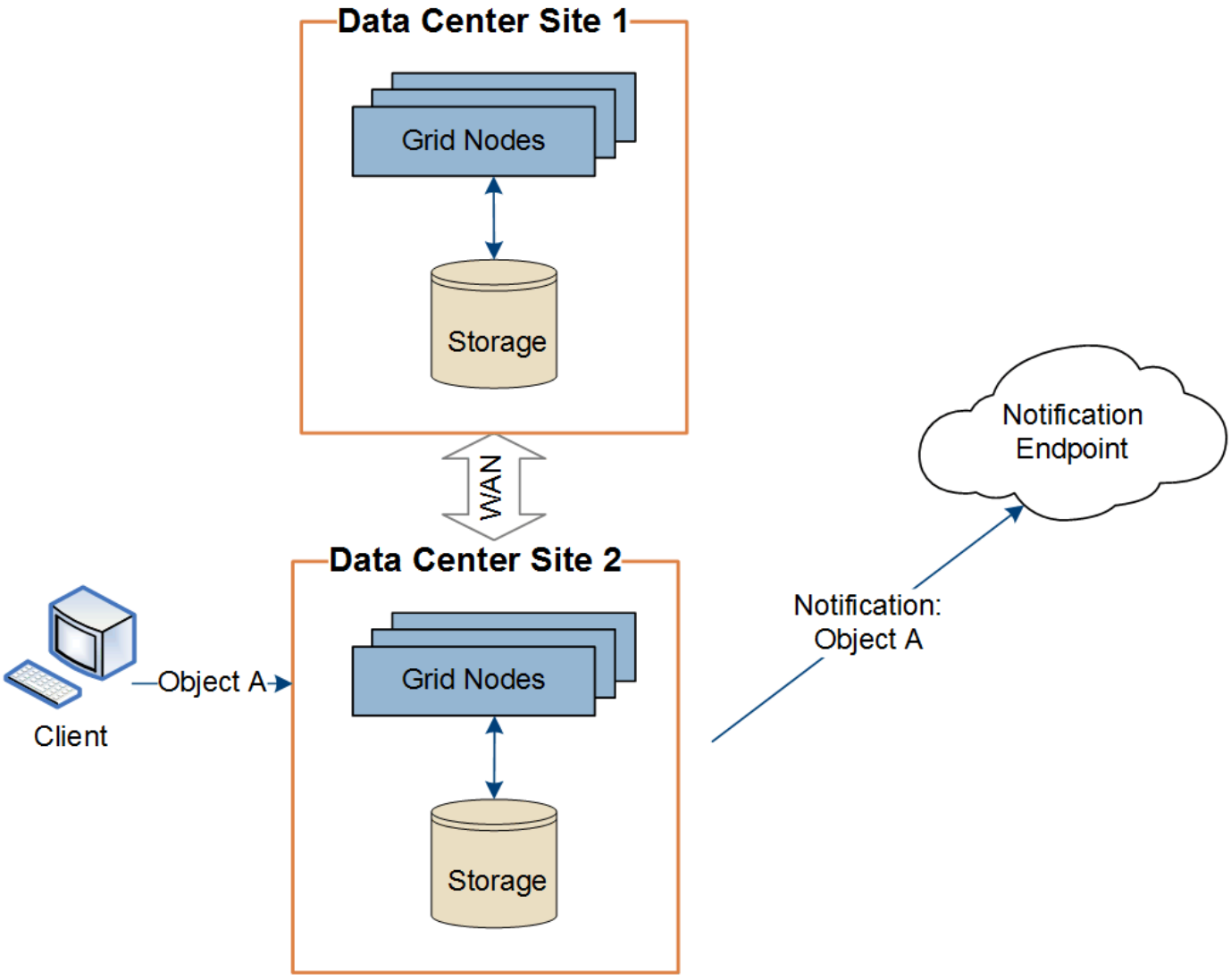
**Entrega por local de mensagens de serviços de plataforma**

Todas as operações de serviços de plataforma são realizadas por local.

Ou seja, se um locatário usar um cliente para executar uma operação de criação de API S3 em um objeto conetando-se a um nó de gateway no Data Center Site 1, a notificação sobre essa ação será acionada e enviada a partir do Data Center Site 1.




Se o cliente executar posteriormente uma operação de exclusão de API S3 nesse mesmo objeto do Data Center Site 2, a notificação sobre a ação de exclusão será acionada e enviada do Data Center Site 2.




Certifique-se de que a rede em cada local está configurada de forma a que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

**Solução de problemas de serviços da plataforma**

Os endpoints usados nos serviços de plataforma são criados e mantidos por usuários de inquilinos no Gerenciador de inquilinos; no entanto, se um locatário tiver problemas para configurar ou usar serviços de plataforma, talvez você possa usar o Gerenciador de Grade para ajudar a resolver o problema.

**Problemas com novos endpoints**

Antes que um locatário possa usar os serviços da plataforma, ele deve criar um ou mais pontos de extremidade usando o Gerenciador do locatário. Cada endpoint representa um destino externo para um serviço de plataforma, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do serviço de notificação simples ou um cluster do Elasticsearch hospedado localmente ou na AWS. Cada endpoint inclui a localização do recurso externo e as credenciais necessárias para acessar esse recurso.

Quando um locatário cria um endpoint, o sistema StorageGRID valida que o endpoint existe e que ele pode ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.

Se a validação do endpoint falhar, uma mensagem de erro explica por que a validação do endpoint falhou. O usuário do locatário deve resolver o problema e tentar criar o endpoint novamente.

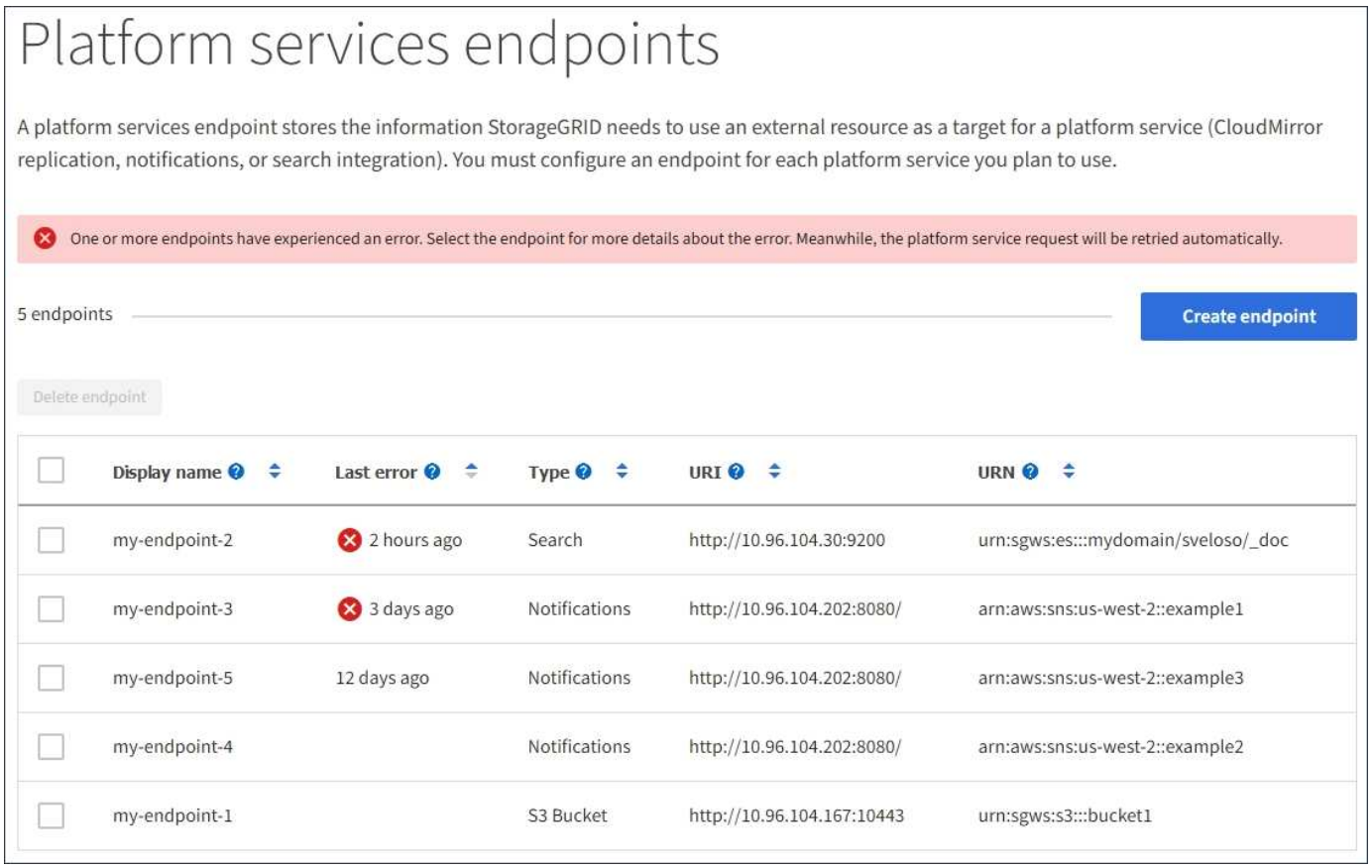
A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para a conta do locatário.

**Problemas com endpoints existentes**

Se ocorrer um erro quando o StorageGRID tenta alcançar um endpoint existente, uma mensagem é exibida no Dashboard no Gerenciador de locatário.

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Os usuários do locatário podem ir para a página Endpoints para revisar a mensagem de erro mais recente para cada endpoint e determinar quanto tempo atrás o erro ocorreu. A coluna **último erro** exibe a mensagem de erro mais recente para cada endpoint e indica quanto tempo atrás o erro ocorreu. Erros que incluem o ícone ocorreram nos últimos 7 dias.




Algumas mensagens de erro na coluna **último erro** podem incluir um LOGID entre parênteses. Um administrador de grade ou suporte técnico pode usar esse ID para localizar informações mais detalhadas sobre o erro no bycast.log.

**Problemas relacionados aos servidores proxy**

Se você tiver configurado um proxy de storage entre nós de storage e endpoints de serviço de plataforma,

poderão ocorrer erros se o serviço proxy não permitir mensagens do StorageGRID. Para resolver esses problemas, verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma não sejam bloqueadas.

#### Determinar se ocorreu um erro

Se algum erro de endpoint tiver ocorrido nos últimos 7 dias, o Dashboard no Gerenciador de inquilinos exibirá uma mensagem de alerta. Pode aceder à página Endpoints para ver mais detalhes sobre o erro.

#### Falha nas operações do cliente

Alguns problemas de serviços de plataforma podem causar falha nas operações do cliente no bucket do S3. Por exemplo, as operações do cliente S3 falharão se o serviço interno da Máquina de Estado replicado (RSM) parar ou se houver muitas mensagens de serviços de plataforma enfileiradas para entrega.

Para verificar o status dos serviços:

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site*** > ***Storage Node*** > **SSM** > **Serviços**.

#### Erros de endpoint recuperáveis e irrecuperáveis

Após a criação de endpoints, os erros de solicitação de serviço da plataforma podem ocorrer por vários motivos. Alguns erros são recuperáveis com a intervenção do usuário. Por exemplo, erros recuperáveis podem ocorrer pelos seguintes motivos:

- As credenciais do usuário foram excluídas ou expiraram.
- O intervalo de destino não existe.
- A notificação não pode ser entregue.

Se o StorageGRID encontrar um erro recuperável, a solicitação de serviço da plataforma será tentada novamente até que seja bem-sucedida.

Outros erros são irrecuperáveis. Por exemplo, um erro irrecuperável ocorre se o endpoint for excluído.

Se o StorageGRID encontrar um erro de endpoint irrecuperável, o alarme de Eventos totais (SMTT) é acionado no Gerenciador de Grade. Para visualizar o alarme Total de Eventos:

1. Selecione **nós**.
2. Selecione ***site*** > ***grid node*** > **Eventos**.
3. Veja o último evento na parte superior da tabela.

   As mensagens de evento também são listadas em `/var/local/log/bycast-err.log`.

4. Siga as orientações fornecidas no conteúdo do alarme SMTT para corrigir o problema.
5. Clique em **Redefinir contagens de eventos**.
6. Notificar o locatário dos objetos cujas mensagens de serviços da plataforma não foram entregues.
7. Instrua o locatário a reativar a replicação ou notificação com falha atualizando os metadados ou as tags do objeto.

   O locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

#### As mensagens dos serviços da plataforma não podem ser entregues

Se o destino encontrar um problema que o impeça de aceitar mensagens de serviços da plataforma, a operação do cliente no bucket será bem-sucedida, mas a mensagem de serviços da plataforma não será entregue. Por exemplo, esse erro pode acontecer se as credenciais forem atualizadas no destino, de modo que o StorageGRID não possa mais se autenticar no serviço de destino.

Se as mensagens dos serviços da plataforma não puderem ser entregues devido a um erro irrecuperável, o alarme de Eventos totais (SMTT) é acionado no Gerenciador de Grade.

#### Desempenho mais lento para solicitações de serviço de plataforma

O software StorageGRID pode controlar as solicitações recebidas do S3 para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o endpoint de destino pode receber as solicitações. O estrangulamento só ocorre quando há um backlog de solicitações aguardando para serem enviadas para o endpoint de destino.

O único efeito visível é que as solicitações S3 recebidas demorarão mais tempo para serem executadas. Se você começar a detetar desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o backlog de solicitações continuar a crescer, as operações do cliente S3 (como SOLICITAÇÕES PUT) acabarão falhando.

As solicitações do CloudMirror são mais propensas a serem afetadas pelo desempenho do endpoint de destino, pois essas solicitações geralmente envolvem mais transferência de dados do que solicitações de integração de pesquisa ou notificação de eventos.

#### As solicitações de serviço da plataforma falham

Para visualizar a taxa de falha da solicitação para serviços de plataforma:

1. Selecione **nós**.
2. Selecione ***site*** > **Serviços de Plataforma**.
3. Veja o gráfico taxa de falha de solicitação.


**Alerta de serviços de plataforma indisponíveis**

O alerta **Platform services unavailable** indica que nenhuma operação de serviço de plataforma pode ser executada em um local porque poucos nós de storage com o serviço RSM estão em execução ou disponíveis.

O serviço RSM garante que as solicitações de serviço da plataforma sejam enviadas para seus respetivos endpoints.

Para resolver esse alerta, determine quais nós de storage no local incluem o serviço RSM. (O serviço RSM está presente nos nós de storage que também incluem o serviço ADC.) Em seguida, certifique-se de que uma maioria simples desses nós de storage esteja em execução e disponível.

Se mais de um nó de storage que contém o serviço RSM falhar em um local, você perderá quaisquer solicitações de serviço de plataforma pendentes para esse site.

**Orientação adicional para solução de problemas para endpoints de serviços de plataforma**

Para obter informações adicionais sobre a solução de problemas de endpoints de serviços de plataforma, consulte as instruções para o uso de contas de locatário.

"Use uma conta de locatário"

**Informações relacionadas**

"Monitorizar Resolução de problemas"

"Configurando as configurações de proxy de armazenamento"

# Configurando conexões de cliente S3 e Swift

Como administrador de grade, você gerencia as opções de configuração que controlam como os locatários S3 e Swift podem conetar aplicativos clientes ao seu sistema StorageGRID para armazenar e recuperar dados. Existem várias opções diferentes para atender a diferentes requisitos de cliente e locatário.

Os aplicativos clientes podem armazenar ou recuperar objetos conetando-se a qualquer um dos seguintes:

- O serviço Load Balancer em nós de administração ou nós de gateway, ou, opcionalmente, o endereço IP virtual de um grupo de alta disponibilidade (HA) de nós de administração ou nós de gateway
- O serviço CLB em nós de Gateway, ou, opcionalmente, o endereço IP virtual de um grupo de nós de gateway de alta disponibilidade

  O serviço CLB está obsoleto. Os clientes configurados antes da versão do StorageGRID 11,3 podem continuar a usar o serviço CLB nos nós de gateway. Todos os outros aplicativos clientes que dependem do StorageGRID para fornecer balanceamento de carga devem se conetar usando o serviço de balanceamento de carga.

- Nós de storage, com ou sem um balanceador de carga externo

Opcionalmente, você pode configurar os seguintes recursos em seu sistema StorageGRID:

- **Serviço de balanceamento de carga**: Você permite que os clientes usem o serviço de balanceamento de carga criando pontos de extremidade do balanceador de carga para conexões de cliente. Ao criar um endpoint de balanceador de carga, você especifica um número de porta, se o endpoint aceita conexões HTTP ou HTTPS, o tipo de cliente (S3 ou Swift) que usará o endpoint e o certificado a ser usado para conexões HTTPS (se aplicável).
- **Rede Cliente não confiável**: Você pode tornar a rede Cliente mais segura configurando-a como não confiável. Quando a rede do cliente não é confiável, os clientes só podem se conetar usando pontos de extremidade do balanceador de carga.
- **Grupos de alta disponibilidade**: Você pode criar um grupo de HA de nós de Gateway ou nós de administrador para criar uma configuração de backup ativo ou usar DNS de round-robin ou um balanceador de carga de terceiros e vários grupos de HA para obter uma configuração ativo-ativo. As conexões de cliente são feitas usando os endereços IP virtuais de grupos HA.

Você também pode habilitar o uso de HTTP para clientes que se conetam ao StorageGRID diretamente aos nós de armazenamento ou usando o serviço CLB (obsoleto), e você pode configurar nomes de domínio de endpoint de API S3 para clientes S3.

## Resumo: Endereços IP e portas para conexões de clientes

Os aplicativos clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de grade e o número da porta de um serviço nesse nó. Se os grupos de alta disponibilidade (HA) estiverem configurados, os aplicativos clientes poderão se conetar usando o endereço IP virtual do grupo HA.

**Sobre esta tarefa**

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conetar ao StorageGRID e os endereços IP e as portas usadas para cada tipo de conexão. As instruções descrevem como localizar essas informações no Gerenciador de Grade se os pontos de extremidade do balanceador de carga e os grupos de alta disponibilidade (HA) já estiverem configurados.

| Onde a conexão é feita | Serviço ao qual o cliente se coneta | Endereço IP | Porta |
|---|---|---|---|
| Grupo HA | Balanceador de carga | Endereço IP virtual de um grupo HA | • Porta de extremidade do balanceador de carga |
| Grupo HA | CLB<br><br>**Nota:** o serviço CLB está obsoleto. | Endereço IP virtual de um grupo HA | Portas S3 padrão:<br>• HTTPS: 8082<br>• HTTP: 8084<br>Portas Swift padrão:<br>• HTTPS:8083<br>• HTTP:8085 |
| Nó de administração | Balanceador de carga | Endereço IP do nó Admin | • Porta de extremidade do balanceador de carga |
| Nó de gateway | Balanceador de carga | Endereço IP do nó de gateway | • Porta de extremidade do balanceador de carga |

| Onde a conexão é feita | Serviço ao qual o cliente se coneta | Endereço IP | Porta |
|---|---|---|---|
| Nó de gateway | CLB<br><br>**Nota:** o serviço CLB está obsoleto. | Endereço IP do nó de gateway<br><br>**Nota:** por padrão, as portas HTTP para CLB e LDR não estão ativadas. | Portas S3 padrão:<br>• HTTPS: 8082<br>• HTTP: 8084<br>Portas Swift padrão:<br>• HTTPS:8083<br>• HTTP:8085 |
| Nó de storage | LDR | Endereço IP do nó de armazenamento | Portas S3 padrão:<br>• HTTPS: 18082<br>• HTTP: 18084<br>Portas Swift padrão:<br>• HTTPS: 18083<br>• HTTP:18085 |

**Exemplos**

Para conetar um cliente S3 ao ponto de extremidade do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

- `https://VIP-of-HA-group:LB-endpoint-port`

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.5 e o número da porta de um endpoint do balanceador de carga S3 for 10443, um cliente S3 poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.5:10443`

Para conetar um cliente Swift ao endpoint do Load Balancer de um grupo de HA de nós de Gateway, use um URL estruturado como mostrado abaixo:

- `https://VIP-of-HA-group:LB-endpoint-port`

Por exemplo, se o endereço IP virtual do grupo HA for 192.0.2.6 e o número da porta de um endpoint do Swift Load Balancer for 10444, um cliente Swift poderá usar o seguinte URL para se conetar ao StorageGRID:

- `https://192.0.2.6:10444`

É possível configurar um nome DNS para o endereço IP que os clientes usam para se conetar ao StorageGRID. Contacte o administrador da rede local.

**Passos**

1. Faça login no Gerenciador de Grade usando um navegador compatível.

2. Para localizar o endereço IP de um nó de grade:
   a. Selecione **nós**.
   b. Selecione o nó de administração, nó de gateway ou nó de armazenamento ao qual deseja se conetar.
   c. Selecione a guia **Visão geral**.
   d. Na seção informações do nó, observe os endereços IP do nó.
   e. Clique em **Mostrar mais** para visualizar endereços IPv6 e mapeamentos de interface.

      Você pode estabelecer conexões de aplicativos cliente para qualquer um dos endereços IP na lista:

      - **eth0:** rede de Grade
      - **eth1:** Admin Network (opcional)
      - **eth2:** rede de clientes (opcional)

      > Se você estiver exibindo um nó de administrador ou um nó de gateway e for o nó ativo em um grupo de alta disponibilidade, o endereço IP virtual do grupo de HA será exibido em eth2.

3. Para localizar o endereço IP virtual de um grupo de alta disponibilidade:
   a. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.
   b. Na tabela, anote o endereço IP virtual do grupo HA.
4. Para localizar o número da porta de um endpoint do Load Balancer:
   a. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

      A página Load Balancer Endpoints é exibida, mostrando a lista de endpoints que já foram configurados.

   b. Selecione um endpoint e clique em **Editar endpoint**.

      A janela Editar ponto final abre-se e apresenta detalhes adicionais sobre o ponto final.

   c. Confirme se o endpoint selecionado está configurado para uso com o protocolo correto (S3 ou Swift) e, em seguida, clique em **Cancelar**.
   d. Observe o número da porta do endpoint que você deseja usar para uma conexão de cliente.

      > Se o número da porta for 80 ou 443, o endpoint será configurado apenas em nós de Gateway, uma vez que essas portas estão reservadas em nós de administração. Todas as outras portas são configuradas nos nós de Gateway e nos de Admin.

## Gerenciamento do balanceamento de carga

Você pode usar as funções de balanceamento de carga do StorageGRID para lidar com cargas de trabalho de ingestão e recuperação de clientes S3 e Swift. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo cargas de trabalho e conexões entre vários nós de storage.

Você pode obter balanceamento de carga em seu sistema StorageGRID das seguintes maneiras:

- Use o serviço Load Balancer, que é instalado em nós de administração e nós de gateway. O serviço Load Balancer fornece balanceamento de carga de camada 7 e executa o encerramento TLS das solicitações do cliente, inspeciona as solicitações e estabelece novas conexões seguras aos nós de storage. Este é o mecanismo de balanceamento de carga recomendado.
- Use o serviço CLB (Connection Load Balancer), que é instalado somente em nós de Gateway. O serviço CLB fornece balanceamento de carga da camada 4 e suporta custos de link.

  O serviço CLB está obsoleto.

- Integre um balanceador de carga de terceiros. Entre em Contato com o representante da sua conta NetApp para obter detalhes.

**Como funciona o balanceamento de carga - Serviço do Load Balancer**

## O serviço Load Balancer distribui conexões de rede recebidas de aplicativos clientes para nós de storage. Para ativar o balanceamento de carga, você deve configurar pontos de extremidade do balanceador de carga usando o Gerenciador de Grade.

Você pode configurar pontos de extremidade do balanceador de carga somente para nós de administrador ou nós de gateway, uma vez que esses tipos de nó contêm o serviço Load Balancer. Não é possível configurar pontos de extremidade para nós de storage ou nós de arquivamento.

Cada ponto de extremidade do balanceador de carga especifica uma porta, um protocolo (HTTP ou HTTPS), um tipo de serviço (S3 ou Swift) e um modo de encadernação. Os endpoints HTTPS requerem um certificado de servidor. Os modos de vinculação permitem restringir a acessibilidade das portas de endpoint a:

- Endereços IP virtuais (VIPs) específicos de alta disponibilidade (HA)
- Interfaces de rede específicas de nós específicos

#### Considerações de porta

Os clientes podem acessar qualquer um dos pontos de extremidade que você configurar em qualquer nó executando o serviço Load Balancer, com duas exceções: As portas 80 e 443 são reservadas em nós de administração, portanto, os pontos de extremidade configurados nessas portas suportam operações de balanceamento de carga somente em nós de Gateway.

Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

O serviço CLB está obsoleto.

#### Disponibilidade da CPU

O serviço Load Balancer em cada nó de administração e nó de gateway opera independentemente ao encaminhar tráfego S3 ou Swift para os nós de storage. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de storage com maior disponibilidade de CPU. As informações de carga da CPU do nó são atualizadas a cada poucos minutos, mas a ponderação pode ser atualizada com mais frequência. Todos os nós de storage recebem um valor mínimo de peso básico, mesmo que um nó informe a utilização de 100% ou não consiga relatar sua utilização.

Em alguns casos, as informações sobre a disponibilidade da CPU estão limitadas ao local onde o serviço Load Balancer está localizado.

**Informações relacionadas**

"Manter recuperar"

### Configuração dos pontos de extremidade do balanceador de carga

Você pode criar, editar e remover pontos de extremidade do balanceador de carga.

#### Criação de pontos de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga especifica uma porta, um protocolo de rede (HTTP ou HTTPS) e um tipo de serviço (S3 ou Swift). Se criar um endpoint HTTPS, tem de carregar ou gerar um certificado de servidor.

**O que você vai precisar**

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Se você tiver anteriormente as portas remapeadas que pretende usar para o serviço Load Balancer, você deve ter removido os remapes.

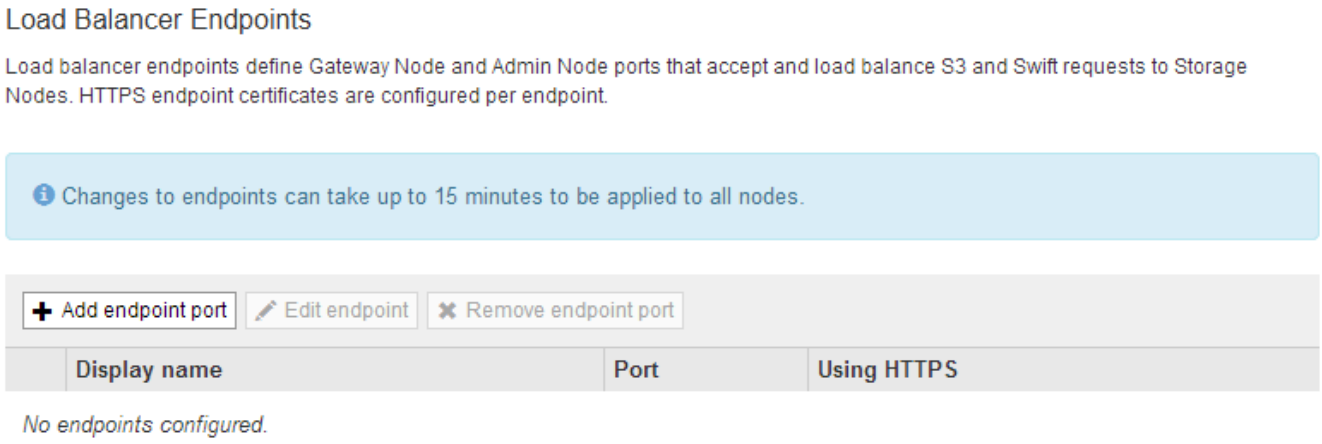
> Se você tiver remapeado quaisquer portas, não poderá usar as mesmas portas para configurar pontos de extremidade do balanceador de carga. Você pode criar endpoints usando portas remapeadas, mas esses endpoints serão remapeados para as portas e serviços CLB originais, não para o serviço Load Balancer. Siga as etapas nas instruções de recuperação e manutenção para remover os remapas de portas.

> O serviço CLB está obsoleto.

**Passos**

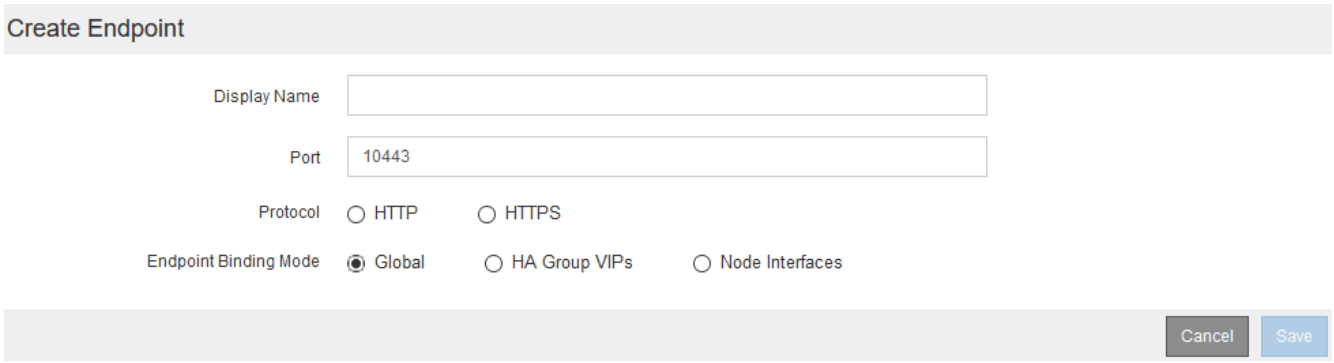
1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida.




2. Selecione **Adicionar endpoint**.

A caixa de diálogo criar ponto final é exibida.



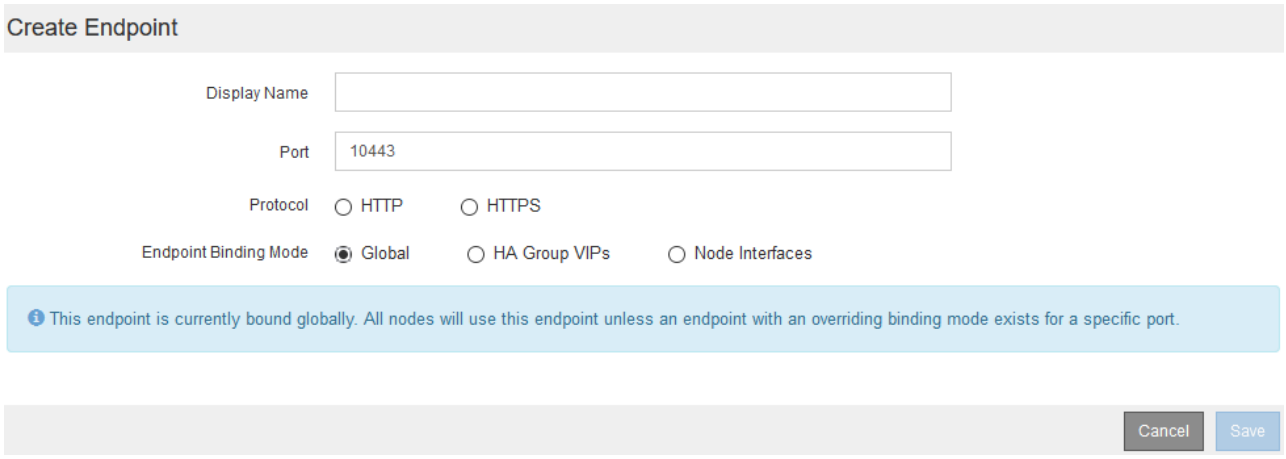

3. Insira um nome de exibição para o endpoint, que aparecerá na lista na página Load Balancer Endpoints.
4. Introduza um número de porta ou deixe o número de porta pré-preenchido como está.

   Se você inserir o número da porta 80 ou 443, o endpoint será configurado somente nos nós do Gateway, uma vez que essas portas serão reservadas nos nós de administração.

   > As portas usadas por outros serviços de grade não são permitidas. Consulte as diretrizes de rede para obter uma lista de portas usadas para comunicações internas e externas.

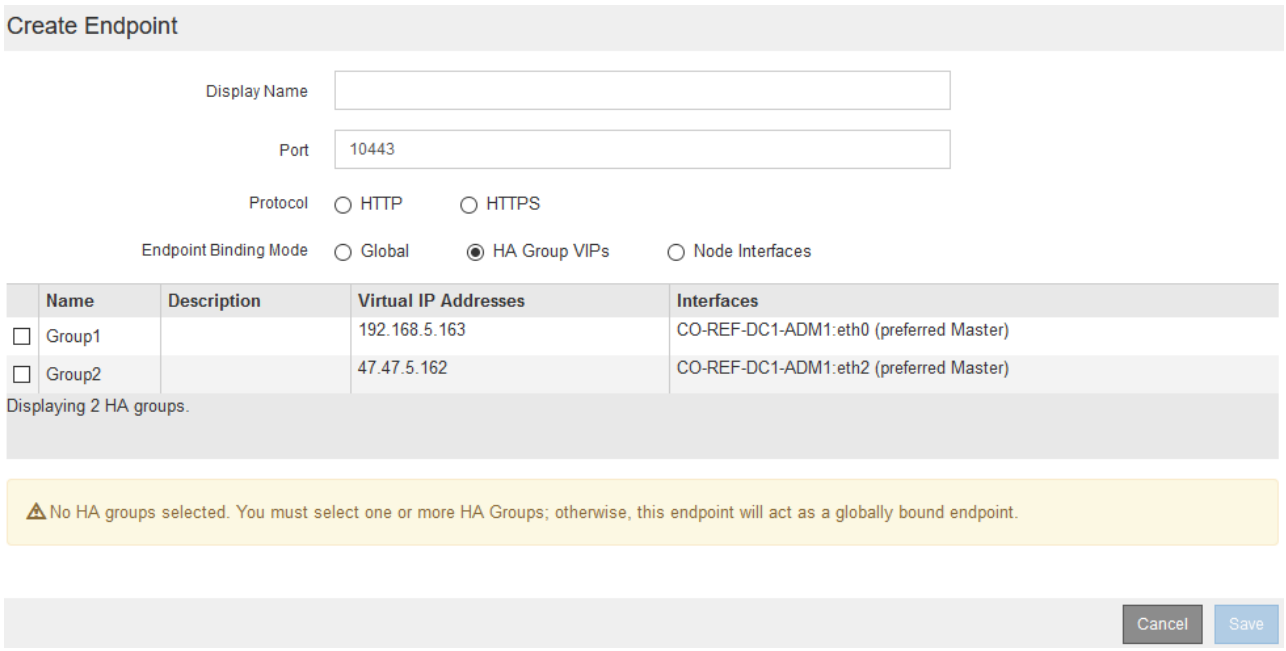
5. Selecione **HTTP** ou **HTTPS** para especificar o protocolo de rede para este endpoint.
6. Selecione um modo de encadernação de endpoint.

   - **Global** (padrão): O endpoint está acessível em todos os nós de Gateway e nós de Admin no número de porta especificado.



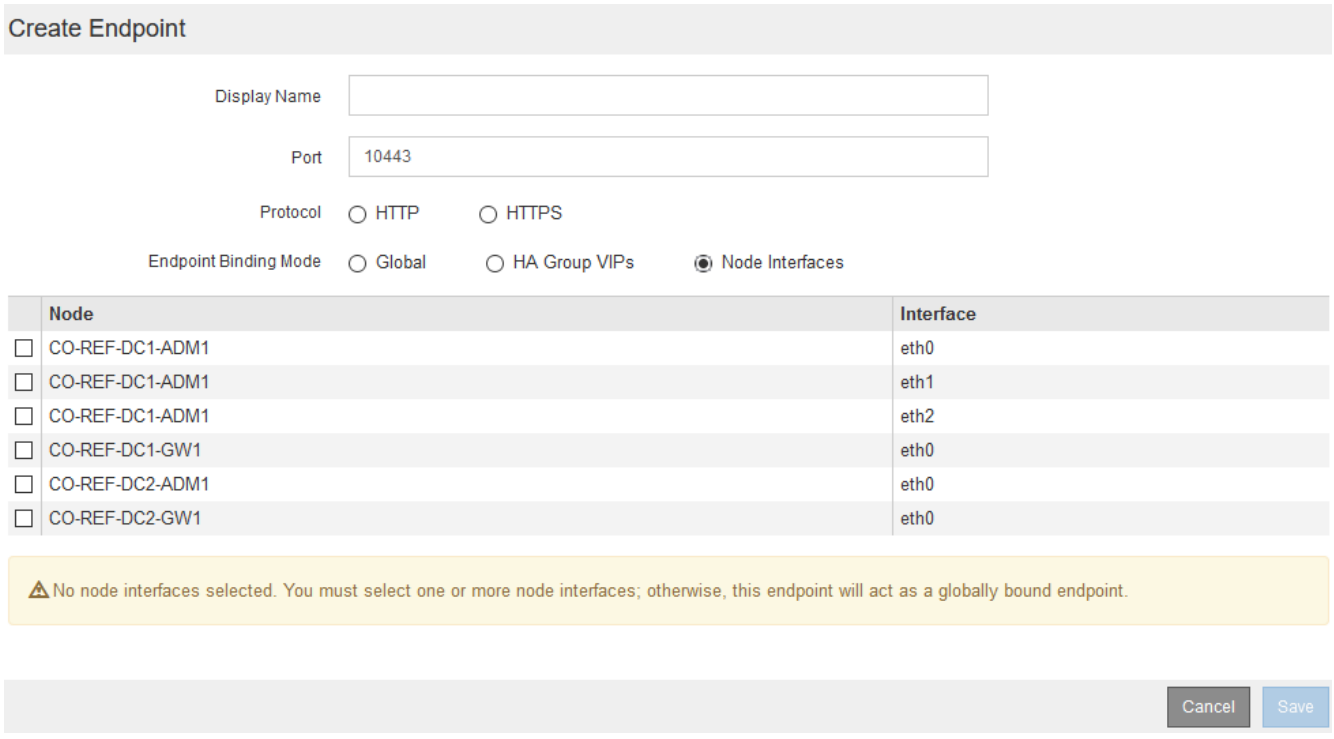

   - **VIPs do grupo HA**: O endpoint só pode ser acessado através dos endereços IP virtuais definidos para os grupos de HA selecionados. Os endpoints definidos neste modo podem reutilizar o mesmo número de porta, desde que os grupos de HA definidos por esses endpoints não se sobreponham entre si.

     Selecione os grupos de HA com os endereços IP virtuais onde deseja que o endpoint apareça.




- * Interfaces de nó*: O ponto de extremidade é acessível apenas nos nós designados e interfaces de rede. Os endpoints definidos neste modo podem reutilizar o mesmo número de porta desde que essas interfaces não se sobreponham umas às outras.

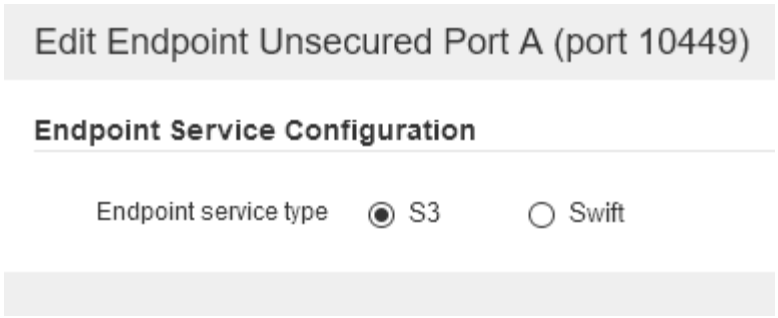
  Selecione as interfaces de nó em que você deseja que o endpoint apareça.




7. Selecione **Guardar**.

   A caixa de diálogo Editar ponto final é exibida.

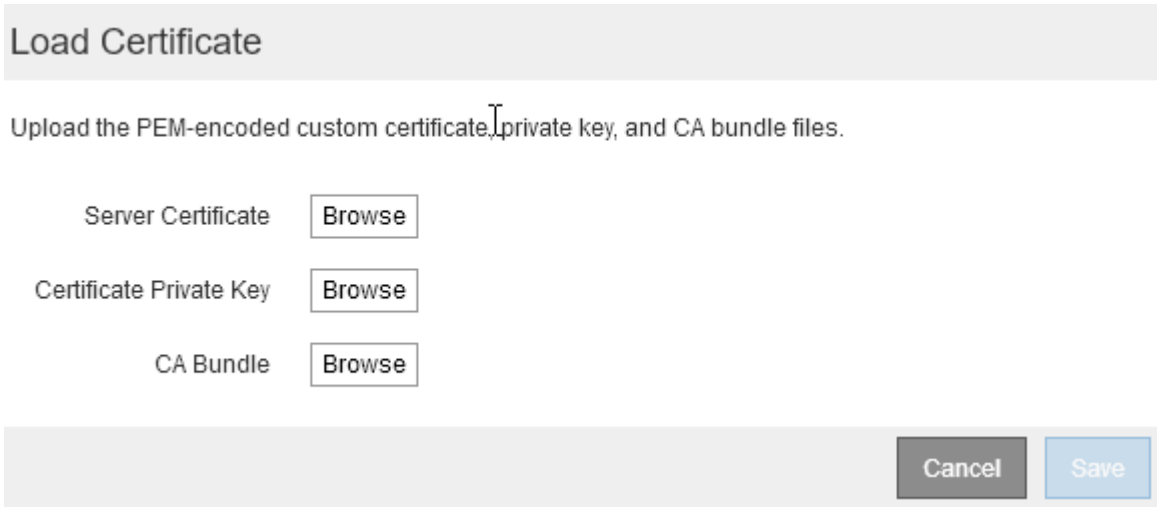
8. Selecione **S3** ou **Swift** para especificar o tipo de tráfego que este endpoint irá servir.




9. Se você selecionou **HTTP**, selecione **Salvar**.

   O ponto final não protegido é criado. A tabela na página Load Balancer Endpoints lista o nome de exibição, o número da porta, o protocolo e o ID do endpoint.

10. Se selecionou **HTTPS** e pretende carregar um certificado, selecione **carregar certificado**.




    a. Procure o certificado do servidor e a chave privada do certificado.

       Para permitir que os clientes S3 se conetem usando um nome de domínio de endpoint da API S3, use um certificado de domínio multidomínio ou curinga que corresponda a todos os nomes de domínio que o cliente possa usar para se conetar à grade. Por exemplo, o certificado do servidor pode usar o nome de domínio `*.example.com` .

"Configurando nomes de domínio de endpoint da API S3"

    a. Opcionalmente, procure um pacote de CA.
    b. Selecione **Guardar**.

       Os dados de certificado codificados em PEM para o endpoint são exibidos.

11. Se você selecionou **HTTPS** e deseja gerar um certificado, selecione **Generate Certificate**.


a. Introduza um nome de domínio ou um endereço IP.

   Você pode usar wildcards para representar os nomes de domínio totalmente qualificados de todos os nós de administrador e nós de gateway que executam o serviço Load Balancer. Por exemplo, `*.sgws.foo.com` usa o caractere curinga * para representar `gn1.sgws.foo.com` e `gn2.sgws.foo.com`.

"Configurando nomes de domínio de endpoint da API S3"

a. ➕Selecione para adicionar outros nomes de domínio ou endereços IP.

   Se você estiver usando grupos de alta disponibilidade (HA), adicione os nomes de domínio e endereços IP dos IPs virtuais de HA.

b. Opcionalmente, insira um assunto X,509, também chamado de Nome distinto (DN), para identificar quem possui o certificado.
c. Opcionalmente, selecione o número de dias em que o certificado é válido. O padrão é de 730 dias.
d. Selecione **Generate**.

   Os metadados do certificado e os dados do certificado codificados em PEM para o endpoint são exibidos.

12. Clique em **Salvar**.

    O endpoint é criado. A tabela na página Load Balancer Endpoints lista o nome de exibição, o número da porta, o protocolo e o ID do endpoint.

**Informações relacionadas**

"Manter recuperar"

"Diretrizes de rede"

"Gerenciamento de grupos de alta disponibilidade"

"Gerenciando redes de clientes não confiáveis"

#### Editar pontos de extremidade do balanceador de carga

Para um endpoint não protegido (HTTP), você pode alterar o tipo de serviço de endpoint entre S3 e Swift. Para um endpoint seguro (HTTPS), você pode editar o tipo de serviço de endpoint e exibir ou alterar o certificado de segurança.

**O que você vai precisar**

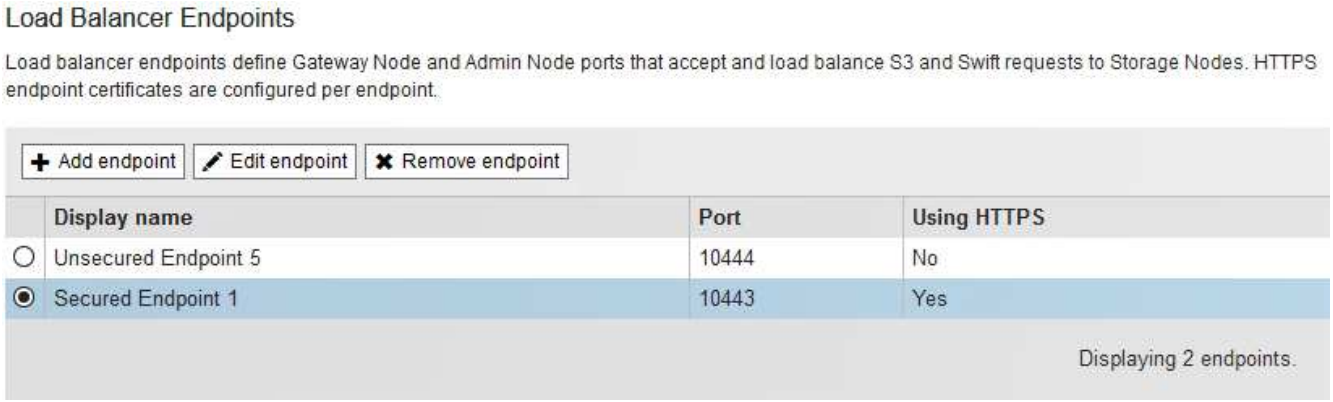
- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

**Passos**

1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida. Os endpoints existentes são listados na tabela.

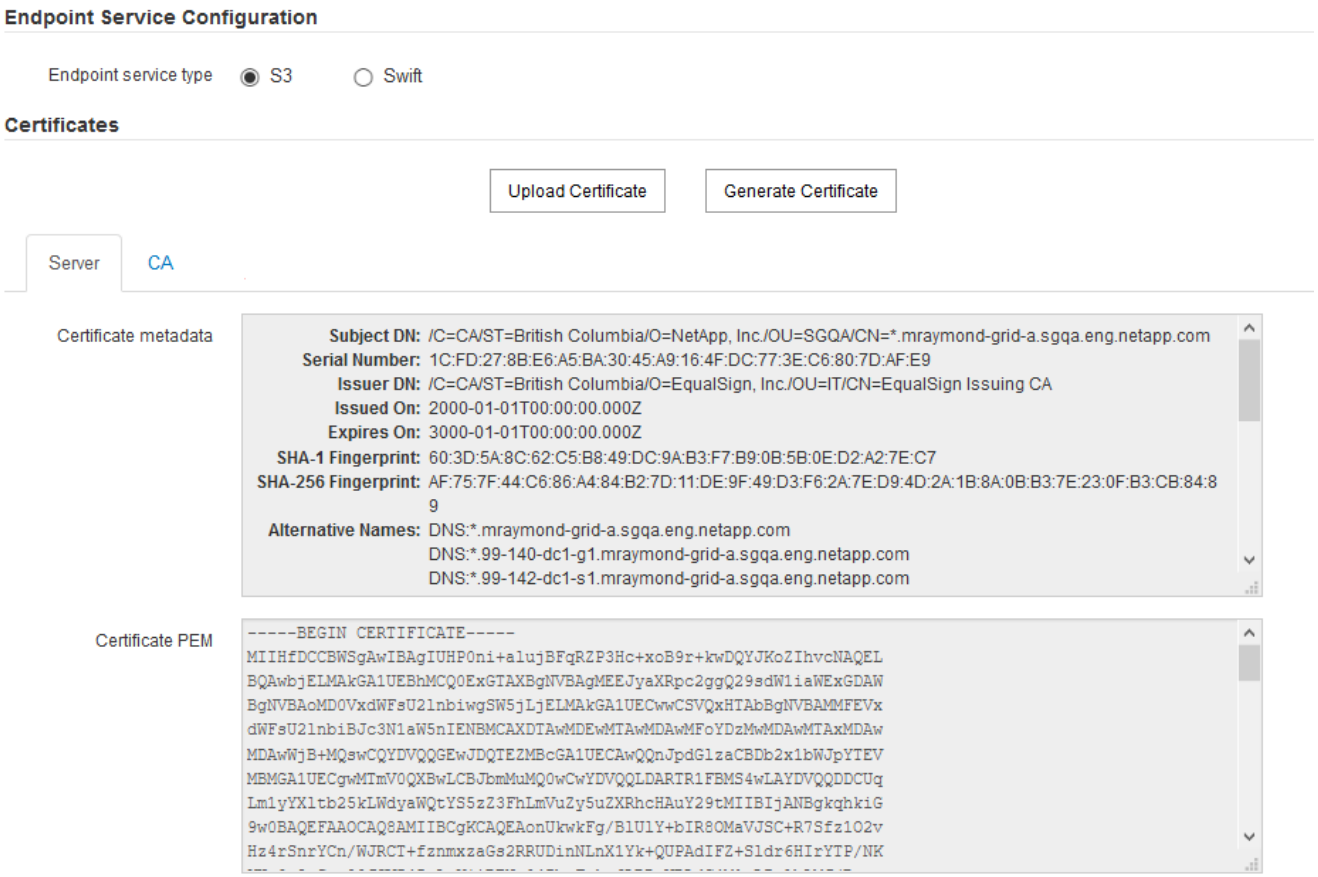
   Endpoints com certificados que expirarão em breve são identificados na tabela.




2. Selecione o ponto de extremidade que pretende editar.
3. Clique em **Editar endpoint**.

   A caixa de diálogo Editar ponto final é exibida.

   Para um ponto de extremidade não protegido (HTTP), apenas a secção Configuração do serviço de extremidade da caixa de diálogo é apresentada. Para um ponto de extremidade seguro (HTTPS), as secções Configuração do serviço de extremidade e certificados da caixa de diálogo são apresentadas, conforme ilustrado no exemplo seguinte.




4. Faça as alterações desejadas no endpoint.

   Para um endpoint não protegido (HTTP), você pode:

   - Altere o tipo de serviço de endpoint entre S3 e Swift.
   - Altere o modo de encadernação de endpoint. Para um endpoint seguro (HTTPS), você pode:
   - Altere o tipo de serviço de endpoint entre S3 e Swift.
   - Altere o modo de encadernação de endpoint.
   - Exibir o certificado de segurança.
   - Carregue ou gere um novo certificado de segurança quando o certificado atual estiver expirado ou prestes a expirar.

     Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

   > Para alterar o protocolo de um endpoint existente, por exemplo, de HTTP para HTTPS, você deve criar um novo endpoint. Siga as instruções para criar pontos de extremidade do balanceador de carga e selecione o protocolo desejado.

5. Clique em **Salvar**.

**Informações relacionadas**

Criação de pontos de extremidade do balanceador de carga

#### Remoção dos pontos finais do balanceador de carga

Se você não precisar mais de um ponto de extremidade do balanceador de carga, poderá removê-lo.

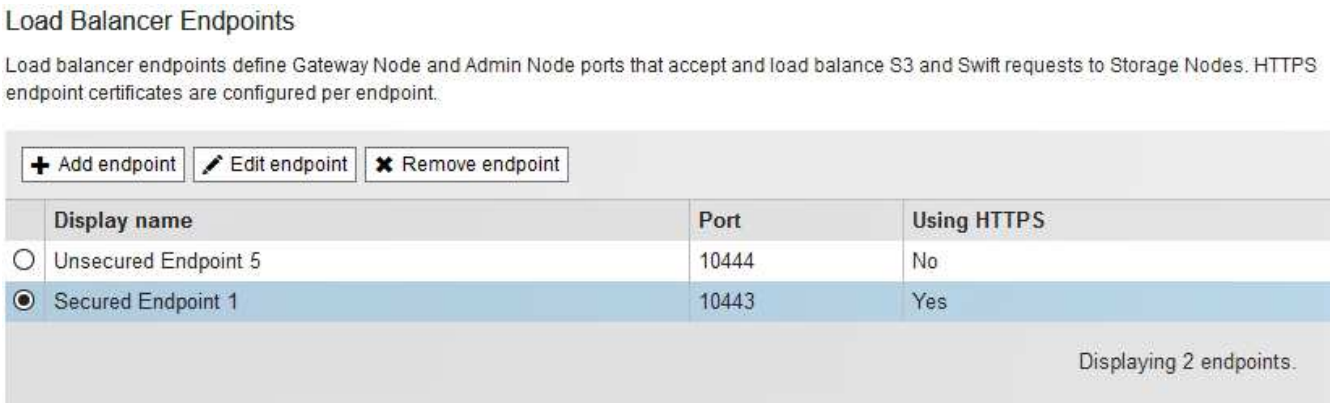
**O que você vai precisar**

- Você deve ter a permissão de acesso root.
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

**Passos**

1. Selecione **Configuration** > **Network Settings** > **Load Balancer Endpoints**.

   A página Load Balancer Endpoints é exibida. Os endpoints existentes são listados na tabela.




2. Selecione o botão de opção à esquerda do ponto de extremidade que pretende remover.
3. Clique em **Remover endpoint**.

   É apresentada uma caixa de diálogo de confirmação.


4. Clique em **OK**.

   O ponto final é removido.

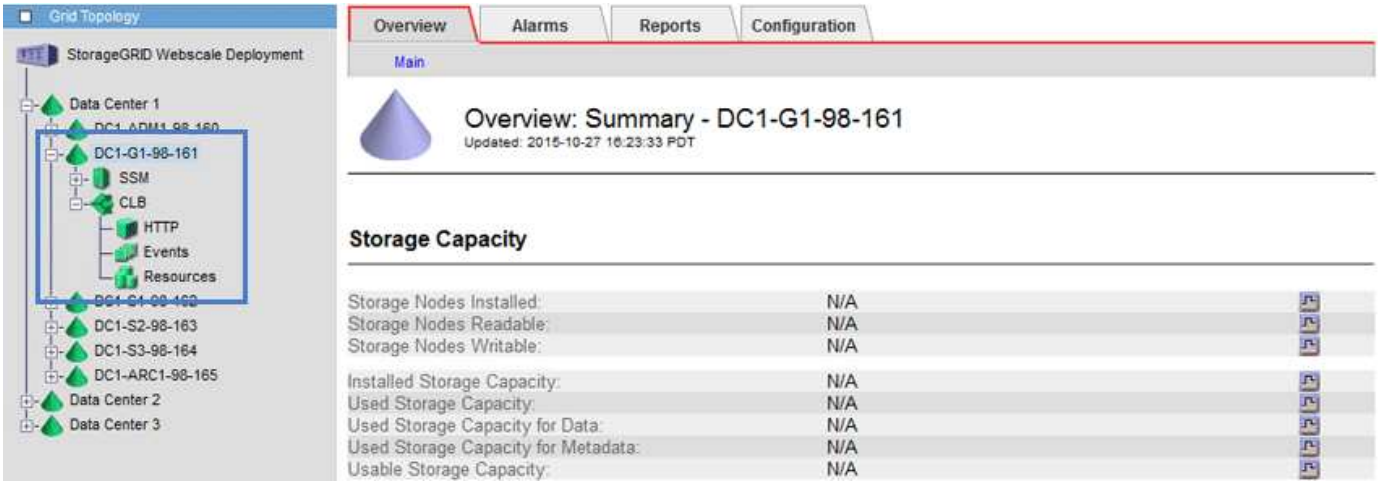
#### Como funciona o balanceamento de carga - serviço CLB

## O serviço CLB (Connection Load Balancer) nos nós de Gateway está obsoleto. O serviço Load Balancer é agora o mecanismo de balanceamento de carga recomendado.

O serviço CLB usa o balanceamento de carga da camada 4 para distribuir conexões de rede TCP de entrada de aplicativos clientes para o nó de armazenamento ideal com base na disponibilidade, carga do sistema e

custo de link configurado pelo administrador. Quando o nó de armazenamento ideal é escolhido, o serviço CLB estabelece uma conexão de rede bidirecional e encaminha o tráfego de e para o nó escolhido. O CLB não considera a configuração da rede de Grade ao direcionar conexões de rede recebidas.

Para visualizar informações sobre o serviço CLB, selecione **Support** > **Tools** > **Grid Topology** e expanda um Gateway Node até selecionar **CLB** e as opções abaixo.




Se você optar por usar o serviço CLB, considere configurar os custos de link para o seu sistema StorageGRID.

**Informações relacionadas**

"Quais são os custos da ligação"

"Atualizar custos de link"

## Gerenciando redes de clientes não confiáveis

Se você estiver usando uma rede cliente, você pode ajudar a proteger o StorageGRID contra ataques hostis aceitando tráfego de clientes de entrada apenas em endpoints configurados explicitamente.

Por padrão, a rede do cliente em cada nó de grade é *confiável*. Ou seja, por padrão, o StorageGRID confia em conexões de entrada para cada nó de grade em todas as portas externas disponíveis (consulte as informações sobre comunicações externas nas diretrizes de rede).

Você pode reduzir a ameaça de ataques hostis em seu sistema StorageGRID especificando que a rede de clientes em cada nó seja *não confiável*. Se a rede de cliente de um nó não for confiável, o nó só aceita conexões de entrada em portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

### Exemplo 1: O Gateway Node aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway recuse todo o tráfego de entrada na rede do cliente, exceto para solicitações HTTPS S3. Você executaria estes passos gerais:

1. Na página Load Balancer Endpoints, configure um ponto de extremidade do balanceador de carga para S3 em HTTPS na porta 443.
2. Na página redes de clientes não confiáveis, especifique que a rede de cliente no nó de gateway não é confiável.

Depois de salvar sua configuração, todo o tráfego de entrada na rede de clientes do nó de Gateway será descartado, exceto para solicitações HTTPS S3 na porta 443 e ICMP echo (ping).

**Exemplo 2: O nó de storage envia S3 solicitações de serviços de plataforma**

Suponha que você queira ativar o tráfego de serviço de plataforma S3 de saída de um nó de armazenamento, mas você deseja impedir quaisquer conexões de entrada para esse nó de armazenamento na rede cliente. Você executaria este passo geral:

- Na página redes de clientes não confiáveis, indique que a rede de cliente no nó de armazenamento não é confiável.

Depois de salvar sua configuração, o nó de armazenamento não aceita mais nenhum tráfego de entrada na rede do cliente, mas continua a permitir solicitações de saída para a Amazon Web Services.

**Informações relacionadas**

"Diretrizes de rede"

"Configuração dos pontos de extremidade do balanceador de carga"

**Especificar a rede cliente de um nó não é confiável**

Se você estiver usando uma rede de cliente, poderá especificar se a rede de cliente de cada nó é confiável ou não confiável. Você também pode especificar a configuração padrão para novos nós adicionados em uma expansão.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.
- Se você quiser que um nó de administrador ou nó de gateway aceite o tráfego de entrada somente em endpoints configurados explicitamente, você definiu os endpoints do balanceador de carga.

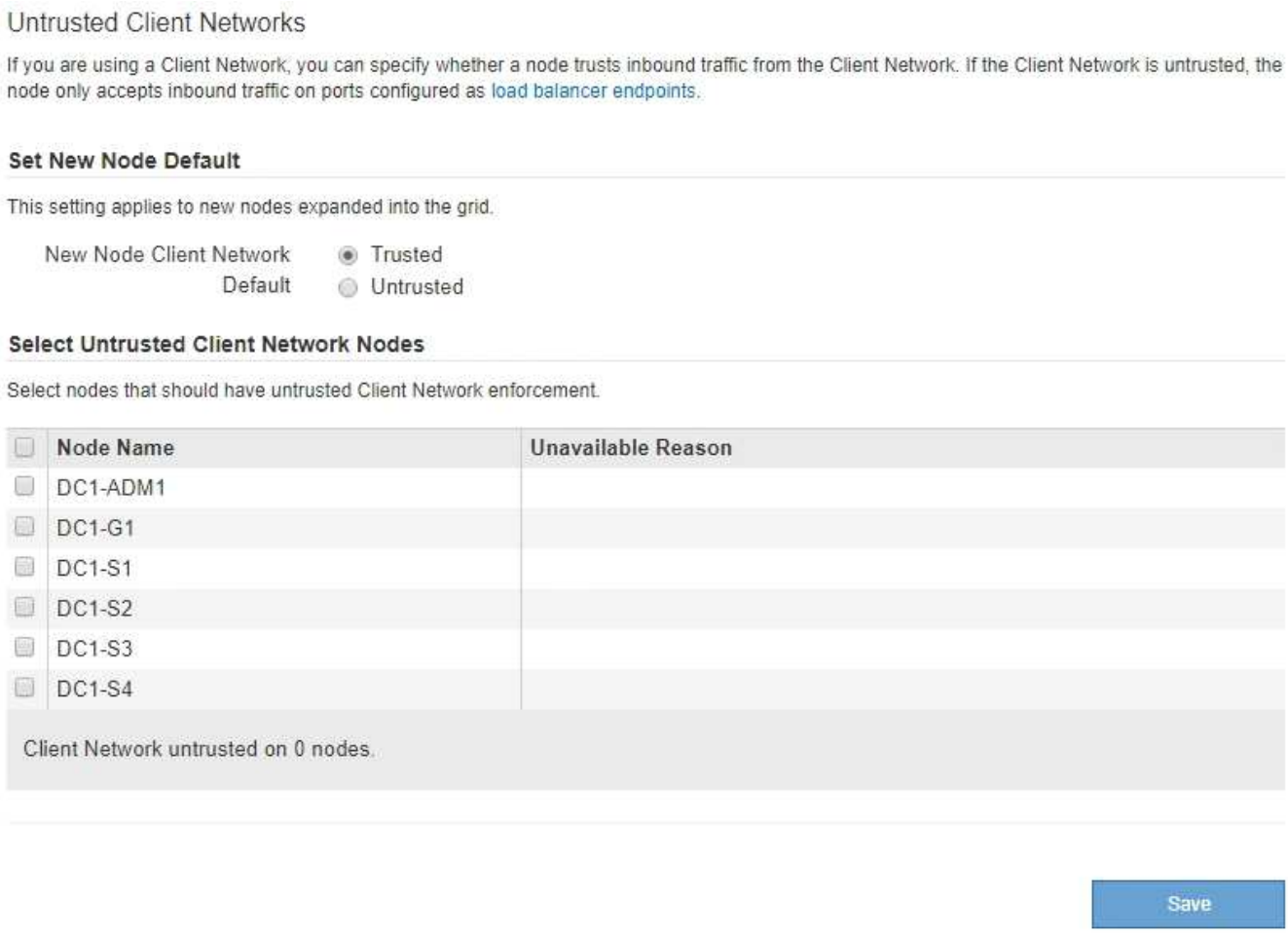
> As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **rede cliente não confiável**.

   A página redes de clientes não confiáveis é exibida.

   Esta página lista todos os nós no seu sistema StorageGRID. A coluna motivo indisponível inclui uma entrada se a rede do cliente no nó tiver de ser fidedigna.




2. Na seção **Definir novo padrão de nó**, especifique qual deve ser a configuração padrão quando novos nós forem adicionados à grade em um procedimento de expansão.
   - **Trusted**: Quando um nó é adicionado em uma expansão, sua rede de clientes é confiável.
   - **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede cliente não é confiável. Conforme necessário, você pode retornar a esta página para alterar a configuração de um novo nó específico.

   Esta configuração não afeta os nós existentes no seu sistema StorageGRID.

3. Na seção **Selecione nós de rede de cliente não confiáveis**, selecione os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga configurados explicitamente.

   Você pode selecionar ou desmarcar a caixa de seleção no título para selecionar ou desmarcar todos os nós.

4. Clique em **Salvar**.

   As novas regras de firewall são imediatamente adicionadas e aplicadas. As conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

**Informações relacionadas**

"Configuração dos pontos de extremidade do balanceador de carga"

## Gerenciamento de grupos de alta disponibilidade

Grupos de alta disponibilidade (HA) podem ser usados para fornecer conexões de dados altamente disponíveis para clientes S3 e Swift. Os GRUPOS HA também podem ser usados para fornecer conexões altamente disponíveis ao Gerenciador de Grade e ao Gerenciador de Locatário.

- "O que é um grupo HA"
- "Como os grupos de HA são usados"
- "Opções de configuração para grupos de HA"
- "Criando um grupo de alta disponibilidade"
- "Edição de um grupo de alta disponibilidade"
- "Removendo um grupo de alta disponibilidade"

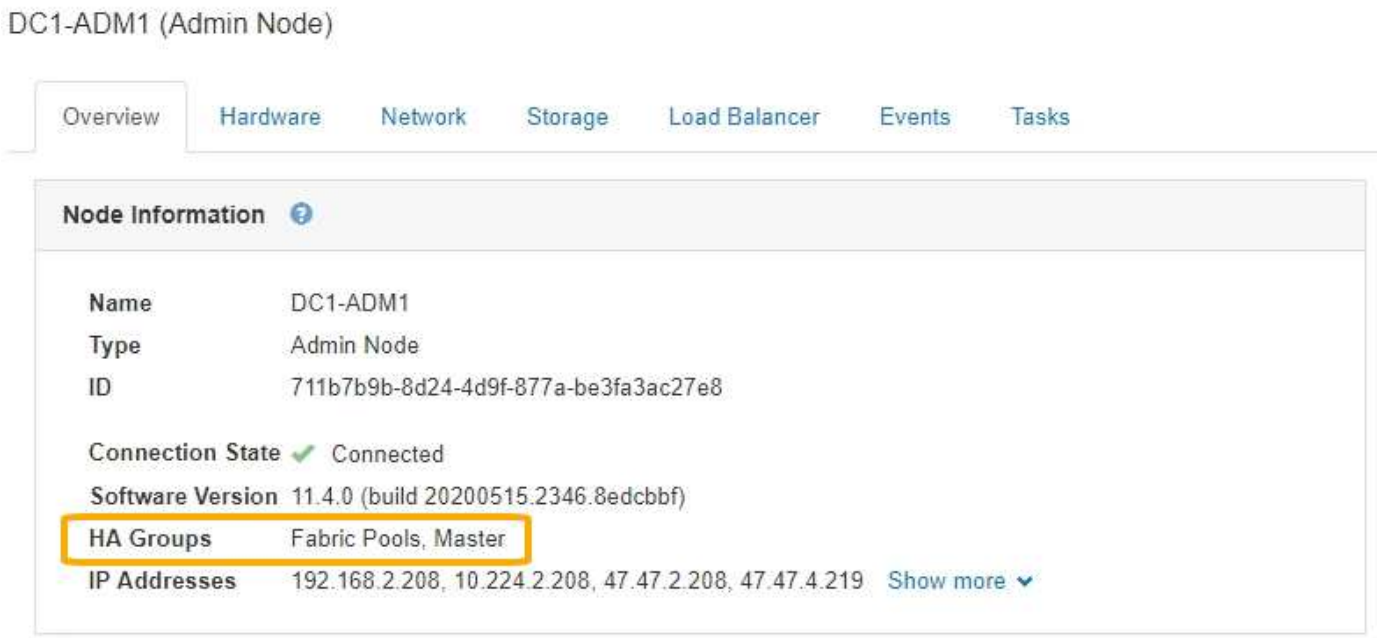
### O que é um grupo HA

Os grupos de alta disponibilidade usam endereços IP virtuais (VIPs) para fornecer acesso de backup ativo aos serviços do nó de gateway ou nó de administrador.

Um grupo de HA consiste em uma ou mais interfaces de rede em nós de administração e nós de gateway. Ao criar um grupo HA, você seleciona interfaces de rede pertencentes à rede Grid (eth0) ou à rede Client (eth2). Todas as interfaces de um grupo HA devem estar dentro da mesma sub-rede de rede.

Um grupo de HA mantém um ou mais endereços IP virtuais que são adicionados à interface ativa no grupo. Se a interface ativa ficar indisponível, os endereços IP virtuais serão movidos para outra interface. Esse processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes tenham pouco impactos e possam confiar em comportamentos normais de repetição para continuar a operação.

A interface ativa em um grupo HA é designada como Master. Todas as outras interfaces são designadas como Backup. Para visualizar estas designações, selecione **nodes** > ***node*** > **Overview**.



Ao criar um grupo HA, você especifica uma interface para ser o mestre preferido. O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup. Quando a falha é resolvida, os endereços VIP são automaticamente movidos de volta para o Master preferido.

O failover pode ser acionado por qualquer um destes motivos:

- O nó no qual a interface está configurada é desativado.
- O nó no qual a interface está configurada perde a conetividade com todos os outros nós por pelo menos 2 minutos
- A interface ativa desce.
- O serviço Load Balancer pára.
- O serviço de alta disponibilidade pára.

> O failover pode não ser acionado por falhas de rede externas ao nó que hospeda a interface ativa. Da mesma forma, o failover não é acionado pela falha do serviço CLB (obsoleto) ou serviços para o Gerenciador de Grade ou o Gerenciador de Tenant.

Se o grupo de HA incluir interfaces de mais de dois nós, a interface ativa poderá ser movida para a interface de qualquer outro nó durante o failover.

**Como os grupos de HA são usados**

Você pode querer usar grupos de alta disponibilidade (HA) por vários motivos.

- Um grupo de HA pode fornecer conexões administrativas altamente disponíveis ao Gerenciador de Grade ou ao Gerente do Locatário.
- Um grupo HA pode fornecer conexões de dados altamente disponíveis para clientes S3 e Swift.
- Um grupo de HA que contém apenas uma interface permite fornecer muitos endereços VIP e definir explicitamente endereços IPv6.

Um grupo de HA poderá fornecer alta disponibilidade somente se todos os nós incluídos no grupo oferecerem os mesmos serviços. Ao criar um grupo de HA, adicione interfaces dos tipos de nós que fornecem os serviços de que você precisa.

- **Admin Nodes**: Inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Gateway Nodes**: Incluem o serviço Load Balancer e o serviço CLB (obsoleto).

| Objetivo do grupo HA | Adicione nós desse tipo ao grupo de HA |
|---|---|
| Acesso ao Grid Manager | • Nó de administração principal (**Mestre preferido**)<br>• Nós de administração não primários<br><br>**Nota:** o nó de administração principal deve ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal. |

| Objetivo do grupo HA | Adicione nós desse tipo ao grupo de HA |
| --- | --- |
| Acesso apenas ao Gestor do Locatário | • Nós de administração primários ou não primários |
| Acesso ao cliente S3 ou Swift — Serviço de Load Balancer | • Nós de administração<br>• Nós de gateway |
| Acesso ao cliente S3 ou Swift — serviço CLB<br><br>**Nota:** o serviço CLB está obsoleto. | • Nós de gateway |

#### Limitações do uso de grupos de HA com Grid Manager ou Tenant Manager

A falha de serviços para o Gerenciador de Grade ou o Gerenciador de locatário não aciona o failover dentro do grupo de HA.

Se você estiver conetado ao Gerenciador de Grade ou ao Gerenciador de Locatário quando ocorrer failover, você será desconetado e deverá fazer login novamente para retomar sua tarefa.

Alguns procedimentos de manutenção não podem ser executados quando o nó de administração principal não está disponível. Durante o failover, você pode usar o Gerenciador de Grade para monitorar seu sistema StorageGRID.

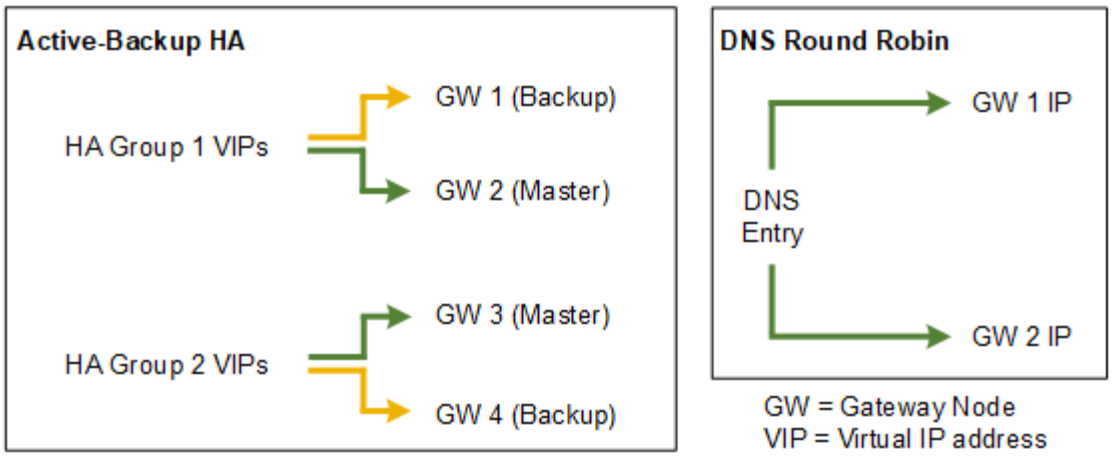
#### Limitações do uso de grupos HA com o serviço CLB

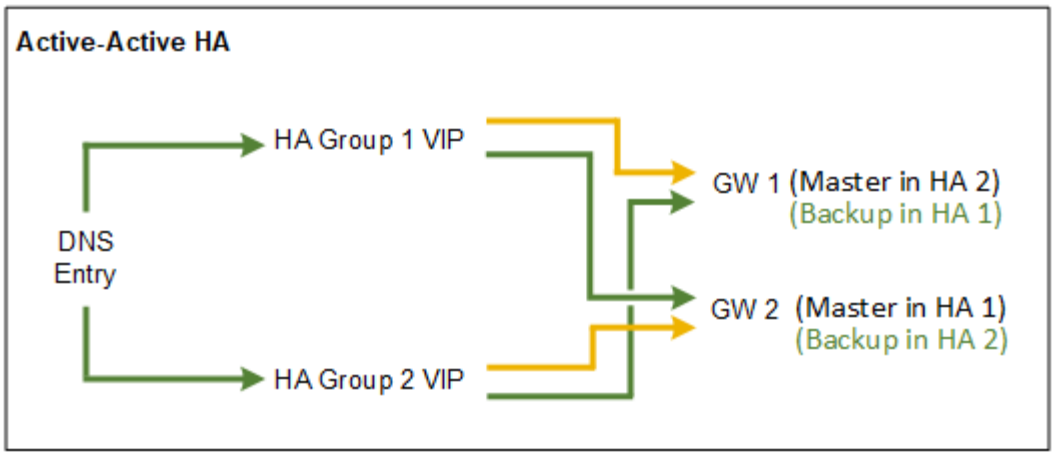
A falha do serviço CLB não aciona o failover no grupo HA.

O serviço CLB está obsoleto.

### Opções de configuração para grupos de HA

Os diagramas a seguir fornecem exemplos de diferentes maneiras de configurar grupos de HA. Cada opção tem vantagens e desvantagens.




Ao criar vários grupos de HA sobrepostos, como mostrado no exemplo de HA ativo-ativo, a taxa de transferência total é dimensionada com o número de nós e grupos de HA. Com três ou mais nós e três ou mais grupos de HA, você também pode continuar as operações usando qualquer um dos VIPs, mesmo durante procedimentos de manutenção que exigem que você coloque um nó off-line.

A tabela resume os benefícios de cada configuração de HA mostrada no diagrama.

| Configuração | Vantagens | Desvantagens |
|---|---|---|
| Active-Backup HA | • Gerenciado pelo StorageGRID sem dependências externas.<br>• Failover rápido. | • Apenas um nó em um grupo de HA está ativo. Pelo menos um nó por grupo de HA ficará inativo. |
| DNS Round Robin | • Maior taxa de transferência agregada.<br>• Sem hosts ociosos. | • Failover lento, que pode depender do comportamento do cliente.<br>• Requer configuração de hardware fora do StorageGRID.<br>• Precisa de uma verificação de integridade implementada pelo cliente. |

| Configuração | Vantagens | Desvantagens |
| --- | --- | --- |
| Ativo-ativo | • O tráfego é distribuído em vários grupos de HA.<br>• Alta taxa de transferência agregada que é dimensionada com o número de grupos de HA.<br>• Failover rápido. | • Mais complexo de configurar.<br>• Requer configuração de hardware fora do StorageGRID.<br>• Precisa de uma verificação de integridade implementada pelo cliente. |

### Criando um grupo de alta disponibilidade

Você pode criar um ou mais grupos de alta disponibilidade (HA) para fornecer acesso altamente disponível aos serviços em nós de administração ou nós de gateway.

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

#### Sobre esta tarefa

Uma interface deve atender às seguintes condições para ser incluída em um grupo HA:

- A interface deve ser para um nó de gateway ou um nó de administrador.
- A interface deve pertencer à rede de Grade (eth0) ou à rede de Cliente (eth2).
- A interface deve ser configurada com endereçamento IP fixo ou estático, não com DHCP.

#### Passos

1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

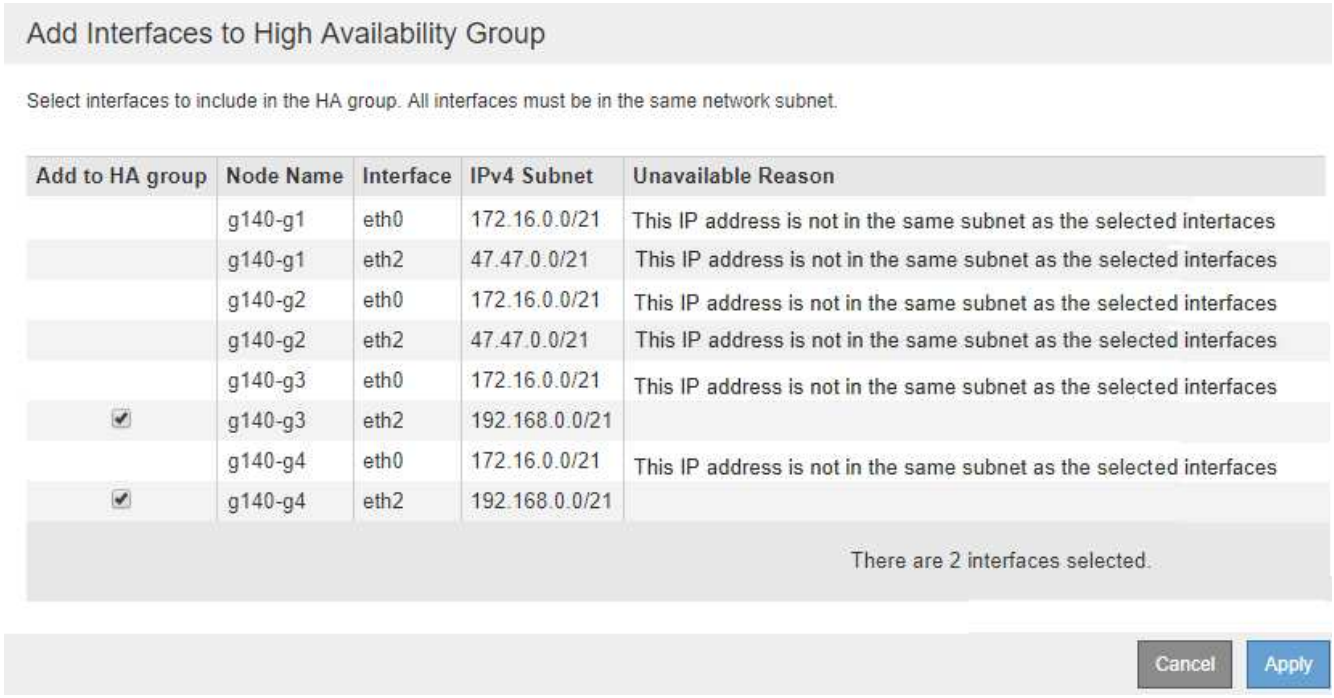
   A página grupos de alta disponibilidade é exibida.


2. Clique em **criar**.

   A caixa de diálogo criar Grupo de alta disponibilidade é exibida.

3. Digite um nome e, se desejado, uma descrição para o grupo HA.
4. Clique em **Select interfaces**.

   A caixa de diálogo Adicionar interfaces ao Grupo de alta disponibilidade é exibida. A tabela lista nós, interfaces e sub-redes IPv4 elegíveis.




Uma interface não aparece na lista se o seu endereço IP for atribuído pelo DHCP.

5. Na coluna **Adicionar ao grupo HA**, marque a caixa de seleção da interface que deseja adicionar ao grupo HA.

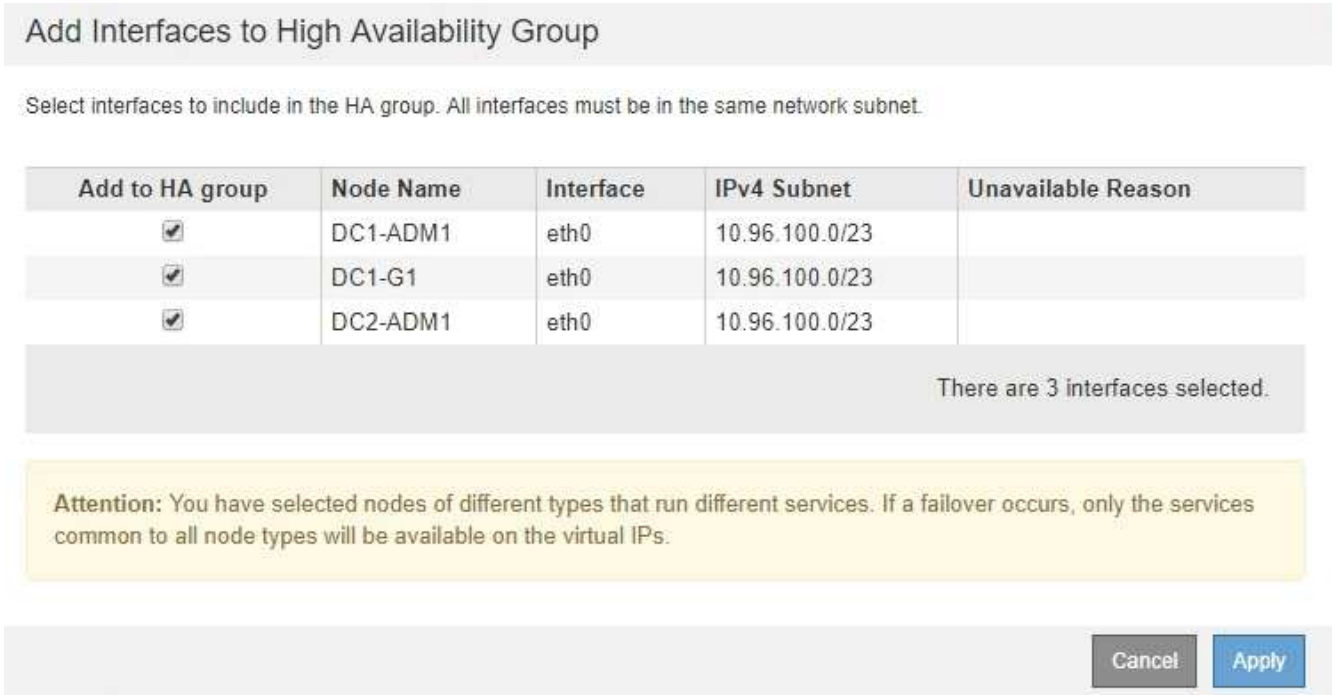
   Observe as seguintes diretrizes para selecionar interfaces:

   - Você deve selecionar pelo menos uma interface.
   - Se você selecionar mais de uma interface, todas as interfaces devem estar na rede de Grade (eth0) ou na rede de Cliente (eth2).
   - Todas as interfaces devem estar na mesma sub-rede ou em sub-redes com um prefixo comum.

     Os endereços IP serão restritos à sub-rede menor (aquela com o maior prefixo).

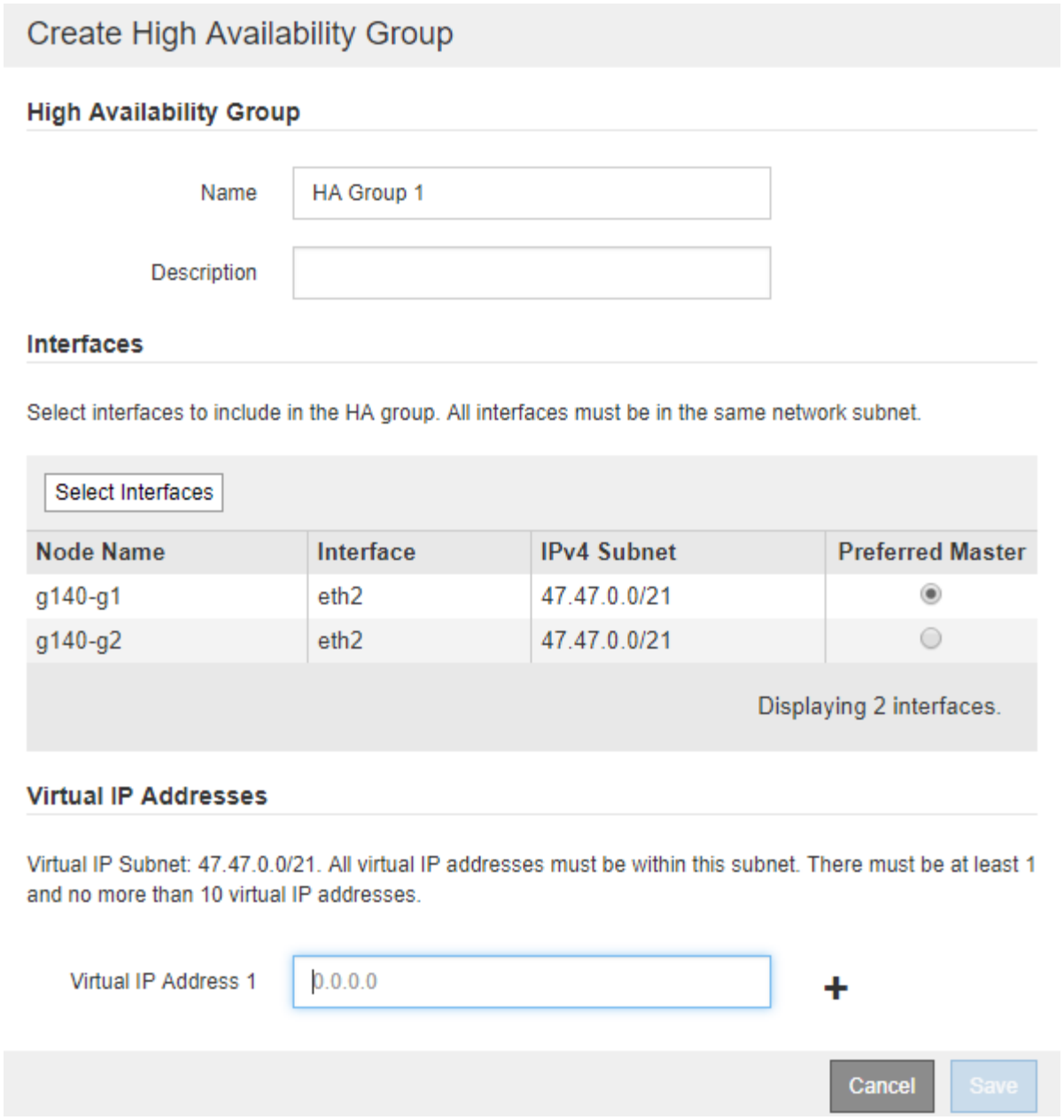
   - Se você selecionar interfaces em diferentes tipos de nós e ocorrer um failover, apenas os serviços comuns aos nós selecionados estarão disponíveis nos IPs virtuais.
     - Selecione dois ou mais nós de administração para proteção de HA do Grid Manager ou do Tenant Manager.
     - Selecione dois ou mais nós de administração, nós de gateway ou ambos para proteção de HA do serviço Load Balancer.
     - Selecione dois ou mais nós de Gateway para proteção de HA do serviço CLB.

       O serviço CLB está obsoleto.




6. Clique em **aplicar**.

   As interfaces selecionadas são listadas na seção interfaces da página criar Grupo de alta disponibilidade. Por padrão, a primeira interface na lista é selecionada como o mestre preferido.




7. Se você quiser que uma interface diferente seja o mestre preferido, selecione essa interface na coluna **Preferred Master**.

   O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup.

   > Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deve selecionar uma interface no nó Admin principal para ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

8. Na seção endereços IP virtuais da página, insira um a 10 endereços IP virtuais para o grupo HA. Clique no sinal de mais (+) para adicionar vários endereços IP.

   Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

   Os endereços IPv4 devem estar dentro da sub-rede IPv4 compartilhada por todas as interfaces membros.

9. Clique em **Salvar**.

   O Grupo HA é criado e agora você pode usar os endereços IP virtuais configurados.

**Informações relacionadas**

"Instale o Red Hat Enterprise Linux ou CentOS"

"Instale o VMware"

"Instale Ubuntu ou Debian"

"Gerenciamento do balanceamento de carga"

### Edição de um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces ou adicionar ou atualizar um endereço IP virtual.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

**Sobre esta tarefa**

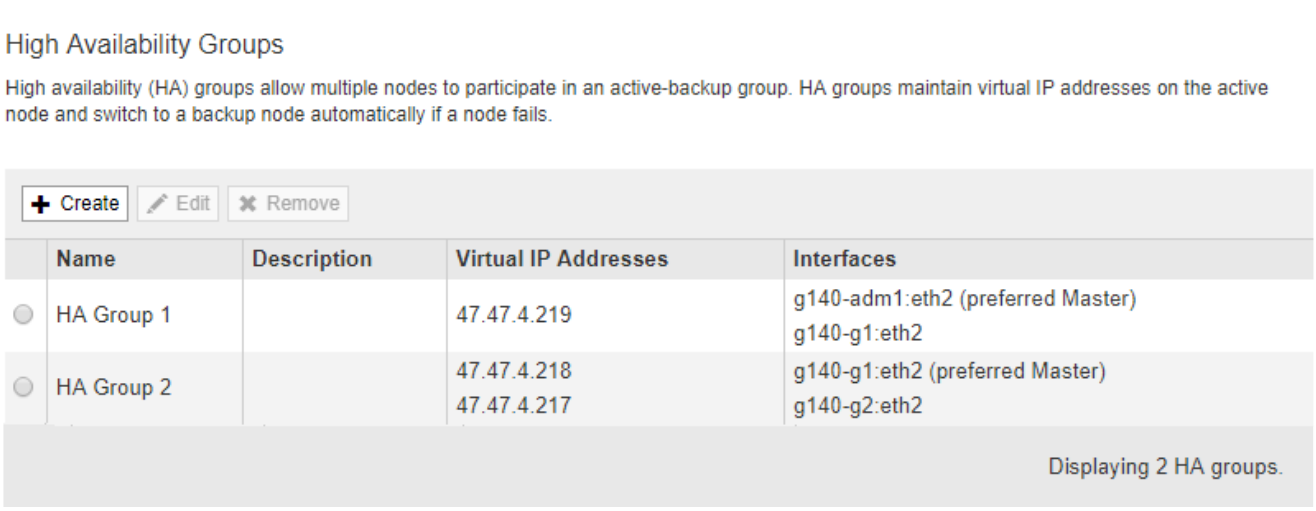
Algumas das razões para editar um grupo HA incluem o seguinte:

- Adicionando uma interface a um grupo existente. O endereço IP da interface deve estar dentro da mesma sub-rede que outras interfaces já atribuídas ao grupo.
- Remover uma interface de um grupo de HA. Por exemplo, você não pode iniciar um procedimento de desativação de site ou nó se a interface de um nó para a rede de Grade ou a rede de cliente for usada em um grupo HA.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

   A página grupos de alta disponibilidade é exibida.

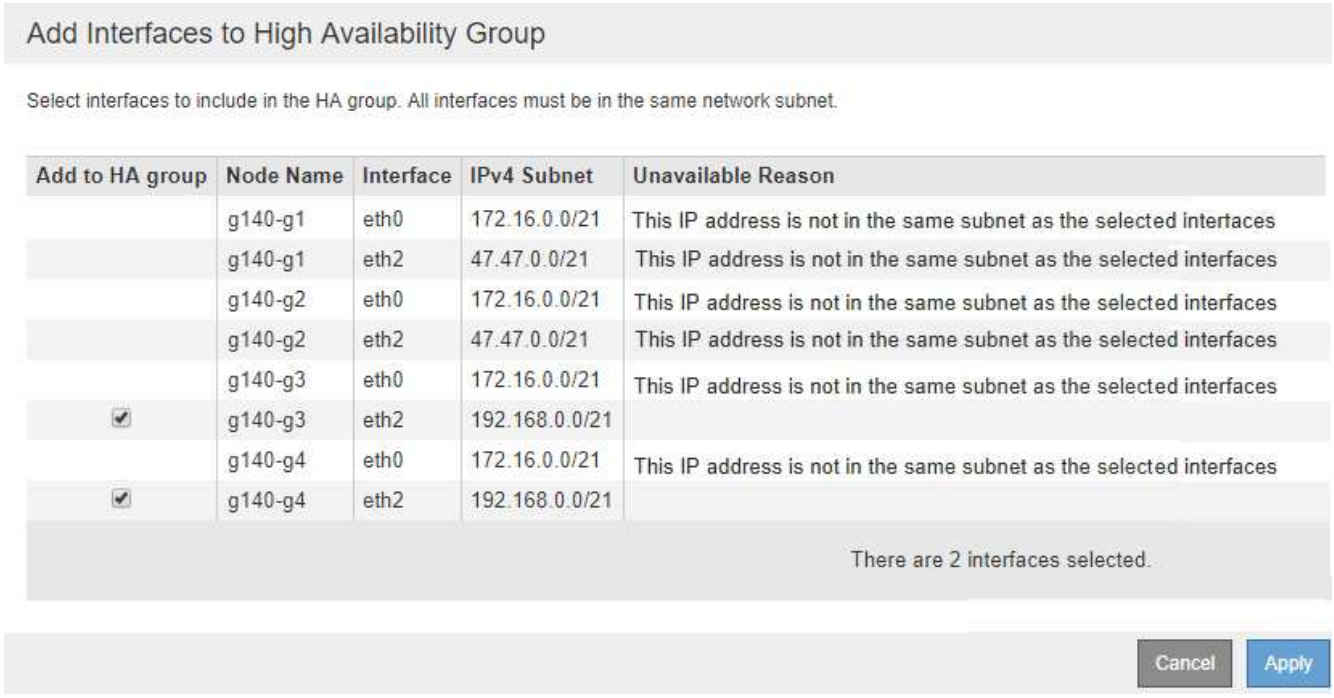


2. Selecione o grupo HA que deseja editar e clique em **Editar**.

   A caixa de diálogo Editar Grupo de alta disponibilidade é exibida.

3. Opcionalmente, atualize o nome ou a descrição do grupo.
4. Opcionalmente, clique em **Select interfaces** para alterar as interfaces do Grupo HA.

   A caixa de diálogo Adicionar interfaces ao Grupo de alta disponibilidade é exibida.




   Uma interface não aparece na lista se o seu endereço IP for atribuído pelo DHCP.

5. Selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.

   Observe as seguintes diretrizes para selecionar interfaces:

   - Você deve selecionar pelo menos uma interface.
   - Se você selecionar mais de uma interface, todas as interfaces devem estar na rede de Grade (eth0) ou na rede de Cliente (eth2).
   - Todas as interfaces devem estar na mesma sub-rede ou em sub-redes com um prefixo comum.

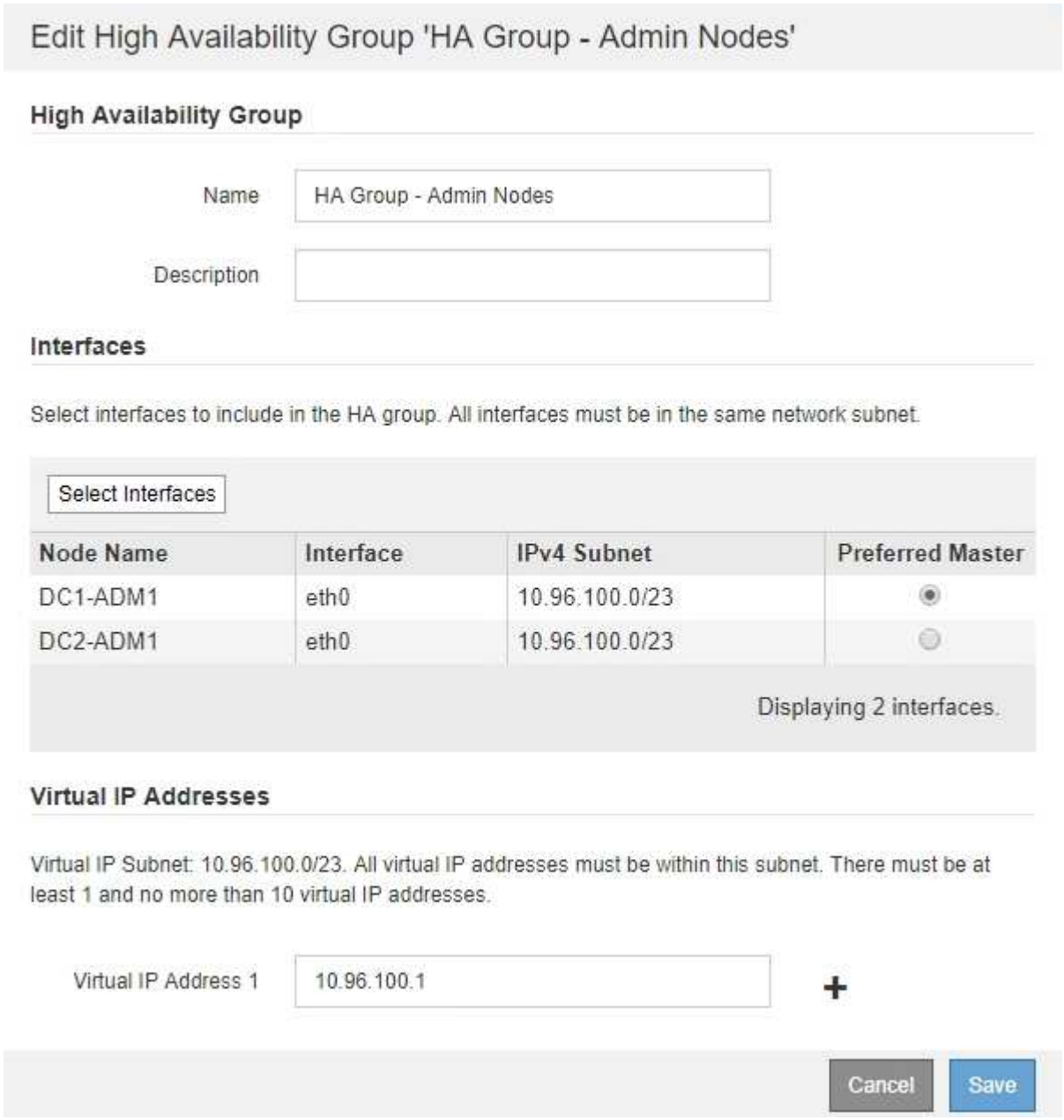
     Os endereços IP serão restritos à sub-rede menor (aquela com o maior prefixo).

   - Se você selecionar interfaces em diferentes tipos de nós e ocorrer um failover, apenas os serviços comuns aos nós selecionados estarão disponíveis nos IPs virtuais.
     - Selecione dois ou mais nós de administração para proteção de HA do Grid Manager ou do Tenant Manager.
     - Selecione dois ou mais nós de administração, nós de gateway ou ambos para proteção de HA do serviço Load Balancer.
     - Selecione dois ou mais nós de Gateway para proteção de HA do serviço CLB.

       O serviço CLB está obsoleto.

6. Clique em **aplicar**.

   As interfaces selecionadas são listadas na seção interfaces da página. Por padrão, a primeira interface na lista é selecionada como o mestre preferido.




7. Se você quiser que uma interface diferente seja o mestre preferido, selecione essa interface na coluna **Preferred Master**.

   O Master preferencial é a interface ativa, a menos que ocorra uma falha que faça com que os endereços VIP sejam reatribuídos a uma interface de backup.

   Se o grupo HA fornecer acesso ao Gerenciador de Grade, você deve selecionar uma interface no nó Admin principal para ser o mestre preferido. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.

8. Opcionalmente, atualize os endereços IP virtuais para o grupo HA.

Você deve fornecer pelo menos um endereço IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

Os endereços IPv4 devem estar dentro da sub-rede IPv4 compartilhada por todas as interfaces membros.

9. Clique em **Salvar**.

   O Grupo HA é atualizado.

### Removendo um grupo de alta disponibilidade

Você pode remover um grupo de alta disponibilidade (HA) que não esteja mais usando.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

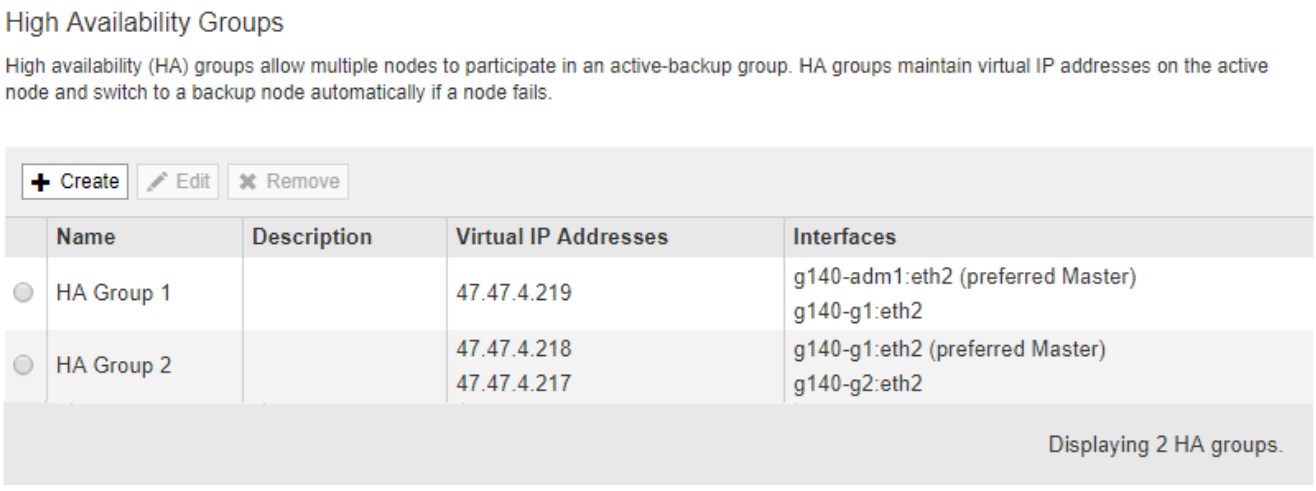
**Aborde esta tarefa**

Se você remover um grupo HA, qualquer cliente S3 ou Swift configurado para usar um dos endereços IP virtuais do grupo não poderá mais se conetar ao StorageGRID. Para evitar interrupções do cliente, você deve atualizar todos os aplicativos clientes S3 ou Swift afetados antes de remover um grupo HA. Atualize cada cliente para se conetar usando outro endereço IP, por exemplo, o endereço IP virtual de um grupo HA diferente ou o endereço IP configurado para uma interface durante a instalação ou usando DHCP.

**Passos**

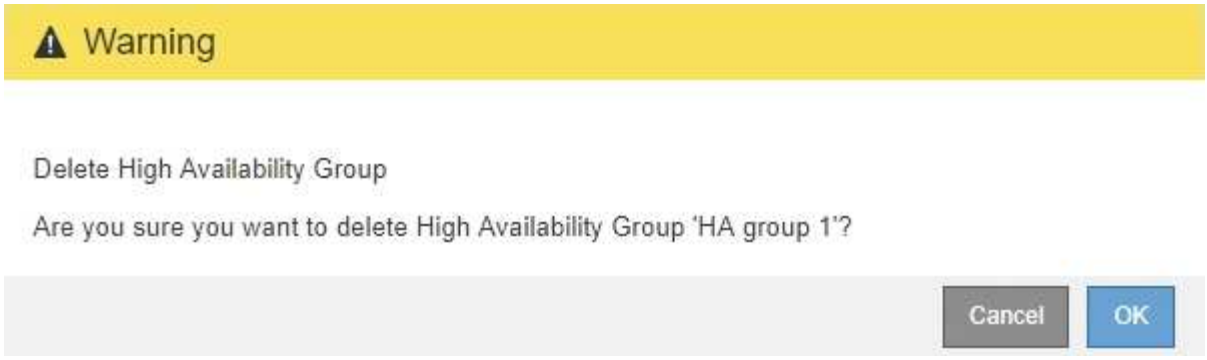
1. Selecione **Configuração** > **Configurações de rede** > **grupos de alta disponibilidade**.

   A página grupos de alta disponibilidade é exibida.




2. Selecione o grupo HA que deseja remover e clique em **Remover**.

   O aviso Excluir Grupo de alta disponibilidade é exibido.




3. Clique em **OK**.

   O grupo HA é removido.

## Configurando nomes de domínio de endpoint da API S3

Para oferecer suporte a solicitações de estilo hospedado virtual S3, você deve usar o Gerenciador de Grade para configurar a lista de nomes de domínio de endpoint aos quais os clientes S3 se conetam.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter confirmado que uma atualização de grade não está em andamento.

> Não faça alterações na configuração do nome de domínio quando uma atualização de grade estiver em andamento.

**Sobre esta tarefa**

Para permitir que os clientes usem nomes de domínio de endpoint S3, você deve executar todas as seguintes tarefas:

- Use o Gerenciador de Grade para adicionar os nomes de domínio de endpoint S3 ao sistema StorageGRID.
- Certifique-se de que o certificado que o cliente usa para conexões HTTPS com o StorageGRID está assinado para todos os nomes de domínio que o cliente requer.

  Por exemplo, se o endpoint for `s3.company.com`, você deve garantir que o certificado usado para conexões HTTPS inclua o `s3.company.com` endpoint e o nome alternativo do assunto universal (SAN) do endpoint: `*.s3.company.com`.

- Configure o servidor DNS usado pelo cliente. Inclua Registros DNS para os endereços IP que os clientes usam para fazer conexões e verifique se os Registros fazem referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes de curinga.

Os clientes podem se conetar ao StorageGRID usando o endereço IP de um nó de gateway, um nó de administrador ou um nó de armazenamento, ou conetando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos cliente se conetam à grade para incluir os endereços IP corretos nos Registros DNS.

O certificado que um cliente usa para conexões HTTPS depende de como o cliente se coneta à grade:

- Se um cliente se conetar usando o serviço Load Balancer, ele usará o certificado para um ponto de extremidade específico do balanceador de carga.

  Cada ponto de extremidade do balanceador de carga tem seu próprio certificado e cada ponto de extremidade pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.

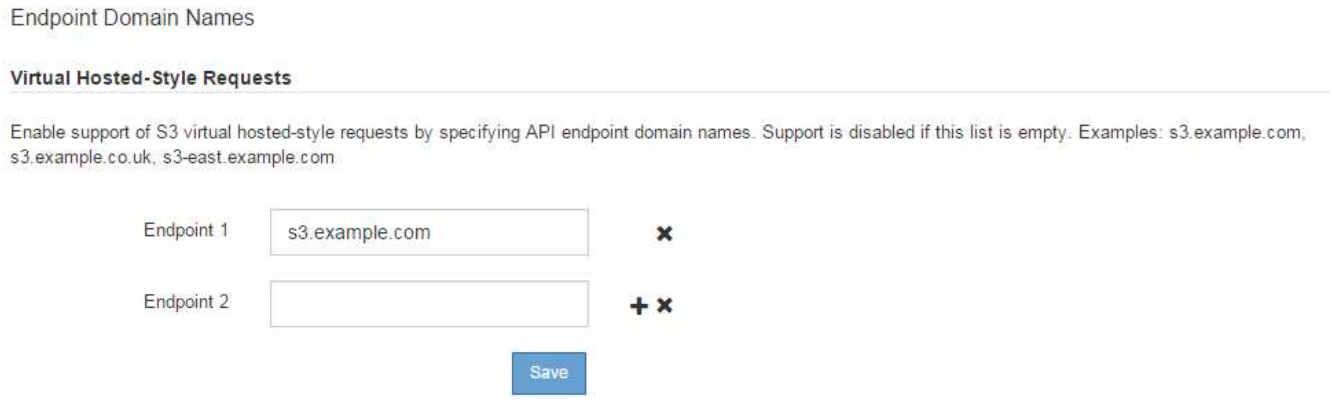
- Se o cliente se conetar a um nó de armazenamento ou ao serviço CLB em um nó de gateway, o cliente usará um certificado de servidor personalizado de grade que foi atualizado para incluir todos os nomes de domínio de endpoint necessários.

  O serviço CLB está obsoleto.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **nomes de domínio**.

   A página nomes de domínio do endpoint é exibida.




2. Para adicionar campos adicionais, insira a lista de nomes de domínio de endpoint da API S3 nos campos **Endpoint**.

   Se esta lista estiver vazia, o suporte para solicitações de estilo hospedado virtual S3 será desativado.

3. Clique em **Salvar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint necessários.
   - Para clientes que usam o serviço Load Balancer, atualize o certificado associado ao ponto de extremidade do balanceador de carga ao qual o cliente se coneta.
   - Para clientes que se conetam diretamente aos nós de storage ou que usam o serviço CLB nos nós de Gateway, atualize o certificado de servidor personalizado para a grade.

5. Adicione os Registros DNS necessários para garantir que as solicitações de nome de domínio de endpoint possam ser resolvidas.

**Resultado**

Agora, quando os clientes usam o endpoint `bucket.s3.company.com`, o servidor DNS resolve para o endpoint correto e o certificado autentica o endpoint como esperado.

**Informações relacionadas**

"Use S3"

"Visualização de endereços IP"

"Criando um grupo de alta disponibilidade"

"Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB"

"Configuração dos pontos de extremidade do balanceador de carga"

## Ativar HTTP para comunicações cliente

Por padrão, os aplicativos clientes usam o protocolo de rede HTTPS para todas as conexões com nós de armazenamento ou para o serviço CLB obsoleto em nós de gateway. Opcionalmente, você pode ativar o HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

**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**

Conclua esta tarefa somente se os clientes S3 e Swift precisarem fazer conexões HTTP diretamente aos nós de armazenamento ou ao serviço CLB obsoleto nos nós de Gateway.

Não é necessário concluir essa tarefa para clientes que usam somente conexões HTTPS ou para clientes que se conetam ao serviço Load Balancer (porque você pode configurar cada ponto de extremidade do Load Balancer para usar HTTP ou HTTPS). Consulte as informações sobre como configurar pontos de extremidade do balanceador de carga para obter mais informações.

"Resumo: Endereços IP e portas para conexões de clientes"Consulte para saber quais portas S3 e clientes Swift usam ao se conetar a nós de armazenamento ou ao serviço CLB obsoleto usando HTTP ou HTTPS

> Tenha cuidado ao ativar o HTTP para uma grade de produção porque as solicitações serão enviadas sem criptografia.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de rede, marque a caixa de seleção **Ativar conexão HTTP** .


3. Clique em **Salvar**.

**Informações relacionadas**

"Configuração dos pontos de extremidade do balanceador de carga"

"Use S3"

"Use Swift"

## Controlar quais operações do cliente são permitidas

Você pode selecionar a opção Prevent Client Modification grid (impedir a modificação do cliente) para negar operações específicas do cliente HTTP.

**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**

Impedir Modificação do Cliente é uma configuração de todo o sistema. Quando a opção impedir modificação de cliente é selecionada, as seguintes solicitações são negadas:

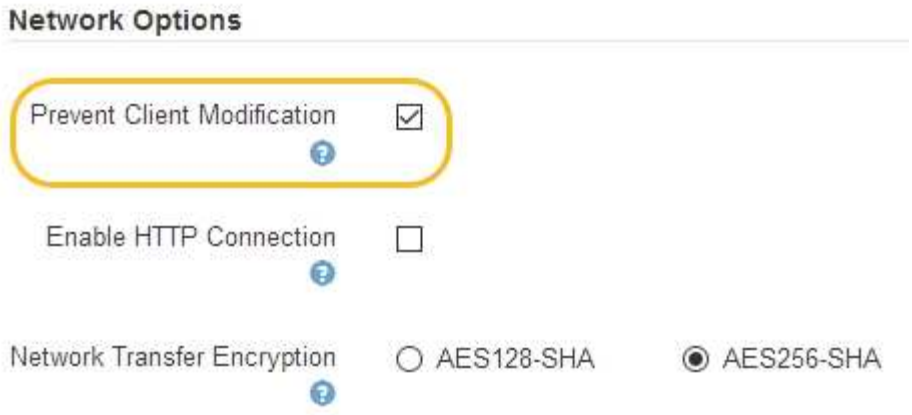
- **S3 API REST**
  - Eliminar pedidos de balde
  - Quaisquer solicitações para modificar os dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

> Esta configuração não se aplica a buckets com controle de versão ativado. O controle de versão já impede modificações nos dados do objeto, metadados definidos pelo usuário e marcação de objetos.

- * Swift REST API*
  - Eliminar pedidos de contentor
  - Solicitações para modificar qualquer objeto existente. Por exemplo, as seguintes operações são negadas: Put Overwrite, Delete, Metadata Update e assim por diante.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de rede, marque a caixa de seleção **impedir modificação de cliente**.




3. Clique em **Salvar**.

# Gerenciamento de redes e conexões StorageGRID

Você pode usar o Gerenciador de Grade para configurar e gerenciar redes e conexões StorageGRID.

"Configurando conexões de cliente S3 e Swift"Consulte para saber como conetar clientes S3 ou Swift.

- "Diretrizes para redes StorageGRID"
- "Visualização de endereços IP"
- "Cifras suportadas para conexões TLS de saída"
- "Alteração da encriptação de transferência de rede"
- "Configurando certificados de servidor"
- "Configurando as configurações de proxy de armazenamento"
- "Configurando as configurações de proxy Admin"
- "Gerir políticas de classificação de tráfego"
- "Quais são os custos da ligação"

## Diretrizes para redes StorageGRID

O StorageGRID suporta até três interfaces de rede por nó de grade, permitindo que você configure a rede para cada nó de grade individual de acordo com seus requisitos de segurança e acesso.

> Para modificar ou adicionar uma rede para um nó de grade, consulte as instruções de recuperação e manutenção. Para obter mais informações sobre a topologia de rede, consulte as instruções de rede.

### Rede de rede

Obrigatório. A rede de grade é usada para todo o tráfego interno do StorageGRID. Ele fornece conetividade entre todos os nós na grade, em todos os sites e sub-redes.

#### Rede de administração

Opcional. A rede de administração é normalmente utilizada para administração e manutenção do sistema. Ele também pode ser usado para acesso ao protocolo cliente. A rede Admin é normalmente uma rede privada e não precisa ser roteável entre sites.

#### Rede de clientes

Opcional. A rede de clientes é uma rede aberta normalmente usada para fornecer acesso a aplicativos clientes S3 e Swift, para que a rede de Grade possa ser isolada e protegida. A rede do cliente pode se comunicar com qualquer sub-rede acessível através do gateway local.

#### Diretrizes

- Cada nó de grade do StorageGRID requer uma interface de rede dedicada, endereço IP, máscara de sub-rede e gateway para cada rede à qual está atribuído.
- Um nó de grade não pode ter mais de uma interface em uma rede.
- Um único gateway, por rede, por nó de grade é suportado e deve estar na mesma sub-rede que o nó. Você pode implementar roteamento mais complexo no gateway, se necessário.
- Em cada nó, cada rede mapeia para uma interface de rede específica.

| Rede | Nome da interface |
|---|---|
| Grelha | eth0 |
| Admin (opcional) | eth1 |
| Cliente (opcional) | eth2 |

- Se o nó estiver conetado a um dispositivo StorageGRID, portas específicas serão usadas para cada rede. Para obter mais detalhes, consulte as instruções de instalação do seu aparelho.
- A rota padrão é gerada automaticamente, por nó. Se o eth2 estiver ativado, o 0,0.0.0/0 usará a rede do cliente no eth2. Se o eth2 não estiver ativado, o 0,0.0.0/0 usará a rede de Grade no eth0.
- A rede do cliente não se torna operacional até que o nó da grade se junte à grade
- A rede Admin pode ser configurada durante a implantação do nó de grade para permitir o acesso à interface do usuário de instalação antes que a grade esteja totalmente instalada.

#### Informações relacionadas

"Manter recuperar"

"Diretrizes de rede"

## Visualização de endereços IP

Você pode exibir o endereço IP de cada nó de grade em seu sistema StorageGRID. Em seguida, você pode usar esse endereço IP para fazer login no nó da grade na linha de comando e executar vários procedimentos de manutenção.

#### O que você vai precisar

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

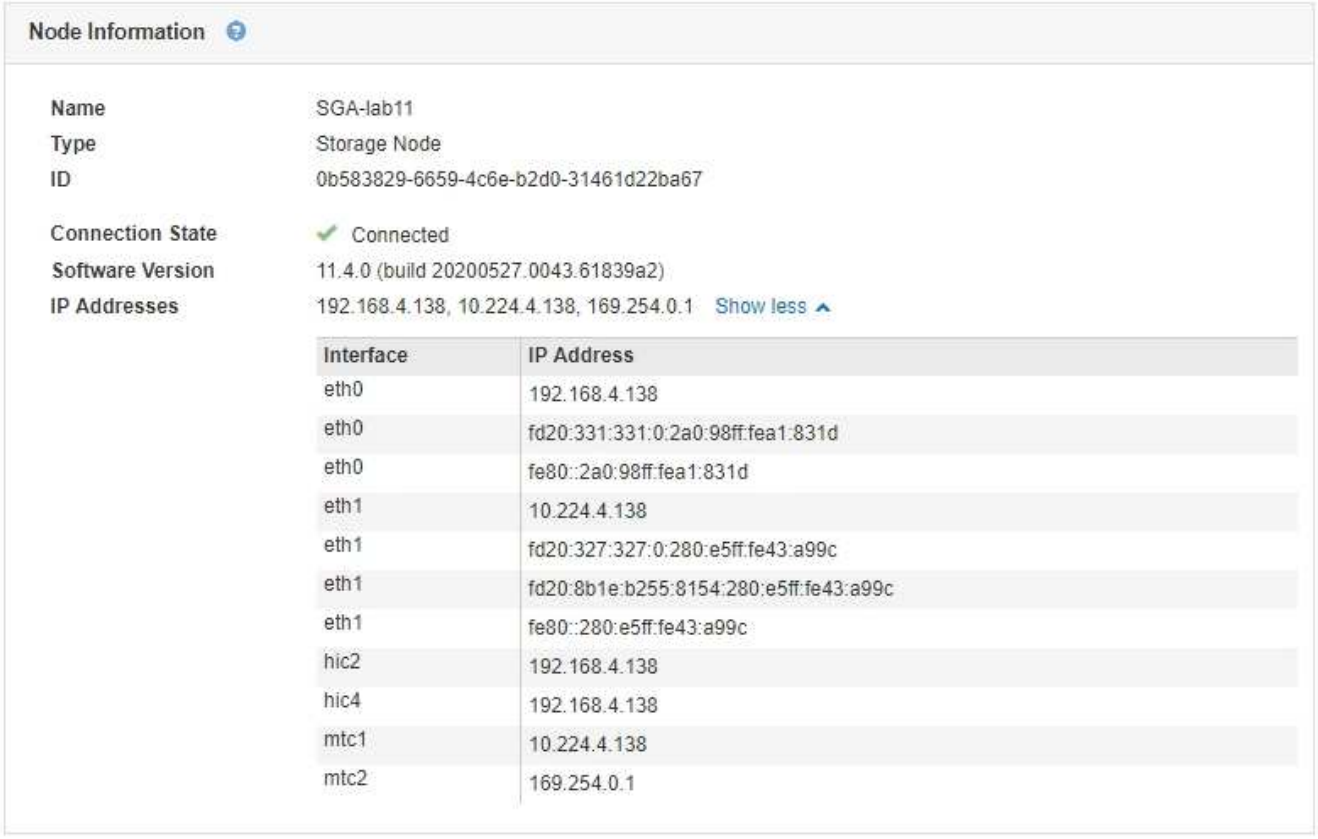
**Sobre esta tarefa**

Para obter informações sobre como alterar endereços IP, consulte as instruções de recuperação e manutenção.

**Passos**

1. Selecione **nodes** > ***grid node*** > **Visão geral**.
2. Clique em **Mostrar mais** à direita do título de endereços IP.

   Os endereços IP desse nó de grade são listados em uma tabela.




**Informações relacionadas**

"Manter recuperar"

## Cifras suportadas para conexões TLS de saída

O sistema StorageGRID oferece suporte a um conjunto limitado de conjuntos de codificação para conexões TLS (Transport Layer Security) com os sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

### Versões suportadas do TLS

O StorageGRID oferece suporte ao TLS 1,2 e TLS 1,3 para conexões a sistemas externos usados para federação de identidade e pools de armazenamento em nuvem.

As cifras TLS que são suportadas para utilização com sistemas externos foram selecionadas para garantir a

compatibilidade com uma gama de sistemas externos. A lista é maior do que a lista de cifras que são suportadas para uso com aplicativos cliente S3 ou Swift.

> As opções de configuração TLS, como versões de protocolo, cifras, algoritmos de troca de chaves e algoritmos MAC, não são configuráveis no StorageGRID. Entre em Contato com o representante da sua conta do NetApp se você tiver solicitações específicas sobre essas configurações.

**Pacotes de codificação TLS 1,2 suportados**

Os seguintes conjuntos de codificação TLS 1,2 são suportados:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

**Pacotes de codificação TLS 1,3 suportados**

Os seguintes conjuntos de codificação TLS 1,3 são suportados:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

## Alteração da encriptação de transferência de rede

O sistema StorageGRID usa a Segurança da camada de Transporte (TLS) para proteger o tráfego de controle interno entre nós de grade. A opção Network Transfer Encryption (encriptação de transferência de rede) define o algoritmo utilizado pelo TLS para encriptar o tráfego de controlo entre nós de grelha. Esta definição não afeta a encriptação de dados.

**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**

Por padrão, a criptografia de transferência de rede usa o algoritmo AES256-SHA. O tráfego de controle também pode ser criptografado usando o algoritmo AES128-SHA.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.

2. Na seção Opções de rede, altere criptografia de transferência de rede para **AES128-SHA** ou **AES256-SHA** (padrão).


3. Clique em **Salvar**.

## Configurando certificados de servidor

Você pode personalizar os certificados de servidor usados pelo sistema StorageGRID.

O sistema StorageGRID usa certificados de segurança para vários fins distintos:

- Certificados de servidor de interface de gerenciamento: Usado 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.
- Certificados de servidor de API de storage: Usado para proteger o acesso aos nós de armazenamento e nós de Gateway, que os aplicativos de cliente de API usam para carregar e baixar dados de objeto.

Você pode usar os certificados padrão criados durante a instalação, ou pode substituir qualquer um desses tipos padrão de certificados por seus próprios certificados personalizados.

### Tipos suportados de certificado de servidor personalizado

O sistema StorageGRID suporta certificados de servidor personalizados criptografados com RSA ou ECDSA (algoritmo de assinatura digital de curva elítica).

Para obter mais informações sobre como o StorageGRID protege conexões de clientes para a API REST, consulte os guias de implementação S3 ou Swift.

### Certificados para pontos de extremidade do balanceador de carga

O StorageGRID gerencia os certificados usados para pontos de extremidade do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, consulte as instruções para configurar os pontos de extremidade do balanceador de carga.

### Informações relacionadas

"Use S3"

"Use Swift"

"Configuração dos pontos de extremidade do balanceador de carga"

### Configurando um certificado de servidor personalizado para o Gerenciador de Grade e o Gerenciador de locatário

Você pode substituir o certificado de servidor StorageGRID padrão por um único certificado de servidor personalizado que permite aos usuários acessar o Gerenciador de Grade e o Gerenciador de locatário sem encontrar avisos de segurança.

#### Sobre esta tarefa

Por padrão, cada nó de administrador é emitido um certificado assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e uma chave privada correspondente.

Como um único certificado de servidor personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado de curinga ou de vários domínios se os clientes precisarem verificar o nome do host ao se conetar ao Gerenciador de Grade e ao Gerenciador de locatário. Defina o certificado personalizado de modo que corresponda a todos os nós de administração na grade.

Você precisa concluir a configuração no servidor e, dependendo da Autoridade de certificação raiz (CA) que você está usando, os usuários também podem precisar instalar o certificado de CA raiz no navegador da Web que eles usarão para acessar o Gerenciador de Grade e o Gerenciador de locatário.

> Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of Server certificate for Management Interface** e o alarme legado de expiração de certificado de Interface de Gerenciamento (MCEP) são acionados quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

> Se você estiver acessando o Gerenciador de Grade ou o Gerenciador de locatário usando um nome de domínio em vez de um endereço IP, o navegador mostrará um erro de certificado sem uma opção para ignorar se uma das seguintes situações ocorrer:
>
> - O certificado do servidor de interface de gerenciamento personalizado expira.
> - Você reverte de um certificado de servidor de interface de gerenciamento personalizado para o certificado de servidor padrão.

#### Passos

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção certificado do servidor de interface de gerenciamento, clique em **Instalar certificado personalizado**.
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

     > As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

   - **CA Bundle**: Um único arquivo contendo os certificados de cada autoridade de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em

PEM, concatenados em ordem de cadeia de certificados.

4. Clique em **Salvar**.

   Os certificados de servidor personalizados são usados para todas as novas conexões de cliente subsequentes.

   Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

   > Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

#### Restaurando os certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário

Você pode reverter para o uso dos certificados de servidor padrão para o Gerenciador de Grade e o Gerenciador de locatário.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Gerenciar certificado do servidor de interface, clique em **usar certificados padrão**.
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

#### Configurando um certificado de servidor personalizado para conexões ao nó de armazenamento ou ao serviço CLB

Você pode substituir o certificado do servidor usado para conexões de cliente S3 ou Swift ao nó de armazenamento ou ao serviço CLB (obsoleto) no nó de gateway. O certificado de servidor personalizado de substituição é específico para a sua organização.

**Sobre esta tarefa**

Por padrão, cada nó de armazenamento é emitido um certificado de servidor X,509 assinado pela CA de grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e uma chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os nós de armazenamento, portanto, você deve especificar o certificado como um certificado curinga ou multi-domínio se os clientes precisarem verificar o nome do host ao se conetar ao endpoint de armazenamento. Defina o certificado personalizado de modo que corresponda a todos os nós de storage na grade.

Depois de concluir a configuração no servidor, os usuários também podem precisar instalar o certificado CA raiz no cliente API S3 ou Swift que eles usarão para acessar o sistema, dependendo da Autoridade de Certificação raiz (CA) que você estiver usando.

Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiration of Server certificate for Storage API Endpoints** e o alarme legacy Storage API Service Endpoints Certificate Expiration (SCEP) são acionados quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode visualizar o número de dias até que o certificado de serviço atual expire selecionando **Support** > **Tools** > **Grid Topology**. Em seguida, selecione ***Primary Admin Node*** > **CMN** > **Resources**.

Os certificados personalizados só são usados se os clientes se conetarem ao StorageGRID usando o serviço CLB obsoleto nos nós do gateway ou se eles se conetarem diretamente aos nós de armazenamento. Os clientes S3 ou Swift que se conetam ao StorageGRID usando o serviço de balanceador de carga em nós de administração ou nós de gateway usam o certificado configurado para o ponto de extremidade do balanceador de carga.

O alerta **Expiration of load balancer endpoint certificate** é acionado para os pontos de extremidade do balanceador de carga que expirarão em breve.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Object Storage API Service Endpoints Server Certificate, clique em **Install Custom Certificate** (Instalar certificado personalizado).
3. Carregue os ficheiros de certificado do servidor necessários:
   - **Certificado do servidor**: O arquivo de certificado do servidor personalizado (`.crt`).
   - **Chave privada do certificado do servidor**: O arquivo de chave privada do certificado do servidor personalizado (`.key`).

     As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

   - **CA Bundle**: Um único arquivo contendo os certificados de cada autoridade de certificação de emissão intermediária (CA). O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.
4. Clique em **Salvar**.

   O certificado de servidor personalizado é usado para todas as novas conexões de cliente API subsequentes.

   Selecione uma guia para exibir informações detalhadas sobre o certificado padrão do servidor StorageGRID ou um certificado assinado pela CA que foi carregado.

   Depois de carregar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados (ou alarmes legados) sejam apagados.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

**Informações relacionadas**

"Use S3"

"Use Swift"

"Configurando nomes de domínio de endpoint da API S3"

### Restaurando os certificados de servidor padrão para os endpoints S3 e Swift REST API

Você pode reverter para o uso dos certificados de servidor padrão para os endpoints da API REST S3 e Swift.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção Object Storage API Service Endpoints Server Certificate (certificado do servidor de Endpoints), clique em **Use Default Certificates** (usar certificados padrão).
3. Clique em **OK** na caixa de diálogo de confirmação.

   Quando você restaura os certificados de servidor padrão para os endpoints da API de armazenamento de objetos, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. Os certificados de servidor padrão são usados para todas as novas conexões de cliente API subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

### Copiar o certificado CA do sistema StorageGRID

O StorageGRID usa uma autoridade de certificação (CA) interna para proteger o tráfego interno. Este certificado não muda se você carregar seus próprios certificados.

**O que você vai precisar**

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

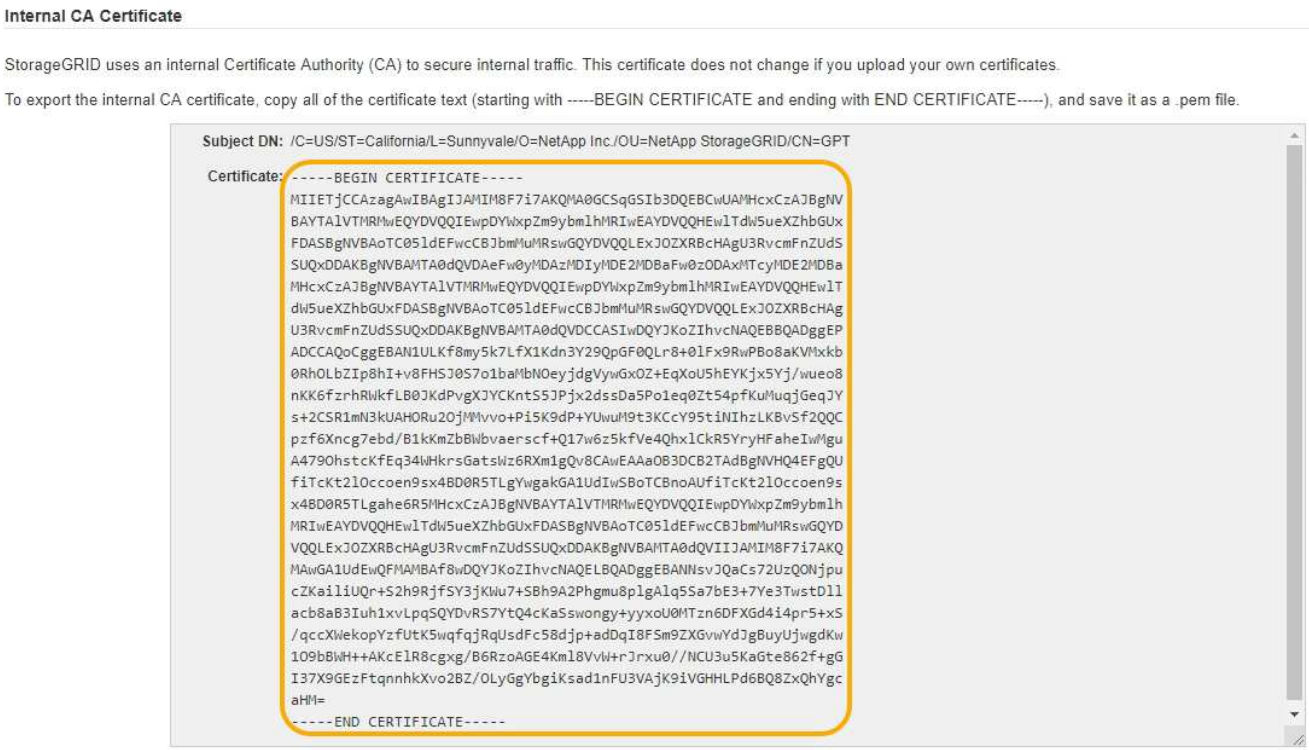
**Sobre esta tarefa**

Se um certificado de servidor personalizado tiver sido configurado, os aplicativos cliente devem verificar o servidor usando o certificado de servidor personalizado. Eles não devem copiar o certificado da CA do sistema StorageGRID.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **certificados de servidor**.
2. Na seção **certificado de CA interno**, selecione todo o texto do certificado.

   Você deve incluir `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` em sua seleção.




3. Clique com o botão direito do rato no texto selecionado e selecione **Copiar**.
4. Cole o certificado copiado em um editor de texto.
5. Salve o arquivo com a extensão `.pem`.

   Por exemplo: `storagegrid_certificate.pem`

### Configurando certificados StorageGRID para FabricPool

Para clientes S3 que executam validação estrita de nome de host e não suportam a desativação estrita de validação de nome de host, como clientes ONTAP que usam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o ponto de extremidade do balanceador de carga.

#### O que você vai precisar

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

#### Sobre esta tarefa

Quando você cria um ponto de extremidade do balanceador de carga, você pode gerar um certificado de servidor autoassinado ou carregar um certificado assinado por uma autoridade de certificação (CA) conhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA conhecida. Os certificados assinados por uma CA podem ser girados sem interrupções. Eles também são mais seguros porque fornecem melhor proteção contra ataques do homem no meio.

As etapas a seguir fornecem diretrizes gerais para clientes S3 que usam FabricPool. Para obter informações e procedimentos mais detalhados, consulte as instruções de configuração do StorageGRID for FabricPool.

O serviço CLB (Connection Load Balancer) separado nos nós de gateway está obsoleto e não é mais recomendado para uso com o FabricPool.

**Passos**

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para uso do FabricPool.
2. Crie um ponto de extremidade do balanceador de carga S3 para o FabricPool usar.

   Quando você cria um endpoint do balanceador de carga HTTPS, é solicitado que você carregue o certificado do servidor, a chave privada do certificado e o pacote CA.

3. Anexar o StorageGRID como uma categoria de nuvem no ONTAP.

   Especifique a porta de endpoint do balanceador de carga e o nome de domínio totalmente qualificado usado no certificado da CA que você carregou. Em seguida, forneça o certificado CA.

   Se uma CA intermediária tiver emitido o certificado StorageGRID, você deverá fornecer o certificado de CA intermediário. Se o certificado StorageGRID tiver sido emitido diretamente pela CA raiz, você deverá fornecer o certificado CA raiz.

**Informações relacionadas**

"Configurar o StorageGRID para FabricPool"

### Gerando um certificado de servidor autoassinado para a interface de gerenciamento

Você pode usar um script para gerar um certificado de servidor auto-assinado para clientes de API de gerenciamento que exigem validação estrita do nome de host.

**O que você vai precisar**

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.

**Sobre esta tarefa**

Em ambientes de produção, você deve usar um certificado assinado por uma autoridade de certificação (CA) conhecida. Os certificados assinados por uma CA podem ser girados sem interrupções. Eles também são mais seguros porque fornecem melhor proteção contra ataques do homem no meio.

**Passos**

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó Admin.
2. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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 `#`.

3. Configure o StorageGRID com um novo certificado autoassinado.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Para `--domains`, use curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração. Por exemplo, `*.ui.storagegrid.example.com` usa o caractere curinga * para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Defina `--type` como `management` para configurar o certificado usado pelo Gerenciador de Grade e pelo Gerenciador de Tenant.
- Por padrão, os certificados gerados são válidos por um ano (365 dias) e devem ser recriados antes de expirarem. Você pode usar o `--days` argumento para substituir o período de validade padrão.

> O período de validade de um certificado começa quando `make-certificate` é executado. Você deve garantir que o cliente da API de gerenciamento esteja sincronizado com a mesma fonte de tempo que o StorageGRID; caso contrário, o cliente poderá rejeitar o certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

A saída resultante contém o certificado público necessário pelo cliente da API de gerenciamento.

4. Selecione e copie o certificado.

   Inclua as tags DE INÍCIO e FIM em sua seleção.

5. Faça logout do shell de comando. `$ exit`
6. Confirme se o certificado foi configurado:
   a. Acesse o Gerenciador de Grade.
   b. Selecione **Configuração** > **certificados de servidor** > **certificado de servidor de interface de gerenciamento**.
7. Configure seu cliente de API de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

## Configurando as configurações de proxy de armazenamento

Se você estiver usando serviços de plataforma ou pools de storage em nuvem, poderá configurar um proxy não transparente entre nós de storage e os pontos de extremidade externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens de serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na Internet.

**O que você vai precisar**

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

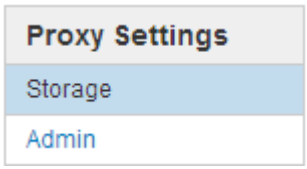
**Sobre esta tarefa**

Você pode configurar as configurações para um único proxy de armazenamento.

**Passos**

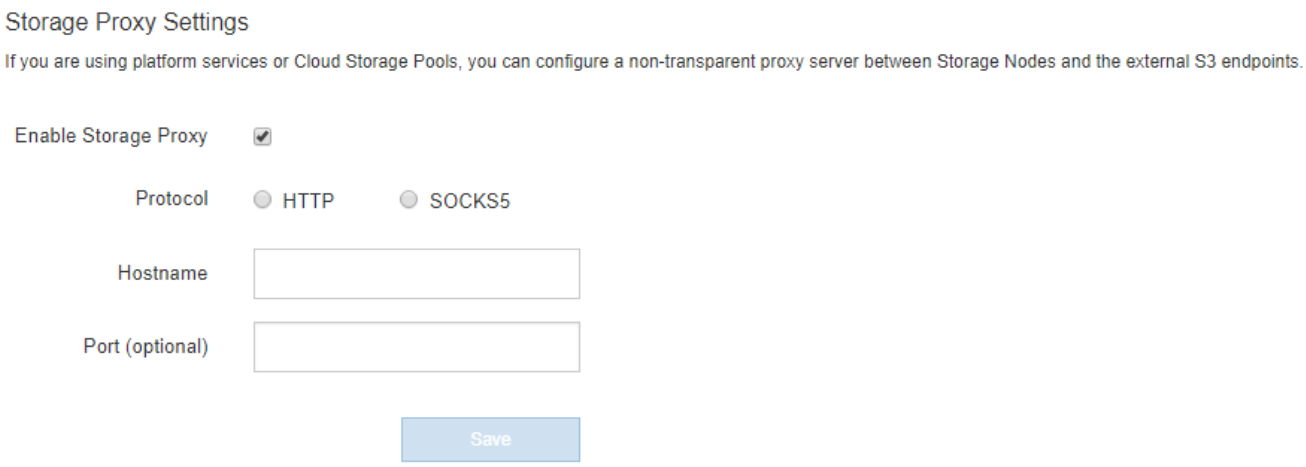
1. Selecione **Configuração** > **Configurações de rede** > **Configurações de proxy**.

   A página Configurações do proxy de armazenamento é exibida. Por padrão, **Storage** está selecionado no menu da barra lateral.

2. Marque a caixa de seleção **Enable Storage Proxy** (Ativar proxy de armazenamento*).

   Os campos para configurar um proxy de armazenamento são exibidos.

3. Selecione o protocolo para o proxy de armazenamento não transparente.
4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para se conetar ao servidor proxy.

   Você pode deixar este campo em branco se usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Clique em **Salvar**.

   Depois que o proxy Storage for salvo, novos endpoints para serviços de plataforma ou pools de armazenamento em nuvem podem ser configurados e testados.

   > As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

7. Verifique as configurações do servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma do StorageGRID não sejam bloqueadas.

**Depois de terminar**

Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção **Ativar proxy de armazenamento** e clique em **Salvar**.

**Informações relacionadas**

"Rede e portas para serviços de plataforma"

"Gerenciar objetos com ILM"

## Configurando as configurações de proxy Admin

Se você enviar mensagens AutoSupport usando HTTP ou HTTPS, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico (AutoSupport).

**O que você vai precisar**

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

**Sobre esta tarefa**

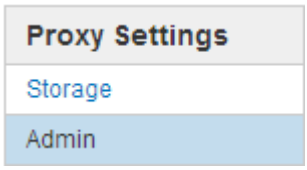
Você pode configurar as configurações para um único proxy Admin.

**Passos**

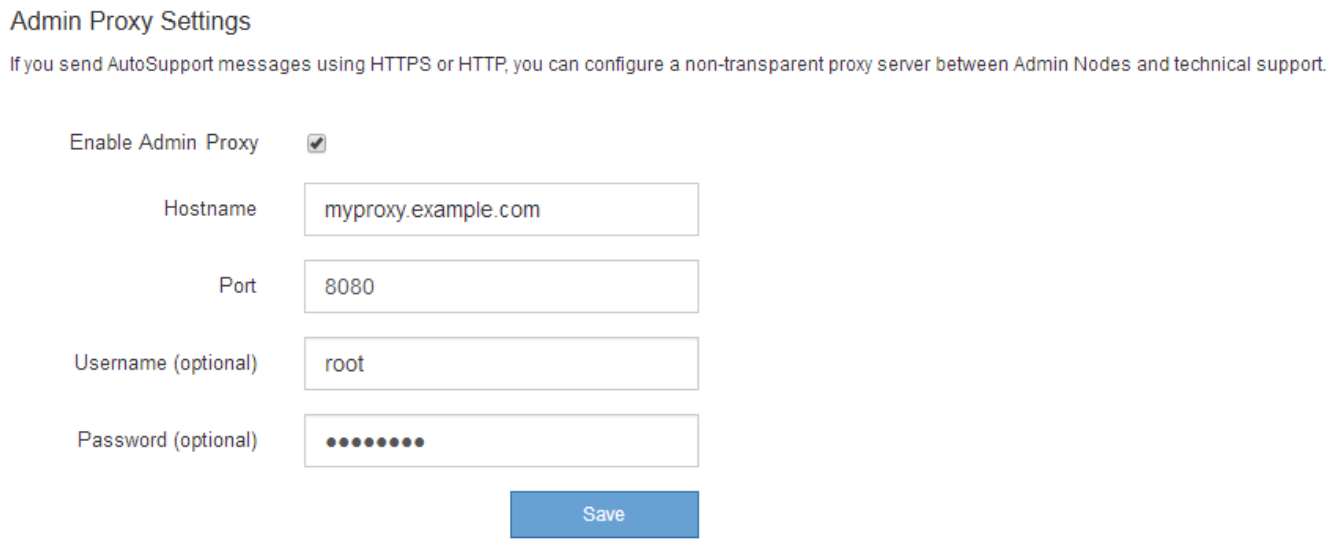
1. Selecione **Configuração** > **Configurações de rede** > **Configurações de proxy**.

   É apresentada a página Admin Proxy Settings (Definições de proxy de administração). Por padrão, **Storage** está selecionado no menu da barra lateral.

2. No menu da barra lateral, selecione **Admin**.




3. Marque a caixa de seleção **Enable Admin Proxy** (Ativar proxy de administrador).




4. Introduza o nome de anfitrião ou o endereço IP do servidor proxy.

5. Introduza a porta utilizada para ligar ao servidor proxy.
6. Opcionalmente, insira o nome de usuário do proxy.

   Deixe este campo em branco se o servidor proxy não exigir um nome de usuário.

7. Opcionalmente, insira a senha do proxy.

   Deixe este campo em branco se o servidor proxy não exigir uma senha.

8. Clique em **Salvar**.

   Depois que o proxy Admin é salvo, o servidor proxy entre nós Admin e o suporte técnico é configurado.

   > As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

9. Se você precisar desativar o proxy, desmarque a caixa de seleção **Ativar proxy Admin** e clique em **Salvar**.

**Informações relacionadas**

"Especificando o protocolo para mensagens AutoSupport"

## Gerir políticas de classificação de tráfego

Para aprimorar suas ofertas de qualidade de serviço (QoS), você pode criar políticas de classificação de tráfego para identificar e monitorar diferentes tipos de tráfego de rede. Essas políticas podem ajudar na limitação e monitoramento de tráfego.

As políticas de classificação de tráfego são aplicadas a pontos de extremidade no serviço de balanceador de carga do StorageGRID para nós de gateway e nós de administração. Para criar políticas de classificação de tráfego, você já deve ter criado pontos de extremidade do balanceador de carga.

### Regras de correspondência e limites opcionais

Cada política de classificação de tráfego contém uma ou mais regras correspondentes para identificar o tráfego de rede relacionado a uma ou mais das seguintes entidades:

- Baldes
- Inquilinos
- Sub-redes (IPv4 sub-redes contendo o cliente)
- Pontos finais (pontos finais do balanceador de carga)

O StorageGRID monitora o tráfego que corresponde a qualquer regra dentro da política de acordo com os objetivos da regra. Qualquer tráfego que corresponda a qualquer regra de uma política é Tratado por essa política. Por outro lado, você pode definir regras para corresponder a todo o tráfego, exceto uma entidade especificada.

Opcionalmente, você pode definir limites para uma política com base nos seguintes parâmetros:

- Agregar largura de banda em
- Agregar largura de banda para fora

- Solicitações de leitura simultânea
- Solicitações de gravação simultânea
- Largura de banda por solicitação in
- Saída de largura de banda por solicitação
- Leia a taxa de solicitação
- Taxa de solicitações de gravação

> Você pode criar políticas para limitar a largura de banda agregada ou limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no tráfego não limitado.

**Limitação de tráfego**

Quando você criou políticas de classificação de tráfego, o tráfego é limitado de acordo com o tipo de regras e limites definidos. Para limites de largura de banda agregada ou por solicitação, as solicitações são transmitidas ou enviadas pela taxa definida. O StorageGRID só pode impor uma velocidade, então a correspondência de política mais específica, por tipo matcher, é a aplicada. Para todos os outros tipos de limite, as solicitações do cliente são atrasadas em 250 milissegundos e recebem uma resposta de retardo 503 para solicitações que excedem qualquer limite de política correspondente.

No Gerenciador de Grade, você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

**Usando políticas de classificação de tráfego com SLAs**

Você pode usar políticas de classificação de tráfego em conjunto com limites de capacidade e proteção de dados para aplicar acordos de nível de serviço (SLAs) que fornecem detalhes sobre capacidade, proteção de dados e desempenho.

Os limites de classificação de tráfego são implementados por balanceador de carga. Se o tráfego for distribuído simultaneamente em vários balanceadores de carga, as taxas máximas totais são vários dos limites de taxa especificados.

O exemplo a seguir mostra três níveis de um SLA. Você pode criar políticas de classificação de tráfego para alcançar os objetivos de desempenho de cada nível de SLA.

| Nível de serviço | Capacidade | Proteção de dados | Desempenho | Custo |
|---|---|---|---|---|
| Ouro | 1 PB de armazenamento permitido | 3 copiar regra ILM | 25 K solicitações/seg<br><br>Largura de banda de 5 GB/seg (40 Gbps) | dólares por mês |

| Nível de serviço | Capacidade | Proteção de dados | Desempenho | Custo |
|---|---|---|---|---|
| Prata | 250 TB de armazenamento permitido | 2 copiar regra ILM | 10 K solicitações/seg<br><br>Largura de banda de 1,25 GB/seg (10 Gbps) | dólares por mês |
| Bronze | 100 TB de armazenamento permitido | 2 copiar regra ILM | 5 K solicitações/seg<br><br>Largura de banda de 1 GB/seg (8 Gbps) | dólares por mês |

### Criando políticas de classificação de tráfego

Você cria políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por intervalo, locatário, sub-rede IP ou ponto de extremidade do balanceador de carga. Opcionalmente, você pode definir limites para uma política com base na largura de banda, no número de solicitações simultâneas ou na taxa de solicitações.

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.
- Você precisa ter criado os pontos de extremidade do balanceador de carga que você deseja corresponder.
- Você deve ter criado os inquilinos que você deseja corresponder.

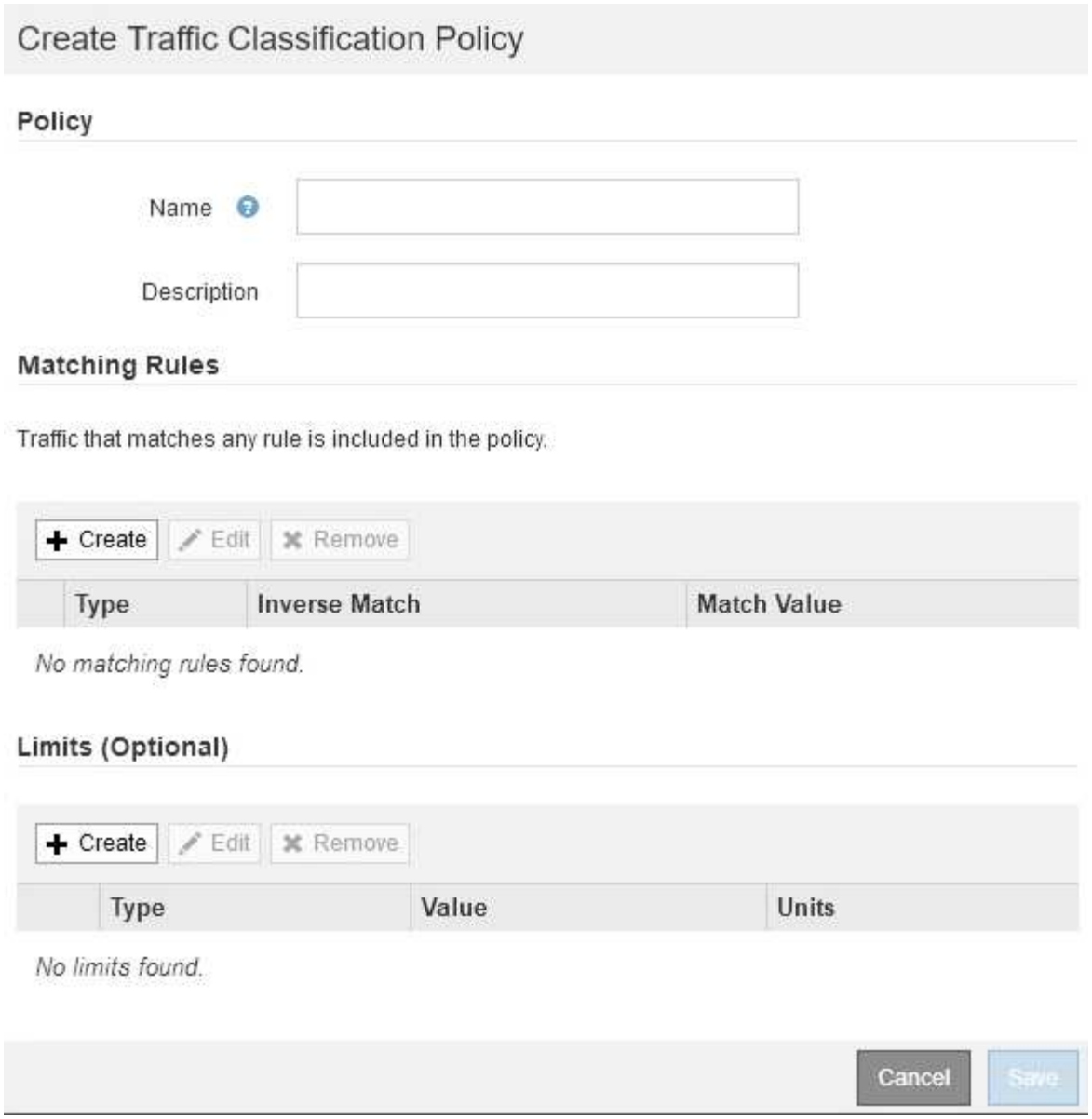
#### Passos

1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   É apresentada a página políticas de classificação de tráfego.


2. Clique em **criar**.

   É apresentada a caixa de diálogo criar política de classificação de tráfego.




3. No campo **Nome**, insira um nome para a política.

   Introduza um nome descritivo para que possa reconhecer a política.

4. Opcionalmente, adicione uma descrição para a política no campo **Description**.

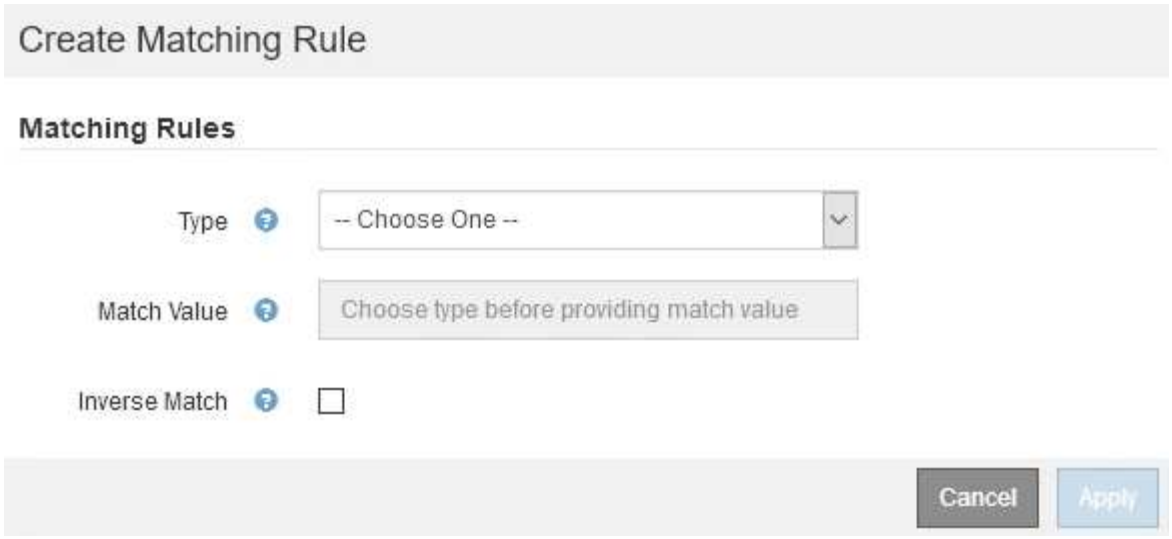
   Por exemplo, descreva ao que esta política de classificação de tráfego se aplica e ao que ela limitará.

5. Crie uma ou mais regras correspondentes para a política.

   Regras de correspondência controlam quais entidades serão afetadas por esta política de classificação de tráfego. Por exemplo, selecione Locatário se desejar que essa diretiva se aplique ao tráfego de rede de um locatário específico. Ou selecione ponto final se pretender que esta política se aplique ao tráfego de rede num ponto de extremidade do balanceador de carga específico.

   a. Clique em **criar** na seção **regras correspondentes**.

      A caixa de diálogo criar regra de correspondência é exibida.




b. Na lista suspensa **Type**, selecione o tipo de entidade a ser incluída na regra correspondente.

c. No campo **valor de correspondência**, insira um valor de correspondência com base no tipo de entidade que você escolheu.

   - Balde: Introduza um nome de intervalo.
   - Bucket Regex: Insira uma expressão regular que será usada para corresponder a um conjunto de nomes de bucket.

     A expressão regular não está ancorada. Use a âncora "caret" para corresponder ao início do nome do intervalo e use a âncora "doll" para corresponder ao final do nome.

   - CIDR: Insira uma sub-rede IPv4, na notação CIDR, que corresponda à sub-rede desejada.
   - Endpoint: Selecione um endpoint na lista de endpoints existentes. Esses são os pontos finais do balanceador de carga definidos na página pontos finais do balanceador de carga.
   - Locatário: Selecione um locatário na lista de inquilinos existentes. A correspondência de inquilinos baseia-se na propriedade do bucket que está sendo acessado. O acesso anônimo a um bucket corresponde ao locatário que possui o bucket.

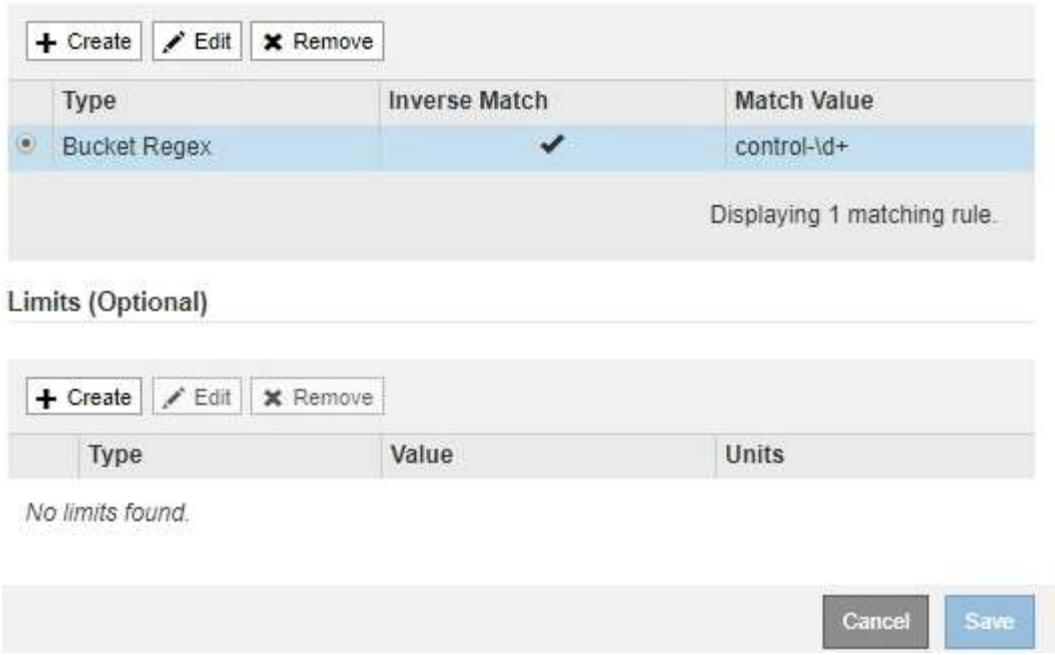
d. Se você quiser corresponder todo tráfego de rede *exceto* tráfego consistente com o valor tipo e correspondência definido, marque a caixa de seleção **Inverse**. Caso contrário, deixe a caixa de seleção desmarcada.

   Por exemplo, se você quiser que essa política se aplique a todos os pontos finais do balanceador de carga, especifique o ponto final do balanceador de carga a ser excluído e selecione **inverso**.

   > Para uma política que contenha vários matchers em que pelo menos um é um matcher inverso, tenha cuidado para não criar uma política que corresponda a todas as solicitações.

e. Clique em **aplicar**.

   A regra é criada e está listada na tabela regras correspondentes.




a. Repita estas etapas para cada regra que você deseja criar para a política.

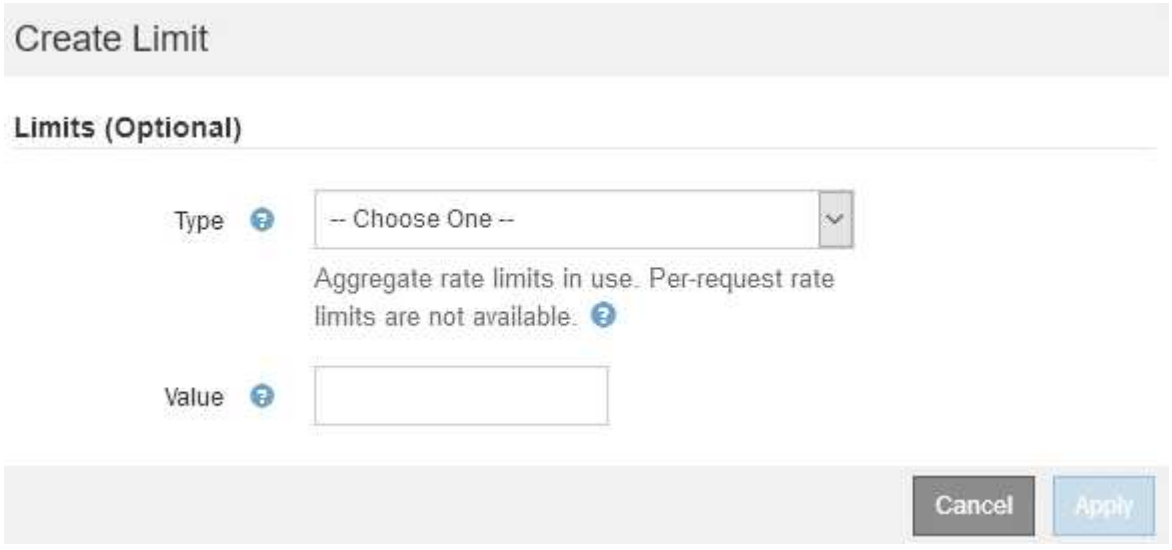
> O tráfego que corresponde a qualquer regra é Tratado pela política.

6. Opcionalmente, crie limites para a política.

> Mesmo que você não crie limites, o StorageGRID coleta métricas para que você possa monitorar o tráfego de rede que corresponde à política.

a. Clique em **criar** na seção **limites**.

A caixa de diálogo criar limite é exibida.




b. Na lista suspensa **Type**, selecione o tipo de limite que deseja aplicar à política.

Na lista a seguir, **in** refere-se ao tráfego de clientes S3 ou Swift para o balanceador de carga StorageGRID, e **OUT** refere-se ao tráfego do balanceador de carga para clientes S3 ou Swift.

- Agregar largura de banda em
- Agregar largura de banda para fora
- Solicitações de leitura simultânea
- Solicitações de gravação simultânea
- Largura de banda por solicitação in
- Saída de largura de banda por solicitação
- Leia a taxa de solicitação
- Taxa de solicitações de gravação

> Você pode criar políticas para limitar a largura de banda agregada ou limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda agregada podem impor um impactos menor no desempenho adicional no tráfego não limitado.

Para limites de largura de banda, o StorageGRID aplica a política que melhor corresponde ao tipo de limite definido. Por exemplo, se você tem uma política que limita o tráfego em apenas uma direção, então o tráfego na direção oposta será ilimitado, mesmo que haja tráfego que corresponda a políticas adicionais que tenham limites de largura de banda. A StorageGRID implementa as correspondências "melhores" para limites de largura de banda na seguinte ordem:

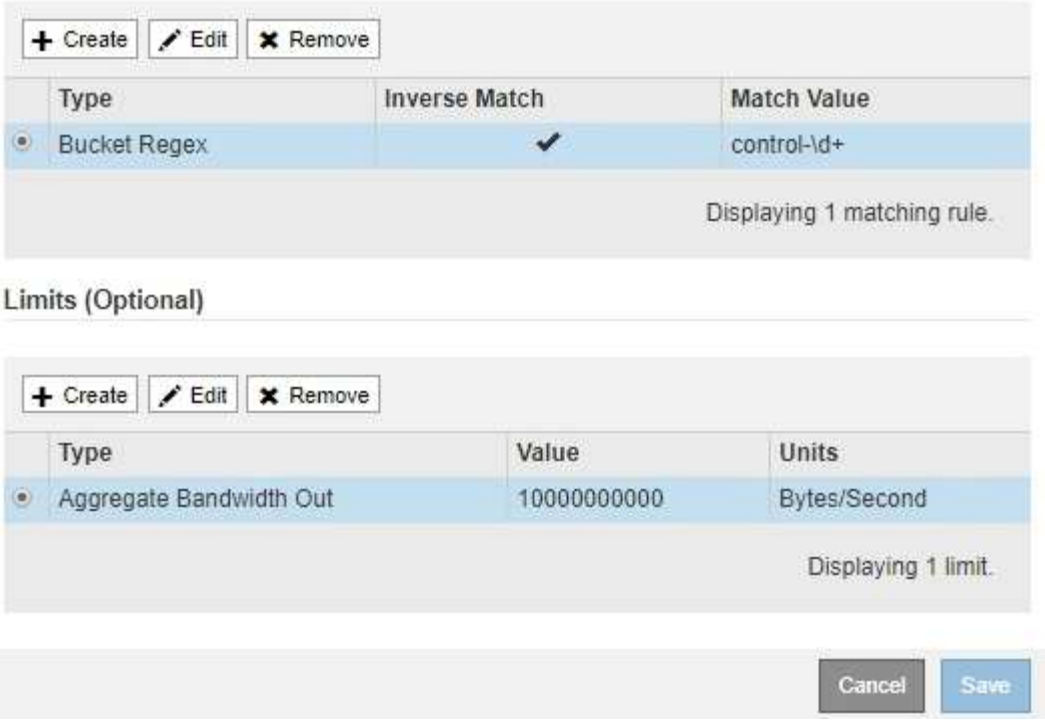
- Endereço IP exato (/máscara 32)
- Nome exato do balde
- Regex do balde
- Locatário
- Endpoint
- Correspondências CIDR não exatas (não /32)
- Correspondências inversas

c. No campo **value**, insira um valor numérico para o tipo de limite escolhido.

   As unidades esperadas são mostradas quando você seleciona um limite.

d. Clique em **aplicar**.

   O limite é criado e é listado na tabela limites.



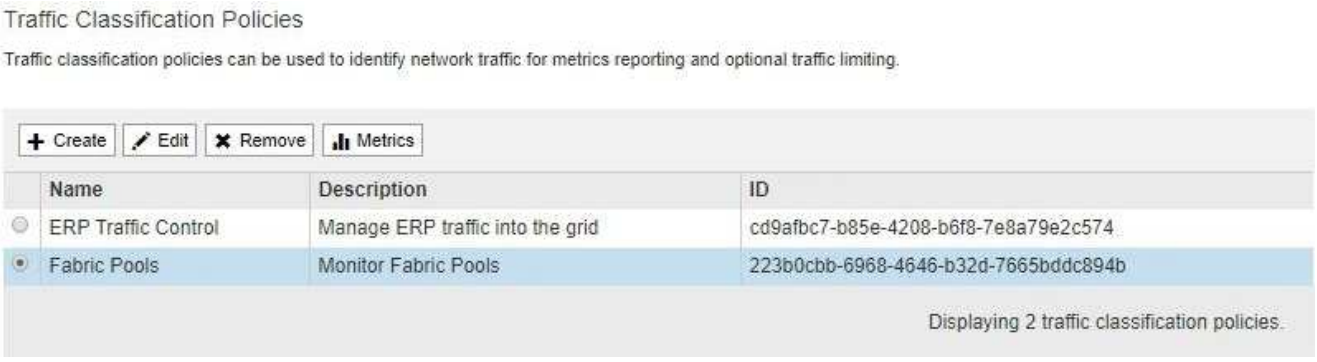

e. Repita estas etapas para cada limite que você deseja adicionar à política.

   Por exemplo, se você quiser criar um limite de largura de banda de 40 Gbps para um nível SLA, crie uma largura de banda agregada no limite e um limite de largura de banda agregada para fora e defina cada um para 40 Gbps.

   Para converter megabytes por segundo em gigabits por segundo, multiplique por oito. Por exemplo, 125 MB/s é equivalente a 1.000 Mbps ou 1 Gbps.

7. Quando terminar de criar regras e limites, clique em **Salvar**.

   A política é guardada e está listada na tabela políticas de classificação de tráfego.




   O tráfego de clientes S3 e Swift agora é Tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

**Informações relacionadas**

"Gerenciamento do balanceamento de carga"

"Visualização de métricas de tráfego de rede"

### Editar uma política de classificação de tráfego

Você pode editar uma política de classificação de tráfego para alterar seu nome ou descrição, ou para criar, editar ou excluir quaisquer regras ou limites para a política.

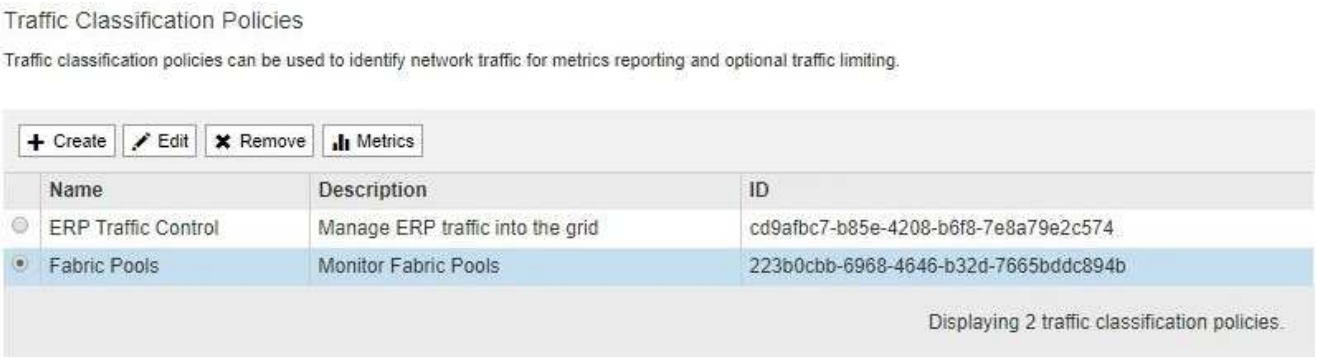
**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

**Passos**

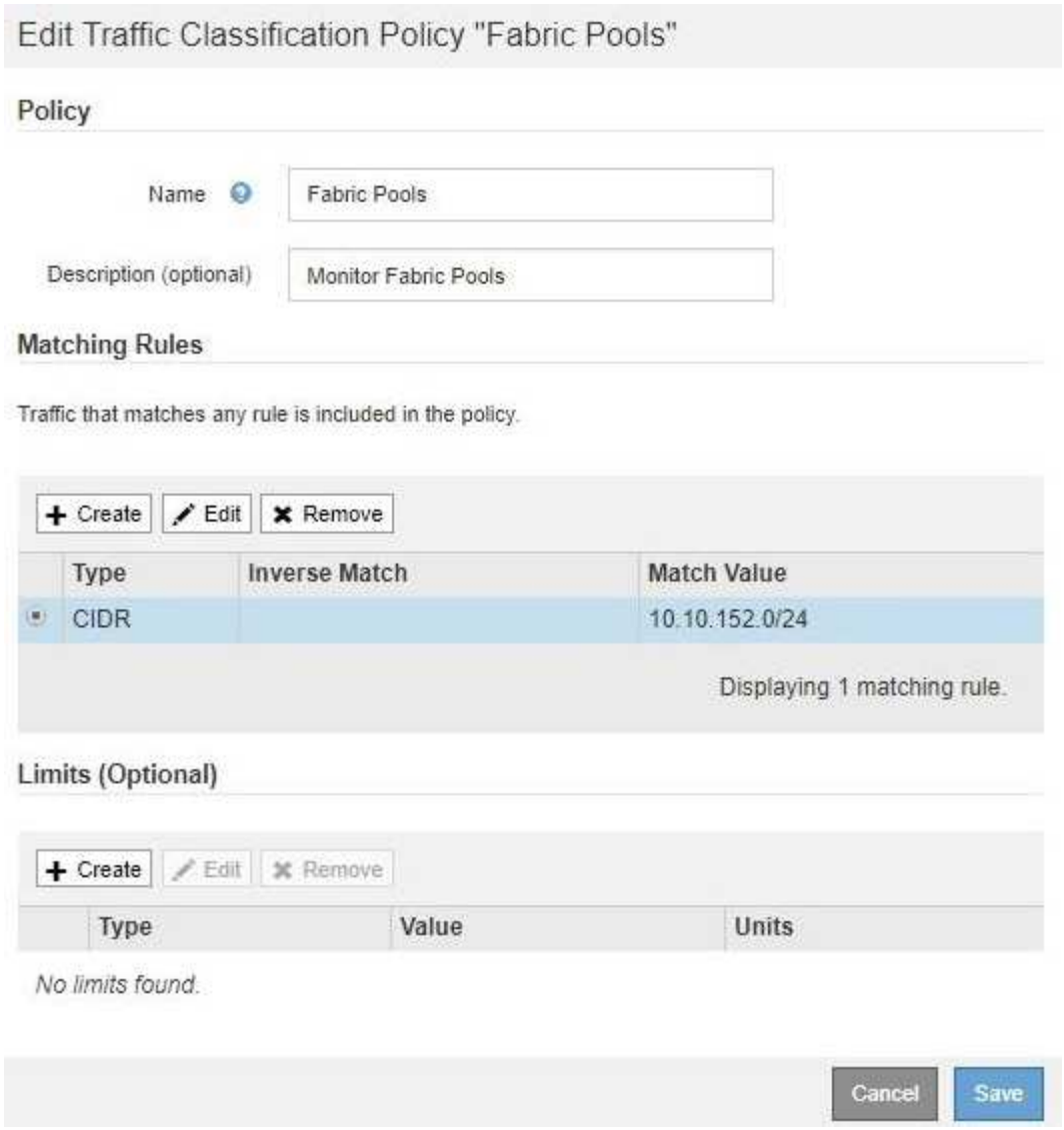
1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.




2. Selecione o botão de opção à esquerda da política que pretende editar.
3. Clique em **Editar**.

   A caixa de diálogo Editar diretiva de classificação de tráfego é exibida.




4. Crie, edite ou remova regras e limites correspondentes conforme necessário.
   a. Para criar uma regra ou limite correspondente, clique em **criar** e siga as instruções para criar uma regra ou criar um limite.
   b. Para editar uma regra ou limite correspondente, selecione o botão de opção para a regra ou limite, clique em **Editar** na seção **regras correspondentes** ou na seção **limites** e siga as instruções para criar uma regra ou criar um limite.
   c. Para remover uma regra ou limite correspondente, selecione o botão de opção para a regra ou limite e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover a regra ou limite.
5. Quando terminar de criar ou editar uma regra ou um limite, clique em **aplicar**.
6. Quando terminar de editar a política, clique em **Salvar**.

   As alterações feitas na política são salvas e o tráfego de rede é agora Tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego esperados.

#### Eliminar uma política de classificação de tráfego

Se você não precisar mais de uma política de classificação de tráfego, você pode excluí-

la.

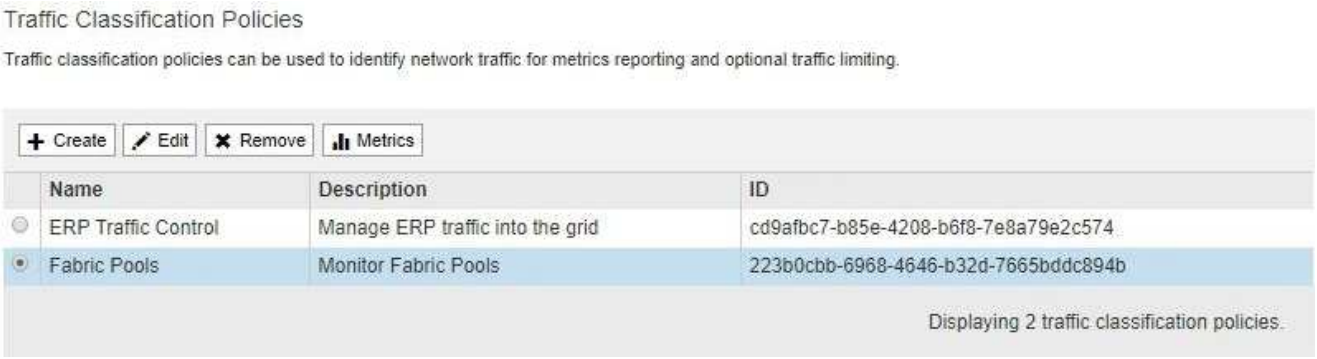
**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.




2. Selecione o botão de opção à esquerda da política que pretende eliminar.
3. Clique em **Remover**.

   É apresentada uma caixa de diálogo Aviso.


4. Clique em **OK** para confirmar que deseja excluir a política.

   A política é eliminada.

### Visualização de métricas de tráfego de rede

Pode monitorizar o tráfego de rede visualizando os gráficos disponíveis na página políticas de classificação de tráfego.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

**Sobre esta tarefa**

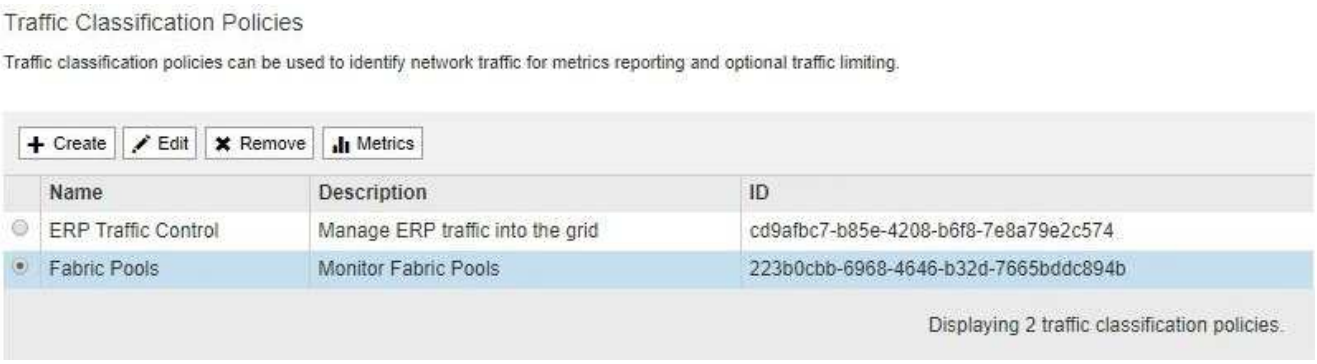
Para qualquer política de classificação de tráfego existente, você pode exibir métricas para o serviço Load Balancer para determinar se a diretiva está limitando com êxito o tráfego na rede. Os dados nos gráficos podem ajudá-lo a determinar se você precisa ajustar a política.

Mesmo que nenhum limite seja definido para uma política de classificação de tráfego, as métricas são coletadas e os gráficos fornecem informações úteis para entender as tendências de tráfego.

**Passos**

1. Selecione **Configuração** > **Configurações de rede** > **classificação de tráfego**.

   A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.




2. Selecione o botão de opção à esquerda da política para a qual deseja exibir as métricas.
3. Clique em **Metrics**.

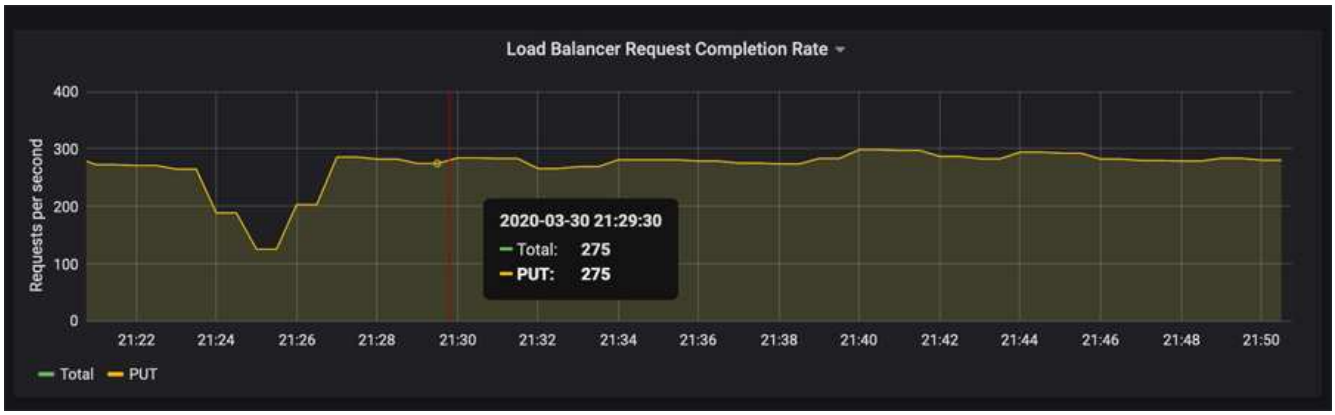
   Uma nova janela do navegador é aberta e os gráficos da Política de classificação de tráfego são exibidos. Os gráficos exibem métricas apenas para o tráfego que corresponde à política selecionada.

   Você pode selecionar outras políticas para exibir usando a lista suspensa **policy**.

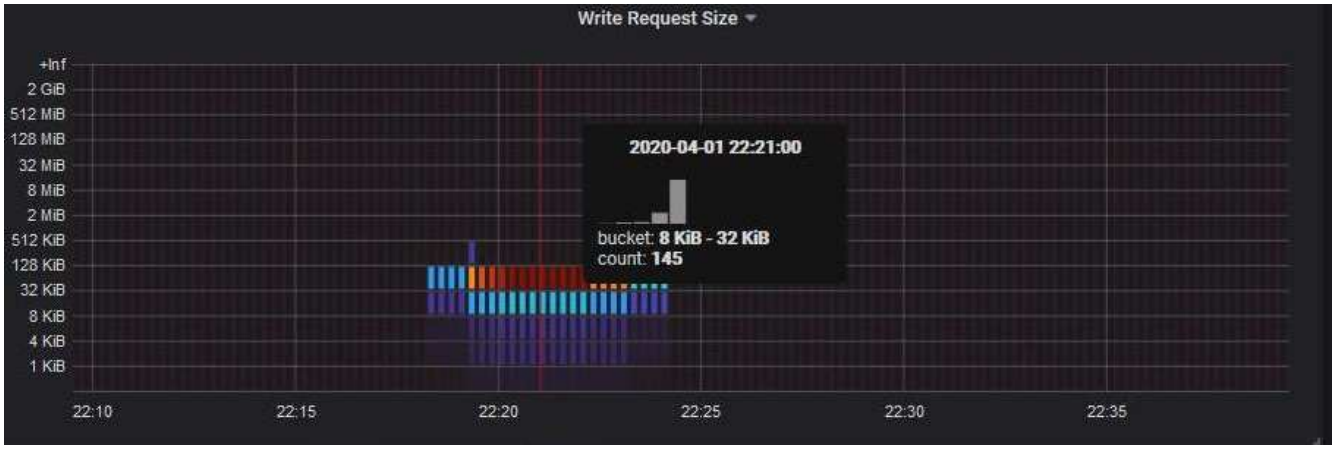

   Os gráficos a seguir estão incluídos na página da Web.

- Tráfego de solicitação do Load Balancer: Este gráfico fornece uma média móvel de 3 minutos da taxa de transferência de dados transmitidos entre os pontos de extremidade do balanceador de carga e os clientes que fazem as solicitações, em bits por segundo.
- Taxa de conclusão da solicitação do Load Balancer: Este gráfico fornece uma média móvel de 3 minutos do número de solicitações concluídas por segundo, discriminada por tipo de solicitação (OBTER, COLOCAR, CABEÇA e EXCLUIR). Este valor é atualizado quando os cabeçalhos de uma nova solicitação tiverem sido validados.
- Taxa de resposta de erro: Este gráfico fornece uma média móvel de 3 minutos do número de respostas de erro retornadas aos clientes por segundo, discriminada pelo código de resposta de erro.
- Duração média da solicitação (não-erro): Este gráfico fornece uma média móvel de 3 minutos de duração da solicitação, discriminada por tipo de solicitação (OBTER, COLOCAR, CABEÇA e EXCLUIR). Cada duração da solicitação começa quando um cabeçalho de solicitação é analisado pelo serviço Load Balancer e termina quando o corpo de resposta completo é retornado ao cliente.
- Taxa de solicitação de gravação por tamanho do objeto: Este mapa de calor fornece uma média móvel de 3 minutos da taxa na qual as solicitações de gravação são concluídas com base no tamanho do objeto. Neste contexto, as solicitações de escrita referem-se apenas a SOLICITAÇÕES PUT.
- Taxa de solicitação de leitura por tamanho do objeto: Este mapa de calor fornece uma média móvel de 3 minutos da taxa na qual as solicitações de leitura são concluídas com base no tamanho do objeto. Neste contexto, as solicitações de leitura referem-se apenas a SOLICITAÇÕES GET. As cores no mapa de calor indicam a frequência relativa de um tamanho de objeto dentro de um gráfico individual. As cores mais frias (por exemplo, roxo e azul) indicam taxas relativas mais baixas, e as cores mais quentes (por exemplo, laranja e vermelho) indicam taxas relativas mais altas.

4. Passe o cursor sobre um gráfico de linhas para ver um pop-up de valores em uma parte específica do gráfico.




5. Passe o cursor sobre um mapa de calor para ver um pop-up que mostra a data e a hora da amostra, os tamanhos de objetos que são agregados na contagem e o número de solicitações por segundo durante esse período de tempo.




6. Use a lista suspensa **Policy** (Política*) no canto superior esquerdo para selecionar uma política diferente.

   São apresentados os gráficos da política selecionada.

7. Em alternativa, aceda aos gráficos a partir do menu **Support**.
   a. Selecione **Support** > **Tools** > **Metrics**.
   b. Na seção **Grafana** da página, selecione **Política de classificação de tráfego**.
   c. Selecione a política na lista suspensa no canto superior esquerdo da página.

      As políticas de classificação de tráfego são identificadas pelo seu ID. Os IDs de política são listados na página políticas de classificação de tráfego.

8. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustar a política.

**Informações relacionadas**

"Monitorizar Resolução de problemas"

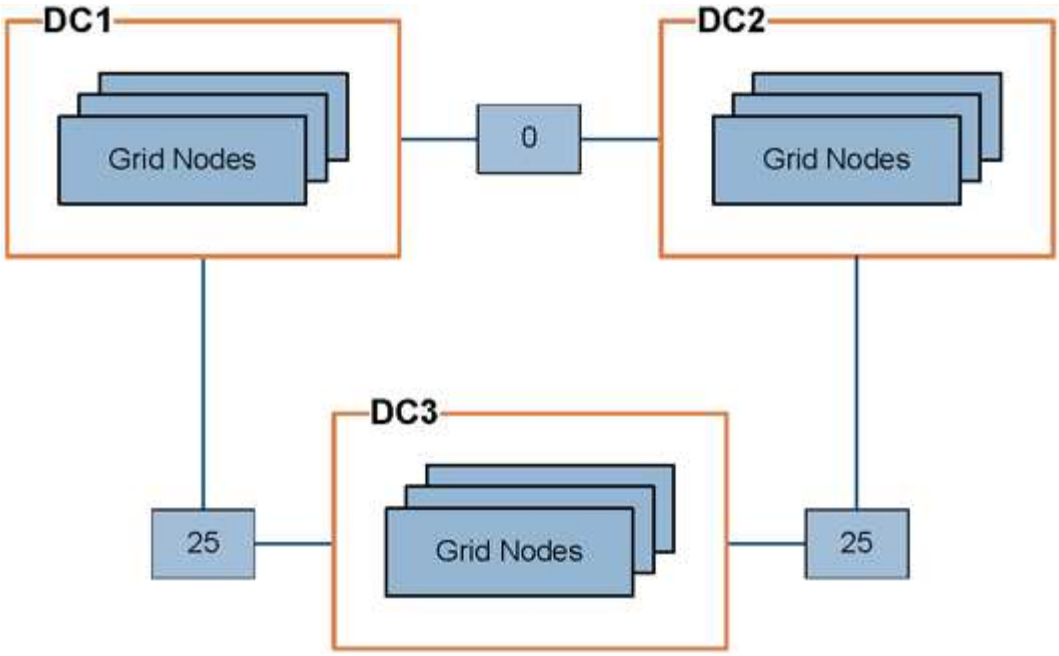
## Quais são os custos da ligação

Os custos de link permitem que você priorize qual local do data center fornece um serviço solicitado quando existem dois ou mais locais de data center. Você pode ajustar os custos de link para refletir a latência entre sites.

- Os custos de link são usados para priorizar qual cópia de objeto é usada para cumprir recuperações de objetos.
- Os custos de link são usados pela API de gerenciamento de grade e pela API de gerenciamento de locatário para determinar quais serviços internos do StorageGRID devem ser usados.
- Os custos de link são usados pelo serviço CLB nos nós do Gateway para direcionar as conexões do cliente.

  O serviço CLB está obsoleto.

O diagrama mostra uma grade de três sites que tem custos de link configurados entre sites:




- O serviço CLB nos nós de Gateway distribui igualmente as conexões de cliente para todos os nós de armazenamento no mesmo local do data center e para qualquer local do data center com um custo de link de 0.

  No exemplo, um nó de gateway no local do data center 1 (DC1) distribui igualmente as conexões de cliente para nós de storage em DC1 e para nós de storage em DC2. Um nó de gateway em DC3 envia conexões de cliente somente para nós de storage em DC3.

- Ao recuperar um objeto que existe como várias cópias replicadas, o StorageGRID recupera a cópia no data center que tem o menor custo de link.

  No exemplo, se um aplicativo cliente em DC2 recupera um objeto que é armazenado em DC1 e DC3, o objeto é recuperado de DC1, porque o custo do link de DC1 para D2 é 0, o que é menor do que o custo do link de DC3 para DC2 (25).

Os custos de ligação são números relativos arbitrários sem unidade de medida específica. Por exemplo, um custo de link de 50 é usado menos preferencialmente do que um custo de link de 25. A tabela mostra os custos de link comumente usados.

| Link | Custo da ligação | Notas |
|---|---|---|
| Entre locais de data center físico | 25 (predefinição) | Data centers conectados por um link WAN. |
| Entre locais lógicos de data center no mesmo local físico | 0 | Data centers lógicos no mesmo prédio físico ou campus conetados por uma LAN. |

**Informações relacionadas**

"Como funciona o balanceamento de carga - serviço CLB"

### Atualizar custos de link

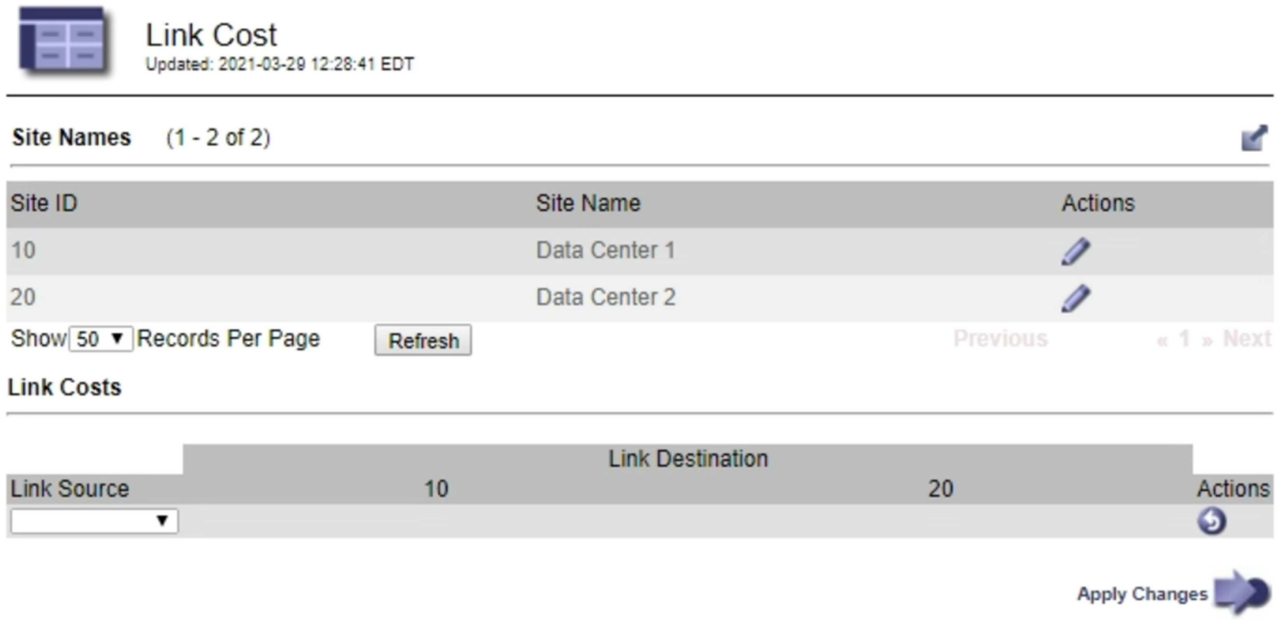
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão Configuração da Página de topologia de Grade.

**Passos**

1. Selecione **Configuração** > **Definições de rede** > **custo de ligação**.




2. Selecione um site em **Link Source** e insira um valor de custo entre 0 e 100 em **Link Destination**.

   Não é possível alterar o custo do link se a origem for igual ao destino.

   Para cancelar as alterações, clique em **Revert**.

3. Clique em **aplicar alterações**.

# Configurando o AutoSupport

O recurso AutoSupport permite que o sistema StorageGRID envie mensagens de status e integridade para o suporte técnico. O uso do AutoSupport pode acelerar significativamente a determinação e resolução de problemas. O suporte técnico também pode monitorar as necessidades de storage do seu sistema e ajudá-lo a determinar se precisa adicionar novos nós ou sites. Opcionalmente, você pode configurar as mensagens do AutoSupport para serem enviadas para um destino adicional.

## Informações incluídas nas mensagens do AutoSupport

As mensagens do AutoSupport incluem informações como as seguintes:

- Versão do software StorageGRID
- Versão do sistema operativo
- Informações sobre atributos no nível do sistema e no nível da localização
- Alertas e alarmes recentes (sistema legado)
- Status atual de todas as tarefas de grade, incluindo dados históricos
- Informações de eventos conforme listado na página **nós** > ***Grid Node*** > **Eventos**
- Utilização da base de dados do Admin Node
- Número de objetos perdidos ou perdidos
- Definições de configuração da grelha
- Entidades NMS
- Política ILM ativa
- Arquivo de especificação de grade provisionada
- Métricas de diagnóstico

Você pode ativar o recurso AutoSupport e as opções individuais do AutoSupport quando instalar o StorageGRID pela primeira vez, ou ativá-los posteriormente. Se o AutoSupport não estiver habilitado, uma mensagem será exibida no Painel de Gerenciamento de Grade. A mensagem inclui um link para a página de configuração do AutoSupport.


Você pode selecionar o símbolo "x" para fechar a mensagem. A mensagem não aparecerá novamente até que o cache do navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

## Usando o Active IQ

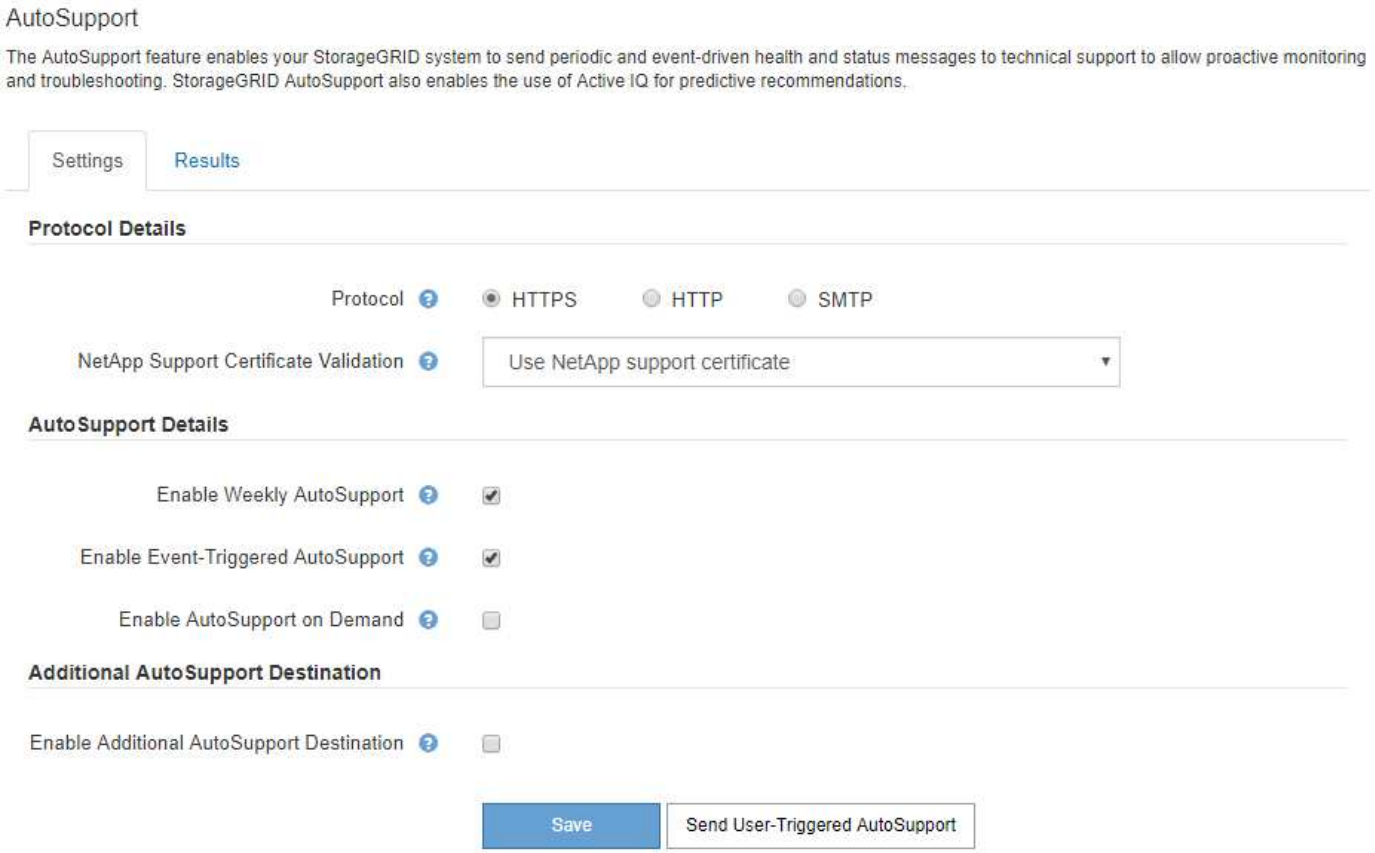
O Active IQ é um consultor digital baseado na nuvem que utiliza as análises preditivas e o conhecimento da comunidade da base instalada da NetApp. Suas avaliações de risco contínuas, alertas preditivos, orientações prescritivas e ações automatizadas ajudam a evitar problemas antes que eles ocorram, levando a uma melhor integridade do sistema e maior disponibilidade do sistema.

Você deve habilitar o AutoSupport se quiser usar os painéis e a funcionalidade do Active IQ no site de suporte da NetApp.

"Documentação do consultor digital da Active IQ"

## Aceder às definições do AutoSupport

Você configura o AutoSupport usando o Gerenciador de Grade (**suporte** > **Ferramentas** > **AutoSupport**). A página **AutoSupport** tem duas guias: **Configurações** e **resultados**.




## Protocolos para envio de mensagens AutoSupport

Você pode escolher um dos três protocolos para enviar mensagens AutoSupport:

- HTTPS
- HTTP
- SMTP

Se você enviar mensagens AutoSupport usando HTTPS ou HTTP, poderá configurar um servidor proxy não transparente entre nós de administração e suporte técnico.

Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de configurar um servidor de correio SMTP.

## Opções de AutoSupport

Você pode usar qualquer combinação das seguintes opções para enviar mensagens do AutoSupport para o suporte técnico:

- **Semanal**: Enviar automaticamente mensagens AutoSupport uma vez por semana. Predefinição: Activado.
- **Event-dispolled**: Envie automaticamente mensagens AutoSupport a cada hora ou quando ocorrerem eventos significativos do sistema. Predefinição: Activado.
- **Sob demanda**: Permita que o suporte técnico solicite que seu sistema StorageGRID envie mensagens AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer protocolo de transmissão HTTPS AutoSupport). Predefinição: Desativada.
- **Ativado pelo usuário**: Envie mensagens AutoSupport manualmente a qualquer momento.

**Informações relacionadas**

"Suporte à NetApp"

## Especificando o protocolo para mensagens AutoSupport

Você pode usar um dos três protocolos para enviar mensagens AutoSupport.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.
- Se você usar o protocolo HTTPS ou HTTP para enviar mensagens AutoSupport, você deve ter fornecido acesso de saída à Internet para o nó de administração principal, diretamente ou usando um servidor proxy (conexões de entrada não necessárias).
- Se utilizar o protocolo HTTPS ou HTTP e pretender utilizar um servidor proxy, tem de ter configurado um servidor proxy Admin.
- Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de ter configurado um servidor de correio SMTP. A mesma configuração do servidor de e-mail é usada para notificações de e-mail de alarme (sistema legado).

**Sobre esta tarefa**

As mensagens AutoSupport podem ser enviadas usando qualquer um dos seguintes protocolos:

- **HTTPS**: Esta é a configuração padrão e recomendada para novas instalações. O protocolo HTTPS utiliza a porta 443. Se pretender ativar a funcionalidade AutoSupport On Demand, tem de utilizar o protocolo HTTPS.
- **HTTP**: Este protocolo não é seguro, a menos que seja usado em um ambiente confiável onde o servidor proxy converte para HTTPS ao enviar dados pela Internet. O protocolo HTTP usa a porta 80.
- **SMTP**: Use esta opção se quiser que as mensagens do AutoSupport sejam enviadas por e-mail. Se utilizar SMTP como protocolo para mensagens AutoSupport, tem de configurar um servidor de correio SMTP na página Configuração de e-mail legado (**suporte** > **Alarmes (legado)** > **Configuração de e-mail legado**).

> ⓘ O SMTP era o único protocolo disponível para mensagens AutoSupport antes do lançamento do StorageGRID 11,2. Se você instalou uma versão anterior do StorageGRID inicialmente, o SMTP pode ser o protocolo selecionado.

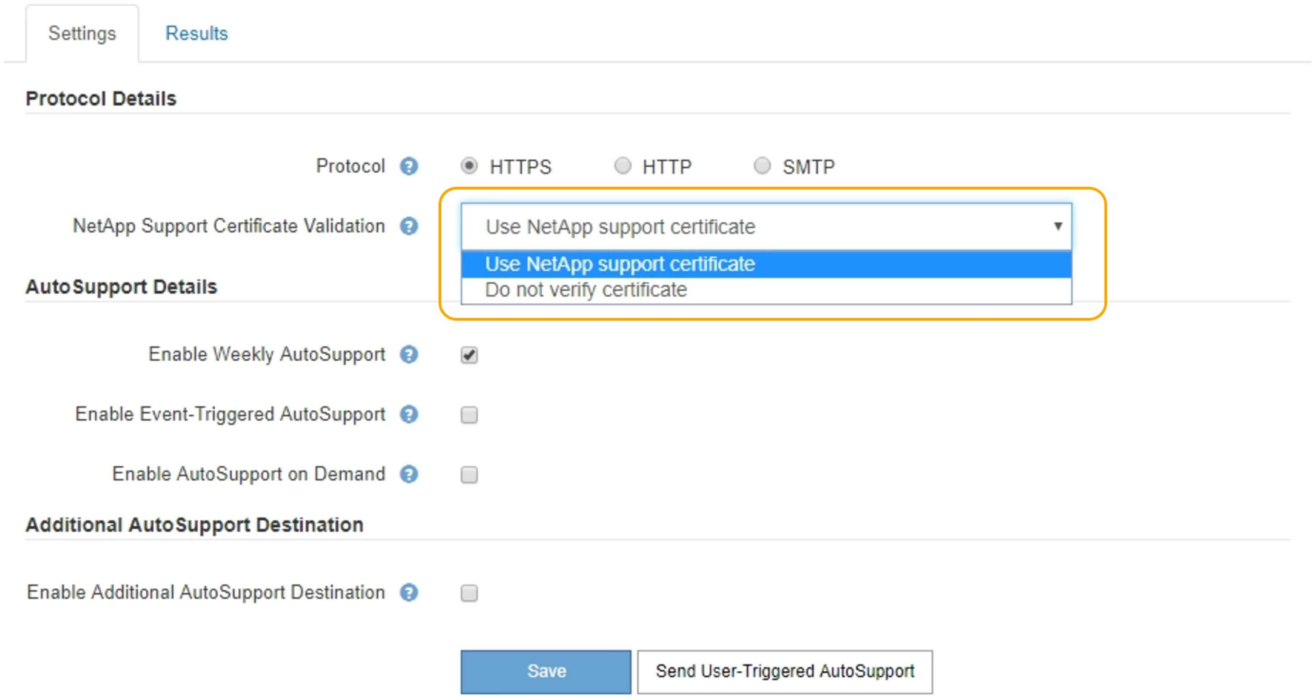
O protocolo definido é utilizado para enviar todos os tipos de mensagens AutoSupport.

**Passos**

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

   A página AutoSupport é exibida e a guia **Configurações** é selecionada.

2. Selecione o protocolo que pretende utilizar para enviar mensagens AutoSupport.




3. Selecione sua escolha para **Validação de certificado de suporte NetApp**.
   - Use o certificado de suporte NetApp (padrão): A validação do certificado garante que a transmissão de mensagens AutoSupport seja segura. O certificado de suporte do NetApp já está instalado com o software StorageGRID.
   - Não verificar certificado: Selecione esta opção apenas quando tiver um bom motivo para não utilizar a validação do certificado, como por exemplo, quando houver um problema temporário com um certificado.
4. Selecione **Guardar**.

   Todas as mensagens semanais, acionadas pelo utilizador e acionadas por eventos são enviadas utilizando o protocolo selecionado.

**Informações relacionadas**

"Configurando as configurações de proxy Admin"

## Habilitando o AutoSupport sob demanda

O AutoSupport On Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente. Quando você ativa o AutoSupport sob demanda, o suporte técnico pode solicitar que as mensagens do AutoSupport sejam enviadas sem a necessidade de sua intervenção.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.
- Você deve ter ativado mensagens AutoSupport semanais.
- Tem de ter definido o protocolo de transporte como HTTPS.

**Sobre esta tarefa**

Quando você ativa esse recurso, o suporte técnico pode solicitar que seu sistema StorageGRID envie mensagens do AutoSupport automaticamente. O suporte técnico também pode definir o intervalo de tempo de polling para consultas AutoSupport On Demand.

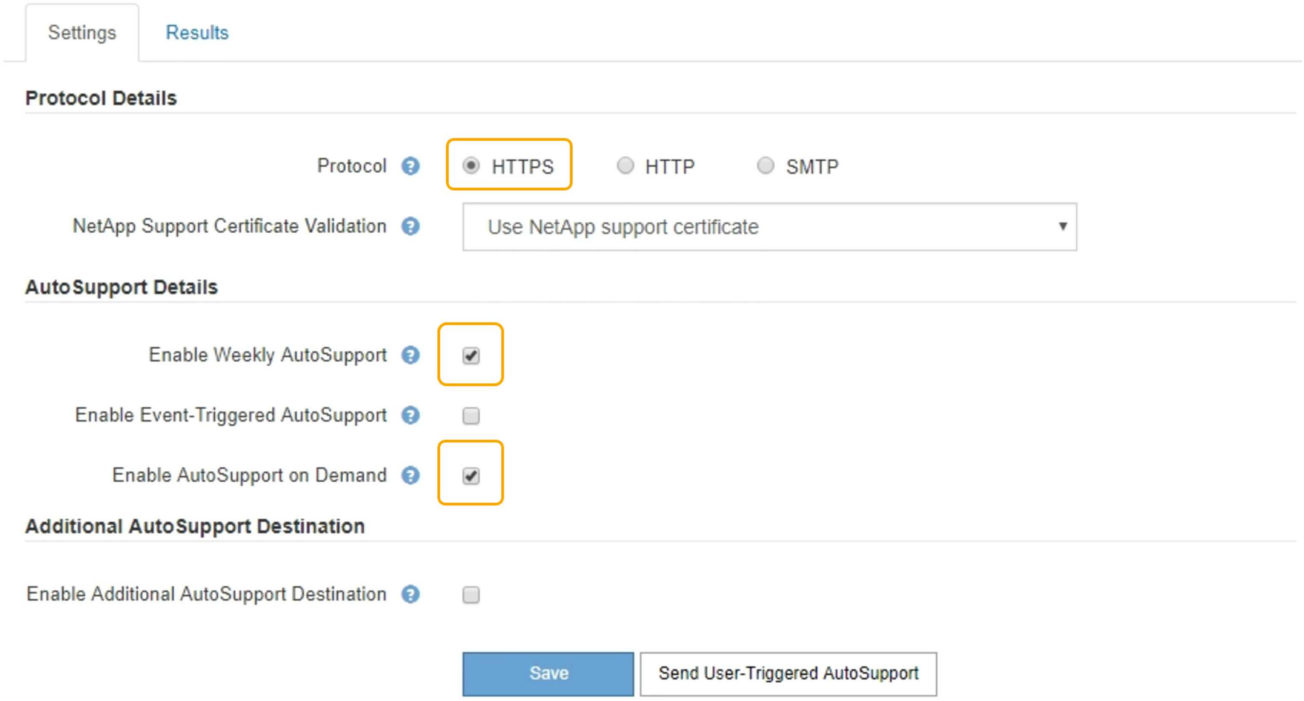
O suporte técnico não pode ativar ou desativar o AutoSupport a pedido.

**Passos**

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

   A página AutoSupport é exibida com a guia **Configurações** selecionada.

2. Selecione o botão de opção HTTPS na secção **Protocol Details** (Detalhes do protocolo) da página.




3. Marque a caixa de seleção **Enable Weekly** (Ativar AutoSupport semanal*).
4. Marque a caixa de seleção **Enable on Demand** (Ativar AutoSupport on Demand*).
5. Selecione **Guardar**.

   O AutoSupport On Demand está ativado e o suporte técnico pode enviar solicitações AutoSupport On Demand para o StorageGRID.

## Desativar mensagens AutoSupport semanais

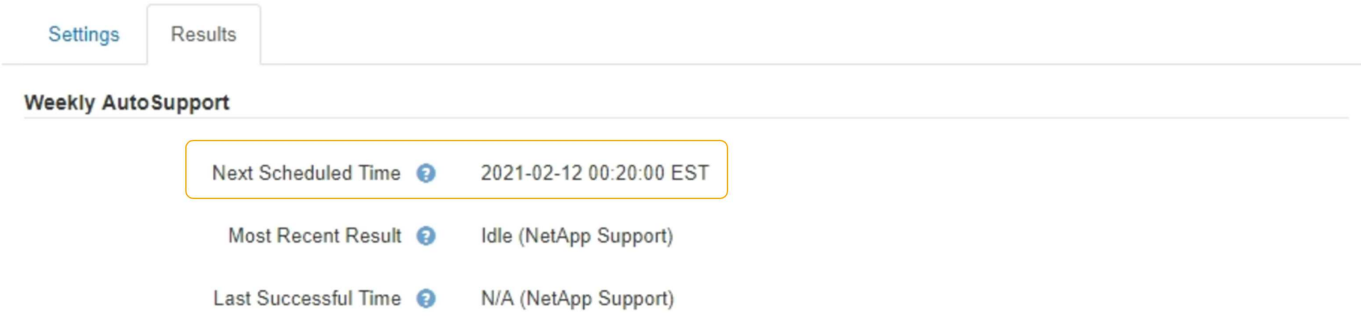
Por padrão, o sistema StorageGRID está configurado para enviar uma mensagem AutoSupport para o suporte da NetApp uma vez por semana.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

**Sobre esta tarefa**

Para determinar quando a mensagem AutoSupport semanal é enviada, consulte **hora programada seguinte** em **AutoSupport semanal** na página **AutoSupport** > **resultados**.



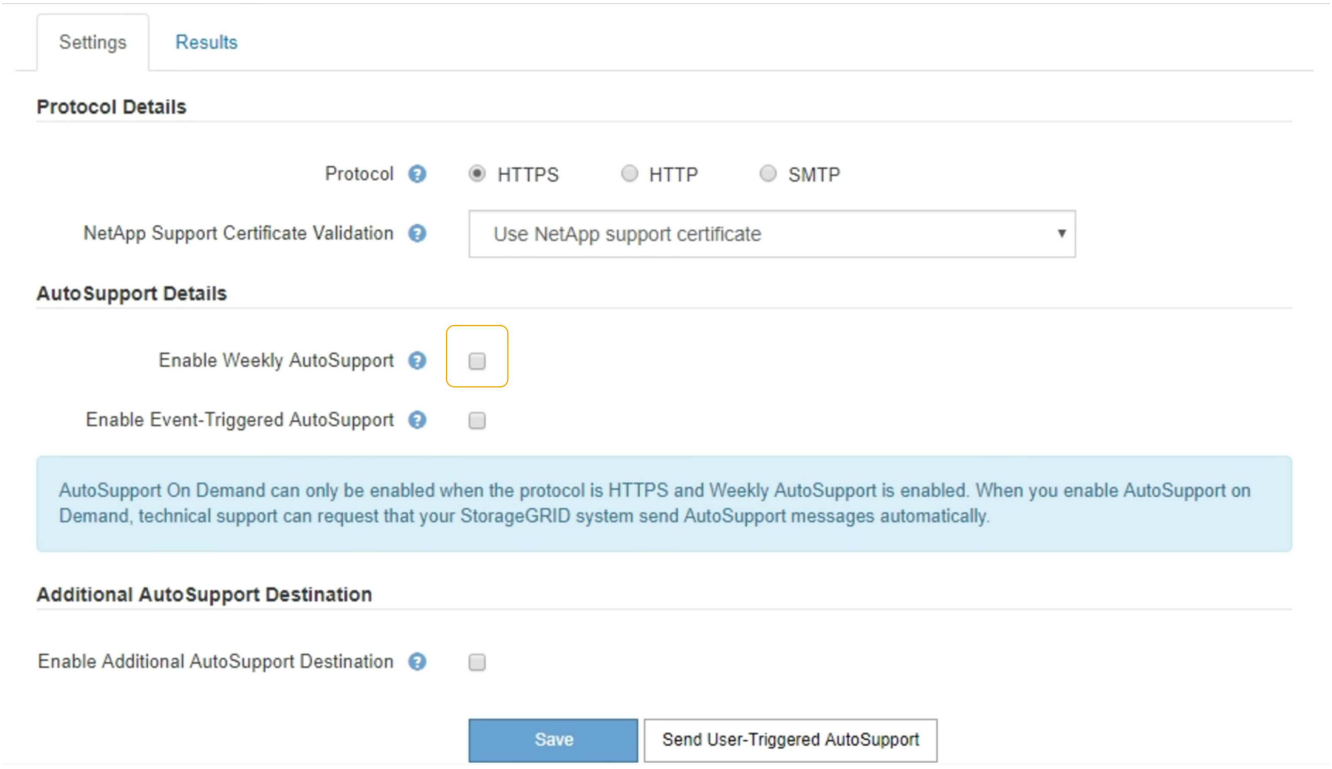

Pode desativar o envio automático de uma mensagem AutoSupport a qualquer momento.

**Passos**

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

   A página AutoSupport é exibida com a guia **Configurações** selecionada.

2. Desmarque a caixa de seleção **Ativar AutoSupport semanal**.




3. Selecione **Guardar**.

## Desativando mensagens AutoSupport acionadas por eventos

Por padrão, o sistema StorageGRID é configurado para enviar uma mensagem AutoSupport para o suporte da NetApp quando ocorre um alerta importante ou outro evento significativo do sistema.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

**Sobre esta tarefa**

Você pode desativar as mensagens AutoSupport acionadas por eventos a qualquer momento.

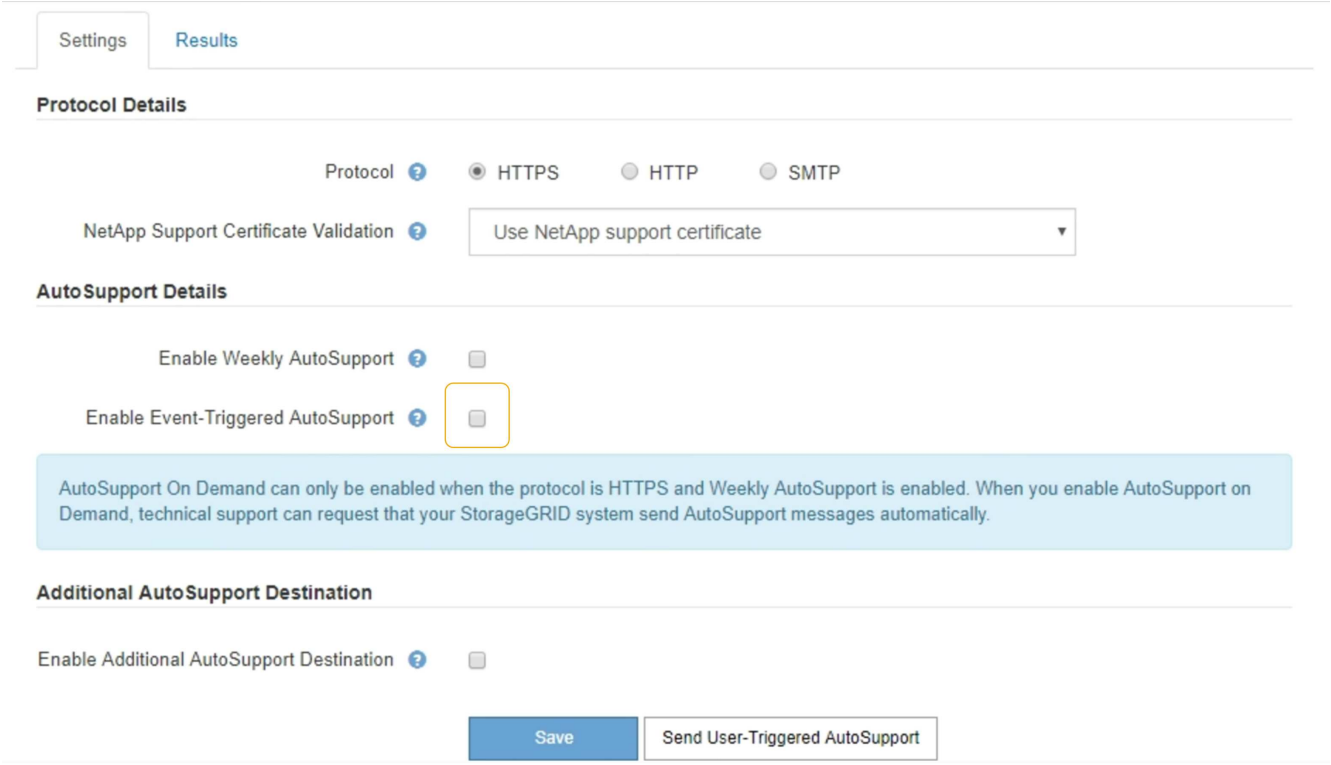
> As mensagens AutoSupport acionadas por eventos também são suprimidas quando você suprime as notificações por e-mail em todo o sistema. (Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**. Em seguida, selecione **notificação suprimir tudo**.)

**Passos**

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

   A página AutoSupport é exibida com a guia **Configurações** selecionada.

2. Desmarque a caixa de seleção **Enable Event-Triggered** (Ativar AutoSupport acionado por evento*).




3. Selecione **Guardar**.

## Acionando manualmente uma mensagem AutoSupport

Para ajudar o suporte técnico na solução de problemas com o sistema StorageGRID, você pode acionar manualmente uma mensagem AutoSupport a ser enviada.

**O que você vai precisar**

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

- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

**Passos**

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

   A página AutoSupport é exibida com a guia **Configurações** selecionada.

2. Selecione **Enviar AutoSupport acionado pelo usuário**.

   O StorageGRID tenta enviar uma mensagem do AutoSupport para o suporte técnico. Se a tentativa for bem-sucedida, os valores **resultado mais recente** e **último tempo bem-sucedido** na guia **resultados** serão atualizados. Se houver um problema, o valor **resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar a mensagem AutoSupport novamente.

   > Depois de enviar uma mensagem AutoSupport acionada pelo usuário, atualize a página AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

## Adicionar um destino AutoSupport adicional

Quando você ativa o AutoSupport, as mensagens de estado e de saúde são enviadas para o suporte do NetApp. Você pode especificar um destino adicional para todas as mensagens do AutoSupport.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de Acesso root ou outra Configuração de Grade.

**Sobre esta tarefa**

Para verificar ou alterar o protocolo usado para enviar mensagens AutoSupport, consulte as instruções para especificar um protocolo AutoSupport.

> Não é possível usar o protocolo SMTP para enviar mensagens AutoSupport para um destino adicional.

"Especificando o protocolo para mensagens AutoSupport"

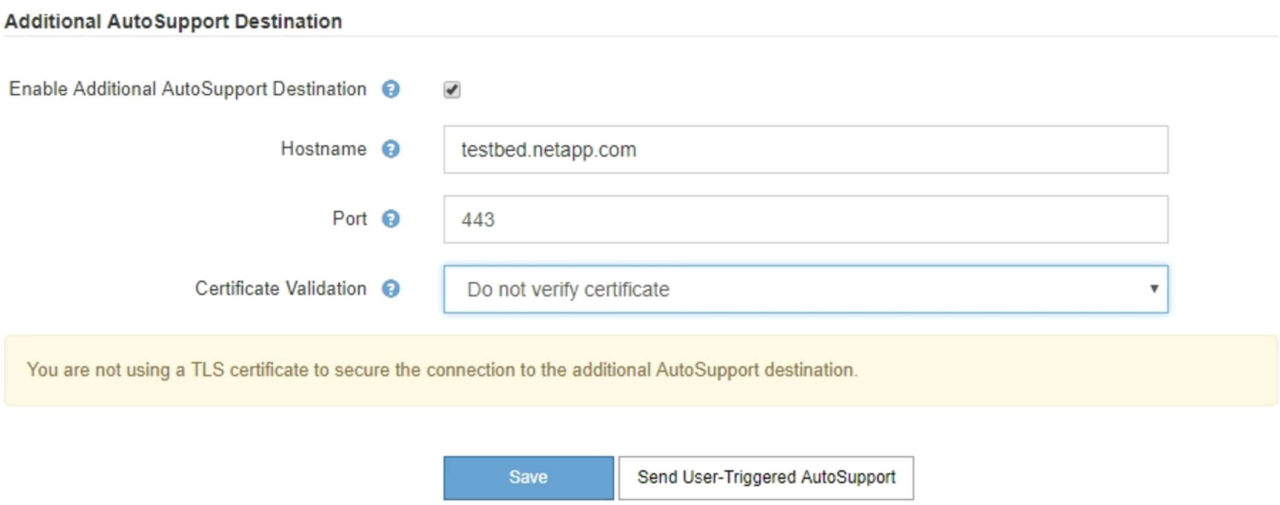
**Passos**

1. Selecione **suporte** > **Ferramentas** > **AutoSupport**.

   A página AutoSupport é exibida com a guia **Configurações** selecionada.

2. Selecione **Ativar destino AutoSupport adicional**.

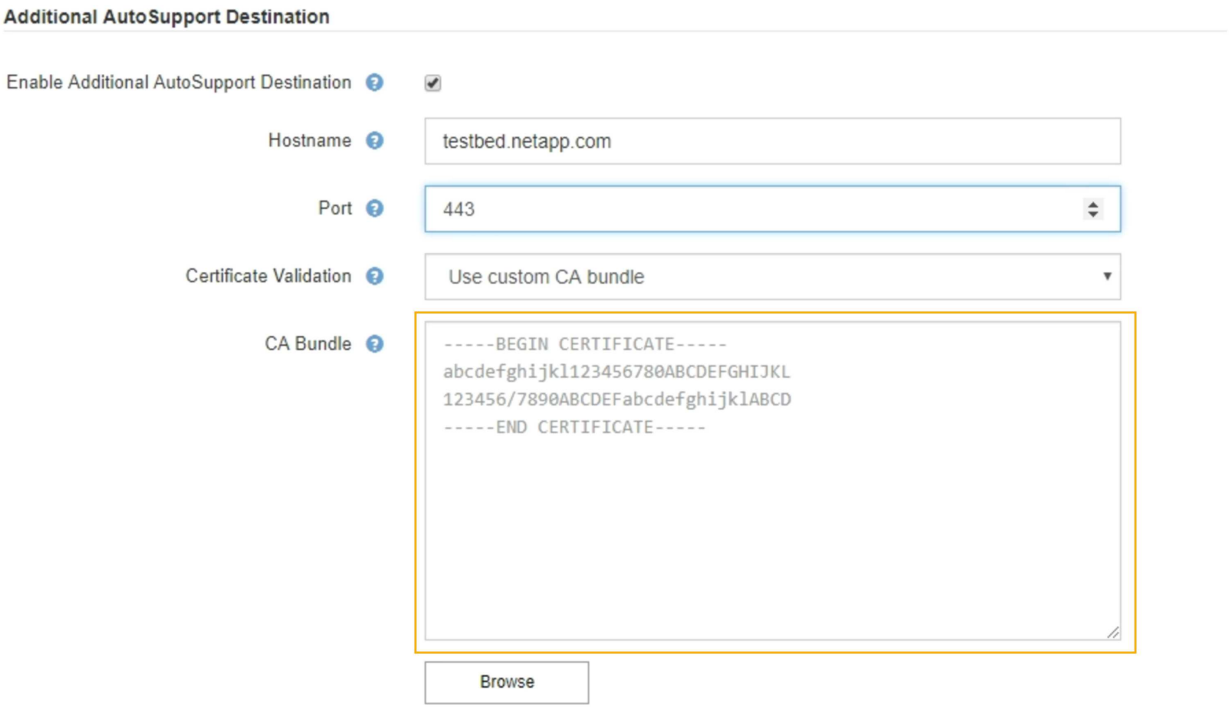
   São apresentados os campos de destino AutoSupport adicional.




3. Introduza o nome de anfitrião do servidor ou o endereço IP de um servidor de destino AutoSupport adicional.

   Pode introduzir apenas um destino adicional.

4. Introduza a porta utilizada para ligar a um servidor de destino AutoSupport adicional (a predefinição é a porta 80 para HTTP ou a porta 443 para HTTPS).
5. Para enviar suas mensagens do AutoSupport com validação de certificado, selecione **Use custom CA bundle** no menu suspenso **Validação de certificado**. Em seguida, execute um dos seguintes procedimentos:
   - Use uma ferramenta de edição para copiar e colar todo o conteúdo de cada um dos arquivos de certificado CA codificados em PEM no campo **CA bundle**, concatenado em ordem de cadeia de certificados. Você deve incluir `----BEGIN CERTIFICATE----` e `----END CERTIFICATE----` em sua seleção.



- Selecione **Procurar**, navegue até o arquivo que contém os certificados e selecione **abrir** para carregar o arquivo. A validação do certificado garante que a transmissão de mensagens AutoSupport é segura.

6. Para enviar suas mensagens do AutoSupport sem validação de certificado, selecione **não verificar certificado** na lista suspensa **Validação de certificado**.

   Selecione esta opção apenas quando tiver um bom motivo para não utilizar a validação do certificado, como por exemplo, quando houver um problema temporário com um certificado.

   Uma mensagem de aviso é exibida: "Você não está usando um certificado TLS para proteger a conexão com o destino AutoSupport adicional."

7. Selecione **Guardar**.

   Todas as futuras mensagens AutoSupport semanais, acionadas por eventos e acionadas pelo usuário serão enviadas para o destino adicional.

## Envio de mensagens do e-Series AutoSupport através do StorageGRID

Você pode enviar mensagens do e-Series SANtricity System Manager AutoSupport para o suporte técnico por meio de um nó de administração do StorageGRID, em vez da porta de gerenciamento do dispositivo de storage.

**O que você vai precisar**

- Você está conetado ao Gerenciador de Grade usando um navegador da Web compatível.
- Você tem a permissão Administrador do dispositivo de armazenamento ou a permissão de acesso root.

> Você deve ter o firmware SANtricity 8,70 ou superior para acessar o Gerenciador de sistema do SANtricity usando o Gerenciador de Grade.

**Sobre esta tarefa**

As mensagens AutoSupport do e-Series contêm detalhes do hardware de armazenamento e são mais específicas do que outras mensagens AutoSupport enviadas pelo sistema StorageGRID.

Configure um endereço de servidor proxy especial no Gerenciador de sistema do SANtricity para fazer com que as mensagens do AutoSupport sejam transmitidas através de um nó de administração do StorageGRID sem o uso da porta de gerenciamento do dispositivo. As mensagens AutoSupport transmitidas desta forma respeitam as definições de proxy do Remetente e administrador preferenciais que podem ter sido configuradas no Gestor de grelha.

Se você quiser configurar o servidor proxy Admin no Gerenciador de Grade, consulte as instruções para configurar as configurações do proxy Admin.

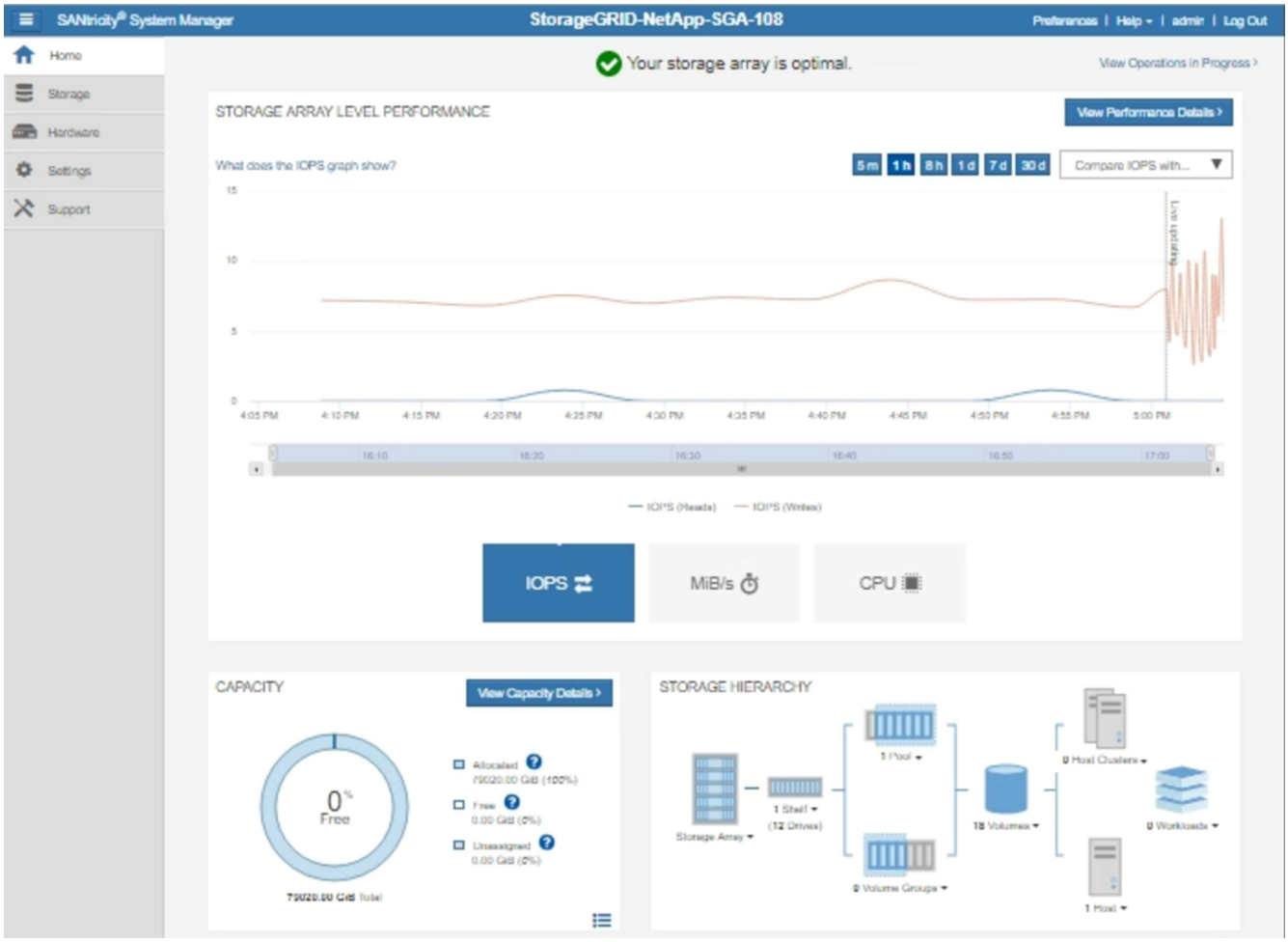
"Configurando as configurações de proxy Admin"

> Este procedimento destina-se apenas à configuração de um servidor proxy StorageGRID para mensagens AutoSupport e-Series. Para obter detalhes adicionais sobre as informações de configuração do e-Series AutoSupport, consulte o centro de documentação do e-Series.
>
> "Centro de Documentação de sistemas NetApp e-Series"

**Passos**

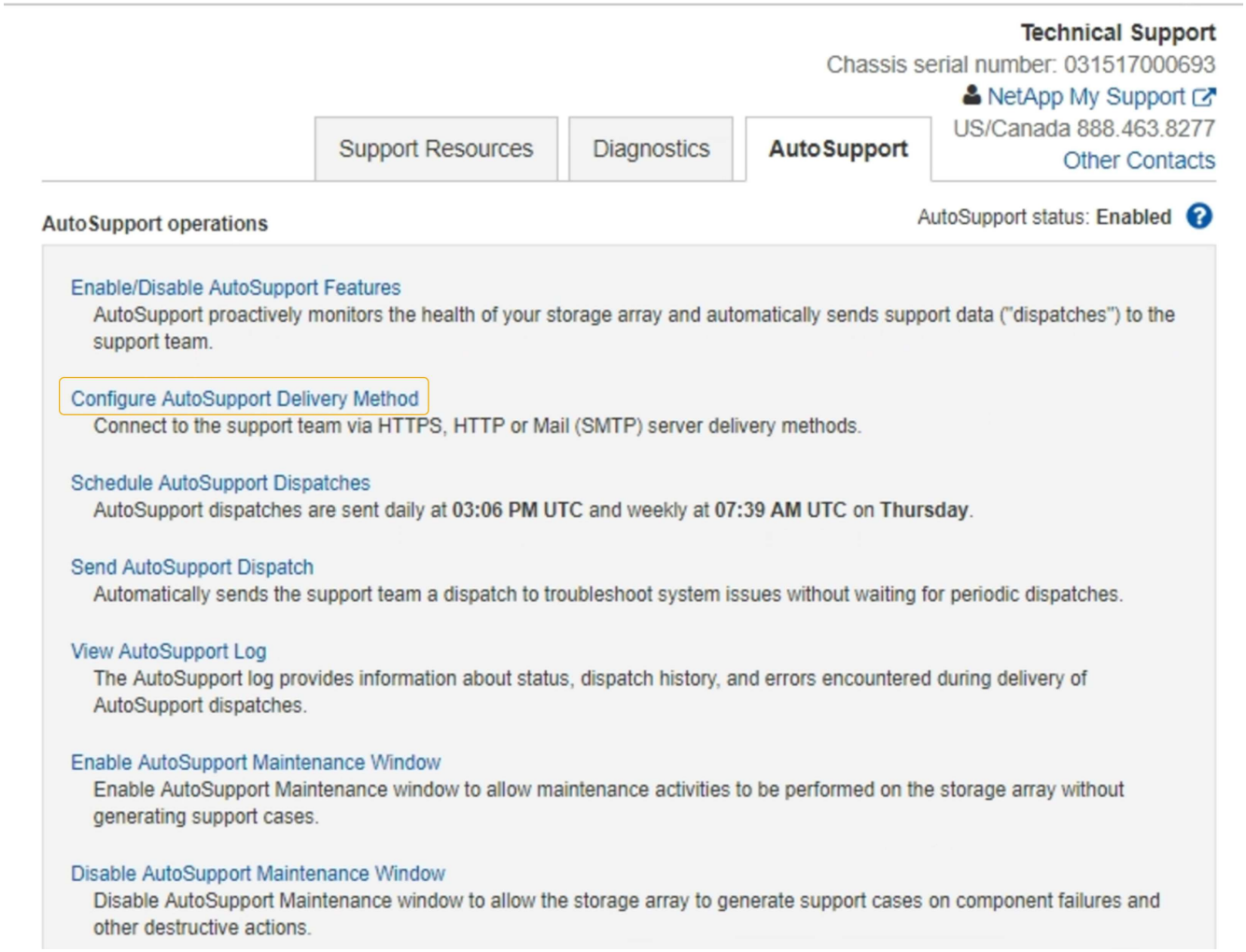
1. No Gerenciador de Grade, selecione **nós**.
2. Na lista de nós à esquerda, selecione o nó do dispositivo de storage que deseja configurar.
3. Selecione **Gerenciador do sistema SANtricity**.

   É apresentada a página inicial do Gestor do sistema SANtricity.



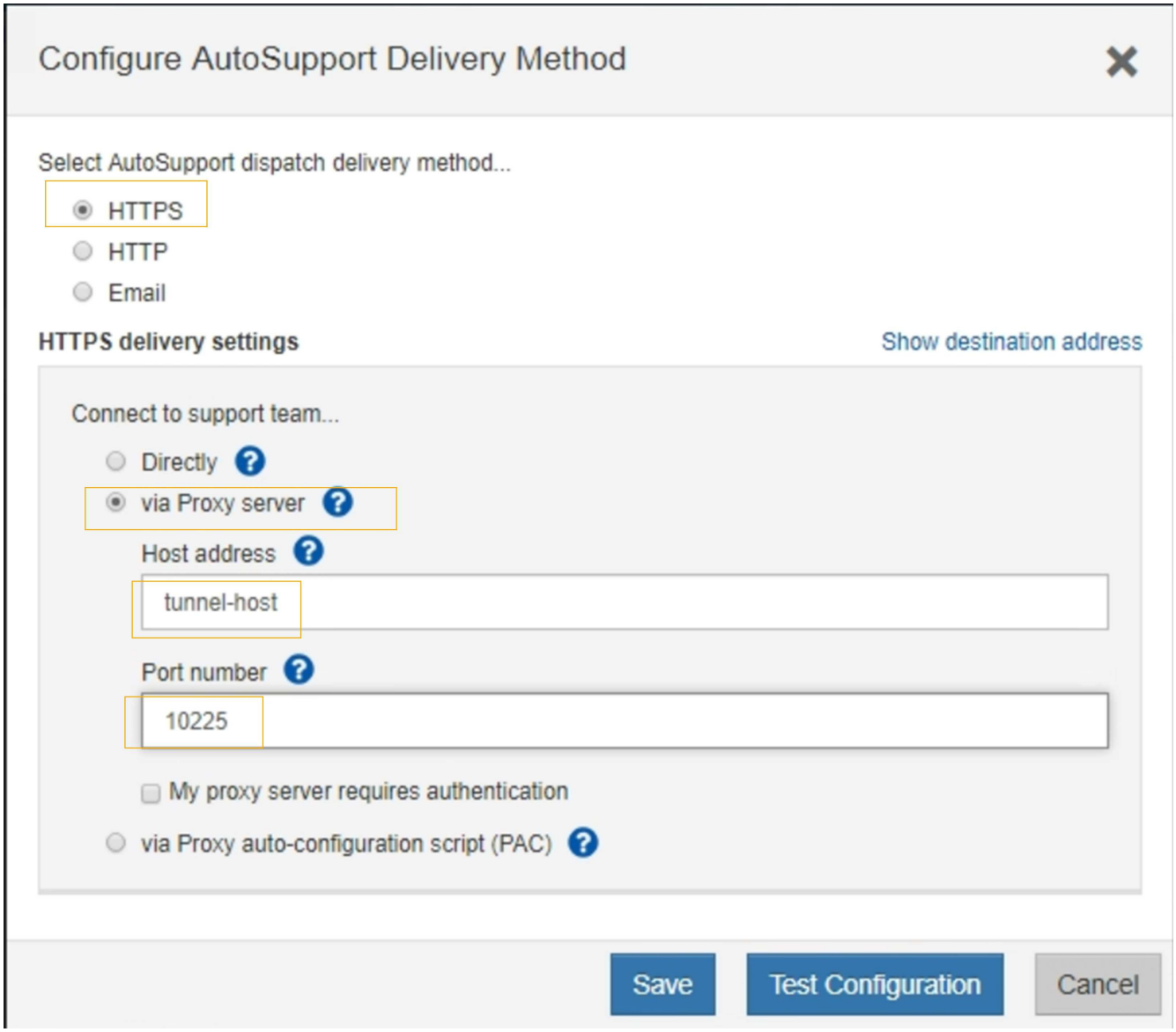

4. Selecione **suporte** > **Centro de suporte** > **AutoSupport**.

   É apresentada a página operations (operações de AutoSupport).




5. Selecione **Configurar método de entrega AutoSupport**.

   A página Configurar método de entrega AutoSupport é exibida.




6. Selecione **HTTPS** para o método de entrega.

   O certificado que ativa o protocolo HTTPS está pré-instalado.

7. Selecione **via servidor Proxy**.
8. Introduza `tunnel-host` o **Endereço anfitrião**.

   `tunnel-host` É o endereço especial para usar um nó de administrador para enviar mensagens AutoSupport da série e.

9. Introduza `10225` o **número da porta**.

   `10225` É o número da porta no servidor proxy StorageGRID que recebe mensagens AutoSupport do controlador e-Series no dispositivo.

10. Selecione **Configuração de teste** para testar o roteamento e a configuração do servidor proxy AutoSupport.

    Se estiver correto, uma mensagem em um banner verde será exibida: ""sua configuração do AutoSupport

foi verificada."

Se o teste falhar, uma mensagem de erro será exibida em um banner vermelho. Verifique as configurações de DNS e a rede do StorageGRID, verifique se o nó de administrador do remetente preferido pode se conetar ao site de suporte do NetApp e tente o teste novamente.

11. Selecione **Guardar**.

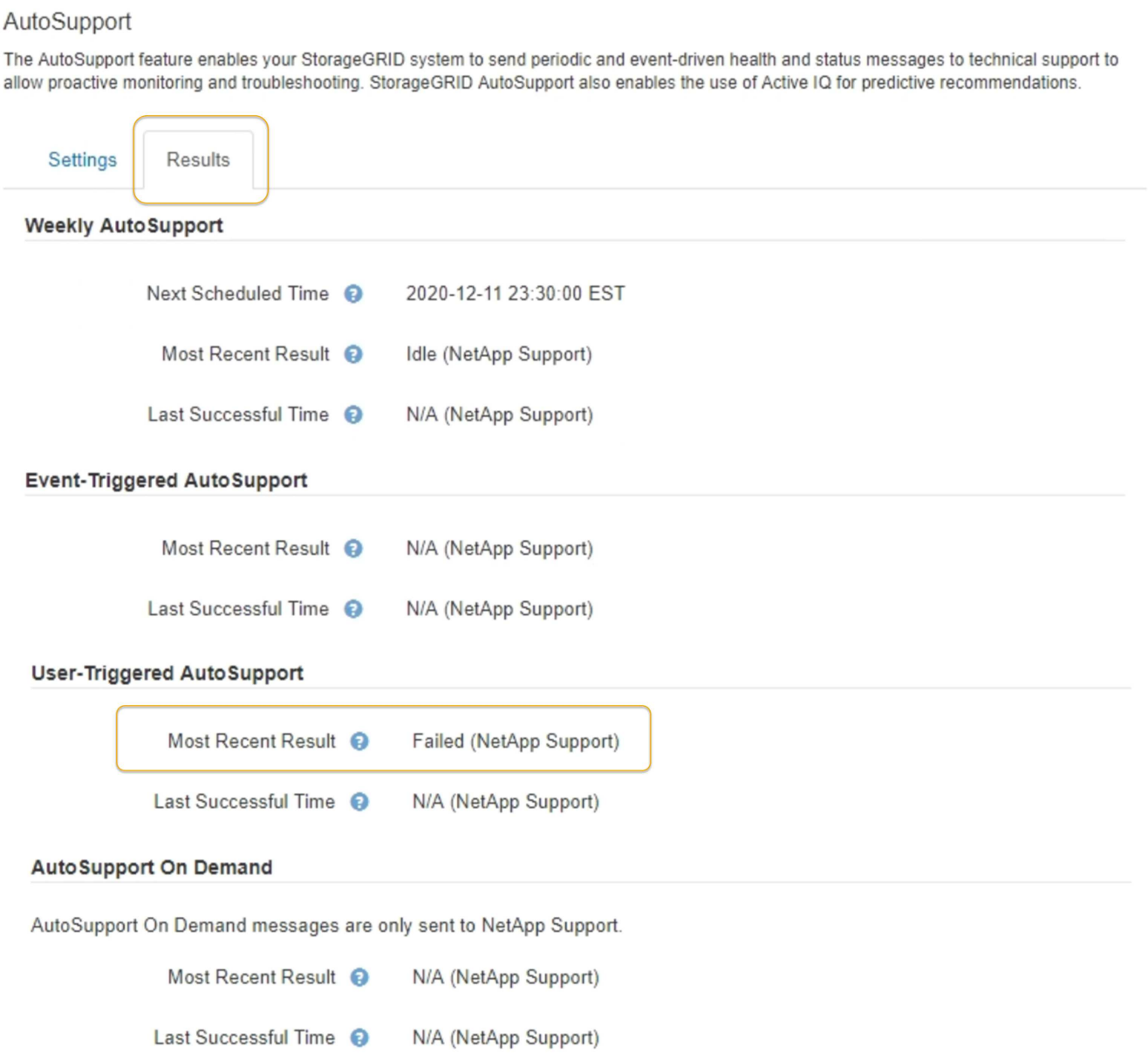
    A configuração é salva e uma mensagem de confirmação aparece: ""o método de entrega AutoSupport foi configurado."

## Solução de problemas de mensagens do AutoSupport

Se uma tentativa de enviar uma mensagem AutoSupport falhar, o sistema StorageGRID executa ações diferentes dependendo do tipo de mensagem AutoSupport. Você pode verificar o status das mensagens do AutoSupport selecionando **suporte** > **Ferramentas** > **AutoSupport** > **resultados**.

> As mensagens AutoSupport acionadas por evento são suprimidas quando você suprime as notificações de e-mail em todo o sistema. (Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**. Em seguida, selecione **notificação suprimir tudo**.)

Quando a mensagem AutoSupport não é enviada, "'Falha'" aparece na guia **resultados** da página **AutoSupport**.




### Falha semanal da mensagem AutoSupport

Se uma mensagem AutoSupport semanal não for enviada, o sistema StorageGRID executa as seguintes ações:

1. Atualiza o atributo de resultado mais recente para tentar novamente.
2. Tenta reenviar a mensagem AutoSupport 15 vezes a cada quatro minutos durante uma hora.
3. Após uma hora de falhas de envio, atualiza o atributo de resultado mais recente para Falha.
4. Tenta enviar uma mensagem AutoSupport novamente na próxima hora programada.
5. Mantém a programação regular do AutoSupport se a mensagem falhar porque o serviço NMS não está disponível e se uma mensagem for enviada antes de sete dias passar.
6. Quando o serviço NMS estiver disponível novamente, envia uma mensagem AutoSupport imediatamente se uma mensagem não tiver sido enviada por sete dias ou mais.

#### Falha de mensagem AutoSupport acionada pelo usuário ou por evento

Se uma mensagem AutoSupport acionada pelo usuário ou por um evento não for enviada, o sistema StorageGRID executará as seguintes ações:

1. Exibe uma mensagem de erro se o erro for conhecido. Por exemplo, se um usuário selecionar o protocolo SMTP sem fornecer as configurações corretas de e-mail, o seguinte erro é exibido: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Não tenta enviar a mensagem novamente.
3. Regista o erro no `nms.log`.

Se ocorrer uma falha e o SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o servidor de e-mail está em execução (**suporte** > **Alarmes (legado)** > **> Configuração de e-mail legado**). A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Saiba como configurar as definições do servidor de correio eletrónico no "monitorar solucionar problemas de instruções".

#### Correção de uma falha de mensagem AutoSupport

Se ocorrer uma falha e o SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o servidor de e-mail está em execução. A seguinte mensagem de erro pode aparecer na página AutoSupport: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

#### Informações relacionadas

"Monitorizar Resolução de problemas"

# Gerenciando nós de storage

Os nós de storage fornecem capacidade e serviços de storage em disco. O gerenciamento de nós de storage envolve o monitoramento da quantidade de espaço utilizável em cada nó, usando configurações de marca d'água e aplicando configurações de nó de storage.

- "O que é um nó de storage"
- "Gerenciando Opções de armazenamento"
- "Gerenciamento do storage de metadados de objetos"
- "Configuração de configurações globais para objetos armazenados"
- "Configurações do nó de storage"
- "Gerenciamento de nós de storage completos"

## O que é um nó de storage

Os nós de storage gerenciam e armazenam dados e metadados de objetos. Cada sistema StorageGRID precisa ter pelo menos três nós de storage. Se você tiver vários

locais, cada local no sistema StorageGRID também precisará ter três nós de storage.

Um nó de armazenamento inclui os serviços e processos necessários para armazenar, mover, verificar e recuperar dados de objetos e metadados no disco. Você pode exibir informações detalhadas sobre os nós de storage na página **nós**.

### O que é o serviço ADC

O serviço controlador de domínio administrativo (ADC) autentica os nós de grade e suas conexões entre si. O serviço ADC é hospedado em cada um dos três primeiros nós de storage em um local.

O serviço ADC mantém informações de topologia, incluindo a localização e disponibilidade dos serviços. Quando um nó de grade requer informações de outro nó de grade ou uma ação a ser executada por outro nó de grade, ele entra em Contato com um serviço ADC para encontrar o melhor nó de grade para processar sua solicitação. Além disso, o serviço ADC retém uma cópia dos pacotes de configuração da implantação do StorageGRID, permitindo que qualquer nó de grade recupere informações de configuração atuais.você pode visualizar informações ADC para um nó de armazenamento na página de topologia de grade (**suporte** > **topologia de grade**).

Para facilitar operações distribuídas e desembarcadas, cada serviço ADC sincroniza certificados, pacotes de configuração e informações sobre serviços e topologia com os outros serviços ADC no sistema StorageGRID.

Em geral, todos os nós de grade mantêm uma conexão com pelo menos um serviço ADC. Isso garante que os nós de grade estejam sempre acessando as informações mais recentes. Quando os nós de grade se conetam, eles armazenam em cache certificados de outros nós de grade, permitindo que os sistemas continuem funcionando com nós de grade conhecidos, mesmo quando um serviço ADC não está disponível. Novos nós de grade só podem estabelecer conexões usando um serviço ADC.

A conexão de cada nó de grade permite que o serviço ADC colete informações de topologia. Essas informações de nó de grade incluem a carga da CPU, o espaço disponível em disco (se ele tiver armazenamento), os serviços suportados e o ID do site do nó de grade. Outros serviços pedem ao serviço ADC informações de topologia por meio de consultas de topologia. O serviço ADC responde a cada consulta com as informações mais recentes recebidas do sistema StorageGRID.

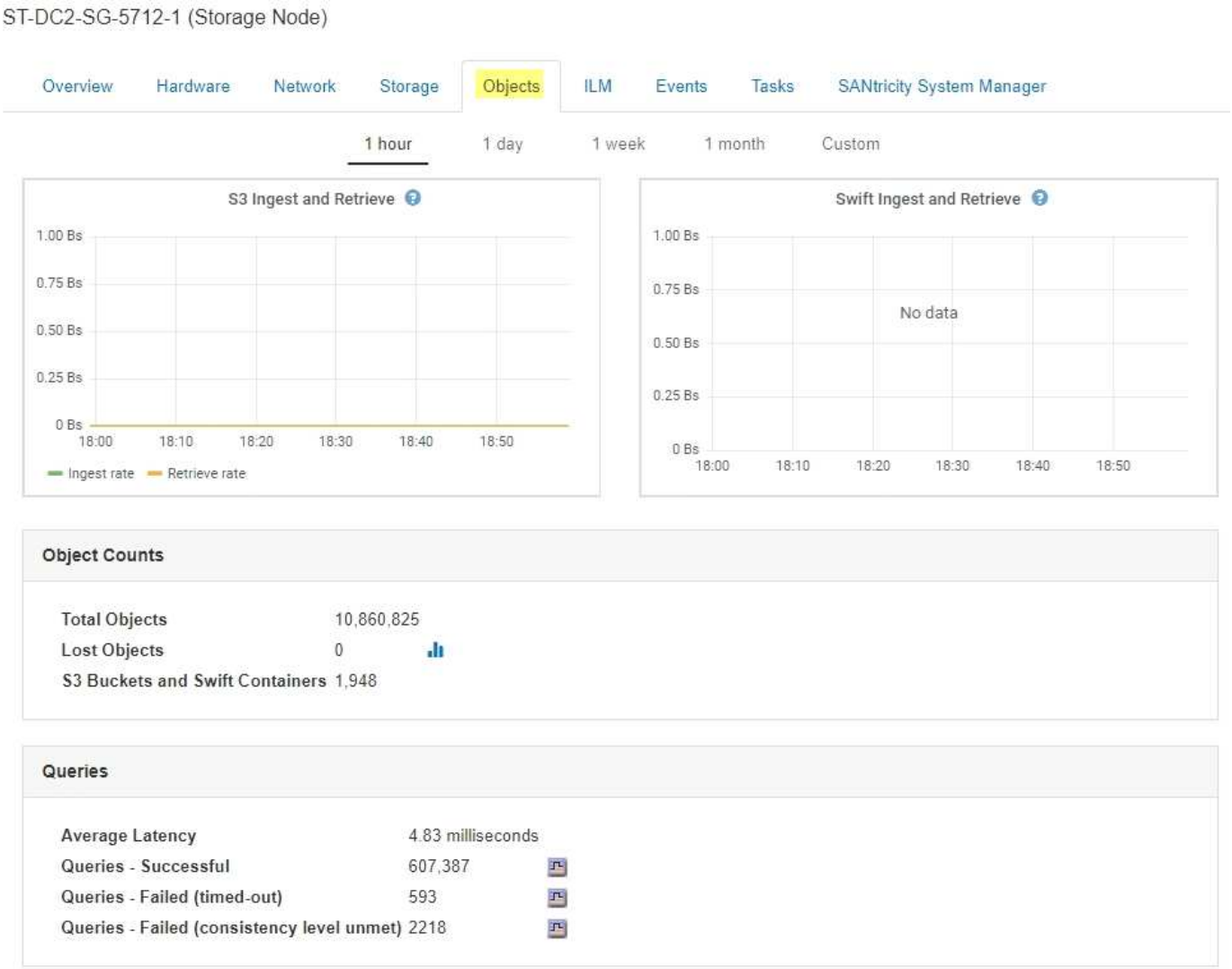
### O que é o serviço DDS

Hospedado por um nó de armazenamento, o serviço armazenamento de dados distribuído (DDS) faz interface com o banco de dados Cassandra para executar tarefas em segundo plano nos metadados de objetos armazenados no sistema StorageGRID.

#### Contagens de objetos

O serviço DDS rastreia o número total de objetos ingeridos no sistema StorageGRID, bem como o número total de objetos ingeridos através de cada uma das interfaces suportadas do sistema (S3 ou Swift).

Você pode ver a contagem total de objetos na página nós > guia objetos para qualquer nó de storage.




**Consultas**

Você pode identificar o tempo médio que leva para executar uma consulta contra o armazenamento de metadados através do serviço DDS específico, o número total de consultas bem-sucedidas e o número total de consultas que falharam devido a um problema de tempo limite.

Você pode querer revisar as informações de consulta para monitorar a integridade do armazenamento de metadados, Cassandra, que afeta o desempenho de ingestão e recuperação do sistema. Por exemplo, se a latência de uma consulta média for lenta e o número de consultas com falha devido a tempos limite for alto, o armazenamento de metadados pode estar encontrando uma carga maior ou executando outra operação.

Você também pode exibir o número total de consultas que falharam devido a falhas de consistência. Falhas no nível de consistência resultam de um número insuficiente de armazenamentos de metadados disponíveis no momento em que uma consulta é realizada através do serviço DDS específico.

Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade. "A executar o diagnóstico"Consulte .

**Garantias de consistência e controles**

O StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer operação GET após uma operação PUT concluída com êxito poderá ler os dados recém-gravados. As

substituições de objetos existentes, atualizações de metadados e exclusões permanecem, eventualmente, consistentes.

### O que é o serviço LDR

Hospedado por cada nó de armazenamento, o serviço de roteador de distribuição local (LDR) lida com o transporte de conteúdo para o sistema StorageGRID. O transporte de conteúdo abrange muitas tarefas, incluindo armazenamento de dados, roteamento e manuseio de solicitações. O serviço LDR faz a maior parte do trabalho árduo do sistema StorageGRID, manipulando cargas de transferência de dados e funções de tráfego de dados.

O serviço LDR lida com as seguintes tarefas:

- Consultas
- Atividade de gerenciamento do ciclo de vida das informações (ILM)
- Exclusão de objeto
- Storage de dados de objetos
- Transferências de dados de objeto de outro serviço LDR (Storage Node)
- Gerenciamento de storage de dados
- Interfaces de protocolo (S3 e Swift)

O serviço LDR também gerencia o mapeamento de objetos S3 e Swift para os "manipuladores de conteúdo" exclusivos que o sistema StorageGRID atribui a cada objeto ingerido.

#### Consultas

As consultas LDR incluem consultas para localização de objetos durante operações de recuperação e arquivamento. Você pode identificar o tempo médio que leva para executar uma consulta, o número total de consultas bem-sucedidas e o número total de consultas que falharam devido a um problema de tempo limite.

Você pode revisar as informações de consulta para monitorar a integridade do armazenamento de metadados, o que afeta o desempenho de ingestão e recuperação do sistema. Por exemplo, se a latência de uma consulta média for lenta e o número de consultas com falha devido a tempos limite for alto, o armazenamento de metadados pode estar encontrando uma carga maior ou executando outra operação.

Você também pode exibir o número total de consultas que falharam devido a falhas de consistência. Falhas no nível de consistência resultam de um número insuficiente de armazenamentos de metadados disponíveis no momento em que uma consulta é executada através do serviço LDR específico.

Você pode usar a página Diagnósticos para obter informações adicionais sobre o estado atual da grade. "A executar o diagnóstico"Consulte .

#### Atividade ILM

As métricas de gerenciamento do ciclo de vida das informações (ILM) permitem monitorar a taxa na qual os objetos são avaliados para a implementação do ILM. Você pode exibir essas métricas no Dashboard ou na página nós > guia ILM para cada nó de storage.

#### Armazenamentos de objetos

O armazenamento de dados subjacente de um serviço LDR é dividido em um número fixo de armazenamentos de objetos (também conhecidos como volumes de armazenamento). Cada armazenamento

de objetos é um ponto de montagem separado.

Você pode ver os armazenamentos de objetos para um nó de storage na página nós > guia armazenamento.

**Object Stores**

| ID | Size | Available | Replicated Data | EC Data | Object Data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 4.40 TB | 1.35 TB | 43.99 GB | 0 bytes | 1.00% | No Errors |
| 0001 | 1.97 TB | 1.57 TB | 44.76 GB | 351.14 GB | 20.09% | No Errors |
| 0002 | 1.97 TB | 1.46 TB | 43.29 GB | 465.20 GB | 25.81% | No Errors |
| 0003 | 1.97 TB | 1.70 TB | 43.51 GB | 223.98 GB | 13.58% | No Errors |
| 0004 | 1.97 TB | 1.92 TB | 44.03 GB | 0 bytes | 2.23% | No Errors |
| 0005 | 1.97 TB | 1.46 TB | 43.67 GB | 463.36 GB | 25.73% | No Errors |
| 0006 | 1.97 TB | 1.92 TB | 43.10 GB | 1.61 GB | 2.27% | No Errors |
| 0007 | 1.97 TB | 1.35 TB | 46.05 GB | 575.24 GB | 31.53% | No Errors |
| 0008 | 1.97 TB | 1.81 TB | 46.00 GB | 112.84 GB | 8.06% | No Errors |
| 0009 | 1.97 TB | 1.57 TB | 43.91 GB | 352.72 GB | 20.13% | No Errors |
| 000A | 1.97 TB | 1.70 TB | 44.31 GB | 226.81 GB | 13.76% | No Errors |
| 000B | 1.97 TB | 1.92 TB | 43.17 GB | 780.07 MB | 2.23% | No Errors |
| 000C | 1.97 TB | 1.58 TB | 44.32 GB | 339.56 GB | 19.48% | No Errors |
| 000D | 1.97 TB | 1.82 TB | 44.47 GB | 107.34 GB | 7.70% | No Errors |
| 000E | 1.97 TB | 1.68 TB | 43.07 GB | 241.70 GB | 14.45% | No Errors |
| 000F | 2.03 TB | 1.50 TB | 44.57 GB | 475.47 GB | 25.67% | No Errors |

Os armazenamentos de objetos em um nó de armazenamento são identificados por um número hexadecimal de 0000 a 002F, que é conhecido como ID de volume. O espaço é reservado no primeiro armazenamento de objetos (volume 0) para metadados de objetos em um banco de dados Cassandra; qualquer espaço restante nesse volume é usado para dados de objeto. Todos os outros armazenamentos de objetos são usados exclusivamente para dados de objetos, o que inclui cópias replicadas e fragmentos codificados por apagamento.

Para garantir até mesmo o uso de espaço para cópias replicadas, os dados de objeto de um determinado objeto são armazenados em um armazenamento de objetos com base no espaço de storage disponível. Quando um ou mais objetos armazenam preenchimento até a capacidade, os armazenamentos de objetos restantes continuam armazenando objetos até que não haja mais espaço no nó de armazenamento.

#### Proteção de metadados

Metadados de objeto são informações relacionadas ou uma descrição de um objeto; por exemplo, tempo de modificação de objeto ou local de armazenamento. O StorageGRID armazena metadados de objetos em um banco de dados Cassandra, que faz interface com o serviço LDR.

Para garantir redundância e, portanto, proteção contra perda, três cópias dos metadados de objetos são mantidas em cada local. As cópias são distribuídas uniformemente por todos os nós de storage em cada local. Esta replicação não é configurável e executada automaticamente.

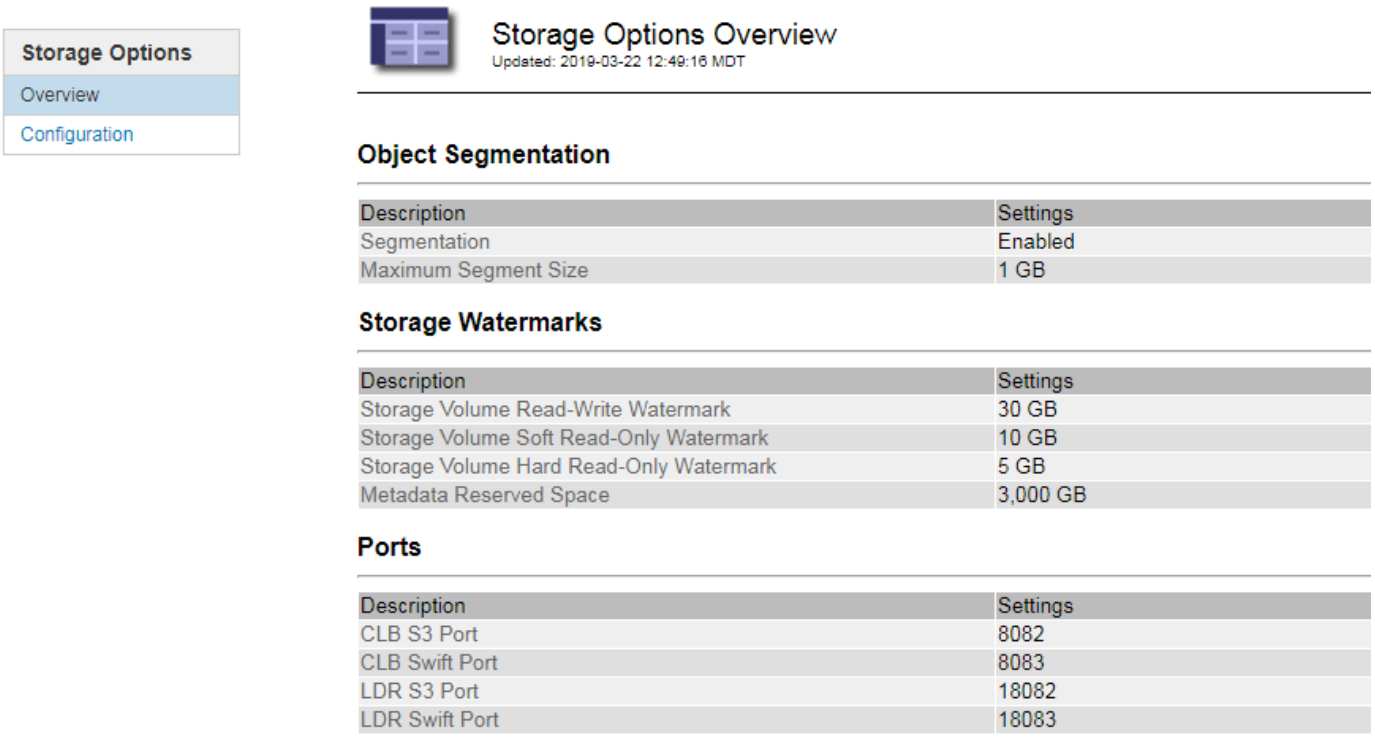
"Gerenciamento do storage de metadados de objetos"

## Gerenciando Opções de armazenamento

Você pode exibir e configurar Opções de armazenamento usando o menu Configuração

no Gerenciador de Grade. As opções de armazenamento incluem as definições de segmentação de objetos e os valores atuais para marcas d'água de armazenamento. Você também pode exibir as portas S3 e Swift usadas pelo serviço CLB obsoleto em nós de Gateway e pelo serviço LDR em nós de armazenamento.

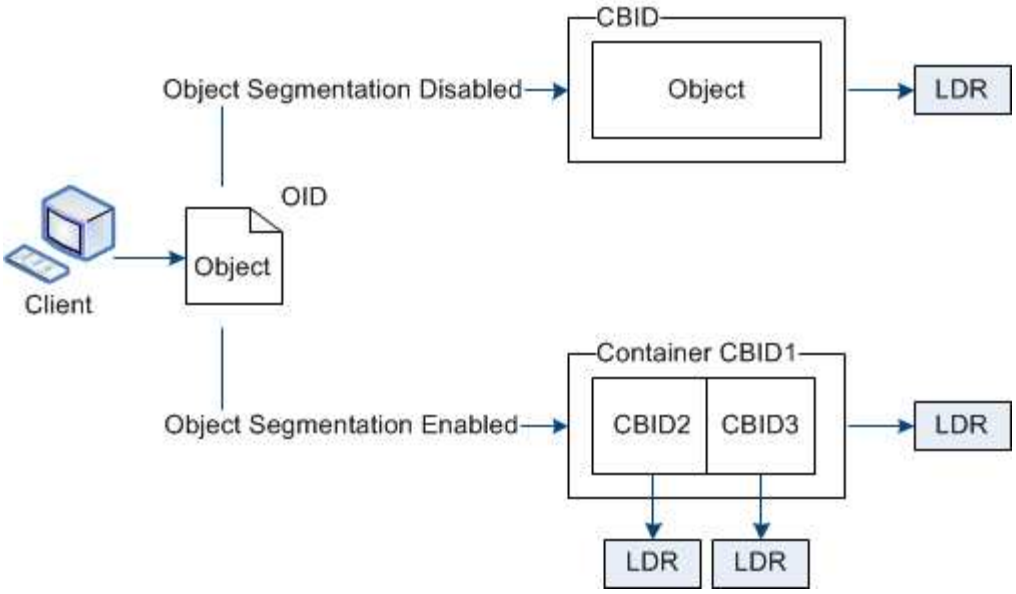
Para obter informações sobre atribuições de portas, "Resumo: Endereços IP e portas para conexões de clientes"consulte .




### Qual é a segmentação de objetos

A segmentação de objetos é o processo de dividir um objeto em uma coleção de objetos menores de tamanho fixo, a fim de otimizar o armazenamento e o uso de recursos para objetos grandes. O upload de várias partes do S3 também cria objetos segmentados, com um objeto representando cada parte.

Quando um objeto é ingerido no sistema StorageGRID, o serviço LDR divide o objeto em segmentos e cria um contentor de segmento que lista as informações do cabeçalho de todos os segmentos como conteúdo.




Se o seu sistema StorageGRID incluir um nó de arquivamento cujo tipo de destino é disposição em camadas na nuvem — Serviço de armazenamento simples e o sistema de armazenamento de arquivamento segmentado for o Amazon Web Services (AWS), o tamanho máximo do segmento deve ser menor ou igual a 4,5 GiB (4.831.838.208 bytes). Esse limite superior garante que a limitação de cinco GBs da AWS não seja excedida. As solicitações à AWS que excedem esse valor falham.

Ao recuperar um contentor de segmento, o serviço LDR monta o objeto original de seus segmentos e retorna o objeto ao cliente.

O contentor e os segmentos não são necessariamente armazenados no mesmo nó de armazenamento. O contentor e os segmentos podem ser armazenados em qualquer nó de armazenamento.

Cada segmento é Tratado pelo sistema StorageGRID de forma independente e contribui para a contagem de atributos, como objetos gerenciados e objetos armazenados. Por exemplo, se um objeto armazenado no sistema StorageGRID for dividido em dois segmentos, o valor de objetos gerenciados aumentará em três após a ingestão ser concluída, da seguinte forma:

segmento de container e segmento 1 e segmento 2 são três objetos armazenados

Você pode melhorar o desempenho ao lidar com objetos grandes, garantindo que:

- Cada Gateway e nó de armazenamento tem largura de banda de rede suficiente para a taxa de transferência necessária. Por exemplo, configure redes Grid e Client separadas em interfaces Ethernet de 10 Gbps.
- Nós de Gateway e storage suficientes são implantados para a taxa de transferência necessária.
- Cada nó de storage tem desempenho de e/S de disco suficiente para a taxa de transferência necessária.

**Quais são as marcas d'água do volume de armazenamento**

O StorageGRID usa marcas d'água de volume de storage para permitir que você monitore a quantidade de espaço utilizável disponível nos nós de storage. Se a quantidade de espaço disponível em um nó for menor do que uma configuração de marca d'água configurada, o alarme de Status do armazenamento (SSTS) será acionado para que você possa determinar se precisa adicionar nós de armazenamento.

Para ver as definições atuais das marcas de água do volume de armazenamento, selecione **Configuração** > **Opções de armazenamento** > **Visão geral**.

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

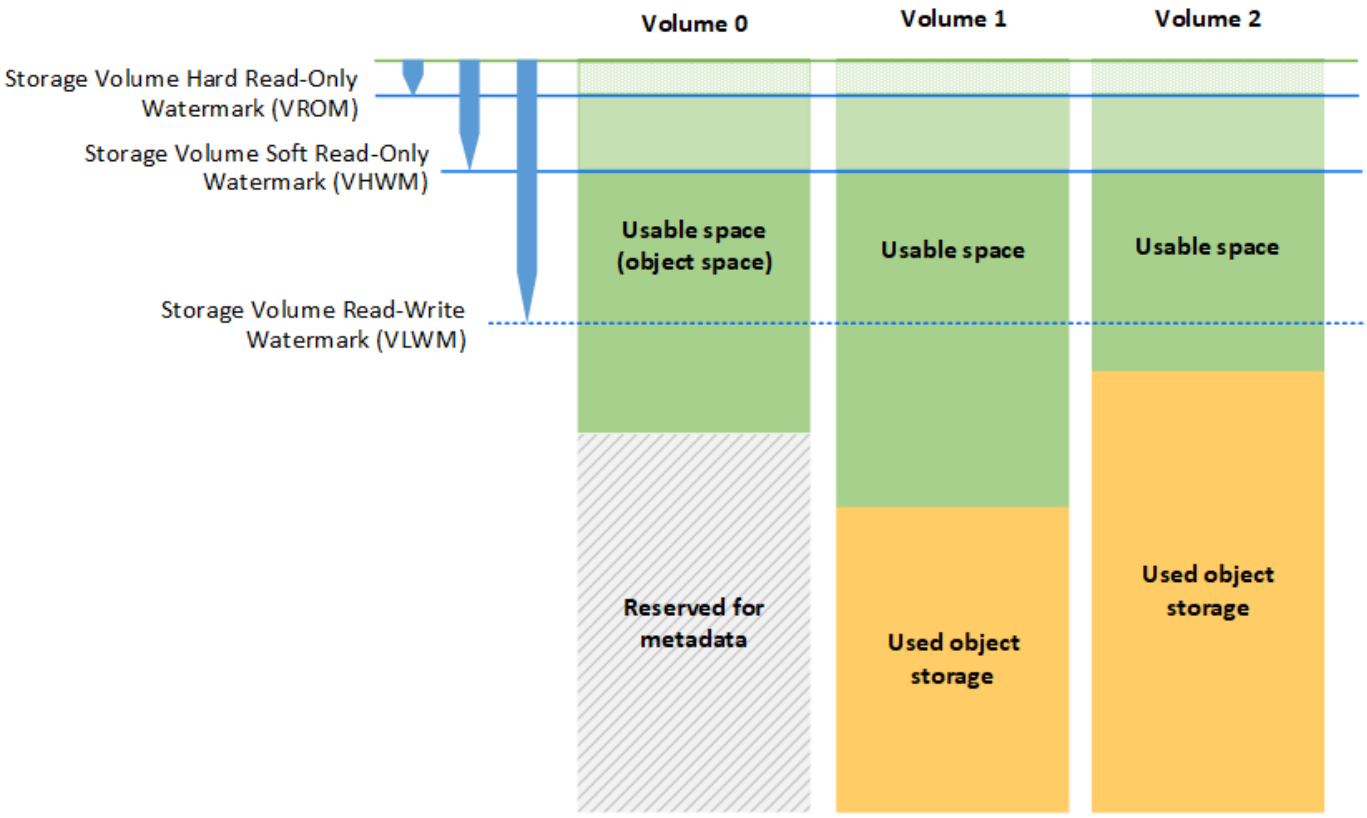
### Object Segmentation

| Description | Settings |
|---|---|
| Segmentation | Enabled |
| Maximum Segment Size | 1 GB |

### Storage Watermarks

| Description | Settings |
|---|---|
| Storage Volume Read-Write Watermark | 30 GB |
| Storage Volume Soft Read-Only Watermark | 10 GB |
| Storage Volume Hard Read-Only Watermark | 5 GB |
| Metadata Reserved Space | 3,000 GB |

A figura a seguir representa um nó de armazenamento que tem três volumes e mostra a posição relativa das três marcas d'água do volume de armazenamento. Em cada nó de storage, o StorageGRID reserva espaço no volume 0 para metadados de objetos. Qualquer espaço restante nesse volume é usado para dados de objetos. Todos os outros volumes são usados exclusivamente para dados de objetos, o que inclui cópias replicadas e fragmentos codificados por apagamento.




As marcas de água do volume de armazenamento são padrões de todo o sistema que indicam a quantidade mínima de espaço livre necessária em cada volume no nó de armazenamento para evitar que o StorageGRID altere o comportamento de leitura e gravação do nó ou acione um alarme. Observe que todos os volumes devem alcançar a marca d'água antes que o StorageGRID tome medidas. Se alguns volumes tiverem mais do que a quantidade mínima necessária de espaço livre, o alarme não será acionado e o comportamento de leitura e gravação do nó não será alterado.

#### Marca d'água suave apenas de leitura (VHWM)

A marca d'água somente leitura suave do volume de armazenamento é a primeira marca d'água a indicar que o espaço utilizável de um nó para dados de objeto está se tornando cheio. Essa marca d'água representa quanto espaço livre deve existir em cada volume em um nó de armazenamento para impedir que o nó entre no "modo somente leitura fácil". O modo somente leitura suave significa que o nó de armazenamento anuncia serviços somente leitura para o resto do sistema StorageGRID, mas atende a todas as solicitações de gravação pendentes.

Se a quantidade de espaço livre em cada volume for inferior à definição desta marca d'água, o alarme de Estado de armazenamento (SSTS) é acionado no nível de aviso e o nó de armazenamento passa para o modo apenas leitura suave.

Por exemplo, suponha que o volume de armazenamento Soft Read-Only Watermark esteja definido como 10 GB, que é o valor padrão. Se menos de 10 GB de espaço livre permanecer em cada volume no nó de armazenamento, o alarme SSTS é acionado no nível de aviso e o nó de armazenamento passa para o modo apenas leitura suave.

#### Marca d'água apenas de leitura (VROM)

A marca d'água somente leitura de volume de armazenamento é a próxima marca d'água para indicar que o espaço utilizável de um nó para dados de objeto está se tornando cheio. Essa marca d'água representa quanto espaço livre deve existir em cada volume em um nó de armazenamento para impedir que o nó entre no modo somente leitura." o modo somente leitura dura significa que o nó de armazenamento é somente leitura e não aceita mais solicitações de gravação.

Se a quantidade de espaço livre em cada volume em um nó de armazenamento for menor do que a configuração desta marca d'água, o alarme de Status de armazenamento (SSTS) será acionado no nível principal e o nó de armazenamento será transferido para o modo somente leitura.

Por exemplo, suponha que o volume de armazenamento Hard Read-Only Watermark esteja definido como 5 GB, que é o seu valor padrão. Se menos de 5 GB de espaço livre permanecer em cada volume de armazenamento no nó de armazenamento, o alarme SSTS é acionado no nível principal e o nó de armazenamento passa para o modo apenas de leitura difícil.

O valor da marca de água de apenas leitura de volume de armazenamento tem de ser inferior ao valor da marca de água de apenas leitura suave do volume de armazenamento.

#### Marca d'água de leitura-escrita do volume de armazenamento (VLWM)

A marca d'água de leitura e gravação do volume de armazenamento aplica-se apenas a nós de armazenamento que tenham sido transferidos para o modo somente leitura. Essa marca d'água determina quando o nó de armazenamento pode ser lido e gravado novamente.

Por exemplo, suponha que um nó de armazenamento tenha sido transferido para o modo somente leitura difícil. Se a marca de água de leitura e gravação do volume de armazenamento estiver definida como 30 GB (padrão), o espaço livre em cada volume de armazenamento no nó de armazenamento deve aumentar de 5 GB para 30 GB antes que o nó possa ser lido e gravado novamente.

O valor da marca de água de leitura-escrita do volume de armazenamento deve ser superior ao valor da marca de água de leitura suave do volume de armazenamento.

#### Informações relacionadas

"Gerenciamento de nós de storage completos"

## Gerenciamento do storage de metadados de objetos

A capacidade de metadados de objetos de um sistema StorageGRID controla o número máximo de objetos que podem ser armazenados nesse sistema. Para garantir que seu sistema StorageGRID tenha espaço adequado para armazenar novos objetos, você deve entender onde e como o StorageGRID armazena os metadados de objetos.

#### O que é metadados de objetos?

Metadados de objetos são qualquer informação que descreva um objeto. O StorageGRID usa metadados de objetos para rastrear os locais de todos os objetos na grade e gerenciar o ciclo de vida de cada objeto ao longo do tempo.

Para um objeto no StorageGRID, os metadados de objeto incluem os seguintes tipos de informações:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket do S3 ou do contentor Swift, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a

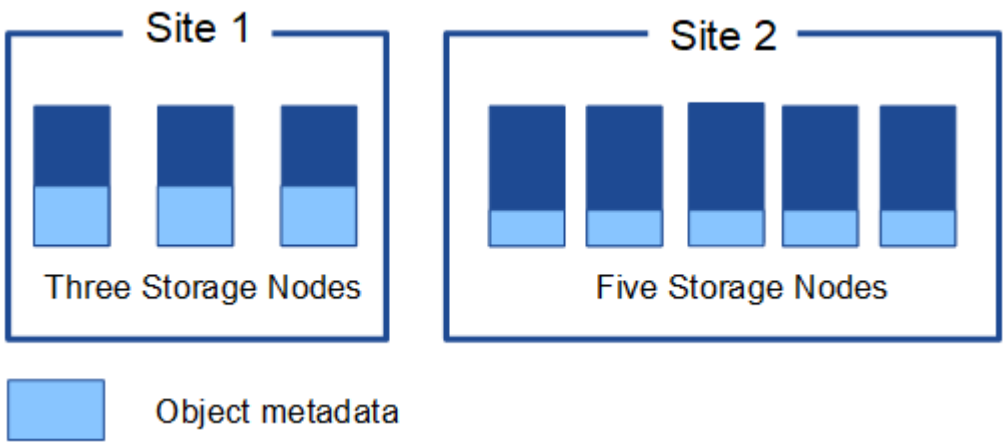
data e hora em que o objeto foi criado pela primeira vez e a data e hora em que o objeto foi modificado pela última vez.

- Quaisquer pares de valor-chave de metadados de usuário personalizados associados ao objeto.
- Para objetos S3D, qualquer par de chave-valor de marca de objeto associado ao objeto.
- Para cópias de objetos replicadas, o local de storage atual de cada cópia.
- Para cópias de objetos com codificação de apagamento, o local de storage atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos multipartes, identificadores de segmento e tamanhos de dados.

**Como os metadados de objetos são armazenados?**

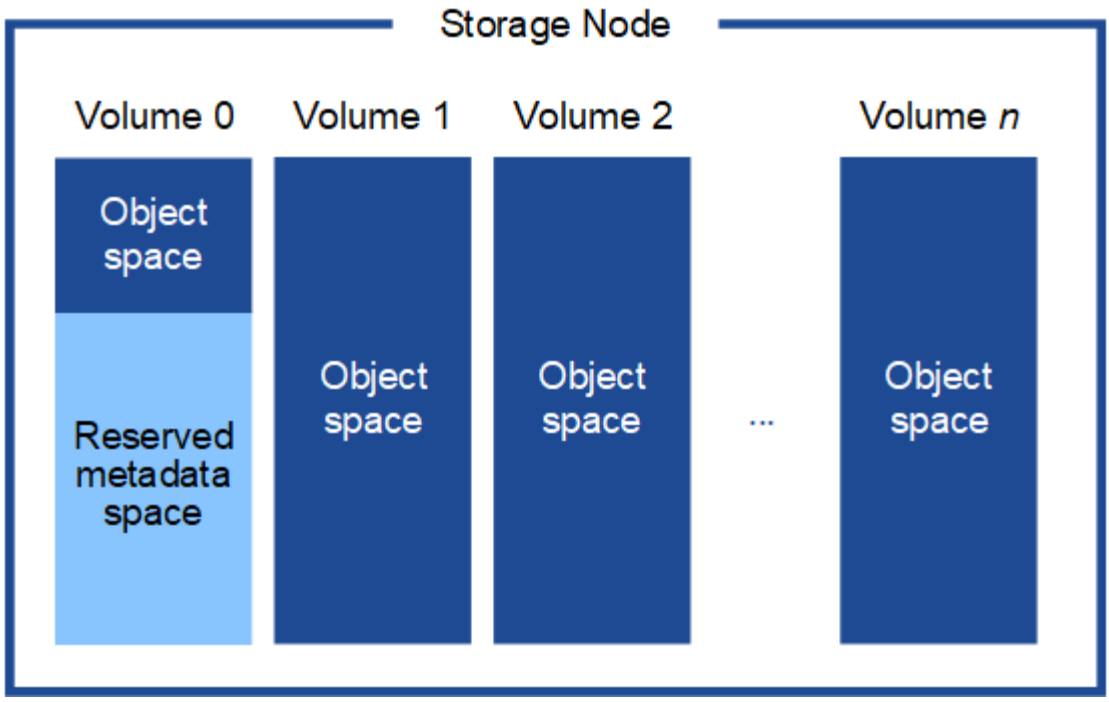
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local. As três cópias dos metadados de objetos são distribuídas uniformemente por todos os nós de storage em cada local.

Essa figura representa os nós de storage em dois locais. Cada local tem a mesma quantidade de metadados de objetos, que é igualmente distribuída pelos nós de storage nesse local.




**Onde os metadados de objetos são armazenados?**

Essa figura representa os volumes de storage de um único nó de storage.




Como mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de storage 0 de cada nó de storage. Ele usa o espaço reservado para armazenar metadados de objetos e executar operações essenciais de banco de dados. Qualquer espaço restante no volume de storage 0 e todos os outros volumes de storage no nó de storage são usados exclusivamente para dados de objetos (cópias replicadas e fragmentos codificados por apagamento).

A quantidade de espaço reservada para metadados de objetos em um nó de storage específico depende de vários fatores, descritos abaixo.

**Definição de espaço reservado metadados**

O *Metadata Reserved Space* é uma configuração em todo o sistema que representa a quantidade de espaço que será reservada para metadados no volume 0 de cada nó de armazenamento. Como mostrado na tabela, o valor padrão dessa configuração para o StorageGRID 11,5 é baseado no seguinte:

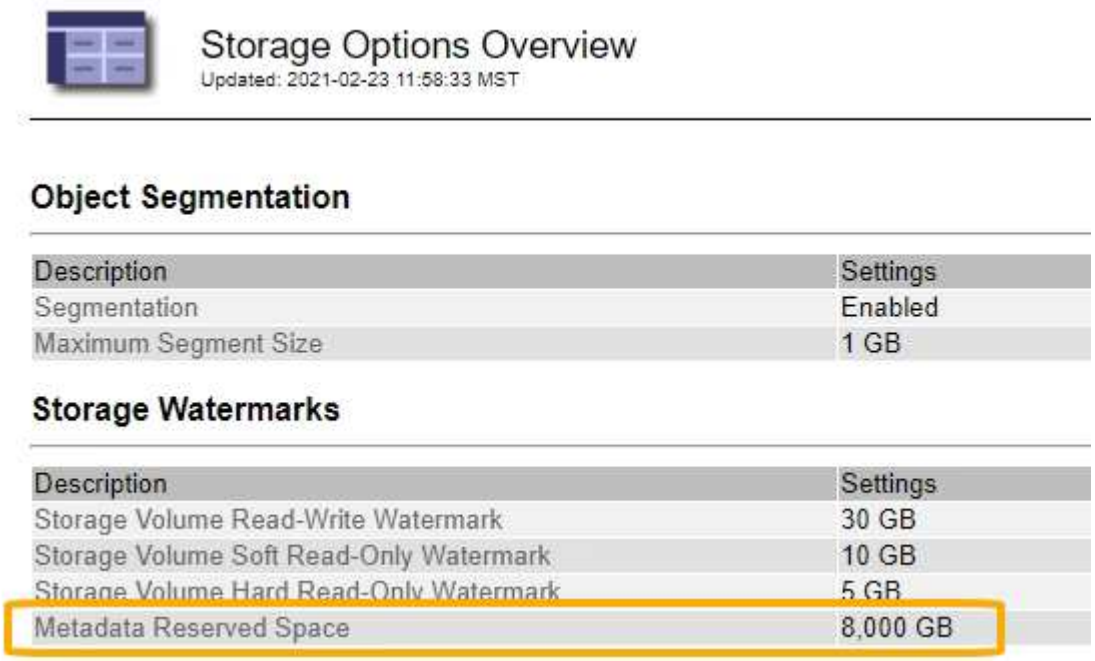
- A versão de software que você estava usando quando você instalou o StorageGRID inicialmente.
- A quantidade de RAM em cada nó de armazenamento.

| Versão utilizada para a instalação inicial do StorageGRID | Quantidade de RAM nos nós de storage | Configuração de espaço reservado de metadados padrão para o StorageGRID 11,5 |
|---|---|---|
| 11,5 | 128 GB ou mais em cada nó de storage na grade | 8 TB (8.000 GB) |
| | Menos de 128 GB em qualquer nó de armazenamento na grade | 3 TB (3.000 GB) |
| 11,1 a 11,4 | 128 GB ou mais em cada nó de armazenamento em qualquer local | 4 TB (4.000 GB) |

| Versão utilizada para a instalação inicial do StorageGRID | Quantidade de RAM nos nós de storage | Configuração de espaço reservado de metadados padrão para o StorageGRID 11,5 |
|---|---|---|
| | Menos de 128 GB em qualquer nó de storage em cada local | 3 TB (3.000 GB) |
| 11,0 ou anterior | Qualquer valor | 2 TB (2.000 GB) |

Para visualizar a definição espaço reservado metadados para o seu sistema StorageGRID:

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de armazenamento**.
2. Na tabela Storage Watermarks (marcas de água de armazenamento), localize **Metadata Reserved Space** (espaço reservado de metadados).




Na captura de tela, o valor **espaço reservado de metadados** é de 8.000 GB (8 TB). Esta é a configuração padrão para uma nova instalação do StorageGRID 11,5 na qual cada nó de armazenamento tem 128 GB ou mais de RAM.

### Espaço reservado real para metadados

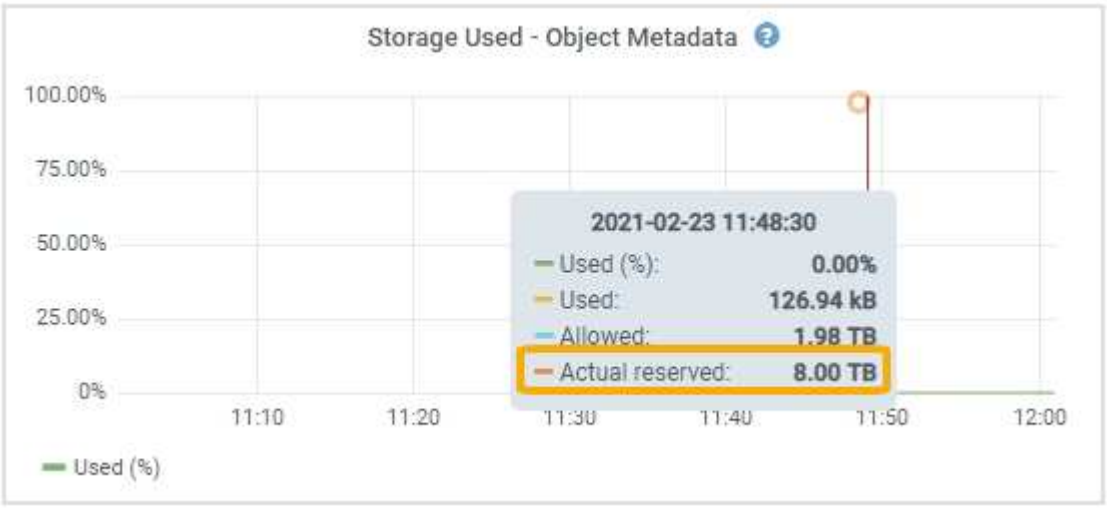
Em contraste com a configuração espaço reservado de metadados em todo o sistema, o *espaço reservado real* para metadados de objetos é determinado para cada nó de armazenamento. Para qualquer nó de armazenamento, o espaço reservado real para metadados depende do tamanho do volume 0 para o nó e da configuração **espaço reservado de metadados** em todo o sistema.

| Tamanho do volume 0 para o nó | Espaço reservado real para metadados |
|---|---|
| Menos de 500 GB (uso não produção) | 10% do volume 0 |

| Tamanho do volume 0 para o nó | Espaço reservado real para metadados |
| --- | --- |
| 500 GB ou mais | O menor desses valores:<br>• Volume 0<br>• Definição de espaço reservado metadados |

Para exibir o espaço reservado real para metadados em um nó de storage específico:

1. No Gerenciador de Grade, selecione **nós** > ***Storage Node***.
2. Selecione a guia **armazenamento**.
3. Passe o cursor sobre o gráfico armazenamento usado — metadados de objetos e localize o valor **atual reservado**.




Na captura de tela, o valor **atual reservado** é de 8 TB. Esta captura de tela é para um nó de armazenamento grande em uma nova instalação do StorageGRID 11,5. Como a configuração espaço reservado de metadados em todo o sistema é menor que o volume 0 para este nó de armazenamento, o espaço reservado real para este nó é igual à configuração espaço reservado de metadados.

O valor **atual reservado** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

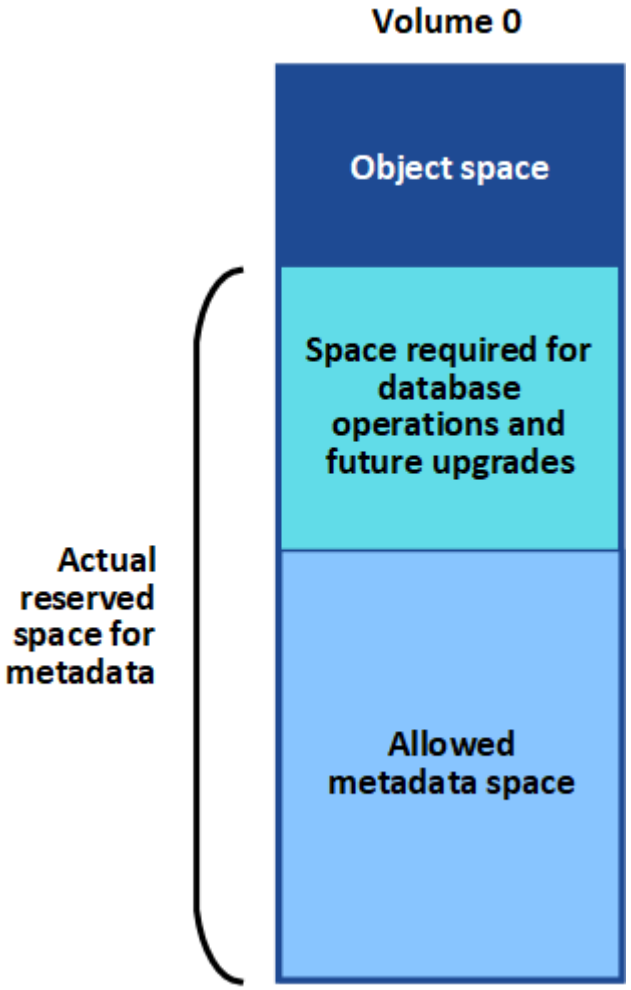
#### Exemplo de espaço reservado real de metadados

Suponha que você instale um novo sistema StorageGRID usando a versão 11,5. Para este exemplo, suponha que cada nó de armazenamento tem mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) é de 6 TB. Com base nestes valores:

- O **Metadata Reserved Space** em todo o sistema está definido para 8 TB. (Este é o valor padrão para uma nova instalação do StorageGRID 11,5 se cada nó de armazenamento tiver mais de 128 GB de RAM.)
- O espaço reservado real para metadados para SN1 é de 6 TB. (Todo o volume é reservado porque o volume 0 é menor do que a configuração **espaço reservado de metadados**.)

### Espaço de metadados permitido

O espaço reservado real de cada nó de storage para metadados é subdividido no espaço disponível para metadados de objetos (o espaço de metadados permitido_) e no espaço necessário para operações essenciais de banco de dados (como compactação e reparo) e futuras atualizações de hardware e software. O espaço de metadados permitido rege a capacidade geral do objeto.



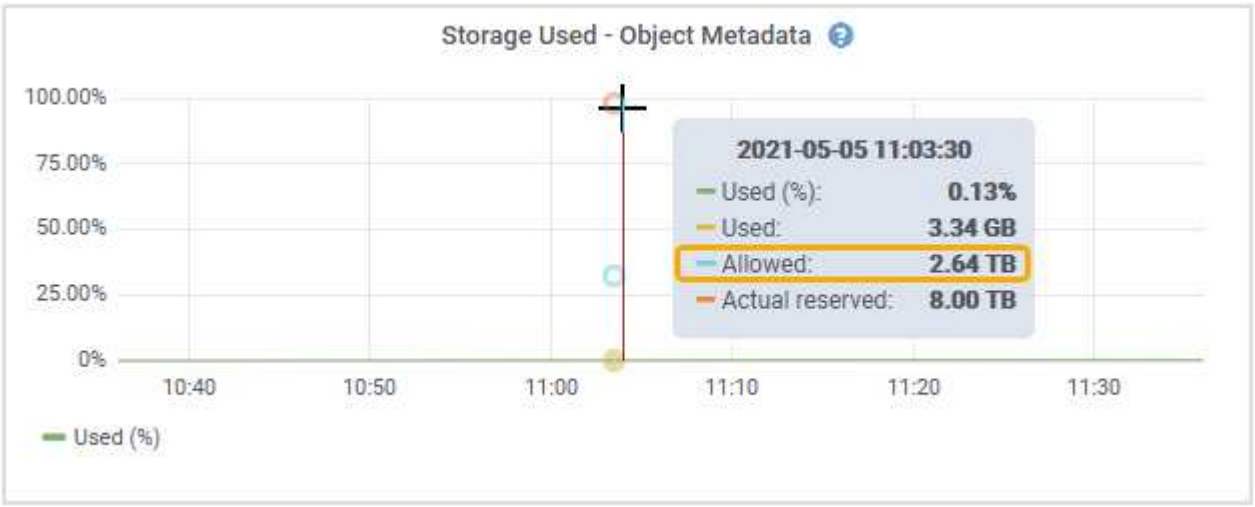

A tabela a seguir resume como o StorageGRID determina o valor de espaço de metadados permitido para um nó de storage.

| Espaço reservado real para metadados | Espaço de metadados permitido |
|---|---|
| 4 TB ou menos | 60% do espaço reservado real para metadados, até um máximo de 1,98 TB |
| Mais de 4 TB | (Espaço reservado real para metadados - 1 TB) x 60%, até um máximo de 2,64 TB |

Se o seu sistema StorageGRID armazenar (ou é esperado que armazene) mais de 2,64 TB de metadados em qualquer nó de armazenamento, o espaço permitido de metadados pode ser aumentado em alguns casos. Se cada um dos nós de storage tiver mais de 128 GB de RAM e espaço livre disponível no volume de armazenamento 0, entre em Contato com o representante da conta do NetApp. O NetApp analisará seus requisitos e aumentará o espaço de metadados permitido para cada nó de storage, se possível.

Para exibir o espaço de metadados permitido para um nó de storage:

1. No Gerenciador de Grade, selecione **Node** > ***Storage Node***.
2. Selecione a guia **armazenamento**.
3. Passe o cursor sobre o gráfico armazenamento usado — metadados de objetos e localize o valor **permitido**.




Na captura de tela, o valor **permitido** é de 2,64 TB, que é o valor máximo para um nó de armazenamento cujo espaço reservado real para metadados é superior a 4 TB.

O valor **allowed** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

**Exemplo de espaço permitido de metadados**

Suponha que você instale um sistema StorageGRID usando a versão 11,5. Para este exemplo, suponha que cada nó de armazenamento tem mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) é de 6 TB. Com base nestes valores:

- O **Metadata Reserved Space** em todo o sistema está definido para 8 TB. (Este é o valor padrão para o StorageGRID 11,5 quando cada nó de armazenamento tem mais de 128 GB de RAM.)
- O espaço reservado real para metadados para SN1 é de 6 TB. (Todo o volume é reservado porque o volume 0 é menor do que a configuração **espaço reservado de metadados**.)
- O espaço permitido para metadados no SN1 é de 2,64 TB. (Este é o valor máximo para o espaço reservado real.)

### Como os nós de storage de diferentes tamanhos afetam a capacidade do objeto

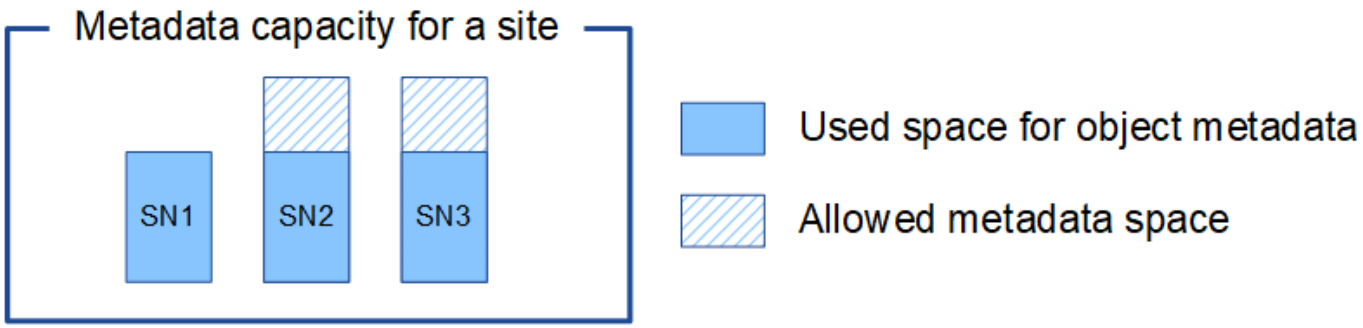
Como descrito acima, o StorageGRID distribui uniformemente os metadados de objetos nos nós de storage em cada local. Por esse motivo, se um site contiver nós de storage de tamanhos diferentes, o menor nó do local determinará a capacidade de metadados do local.

Considere o seguinte exemplo:

- Você tem uma grade de local único que contém três nós de storage de tamanhos diferentes.
- A configuração **Metadata Reserved Space** é de 4 TB.
- Os nós de storage têm os seguintes valores para o espaço de metadados reservado real e o espaço de metadados permitido.

| Nó de storage | Tamanho do volume 0 | Espaço reservado real de metadados | Espaço de metadados permitido |
|---|---|---|---|
| SN1 | 2,2 TB | 2,2 TB | 1,32 TB |
| SN2 | 5 TB | 4 TB | 1,98 TB |
| SN3 | 6 TB | 4 TB | 1,98 TB |

Como os metadados de objetos são distribuídos uniformemente pelos nós de storage em um local, cada nó neste exemplo pode conter apenas 1,32 TB de metadados. Os 0,66 TB adicionais de espaço permitido de metadados para SN2 e SN3 não podem ser usados.




Da mesma forma, como o StorageGRID mantém todos os metadados de objetos para um sistema StorageGRID em cada local, a capacidade geral de metadados de um sistema StorageGRID é determinada pela capacidade de metadados de objetos do menor local.

E como a capacidade de metadados de objetos controla a contagem máxima de objetos, quando um nó fica sem capacidade de metadados, a grade fica efetivamente cheia.

**Informações relacionadas**

- Para saber como monitorar a capacidade de metadados de objetos para cada nó de armazenamento:

  "Monitorizar Resolução de problemas"

- Para aumentar a capacidade dos metadados de objetos do seu sistema, é necessário adicionar novos nós de storage:

"Expanda sua grade"

## Configuração de configurações globais para objetos armazenados

Você pode usar Opções de Grade para configurar as configurações de todos os objetos armazenados no seu sistema StorageGRID, incluindo compactação de objetos armazenados, criptografia de objetos armazenados e hash de objetos armazenados.

- "Configurando a compactação de objetos armazenados"
- "Configurando a criptografia de objeto armazenado"
- "Configurando hash de objeto armazenado"

### Configurando a compactação de objetos armazenados

Você pode usar a opção Compress Stored Objects Grid para reduzir o tamanho dos objetos armazenados no StorageGRID, de modo que os objetos consumam menos storage.

#### 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

A opção Compress Stored Objects Grid (compactar objetos armazenados) está desativada por padrão. Se você habilitar essa opção, o StorageGRID tentará compactar cada objeto ao salvá-lo, usando compactação sem perdas.

> Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

Antes de ativar esta opção, tenha em atenção o seguinte:

- Você não deve ativar a compactação a menos que você saiba que os dados que estão sendo armazenados são compressíveis.
- Os aplicativos que salvam objetos no StorageGRID podem compactar objetos antes de salvá-los. Se um aplicativo cliente já tiver compactado um objeto antes de salvá-lo no StorageGRID, ativar a compactação de objetos armazenados não reduzirá ainda mais o tamanho de um objeto.
- Não ative a compressão se estiver a utilizar o NetApp FabricPool com o StorageGRID.
- Se a opção Compress Stored Objects Grid estiver ativada, os aplicativos cliente S3 e Swift devem evitar executar operações GET Object que especificam um intervalo de bytes serão retornados. Essas operações de leitura de intervalo são ineficientes porque o StorageGRID deve descompactar efetivamente os objetos para acessar os bytes solicitados. As operações GET Object que solicitam um pequeno intervalo de bytes de um objeto muito grande são especialmente ineficientes; por exemplo, é ineficiente ler um intervalo de 10 MB a partir de um objeto compactado de 50 GB.

  Se os intervalos forem lidos a partir de objetos compatados, as solicitações do cliente podem expirar.

Se você precisar compactar objetos e seu aplicativo cliente precisar usar leituras de intervalo, aumente o tempo limite de leitura para o aplicativo.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de objetos armazenados, marque a caixa de seleção **Compress Stored Objects**.


3. Clique em **Salvar**.

### Configurando a criptografia de objeto armazenado

Você pode criptografar objetos armazenados se quiser garantir que os dados não possam ser recuperados de forma legível se um armazenamento de objetos for comprometido. Por padrão, os objetos não são criptografados.

**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**

A criptografia de objetos armazenados permite a criptografia de todos os dados de objetos à medida que são ingeridos através do S3 ou Swift. Quando você ativa a configuração, todos os objetos recém-ingeridos são criptografados, mas nenhuma alteração é feita aos objetos armazenados existentes. Se desativar a encriptação, os objetos atualmente encriptados permanecem encriptados, mas os objetos recentemente ingeridos não são encriptados.

Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

Os objetos armazenados podem ser criptografados usando o algoritmo de criptografia AES-128 ou AES-256.

A configuração criptografia de objeto armazenado se aplica somente a objetos S3 que não tenham sido criptografados por criptografia no nível do bucket ou no nível do objeto.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de objetos armazenados, altere criptografia de objetos armazenados para **nenhum** (padrão), **AES-128** ou **AES-256**.


3. Clique em **Salvar**.

### Configurando hash de objeto armazenado

A opção hash de objeto armazenado especifica o algoritmo de hash usado para verificar a integridade do objeto.

#### O que você vai precisar

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

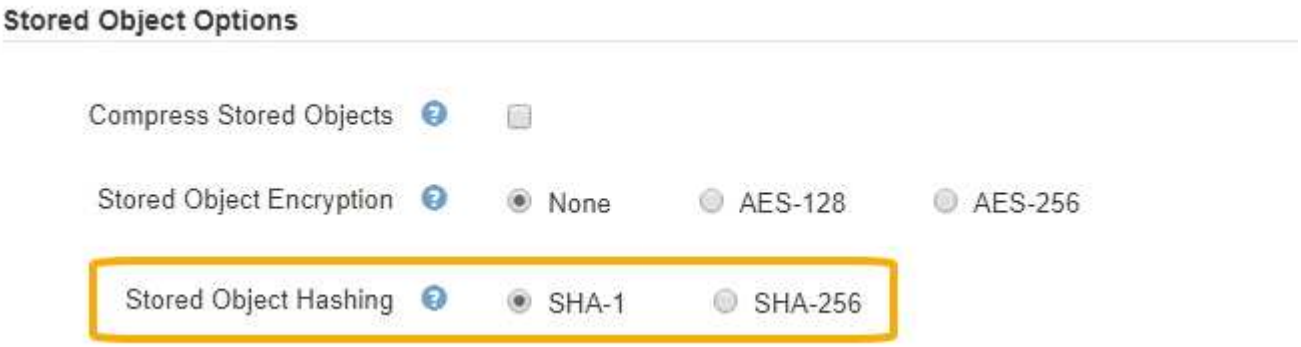
#### Sobre esta tarefa

Por padrão, os dados do objeto são hash usando o algoritmo SHA-1. O algoritmo SHA-256 requer recursos adicionais de CPU e geralmente não é recomendado para verificação de integridade.

Se alterar esta definição, demora cerca de um minuto para a nova definição ser aplicada. O valor configurado é armazenado em cache para desempenho e dimensionamento.

#### Passos

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de grade**.
2. Na seção Opções de objetos armazenados, altere o hash de objetos armazenados para **SHA-1** (padrão) ou **SHA-256**.




3. Clique em **Salvar**.

## Configurações do nó de storage

Cada nó de armazenamento usa várias configurações e contadores. Talvez seja

necessário exibir as configurações atuais ou redefinir contadores para apagar alarmes (sistema legado).

> Exceto quando especificamente instruído na documentação, você deve consultar o suporte técnico antes de modificar qualquer configuração do nó de armazenamento. Conforme necessário, você pode redefinir contadores de eventos para limpar alarmes legados.

Para acessar as configurações e contadores de um nó de armazenamento:

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site*** > ***Storage Node***.
3. Expanda o nó de armazenamento e selecione o serviço ou componente.
4. Selecione a guia **Configuração**.

As tabelas a seguir resumem as configurações do nó de armazenamento.

**LDR**

| Nome do atributo | Código | Descrição |
|---|---|---|
| Estado HTTP | HSTE | O estado atual do protocolo HTTP para S3, Swift e outro tráfego StorageGRID interno:<br>• Offline: Não são permitidas operações e qualquer aplicativo cliente que tente abrir uma sessão HTTP para o serviço LDR recebe uma mensagem de erro. As sessões ativas estão graciosamente fechadas.<br>• Online: A operação continua normalmente |
| Auto-Iniciar HTTP | HTAS | • Se selecionado, o estado do sistema ao reiniciar depende do estado do componente **LDR** > **Storage**. Se o componente **LDR** > **Storage** for somente leitura ao reiniciar, a interface HTTP também será somente leitura. Se o componente **LDR** > **Storage** estiver Online, o HTTP também estará Online. Caso contrário, a interface HTTP permanece no estado Offline.<br>• Se não estiver selecionada, a interface HTTP permanece Offline até explicitamente ativada. |

**LDR > armazenamento de dados**

| Nome do atributo | Código | Descrição |
|---|---|---|
| Repor contagem de objetos perdidos | RCOR | Redefina o contador para o número de objetos perdidos neste serviço. |

**LDR > armazenamento**

| Nome do atributo | Código | Descrição |
| --- | --- | --- |
| Estado de armazenamento — desejado | SSDS | Uma configuração configurável pelo usuário para o estado desejado do componente de armazenamento. O serviço LDR lê este valor e tenta corresponder ao estado indicado por este atributo. O valor é persistente entre as reinicializações.<br><br>Por exemplo, você pode usar essa configuração para forçar o armazenamento a se tornar somente leitura, mesmo quando houver amplo espaço de armazenamento disponível. Isso pode ser útil para a solução de problemas.<br><br>O atributo pode ter um dos seguintes valores:<br><br>• Offline: Quando o estado desejado é Offline, o serviço LDR coloca o componente **LDR** > **Storage** offline.<br>• Somente leitura: Quando o estado desejado é somente leitura, o serviço LDR move o estado de armazenamento para somente leitura e pára de aceitar novo conteúdo. Observe que o conteúdo pode continuar sendo salvo no nó de armazenamento por um curto período de tempo até que as sessões abertas sejam fechadas.<br>• Online: Deixe o valor em Online durante as operações normais do sistema. O estado de armazenamento — a corrente do componente de armazenamento será definida dinamicamente pelo serviço com base na condição do serviço LDR, como a quantidade de espaço de armazenamento de objetos disponível. Se o espaço for baixo, o componente torna-se somente leitura. |
| Tempo limite de verificação de integridade | SHCT | O limite de tempo em segundos no qual um teste de verificação de integridade deve ser concluído para que um volume de armazenamento seja considerado saudável. Altere este valor apenas quando direcionado para o fazer pelo suporte. |

**LDR > Verificação**

| Nome do atributo | Código | Descrição |
| --- | --- | --- |
| Repor contagem de objetos em falta | VCMI | Redefine a contagem de objetos perdidos detetados (OMIS). Utilize apenas após a conclusão da verificação em primeiro plano. Os dados de objeto replicado em falta são restaurados automaticamente pelo sistema StorageGRID. |
| Verifique | FVOV | Selecione armazenamentos de objetos nos quais executar a verificação de primeiro plano. |
| Taxa de verificação | VPRI | Defina a taxa em que a verificação de fundo ocorre. Consulte informações sobre como configurar a taxa de verificação em segundo plano. |
| Repor contagem de objetos corrompidos | VCCR | Redefina o contador para obter dados de objeto replicado corrompidos encontrados durante a verificação em segundo plano. Esta opção pode ser usada para limpar a condição de alarme objetos corrompidos detetados (OCOR). Para obter detalhes, consulte as instruções para monitoramento e solução de problemas do StorageGRID. |
| Excluir objetos em quarentena | OQRT | Exclua objetos corrompidos do diretório de quarentena, redefina a contagem de objetos em quarentena para zero e limpe o alarme objetos em quarentena detetados (OQRT). Esta opção é usada depois que objetos corrompidos foram restaurados automaticamente pelo sistema StorageGRID.<br><br>Se um alarme de objetos perdidos for acionado, o suporte técnico pode querer acessar os objetos em quarentena. Em alguns casos, objetos em quarentena podem ser úteis para a recuperação de dados ou para depurar os problemas subjacentes que causaram as cópias de objetos corrompidas. |

**LDR > codificação de apagamento**

| Nome do atributo | Código | Descrição |
| --- | --- | --- |
| Repor gravações contagem de falhas | RSWF | Redefina o contador para falhas de gravação de dados de objetos codificados por apagamento no nó de storage. |
| A reinicialização lê a contagem de falhas | RSRF | Redefina o contador para falhas de leitura de dados de objetos codificados por apagamento a partir do nó de armazenamento. |

| Nome do atributo | Código | Descrição |
| --- | --- | --- |
| A reposição elimina a contagem de falhas | RSDF | Redefina o contador para falhas de exclusão de dados de objetos codificados por apagamento do nó de storage. |
| Repor contagem de cópias corrompidas detetadas | RSCC | Redefina o contador para o número de cópias corrompidas de dados de objetos codificados por apagamento no nó de storage. |
| Repor a contagem de fragmentos corrompidos detetados | RSCD | Redefina o contador de fragmentos corrompidos de dados de objetos codificados por apagamento no nó de storage. |
| Repor contagem de fragmentos detetados em falta | RSMD | Redefina o contador de fragmentos ausentes de dados de objetos codificados por apagamento no nó de storage. Utilize apenas após a conclusão da verificação em primeiro plano. |

**LDR > replicação**

| Nome do atributo | Código | Descrição |
| --- | --- | --- |
| Repor contagem de falhas de replicação de entrada | RICR | Redefina o contador para falhas de replicação de entrada. Isso pode ser usado para limpar o alarme RIRF (replicação de entrada — Falha). |
| Repor contagem de falhas de replicação efetuada | ROCR | Redefina o contador para falhas de replicação de saída. Isso pode ser usado para limpar o alarme RORF (Outbound replicações — Failed). |
| Desativar replicação de entrada | DSIR | Selecione para desativar a replicação de entrada como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal.<br><br>Quando a replicação de entrada é desativada, os objetos podem ser recuperados do nó de armazenamento para cópia para outros locais no sistema StorageGRID, mas os objetos não podem ser copiados para este nó de armazenamento a partir de outros locais: O serviço LDR é somente leitura. |

| Nome do atributo | Código | Descrição |
| --- | --- | --- |
| Desativar replicação efetuada | DSOR | Selecione para desativar a replicação de saída (incluindo solicitações de conteúdo para recuperações HTTP) como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal.<br><br>Quando a replicação de saída é desativada, os objetos podem ser copiados para este nó de armazenamento, mas os objetos não podem ser recuperados do nó de armazenamento para serem copiados para outros locais no sistema StorageGRID. O serviço LDR é apenas de escrita. |

**Informações relacionadas**

"Monitorizar Resolução de problemas"

## Gerenciamento de nós de storage completos

À medida que os nós de storage atingem a capacidade, você precisa expandir o sistema StorageGRID com a adição de um novo storage. Há três opções disponíveis: Adicionar volumes de storage, adicionar compartimentos de expansão de storage e adicionar nós de storage.

### Adição de volumes de armazenamento

Cada nó de storage oferece suporte a um número máximo de volumes de storage. O máximo definido varia de acordo com a plataforma. Se um nó de armazenamento contiver menos do que o número máximo de volumes de armazenamento, pode adicionar volumes para aumentar a sua capacidade. Consulte as instruções para expandir um sistema StorageGRID.

### Adição de gavetas de expansão de storage

Alguns nós de storage de dispositivos StorageGRID, como o SG6060, podem dar suporte a gavetas de storage adicionais. Se você tiver dispositivos StorageGRID com funcionalidades de expansão que ainda não foram expandidas para a capacidade máxima, poderá adicionar compartimentos de storage para aumentar a capacidade. Consulte as instruções para expandir um sistema StorageGRID.

### Adição de nós de storage

Você pode aumentar a capacidade de storage adicionando nós de storage. Deve-se ter em consideração cuidadosamente as regras de ILM e os requisitos de capacidade atualmente ativos ao adicionar armazenamento. Consulte as instruções para expandir um sistema StorageGRID.

**Informações relacionadas**

"Expanda sua grade"

# Gerenciando nós de administração

Cada local em uma implantação do StorageGRID pode ter um ou mais nós de

administração.

- "O que é um nó Admin"
- "Usando vários nós de administração"
- "Identificando o nó de administração principal"
- "Selecionar um remetente preferido"
- "Exibindo status de notificação e filas"
- "Como os nós de administração mostram alarmes reconhecidos (sistema legado)"
- "Configurando o acesso de cliente de auditoria"

## O que é um nó Admin

Os nós de administração fornecem serviços de gerenciamento, como configuração, monitoramento e log do sistema. Cada grade deve ter um nó de administração principal e pode ter qualquer número de nós de administração não primários para redundância.

Quando você entra no Gerenciador de Grade ou no Gerenciador de Tenant, você está se conetando a um nó Admin. Você pode se conetar a qualquer nó de administrador e cada nó de administrador exibe uma exibição semelhante do sistema StorageGRID. No entanto, os procedimentos de manutenção devem ser executados usando o nó de administração principal.

Os nós Admin também podem ser usados para equilibrar o tráfego de clientes S3 e Swift.

Os nós de administração hospedam os seguintes serviços:

- Serviço AMS
- Serviço CMN
- Serviço NMS
- Prometheus serviço
- Load Balancer e serviços de alta disponibilidade (para suportar tráfego de clientes S3 e Swift)

Os Admin Nodes também suportam a Management Application Program Interface (mgmt-api) para processar solicitações da API Grid Management e da API Tenant Management.

### O que é o serviço AMS

O serviço do sistema de Gestão de Auditoria (AMS) controla a atividade e os eventos do sistema.

### O que é o serviço CMN

O serviço CMN (Configuration Management Node) gerencia configurações de conetividade e recursos de protocolo em todo o sistema necessárias para todos os serviços. Além disso, o serviço CMN é usado para executar e monitorar tarefas de grade. Há apenas um serviço CMN por implantação do StorageGRID. O nó Admin que hospeda o serviço CMN é conhecido como nó Admin principal.

### O que é o serviço NMS

O serviço do sistema de Gerenciamento de rede (NMS) alimenta as opções de monitoramento, relatórios e configuração que são exibidas através do Gerenciador de Grade, a interface baseada no navegador do

sistema StorageGRID.

#### O que é o serviço Prometheus

O serviço Prometheus coleta métricas de séries temporais dos serviços em todos os nós.

#### Informações relacionadas

"Usando a API de gerenciamento de grade"

"Use uma conta de locatário"

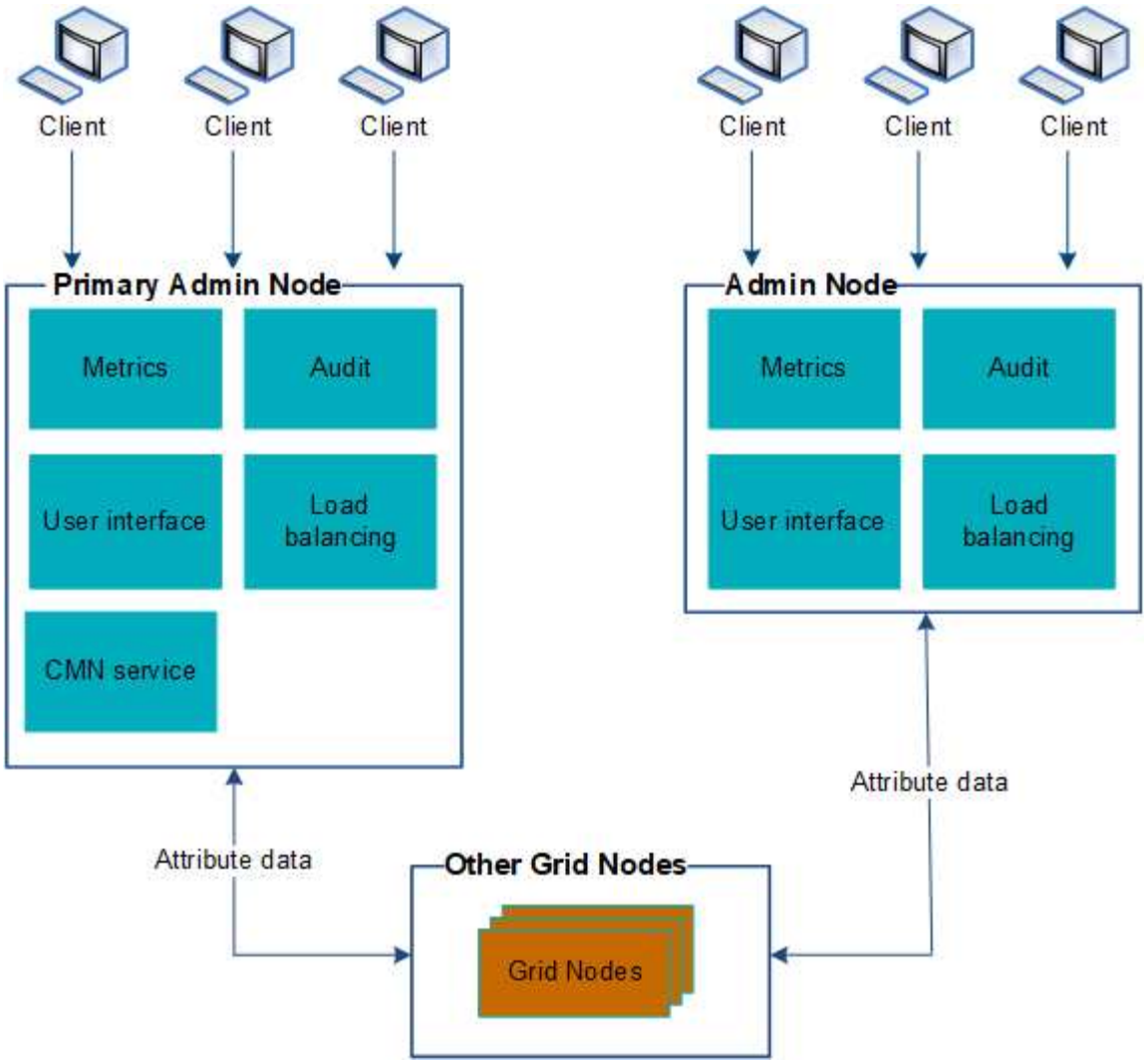
"Gerenciamento do balanceamento de carga"

"Gerenciamento de grupos de alta disponibilidade"

## Usando vários nós de administração

Um sistema StorageGRID pode incluir vários nós de administração para permitir que você monitore e configure continuamente seu sistema StorageGRID, mesmo se um nó de administração falhar.

Se um nó Admin ficar indisponível, o processamento de atributos continuará, alertas e alarmes (sistema legado) ainda serão acionados e notificações de e-mail e mensagens AutoSupport ainda serão enviadas. No entanto, ter vários nós de administração não fornece proteção contra failover, exceto notificações e mensagens AutoSupport. Em particular, os reconhecimentos de alarmes feitos de um nó Admin não são copiados para outros nós Admin.




Existem duas opções para continuar a visualizar e configurar o sistema StorageGRID se um nó de administrador falhar:

- Os clientes da Web podem se reconetar a qualquer outro nó de administração disponível.
- Se um administrador do sistema tiver configurado um grupo de nós de administração de alta disponibilidade, os clientes da Web poderão continuar a aceder ao Gestor de grelha ou ao Gestor de inquilinos utilizando o endereço IP virtual do grupo HA.

> Ao usar um grupo de HA, o acesso é interrompido se o nó de administração principal falhar. Os usuários devem fazer login novamente após o failover do endereço IP virtual do grupo HA para outro nó Admin no grupo.

Algumas tarefas de manutenção só podem ser executadas usando o nó de administração principal. Se o nó de administração principal falhar, ele deve ser recuperado antes que o sistema StorageGRID esteja totalmente funcional novamente.

**Informações relacionadas**

"Gerenciamento de grupos de alta disponibilidade"

## Identificando o nó de administração principal

O nó de administração principal hospeda o serviço CMN. Alguns procedimentos de manutenção só podem ser executados usando o nó de administração principal.

**O que você vai precisar**

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

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***site*** > **Admin Node** e, em seguida, clique ➕ para expandir a árvore de topologia e mostrar os serviços hospedados neste Admin Node.

   O nó de administração principal hospeda o serviço CMN.

3. Se este nó Admin não hospedar o serviço CMN, verifique os outros nós Admin.

## Selecionar um remetente preferido

Se a implantação do StorageGRID incluir vários nós de administração, você poderá selecionar qual nó de administração deve ser o remetente preferido de notificações. Por padrão, o nó Admin principal é selecionado, mas qualquer nó Admin pode ser o remetente preferido.

**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**

A página **Configuração** > **Configurações do sistema** > **Opções de exibição** mostra qual nó Admin está selecionado atualmente para ser o remetente preferido. O nó de administração principal é selecionado por padrão.

Em operações normais do sistema, apenas o remetente preferido envia as seguintes notificações:

- Mensagens AutoSupport
- Notificações SNMP
- E-mails de alerta
- E-mails de alarme (sistema legado)

No entanto, todos os outros nós Admin (remetentes de reserva) monitoram o remetente preferido. Se for detetado um problema, um remetente em espera também pode enviar essas notificações.

Tanto o remetente preferido quanto um remetente em espera podem enviar notificações nestes casos:

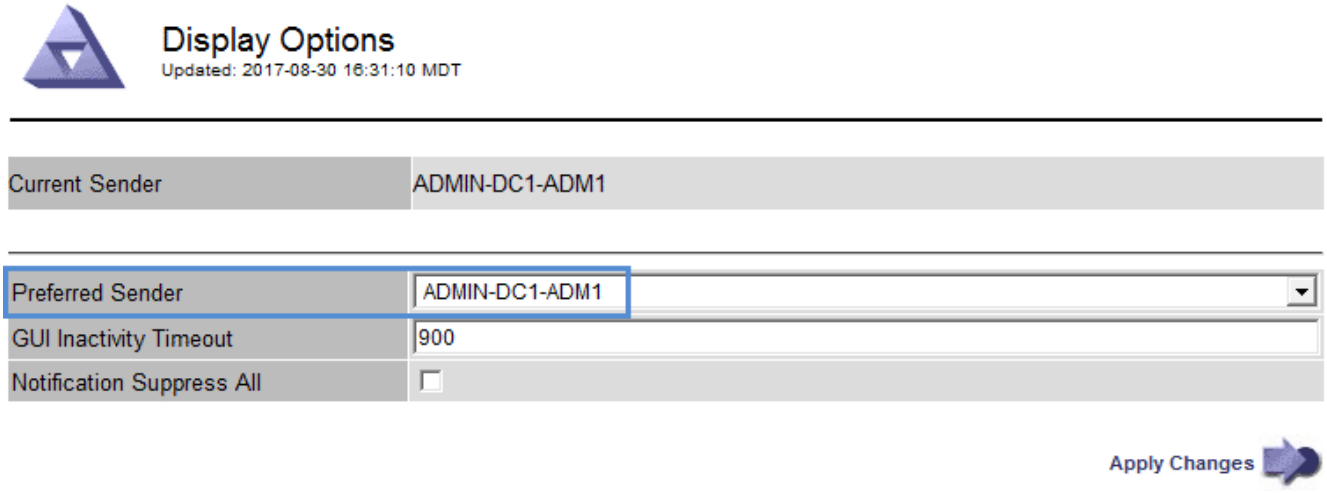
- Se os nós de administrador se tornarem "'desembarcados'" uns dos outros, tanto o remetente preferido quanto o remetente de reserva tentarão enviar notificações, e várias cópias de notificações podem ser recebidas.

- Depois que um remetente em espera detetar problemas com o remetente preferido e começar a enviar notificações, o remetente preferido pode recuperar sua capacidade de enviar notificações. Se isso ocorrer, notificações duplicadas podem ser enviadas. O remetente em espera deixará de enviar notificações quando não detetar mais erros no remetente preferido.

> Quando você testa notificações de alarme e mensagens AutoSupport, todos os nós de administração enviam o e-mail de teste. Ao testar notificações de alerta, você deve entrar em cada nó de administração para verificar a conetividade.

**Passos**

1. Selecione **Configuração** > **Configurações do sistema** > **Opções de exibição**.
2. No menu Opções de exibição, selecione **Opções**.
3. Selecione o nó Admin que deseja definir como o remetente preferido na lista suspensa.



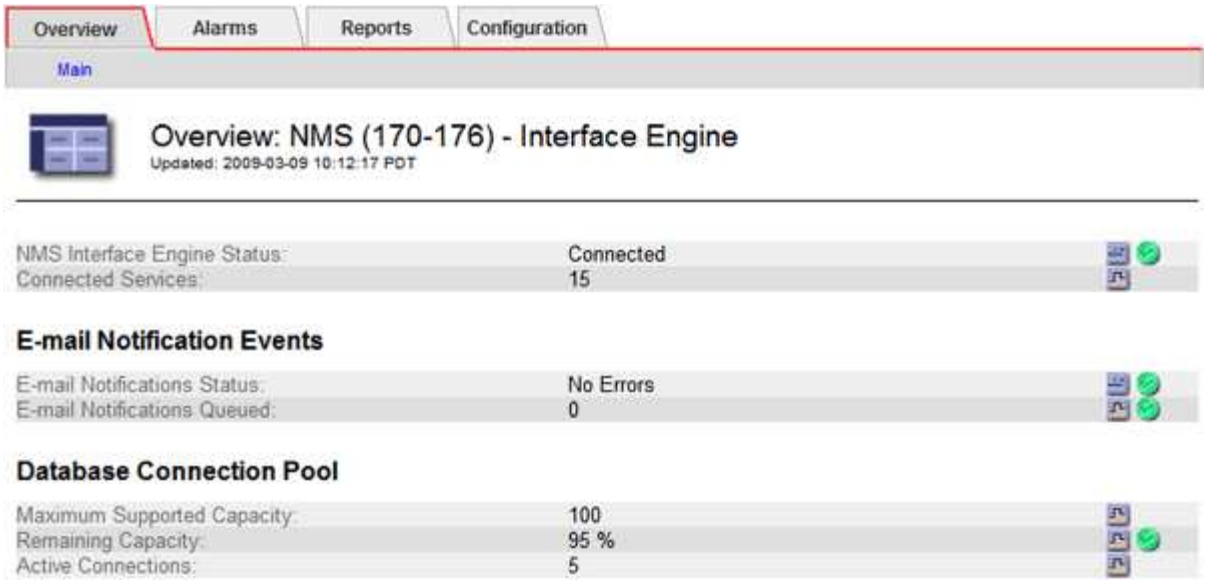

4. Clique em **aplicar alterações**.

   O Admin Node é definido como o remetente preferido de notificações.

## Exibindo status de notificação e filas

O serviço NMS nos Admin Nodes envia notificações para o servidor de e-mail. Você pode visualizar o status atual do serviço NMS e o tamanho de sua fila de notificações na página mecanismo de interface.

Para acessar a página mecanismo de interface, selecione **suporte** > **Ferramentas** > **topologia de grade**. Finalmente, selecione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.

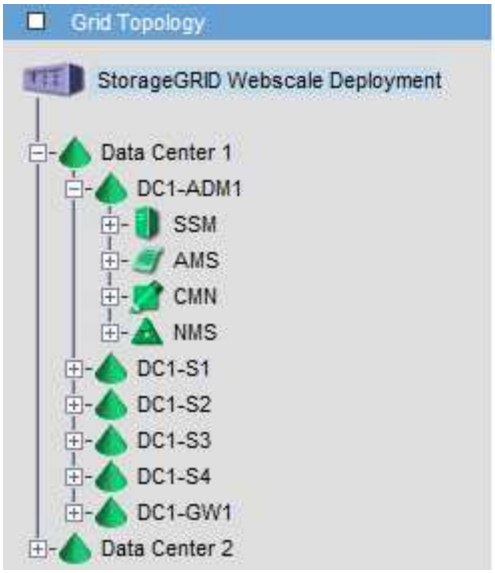


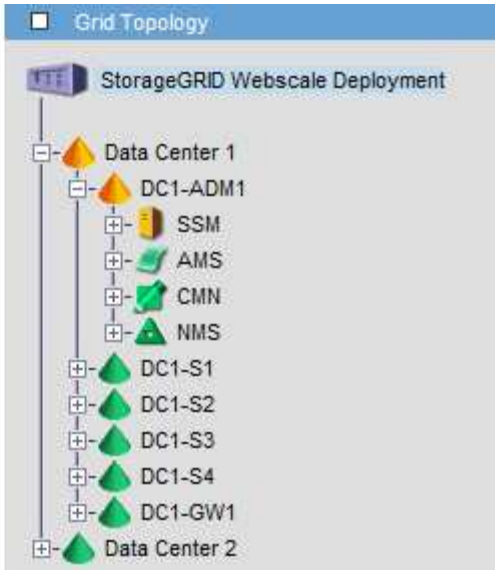

As notificações são processadas através da fila de notificações de e-mail e são enviadas para o servidor de e-mail uma após a outra na ordem em que são acionadas. Se houver um problema (por exemplo, um erro de conexão de rede) e o servidor de e-mail não estiver disponível quando a tentativa for feita para enviar a notificação, uma tentativa de reenviar a notificação para o servidor de e-mail continuará por um período de 60 segundos. Se a notificação não for enviada para o servidor de correio após 60 segundos, a notificação será retirada da fila de notificações e será feita uma tentativa de enviar a próxima notificação na fila. Como as notificações podem ser retiradas da fila de notificações sem serem enviadas, é possível que um alarme possa ser acionado sem que uma notificação seja enviada. No caso de uma notificação ser retirada da fila sem ser enviada, o alarme Minor MINS (Status da notificação por e-mail) é acionado.

## Como os nós de administração mostram alarmes reconhecidos (sistema legado)

Quando você reconhece um alarme em um nó Admin, o alarme reconhecido não é copiado para nenhum outro nó Admin. Como os reconhecimentos não são copiados para outros nós de administração, a árvore de topologia de grade pode não ter a mesma aparência para cada nó de administração.

Essa diferença pode ser útil ao conetar clientes da Web. Os clientes da Web podem ter visualizações diferentes do sistema StorageGRID com base nas necessidades do administrador.




Observe que as notificações são enviadas do nó Admin onde a confirmação ocorre.

## Configurando o acesso de cliente de auditoria

O Admin Node, por meio do serviço do Audit Management System (AMS), Registra todos os eventos do sistema auditados em um arquivo de log disponível por meio do compartilhamento de auditoria, que é adicionado a cada Admin Node na instalação. Para facilitar o acesso aos logs de auditoria, você pode configurar o acesso do cliente para compartilhamentos de auditoria para CIFS e NFS.

O sistema StorageGRID usa reconhecimento positivo para evitar a perda de mensagens de auditoria antes de serem gravadas no arquivo de log. Uma mensagem permanece na fila em um serviço até que o serviço AMS ou um serviço de relé de auditoria intermediária tenha reconhecido o controle dele.

Para obter mais informações, consulte as instruções para entender as mensagens de auditoria.

Se você tiver a opção de usar CIFS ou NFS, escolha NFS.

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

**Informações relacionadas**

"O que é um nó Admin"

"Rever registos de auditoria"

"Atualizar o software"

### Configurando clientes de auditoria para CIFS

O procedimento usado para configurar um cliente de auditoria depende do método de autenticação: Windows Workgroup ou Windows ative Directory (AD). Quando adicionado, o compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

**Informações relacionadas**

"Atualizar o software"

#### Configurando clientes de auditoria para o Workgroup

## Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

**O que você vai precisar**

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

**Sobre esta tarefa**

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

**Passos**

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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. Confirme se todos os serviços têm estado em execução ou verificado: `storagegrid-status`

   Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
-------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------
```

5. Defina a autenticação para o grupo de trabalho do Windows:

   Se a autenticação já tiver sido definida, é apresentada uma mensagem de aviso. Se a autenticação já tiver sido definida, vá para a próxima etapa.

   a. Introduza: `set-authentication`
   b. Quando solicitado para a instalação do Windows Workgroup ou do ative Directory, digite: `workgroup`
   c. Quando solicitado, insira um nome do grupo de trabalho: *`workgroup_name`*
   d. Quando solicitado, crie um nome NetBIOS significativo: *`netbios_name`*

      ou

      Pressione **Enter** para usar o nome do host do Admin Node como o nome NetBIOS.

   O script reinicia o servidor Samba e as alterações são aplicadas. Isso deve levar menos de um minuto. Depois de definir a autenticação, adicione um cliente de auditoria.

   a. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

6. Adicionar um cliente de auditoria:

   a. Introduza: `add-audit-share`

      ⓘ O compartilhamento é adicionado automaticamente como somente leitura.

   b. Quando solicitado, adicione um usuário ou grupo: *`user`*
   c. Quando solicitado, insira o nome de usuário da auditoria: *`audit_user_name`*
   d. Quando solicitado, insira uma senha para o usuário de auditoria: *`password`*
   e. Quando solicitado, digite novamente a mesma senha para confirmá-la: *`password`*
   f. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

Não há necessidade de inserir um diretório. O nome do diretório de auditoria é predefinido.

7. Se mais de um usuário ou grupo tiver permissão para acessar o compartilhamento de auditoria, adicione os usuários adicionais:
   a. Introduza: `add-user-to-share`

      É apresentada uma lista numerada de partilhas ativadas.

   b. Quando solicitado, insira o número do compartilhamento de auditoria-exportação: *`share_number`*
   c. Quando solicitado, adicione um usuário ou grupo: `user`

      ou `group`

   d. Quando solicitado, insira o nome do usuário ou grupo de auditoria: *`audit_user or audit_group`*
   e. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

   f. Repita essas subetapas para cada usuário ou grupo adicional que tenha acesso ao compartilhamento de auditoria.
8. Opcionalmente, verifique sua configuração: `validate-config`

   Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

   ```
   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
   (16384)
   ```

   a. Quando solicitado, pressione **Enter**.

      A configuração do cliente de auditoria é exibida.

   b. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.
9. Feche o utilitário de configuração CIFS: `exit`
10. Inicie o serviço Samba: `service smbd start`
11. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

    ou

    Opcionalmente, se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esse compartilhamento de auditoria conforme necessário:

a. Faça login remotamente no Admin Node de um site:
   i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   iii. Digite o seguinte comando para mudar para root: `su -`
   iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
b. Repita as etapas para configurar o compartilhamento de auditoria para cada nó Admin adicional.
c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`

12. Faça logout do shell de comando: `exit`

**Informações relacionadas**

"Atualizar o software"

#### Configurando clientes de auditoria para o ative Directory

## Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

**O que você vai precisar**

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o nome de usuário e a senha do CIFS ative Directory.
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

> A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

**Passos**

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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. Confirme se todos os serviços têm estado em execução ou verificado: `storagegrid-status`

   Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. Defina a autenticação para o ative Directory: `set-authentication`

   Na maioria das implantações, você deve definir a autenticação antes de adicionar o cliente de auditoria. Se a autenticação já tiver sido definida, é apresentada uma mensagem de aviso. Se a autenticação já tiver sido definida, vá para a próxima etapa.

   a. Quando solicitado para a instalação do Workgroup ou do ative Directory: `ad`
   b. Quando solicitado, insira o nome do domínio AD (nome de domínio curto).
   c. Quando solicitado, insira o endereço IP do controlador de domínio ou o nome de host DNS.
   d. Quando solicitado, insira o nome completo do domínio realm.

      Use letras maiúsculas.

   e. Quando solicitado a ativar o suporte winbind, digite **y**.

      O Winbind é usado para resolver informações de usuários e grupos de servidores AD.

   f. Quando solicitado, insira o nome NetBIOS.
   g. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

6. Junte-se ao domínio:

   a. Se ainda não tiver sido iniciado, inicie o utilitário de configuração CIFS: `config_cifs.rb`
   b. Junte-se ao domínio: `join-domain`
   c. Você será solicitado a testar se o nó Admin é atualmente um membro válido do domínio. Se este nó Admin não tiver aderido anteriormente ao domínio, introduza: `no`
   d. Quando solicitado, forneça o nome de usuário do Administrador: *`administrator_username`*

      ```
      `_administrator_username_`Onde está o nome de usuário do CIFS ative
      Directory, não o nome de usuário do StorageGRID.
      ```

   e. Quando solicitado, forneça a senha do administrador: *`administrator_password`*

Was *administrator_password* é o nome de usuário do CIFS ative Directory, não a senha do StorageGRID.

f. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

7. Verifique se você entrou corretamente no domínio:
   a. Junte-se ao domínio: `join-domain`
   b. Quando solicitado a testar se o servidor é atualmente um membro válido do domínio, digite: `y`

      Se você receber a mensagem ""Join is OK"", você se juntou com sucesso ao domínio. Se você não receber essa resposta, tente configurar a autenticação e ingressar no domínio novamente.

   c. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

8. Adicionar um cliente de auditoria: `add-audit-share`
   a. Quando solicitado a adicionar um usuário ou grupo, digite: `user`
   b. Quando solicitado a inserir o nome de usuário da auditoria, insira o nome de usuário da auditoria.
   c. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

9. Se mais de um usuário ou grupo tiver permissão para acessar o compartilhamento de auditoria, adicione usuários adicionais: `add-user-to-share`

   É apresentada uma lista numerada de partilhas ativadas.

   a. Introduza o número da partilha de auditoria-exportação.
   b. Quando solicitado a adicionar um usuário ou grupo, digite: `group`

      Você será solicitado a fornecer o nome do grupo de auditoria.

   c. Quando solicitado o nome do grupo de auditoria, insira o nome do grupo de usuários de auditoria.
   d. Quando solicitado, pressione **Enter**.

      O utilitário de configuração CIFS é exibido.

   e. Repita esta etapa para cada usuário ou grupo adicional que tenha acesso ao compartilhamento de auditoria.

10. Opcionalmente, verifique sua configuração: `validate-config`

    Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

    - Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-interfaces.inc`
    - Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-filesystem.inc`
    - Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-interfaces.inc`

- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-custom-config.inc`
- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-shares.inc`
- Rlimit_Max: Aumentando rlimit_Max (1024) para o limite mínimo de Windows (16384)

> Não combine a configuração 'anúncios' com o parâmetro 'servidor de senha'. (Por padrão, o Samba irá descobrir o DC correto para entrar em Contato automaticamente).

i. Quando solicitado, pressione **Enter** para exibir a configuração do cliente de auditoria.

ii. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

11. Feche o utilitário de configuração CIFS: `exit`
12. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

ou

Opcionalmente, se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:

a. Faça login remotamente no Admin Node de um site:
   i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
   ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   iii. Digite o seguinte comando para mudar para root: `su -`
   iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
b. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.
c. Feche o login remoto do shell seguro para o Admin Node: `exit`

13. Faça logout do shell de comando: `exit`

**Informações relacionadas**

"Atualizar o software"

#### Adicionando um usuário ou grupo a um compartilhamento de auditoria CIFS

## Você pode adicionar um usuário ou grupo a um compartilhamento de auditoria CIFS integrado à autenticação AD.

**O que você vai precisar**

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

**Sobre esta tarefa**

O procedimento a seguir é para um compartilhamento de auditoria integrado com autenticação AD.

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

**Passos**

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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. Confirme se todos os serviços têm estado em execução ou verificado. Introduza: `storagegrid-status`

   Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Comece a adicionar um usuário ou grupo: `add-user-to-share`

   Uma lista numerada de compartilhamentos de auditoria que foram configurados é exibida.

6. Quando solicitado, insira o número para o compartilhamento de auditoria (auditoria-exportação): *`audit_share_number`*

   Você será perguntado se deseja dar a um usuário ou a um grupo acesso a esse compartilhamento de auditoria.

7. Quando solicitado, adicione um usuário ou grupo: `user` Ou `group`
8. Quando for solicitado o nome do usuário ou grupo para este compartilhamento de auditoria do AD, digite o nome.

   O usuário ou grupo é adicionado como somente leitura para o compartilhamento de auditoria tanto no

sistema operacional do servidor quanto no serviço CIFS. A configuração do Samba é recarregada para permitir que o usuário ou grupo acesse o compartilhamento de cliente de auditoria.

9. Quando solicitado, pressione **Enter**.

   O utilitário de configuração CIFS é exibido.

10. Repita estas etapas para cada usuário ou grupo que tenha acesso ao compartilhamento de auditoria.
11. Opcionalmente, verifique sua configuração: `validate-config`

    Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

    - Não foi possível encontrar include file /etc/samba/includes/cifs-interfaces.inc
    - Não foi possível encontrar include file /etc/samba/includes/cifs-filesystem.inc
    - Não foi possível encontrar include file /etc/samba/includes/cifs-custom-config.inc
    - Não foi possível encontrar include file /etc/samba/includes/cifs-shares.inc
      i. Quando solicitado, pressione **Enter** para exibir a configuração do cliente de auditoria.
      ii. Quando solicitado, pressione **Enter**.
12. Feche o utilitário de configuração CIFS: `exit`
13. Determine se você precisa habilitar compartilhamentos de auditoria adicionais, como a seguir:
    - Se a implantação do StorageGRID for um único local, vá para a próxima etapa.
    - Se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:
      i. Faça login remotamente no Admin Node de um site:
         A. Introduza o seguinte comando: `ssh admin@grid_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.
      ii. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.
      iii. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`
14. Faça logout do shell de comando: `exit`

#### Removendo um usuário ou grupo de um compartilhamento de auditoria CIFS

## Não é possível remover o último usuário ou grupo permitido para acessar o compartilhamento de auditoria.

**O que você vai precisar**

- Você deve ter o `Passwords.txt` arquivo com as senhas da conta root (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

**Sobre esta tarefa**

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

**Passos**

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. Comece a remover um usuário ou grupo: `remove-user-from-share`

   Uma lista numerada de compartilhamentos de auditoria disponíveis para o nó Admin é exibida. O compartilhamento de auditoria é rotulado auditoria-exportação.

4. Introduza o número da partilha de auditoria: *`audit_share_number`*
5. Quando solicitado a remover um usuário ou um grupo: `user` Ou `group`

   É apresentada uma lista numerada de utilizadores ou grupos para a partilha de auditoria.

6. Introduza o número correspondente ao utilizador ou grupo que pretende remover: *`number`*

   O compartilhamento de auditoria é atualizado e o usuário ou grupo não tem mais permissão para acessar o compartilhamento de auditoria. Por exemplo:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Feche o utilitário de configuração CIFS: `exit`
8. Se a implantação do StorageGRID incluir nós de administração em outros sites, desative o compartilhamento de auditoria em cada site, conforme necessário.
9. Faça logout de cada shell de comando quando a configuração estiver concluída: `exit`

**Informações relacionadas**

"Atualizar o software"

#### Alterando um nome de usuário ou grupo de compartilhamento de auditoria CIFS

Você pode alterar o nome de um usuário ou grupo para um compartilhamento de auditoria CIFS adicionando um novo usuário ou grupo e excluindo o antigo.

**Sobre esta tarefa**

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

**Passos**

1. Adicione um novo usuário ou grupo com o nome atualizado ao compartilhamento de auditoria.
2. Exclua o nome de usuário ou grupo antigo.

**Informações relacionadas**

"Atualizar o software"

"Adicionando um usuário ou grupo a um compartilhamento de auditoria CIFS"

"Removendo um usuário ou grupo de um compartilhamento de auditoria CIFS"

#### Verificação da integração da auditoria CIFS

O compartilhamento de auditoria é somente leitura. Os ficheiros de registo destinam-se a ser lidos por aplicações de computador e a verificação não inclui a abertura de um ficheiro. Considera-se verificação suficiente que os arquivos de log de auditoria apareçam em uma janela do Windows Explorer. Após a verificação de conexão, feche

todas as janelas.

#### Configurando o cliente de auditoria para NFS

## O compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.

#### O que você vai precisar

- Tem de ter o `Passwords.txt` ficheiro com a palavra-passe root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).
- O cliente de auditoria deve estar usando o NFS versão 3 (NFSv3).

#### Sobre esta tarefa

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

#### Passos

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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. Confirme se todos os serviços têm estado em execução ou verificado. Introduza: `storagegrid-status`

   Se algum serviço não estiver listado como em execução ou verificado, resolva problemas antes de continuar.

3. Retorne à linha de comando. Pressione **Ctrl** * C*.
4. Inicie o utilitário de configuração NFS. Introduza: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Adicione o cliente de auditoria: `add-audit-share`
   a. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o

compartilhamento de auditoria: `client_IP_address`

b. Quando solicitado, pressione **Enter**.

6. Se mais de um cliente de auditoria tiver permissão para acessar o compartilhamento de auditoria, adicione o endereço IP do usuário adicional: `add-ip-to-share`

   a. Introduza o número da partilha de auditoria: *`audit_share_number`*

   b. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: *`client_IP_address`*

   c. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

   d. Repita essas subetapas para cada cliente de auditoria adicional que tenha acesso ao compartilhamento de auditoria.

7. Opcionalmente, verifique sua configuração.

   a. Introduza o seguinte: `validate-config`

      Os serviços são verificados e exibidos.

   b. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

   c. Feche o utilitário de configuração NFS: `exit`

8. Determine se você deve habilitar compartilhamentos de auditoria em outros sites.

   - Se a implantação do StorageGRID for um único local, vá para a próxima etapa.
   - Se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:

     i. Inicie sessão remotamente no Admin Node do site:

        A. Introduza o seguinte comando: `ssh admin@`*`grid_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.

     ii. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó Admin adicional.

     iii. Feche o login de shell seguro remoto para o Admin Node remoto. Introduza: `exit`

9. Faça logout do shell de comando: `exit`

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento ou remova um cliente de auditoria existente removendo seu endereço IP.

#### Adicionar um cliente de auditoria NFS a um compartilhamento de auditoria

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento de auditoria.

**O que você vai precisar**

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).
- O cliente de auditoria deve estar usando o NFS versão 3 (NFSv3).

**Passos**

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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. Inicie o utilitário de configuração NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

3. Introduza: `add-ip-to-share`

   Uma lista de compartilhamentos de auditoria NFS habilitados no Admin Node é exibida. O compartilhamento de auditoria é listado como: `/var/local/audit/export`

4. Introduza o número da partilha de auditoria: *`audit_share_number`*
5. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: *`client_IP_address`*

   O cliente de auditoria é adicionado ao compartilhamento de auditoria.

6. Quando solicitado, pressione **Enter**.

   O utilitário de configuração NFS é exibido.

7. Repita as etapas para cada cliente de auditoria que deve ser adicionado ao compartilhamento de auditoria.
8. Opcionalmente, verifique sua configuração: `validate-config`

   Os serviços são verificados e exibidos.

   a. Quando solicitado, pressione **Enter**.

      O utilitário de configuração NFS é exibido.

9. Feche o utilitário de configuração NFS: `exit`
10. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

    Caso contrário, se a implantação do StorageGRID incluir nós de administração em outros sites, ative opcionalmente esses compartilhamentos de auditoria, conforme necessário:

    a. Faça login remotamente no Admin Node de um site:
       i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
       ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
       iii. Digite o seguinte comando para mudar para root: `su -`
       iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
    b. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.
    c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`
11. Faça logout do shell de comando: `exit`

#### Verificação da integração da auditoria NFS

Depois de configurar um compartilhamento de auditoria e adicionar um cliente de auditoria NFS, você pode montar o compartilhamento de cliente de auditoria e verificar se os arquivos estão disponíveis no compartilhamento de auditoria.

**Passos**

1. Verifique a conetividade (ou variante para o sistema cliente) usando o endereço IP do lado do cliente do nó Admin que hospeda o serviço AMS. Introduza: `ping IP_address`

   Verifique se o servidor responde, indicando conetividade.

2. Monte o compartilhamento de auditoria somente leitura usando um comando apropriado ao sistema operacional cliente. Um exemplo de comando Linux é (Enter em uma linha):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Use o endereço IP do nó de administração que hospeda o serviço AMS e o nome de compartilhamento predefinido para o sistema de auditoria. O ponto de montagem pode ser qualquer nome selecionado pelo cliente (por exemplo, `myAudit` no comando anterior).

3. Verifique se os arquivos estão disponíveis no compartilhamento de auditoria. Introduza: `ls myAudit /*`

```
`_myAudit_`onde está o ponto de montagem da partilha de auditoria. Deve
haver pelo menos um arquivo de log listado.
```

#### Remover um cliente de auditoria NFS do compartilhamento de auditoria

## Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Você pode remover um cliente de auditoria existente removendo seu endereço IP.

**O que você vai precisar**

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

**Sobre esta tarefa**

Não é possível remover o último endereço IP permitido para acessar o compartilhamento de auditoria.

**Passos**

1. Faça login no nó de administração principal:
   a. Introduza o seguinte comando: `ssh admin@primary_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. Inicie o utilitário de configuração NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

3. Remova o endereço IP do compartilhamento de auditoria: `remove-ip-from-share`

   Uma lista numerada de compartilhamentos de auditoria configurados no servidor é exibida. O compartilhamento de auditoria é listado como: `/var/local/audit/export`

4. Introduza o número correspondente à partilha de auditoria: *`audit_share_number`*

É apresentada uma lista numerada de endereços IP permitidos para aceder à partilha de auditoria.

5. Introduza o número correspondente ao endereço IP que pretende remover.

   O compartilhamento de auditoria é atualizado e o acesso não é mais permitido a partir de qualquer cliente de auditoria com este endereço IP.

6. Quando solicitado, pressione **Enter**.

   O utilitário de configuração NFS é exibido.

7. Feche o utilitário de configuração NFS: `exit`
8. Se a implantação do StorageGRID for uma implantação de vários locais de data center com nós de administração adicionais nos outros sites, desative esses compartilhamentos de auditoria conforme necessário:
   a. Faça login remotamente no Admin Node de cada site:
      i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
      ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
      iii. Digite o seguinte comando para mudar para root: `su -`
      iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
   b. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó Admin adicional.
   c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`
9. Faça logout do shell de comando: `exit`

#### Alterar o endereço IP de um cliente de auditoria NFS

1. Adicione um novo endereço IP a um compartilhamento de auditoria NFS existente.
2. Remova o endereço IP original.

#### Informações relacionadas

"Adicionar um cliente de auditoria NFS a um compartilhamento de auditoria"

"Remover um cliente de auditoria NFS do compartilhamento de auditoria"

# Gerenciando nós de arquivamento

Opcionalmente, cada um dos locais de data center do seu sistema StorageGRID pode ser implantado com um nó de arquivo, que permite que você se conete a um sistema de armazenamento de arquivamento externo direcionado, como o Gerenciador de armazenamento Tivoli (TSM).

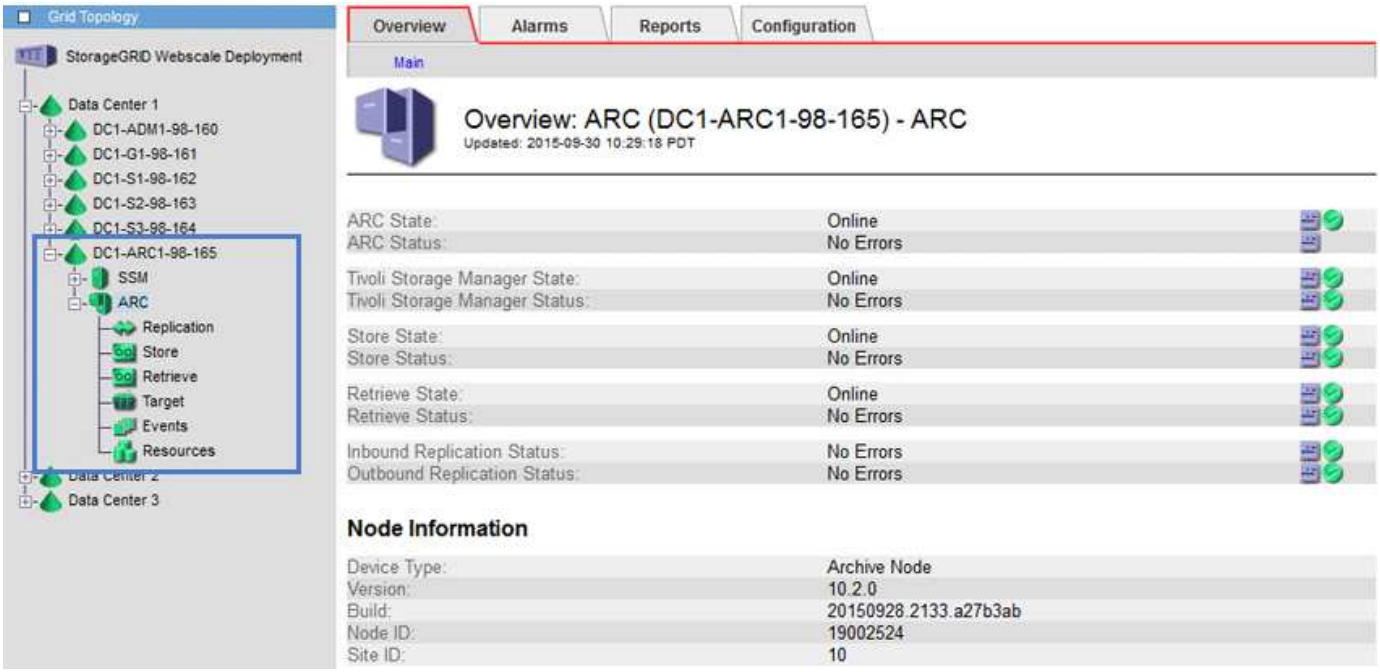
Depois de configurar as ligações ao destino externo, pode configurar o nó de arquivo para otimizar o desempenho do TSM, colocar um nó de arquivo offline quando um servidor TSM estiver a aproximar-se da capacidade ou indisponível, e configurar as definições de replicação e recuperação. Também pode definir alarmes personalizados para o nó de arquivo.

- "O que é um nó de arquivo"

- "Configurando conexões de nó de arquivo para armazenamento de arquivamento"
- "Definir alarmes personalizados para o nó de arquivo"
- "Integração do Tivoli Storage Manager"

## O que é um nó de arquivo

O Archive Node fornece uma interface através da qual você pode segmentar um sistema de storage de arquivamento externo para o armazenamento de dados de objetos a longo prazo. O nó de arquivo também monitora essa conexão e a transferência de dados de objetos entre o sistema StorageGRID e o sistema de armazenamento de arquivamento externo direcionado.




Os dados de objetos que não podem ser excluídos, mas não são acessados regularmente, podem, a qualquer momento, ser movidos dos discos giratórios de um nó de storage e para um storage de arquivamento externo, como a nuvem ou a fita. Este arquivamento de dados de objetos é realizado através da configuração do nó de arquivo de um site de data center e, em seguida, a configuração de regras ILM em que este nó de arquivo é selecionado como o "destino" para instruções de posicionamento de conteúdo. O nó de arquivo não gerencia os dados de objeto arquivados em si; isso é obtido pelo dispositivo de arquivamento externo.

Os metadados de objetos não são arquivados, mas permanecem em nós de storage.

### O que é o serviço ARC

O serviço Archive Node (ARC) fornece a interface de gerenciamento que você pode usar para configurar conexões com armazenamento de arquivos externo, como fita por meio do middleware TSM.

É o serviço ARC que interage com um sistema de armazenamento de arquivos externo, enviando dados de objetos para armazenamento near-line e realizando recuperações quando um aplicativo cliente solicita um objeto arquivado. Quando um aplicativo cliente solicita um objeto arquivado, um nó de armazenamento solicita os dados do objeto do serviço ARC. O serviço ARC faz uma solicitação para o sistema de armazenamento de

arquivos externo, que recupera os dados de objeto solicitados e os envia para o serviço ARC. O serviço ARC verifica os dados do objeto e os encaminha para o nó de armazenamento, que por sua vez retorna o objeto para o aplicativo cliente solicitante.

As solicitações de dados de objetos arquivados em fita por meio do middleware TSM são gerenciadas para eficiência de recuperações. As solicitações podem ser solicitadas para que os objetos armazenados em ordem sequencial na fita sejam solicitados na mesma ordem sequencial. As solicitações são então enfileiradas para envio para o dispositivo de armazenamento. Dependendo do dispositivo de arquivamento, várias solicitações de objetos em diferentes volumes podem ser processadas simultaneamente.

## Configurando conexões de nó de arquivo para armazenamento de arquivamento

Ao configurar um nó de arquivo para se conetar a um arquivo externo, você deve selecionar o tipo de destino.

O sistema StorageGRID suporta o arquivamento de dados de objetos para a nuvem através de uma interface S3 ou fita através do middleware Tivoli Storage Manager (TSM).

> Uma vez configurado o tipo de destino de arquivo para um nó de arquivo, o tipo de destino não pode ser alterado.

- "Arquivamento na nuvem por meio da API S3"
- "Arquivamento para fita através do middleware TSM"
- "Configurar as definições de recuperação do nó de arquivo"
- "Configurando a replicação do Archive Node"

### Arquivamento na nuvem por meio da API S3

Você pode configurar um nó de arquivo para se conetar diretamente à Amazon Web Services (AWS) ou a qualquer outro sistema que possa fazer interface com o sistema StorageGRID por meio da API S3.

> Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo por meio da API S3 foi substituído por ILM Cloud Storage Pools, que oferecem mais funcionalidade. A opção **Cloud Tiering - Simple Storage Service (S3)** ainda é suportada, mas você pode preferir implementar Cloud Storage Pools.

Se você estiver usando um nó de arquivamento com a opção **Cloud Tiering - Simple Storage Service (S3)**, considere migrar seus objetos para um pool de armazenamento em nuvem. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

#### Informações relacionadas

"Gerenciar objetos com ILM"

#### Configuração das configurações de conexão para a API S3

Se você estiver se conetando a um nó de Arquivo usando a interface S3, você deverá configurar as configurações de conexão para a API S3. Até que essas configurações sejam configuradas, o serviço ARC permanece em um estado de alarme principal, pois não é possível se comunicar com o sistema de armazenamento de arquivos externo.

Mover objetos de um nó de arquivamento para um sistema de armazenamento de arquivamento externo por meio da API S3 foi substituído por ILM Cloud Storage Pools, que oferecem mais funcionalidade. A opção **Cloud Tiering - Simple Storage Service (S3)** ainda é suportada, mas você pode preferir implementar Cloud Storage Pools.

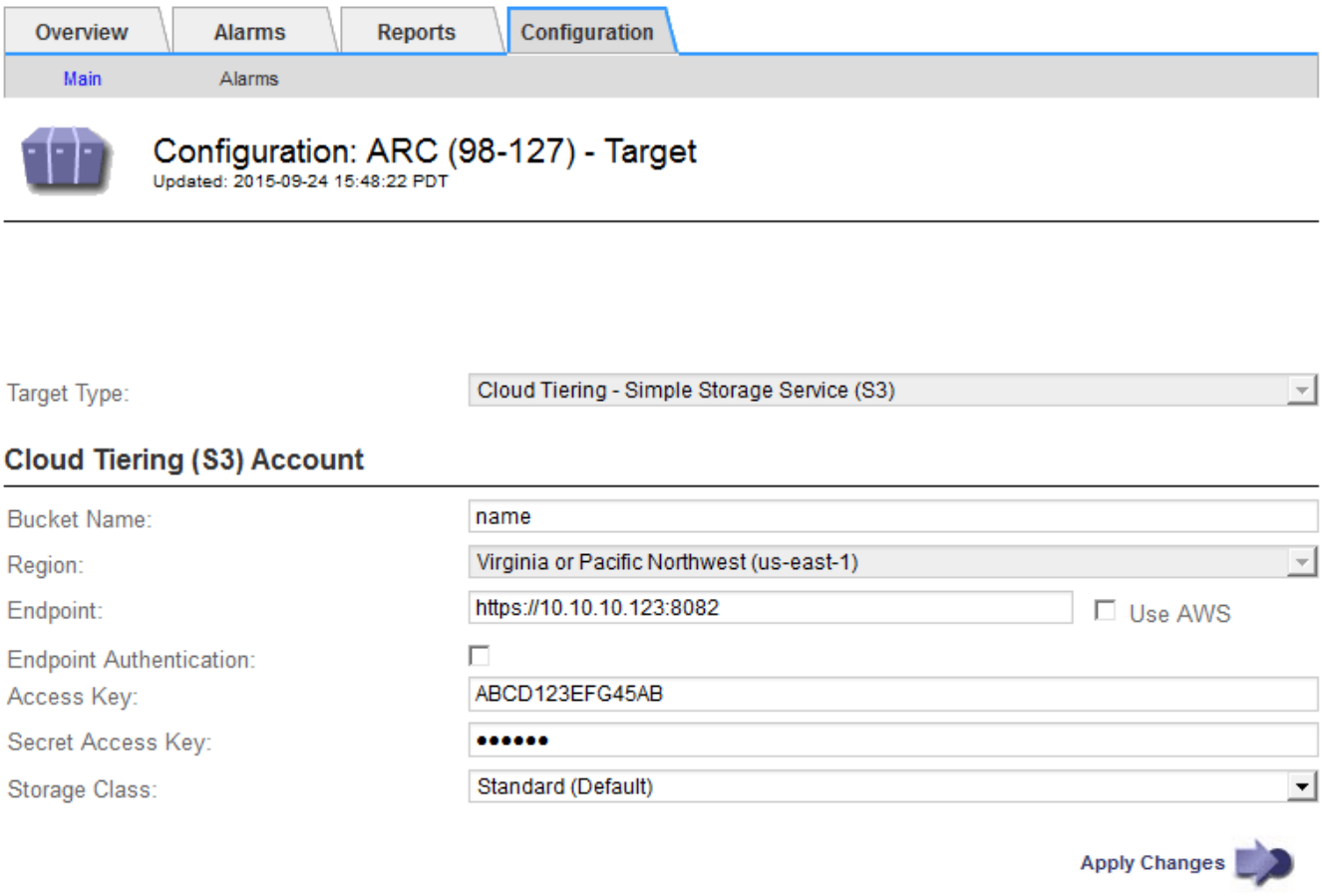
Se você estiver usando um nó de arquivamento com a opção **Cloud Tiering - Simple Storage Service (S3)**, considere migrar seus objetos para um pool de armazenamento em nuvem. Consulte as instruções para gerenciar objetos com gerenciamento do ciclo de vida das informações.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você precisa ter criado um bucket no sistema de storage de arquivamento de destino:
  - O bucket deve ser dedicado a um único nó de arquivo. Ele não pode ser usado por outros nós de arquivamento ou outras aplicações.
  - O balde tem de ter a região adequada selecionada para a sua localização.
  - O bucket deve ser configurado com o controle de versão suspenso.
- A Segmentação de objetos deve estar ativada e o tamanho máximo do segmento deve ser menor ou igual a 4,5 GiB (4.831.838.208 bytes). S3 solicitações de API que excederem esse valor falharão se S3 for usado como sistema de armazenamento de arquivamento externo.

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione **Archive Node** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.




4. Selecione **disposição em camadas na nuvem - Serviço de armazenamento simples (S3)** na lista suspensa tipo de destino.

   As configurações ficam indisponíveis até que você selecione um tipo de destino.

5. Configurar a conta Cloud Tiering (S3) através da qual o Archive Node se conetará ao sistema de storage de arquivamento externo de destino com capacidade para S3.

   A maioria dos campos nesta página são auto-explicativos. A seguir descreve os campos para os quais você pode precisar de orientação.

   - **Região**: Disponível somente se **usar AWS** estiver selecionado. A região selecionada tem de corresponder à região do balde.
   - **Endpoint** e **Use AWS**: Para Amazon Web Services (AWS), selecione **Use AWS**. **Endpoint** é então preenchido automaticamente com um URL de endpoint baseado nos atributos Nome do bucket e região. Por exemplo:

     ```
     https://bucket.region.amazonaws.com
     ```

     Para um destino que não seja AWS, insira o URL do sistema que hospeda o bucket, incluindo o número da porta. Por exemplo:

```
https://system.com:1080
```

   - **Autenticação de ponto final**: Ativada por padrão. Se a rede para o sistema de armazenamento de arquivos externo for confiável, você poderá desmarcar a caixa de seleção para desativar o certificado SSL de endpoint e a verificação de nome de host para o sistema de armazenamento de arquivos

externo de destino. Se outra instância de um sistema StorageGRID for o dispositivo de armazenamento de arquivamento de destino e o sistema estiver configurado com certificados assinados publicamente, você poderá manter a caixa de seleção selecionada.

- **Classe de armazenamento**: Selecione **Standard (padrão)** para armazenamento regular. Selecione **redundância reduzida** apenas para objetos que possam ser facilmente recriados. **Redundância reduzida** fornece armazenamento de menor custo com menos confiabilidade. Se o sistema de armazenamento de arquivos de destino for outra instância do sistema StorageGRID, **Classe de armazenamento** controla quantas cópias provisórias do objeto são feitas na ingestão no sistema de destino, se a confirmação dupla for usada quando os objetos forem ingeridos lá.

6. Clique em **aplicar alterações**.

   As configurações especificadas são validadas e aplicadas ao seu sistema StorageGRID. Uma vez configurado, o destino não pode ser alterado.

**Informações relacionadas**

"Gerenciar objetos com ILM"

#### Modificação das configurações de conexão para a API S3

Depois que o nó de arquivo é configurado para se conetar a um sistema de armazenamento de arquivos externo através da API S3, você pode modificar algumas configurações caso a conexão seja alterada.

**O que você vai precisar**

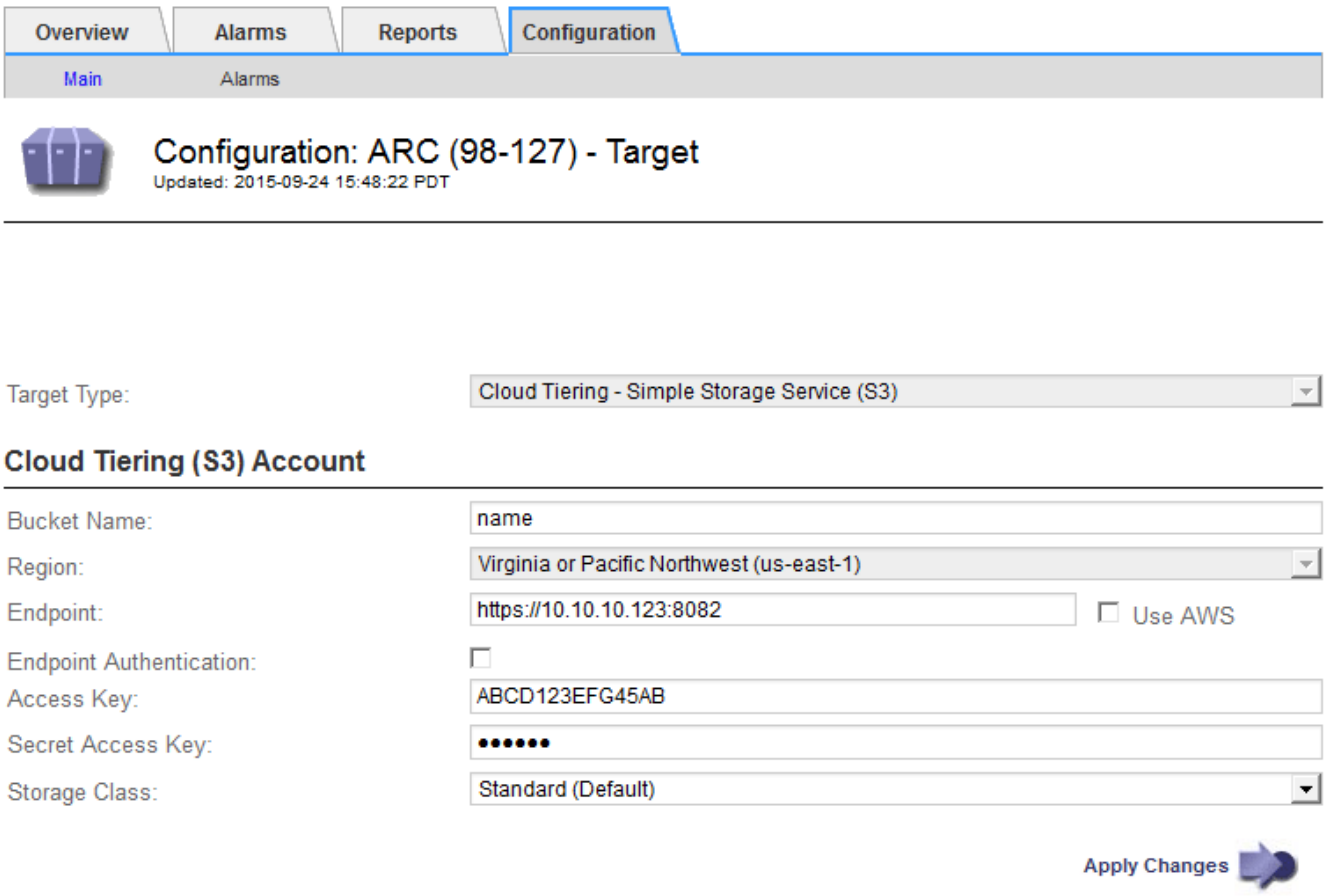
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

**Sobre esta tarefa**

Se você alterar a conta do Cloud Tiering (S3), deverá garantir que as credenciais de acesso do usuário tenham acesso de leitura/gravação ao bucket, incluindo todos os objetos que foram ingeridos anteriormente pelo Archive Node ao bucket.

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.




4. Modifique as informações da conta, conforme necessário.

   Se você alterar a classe de armazenamento, os novos dados de objeto serão armazenados com a nova classe de armazenamento. O objeto existente continua a ser armazenado sob o conjunto de classes de armazenamento quando ingerido.

   Nome do bucket, região e ponto final, use valores da AWS e não pode ser alterado.

5. Clique em **aplicar alterações**.

#### Modificação do estado Cloud Tiering Service

Você pode controlar a capacidade de leitura e gravação do nó de arquivamento no sistema de storage de arquivamento externo de destino que se conecta pela API S3, alterando o estado do Cloud Tiering Service.

**O que você vai precisar**

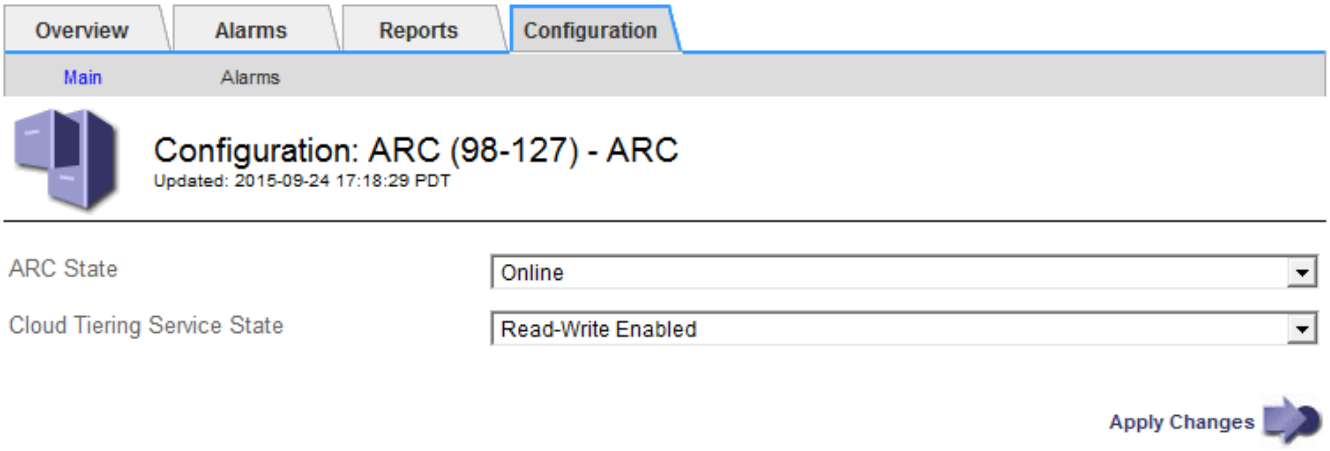
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- O nó de arquivo deve ser configurado.

**Sobre esta tarefa**

Você pode efetivamente colocar o nó de arquivo offline alterando o estado do Serviço de disposição em categorias na nuvem para **leitura-escrita desativada**.

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC**.
3. Selecione **Configuração** > **Principal**.




4. Selecione um **Estado do Serviço de disposição em camadas na nuvem**.
5. Clique em **aplicar alterações**.

#### Redefinir a contagem de falhas de armazenamento para conexão com a API S3

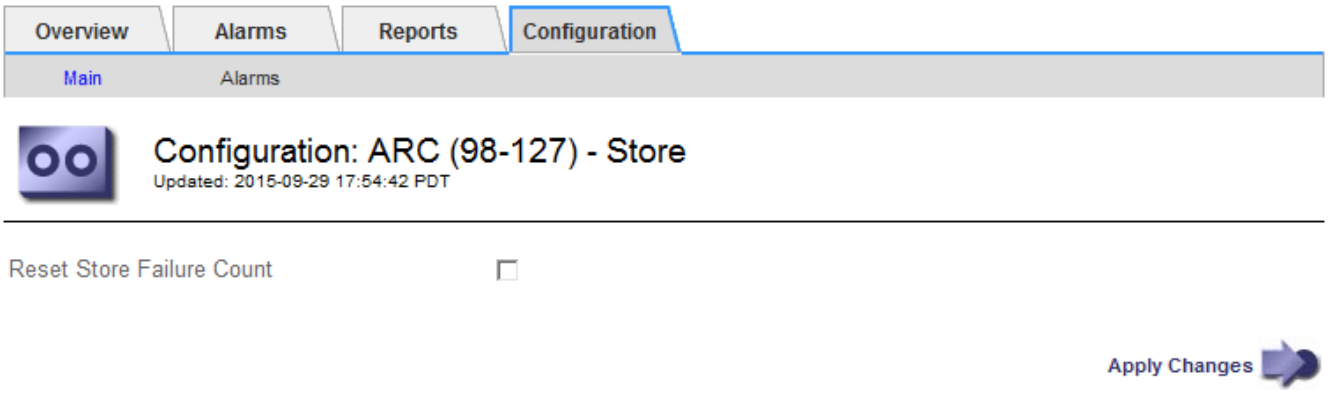
Se o seu nó de arquivo se conetar a um sistema de armazenamento de arquivos por meio da API S3, você poderá redefinir a contagem de falhas de armazenamento, que pode ser usada para limpar o alarme ARVF (falhas de armazenamento).

**O que você vai precisar**

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

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.




4. Selecione **Repor contagem de falhas de armazenamento**.

5. Clique em **aplicar alterações**.

   O atributo Store Failures (falhas de armazenamento) é reposto a zero.

#### Migração de objetos do Cloud Tiering - S3 para um Cloud Storage Pool

Se você estiver usando o recurso **Cloud Tiering - Simple Storage Service (S3)** para categorizar dados de objetos em um bucket do S3, considere migrar seus objetos para um pool de armazenamento em nuvem. Os pools de storage em nuvem fornecem uma abordagem dimensionável que aproveita todos os nós de storage do seu sistema StorageGRID.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você já armazenou objetos no bucket do S3 configurado para o Cloud Tiering.

> Antes de migrar dados de objeto, entre em Contato com o representante da conta do NetApp para entender e gerenciar quaisquer custos associados.

**Sobre esta tarefa**

Do ponto de vista do ILM, um Cloud Storage Pool é semelhante a um pool de storage. No entanto, embora os pools de storage consistam em nós de storage ou nós de arquivamento no sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo do S3.

Antes de migrar objetos do Cloud Tiering - S3 para um pool de armazenamento em nuvem, primeiro você deve criar um bucket do S3 e, em seguida, criar o pool de armazenamento em nuvem no StorageGRID. Em seguida, você pode criar uma nova política de ILM e substituir a regra ILM usada para armazenar objetos no bucket do Cloud Tiering por uma regra ILM clonada que armazena os mesmos objetos no Cloud Storage Pool.

> Quando os objetos são armazenados em um pool de storage de nuvem, as cópias desses objetos também não podem ser armazenadas no StorageGRID. Se a regra ILM que você está usando atualmente para o Cloud Tiering estiver configurada para armazenar objetos em vários locais ao mesmo tempo, considere se você ainda deseja executar essa migração opcional porque perderá essa funcionalidade. Se você continuar com essa migração, crie novas regras em vez de clonar as existentes.

**Passos**

1. Crie um pool de storage em nuvem.

   Use um novo bucket do S3 para o Cloud Storage Pool para garantir que ele contenha apenas os dados gerenciados pelo Cloud Storage Pool.

2. Localize quaisquer regras de ILM na política de ILM ativa que façam com que os objetos sejam armazenados no bucket do Cloud Tiering.
3. Clone cada uma dessas regras.
4. Nas regras clonadas, altere o local de posicionamento para o novo Cloud Storage Pool.
5. Salve as regras clonadas.

6. Crie uma nova política que use as novas regras.
7. Simule e ative a nova política.

   Quando a nova política é ativada e a avaliação ILM ocorre, os objetos são movidos do bucket do S3 configurado para o bucket do Cloud Tiering para o bucket do S3 configurado para o pool de armazenamento em nuvem. O espaço utilizável na grade não é afetado. Depois que os objetos são movidos para o Cloud Storage Pool, eles são removidos do bucket do Cloud Tiering.

**Informações relacionadas**

"Gerenciar objetos com ILM"

### Arquivamento para fita através de middleware TSM

Você pode configurar um nó de arquivo para segmentar um servidor Tivoli Storage Manager (TSM) que fornece uma interface lógica para armazenar e recuperar dados de objetos em dispositivos de armazenamento de acesso aleatório ou sequencial, incluindo bibliotecas de fitas.

O serviço ARC do Archive Node atua como um cliente para o servidor TSM, usando o Tivoli Storage Manager como middleware para comunicação com o sistema de armazenamento de arquivos.

#### Classes de gestão TSM

As classes de gerenciamento definidas pelo middleware TSM descrevem como as operações de backup e arquivamento do TSMs funcionam e podem ser usadas para especificar regras para conteúdo que são aplicadas pelo servidor TSM. Essas regras operam independentemente da política ILM do sistema StorageGRID e devem ser consistentes com o requisito do sistema StorageGRID de que os objetos são armazenados permanentemente e estão sempre disponíveis para recuperação pelo nó de arquivo. Depois que os dados do objeto são enviados para um servidor TSM pelo nó de arquivo, as regras de ciclo de vida e retenção do TSM são aplicadas enquanto os dados do objeto são armazenados em fita gerenciada pelo servidor TSM.

A classe de gerenciamento TSM é usada pelo servidor TSM para aplicar regras de localização ou retenção de dados depois que os objetos são enviados para o servidor TSM pelo nó de arquivamento. Por exemplo, os objetos identificados como backups de banco de dados (conteúdo temporário que pode ser substituído por dados mais recentes) podem ser tratados de forma diferente dos dados da aplicação (conteúdo fixo que deve ser mantido indefinidamente).

#### Configurando conexões com middleware TSM

Antes que o nó de arquivo possa se comunicar com o middleware Tivoli Storage Manager (TSM), você deve configurar várias configurações.

**O que você vai precisar**

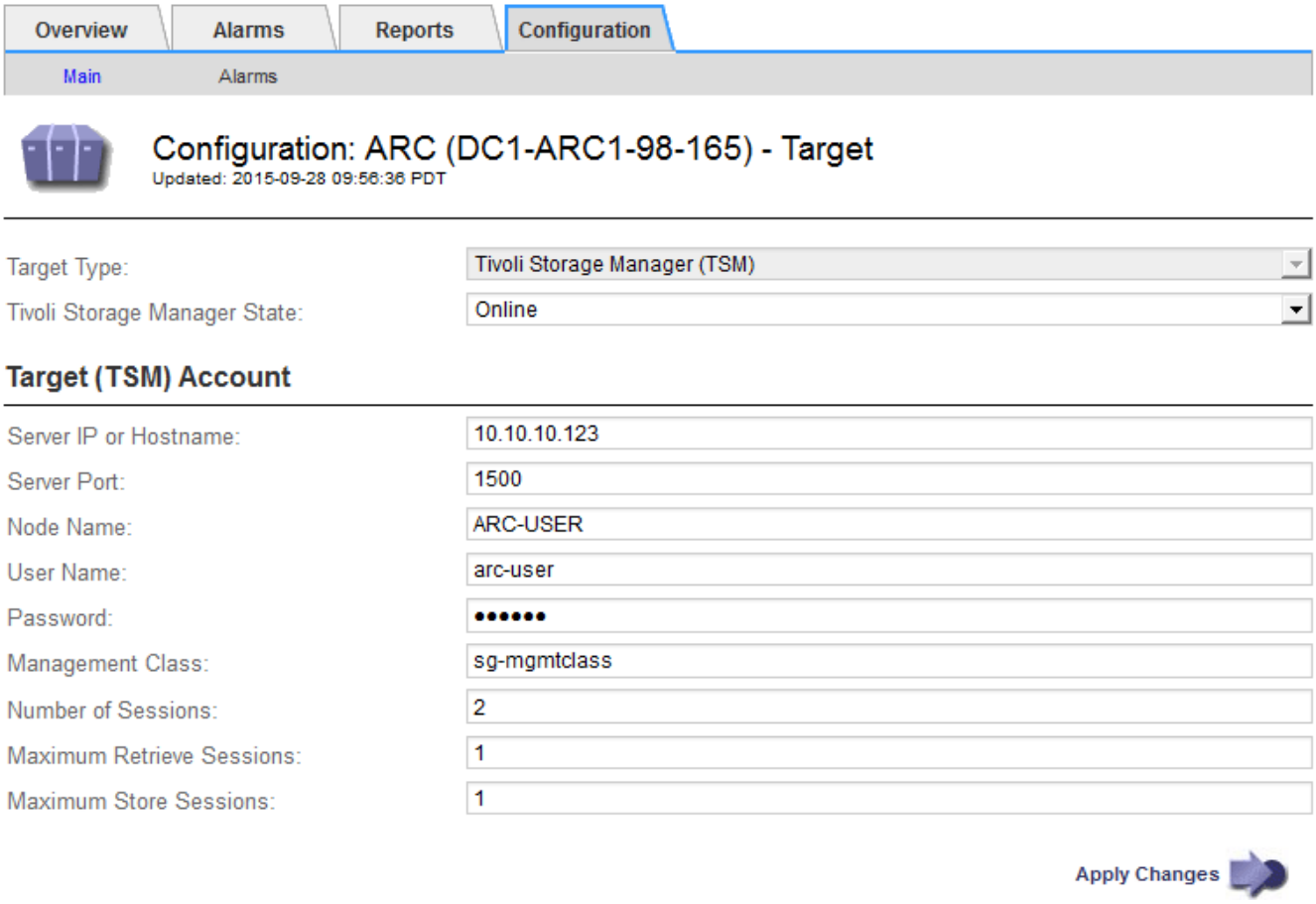
- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

**Sobre esta tarefa**

Até que essas configurações sejam configuradas, o serviço ARC permanece em um estado de alarme principal, pois não é possível se comunicar com o Tivoli Storage Manager.

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.




4. Na lista suspensa **tipo de destino**, selecione **Tivoli Storage Manager (TSM)**.
5. Para o **Tivoli Storage Manager State**, selecione **Offline** para evitar recuperações do servidor de middleware TSM.

   Por padrão, o Tivoli Storage Manager State é definido como Online, o que significa que o Archive Node é capaz de recuperar dados de objetos do servidor middleware TSM.

6. Preencha as seguintes informações:

   - **IP do servidor ou Nome de host**: Especifique o endereço IP ou nome de domínio totalmente qualificado do servidor middleware TSM usado pelo serviço ARC. O endereço IP padrão é 127,0.0,1.
   - **Server Port**: Especifique o número da porta no servidor middleware TSM ao qual o serviço ARC se conetará. A predefinição é 1500.
   - **Nome do nó**: Especifique o nome do nó de arquivo. Você deve inserir o nome (usuário ARC) registrado no servidor de middleware TSM.
   - **Nome de usuário**: Especifique o nome de usuário que o serviço ARC usa para fazer login no servidor TSM. Introduza o nome de utilizador predefinido (ARC-user) ou o utilizador administrativo que especificou para o nó de arquivo.
   - **Senha**: Especifique a senha usada pelo serviço ARC para fazer login no servidor TSM.

- **Classe de gerenciamento**: Especifique a classe de gerenciamento padrão a ser usada se uma classe de gerenciamento não for especificada quando o objeto estiver sendo salvo no sistema StorageGRID, ou a classe de gerenciamento especificada não estiver definida no servidor de middleware TSM.
- **Número de sessões**: Especifique o número de unidades de fita no servidor middleware TSM que são dedicadas ao nó de arquivo. O nó de arquivo cria simultaneamente um máximo de uma sessão por ponto de montagem mais um pequeno número de sessões adicionais (menos de cinco).

  Tem de alterar este valor para ser o mesmo que o valor definido para MAXNUMMP (número máximo de pontos de montagem) quando o nó de arquivo foi registado ou atualizado. (No comando register, o valor predefinido de MAXNUMMP utilizado é 1, se nenhum valor estiver definido.)

Você também deve alterar o valor de MAXSESSIONS para o servidor TSM para um número que seja pelo menos tão grande quanto o número de sessões definido para o serviço ARC. O valor padrão de MAXSESSIONS no servidor TSM é 25.

- * Sessões de recuperação máxima*: Especifique o número máximo de sessões que o serviço ARC pode abrir para o servidor middleware TSM para operações de recuperação. Na maioria dos casos, o valor apropriado é o número de sessões menos sessões de armazenamento máximo. Se você precisar compartilhar uma unidade de fita para armazenamento e recuperação, especifique um valor igual ao número de sessões.
- **Maximum Store Sessions**: Especifique o número máximo de sessões simultâneas que o serviço ARC pode abrir para o servidor middleware TSM para operações de arquivamento.

  Esse valor deve ser definido como um, exceto quando o sistema de armazenamento de arquivos de destino estiver cheio e somente recuperações podem ser executadas. Defina esse valor como zero para usar todas as sessões para recuperações.

7. Clique em **aplicar alterações**.

#### Otimizando um nó de arquivo para sessões de middleware TSM

## Você pode otimizar o desempenho de um nó de arquivo que se coneta ao Tivoli Server Manager (TSM) configurando as sessões do nó de arquivo.

**O que você vai precisar**

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

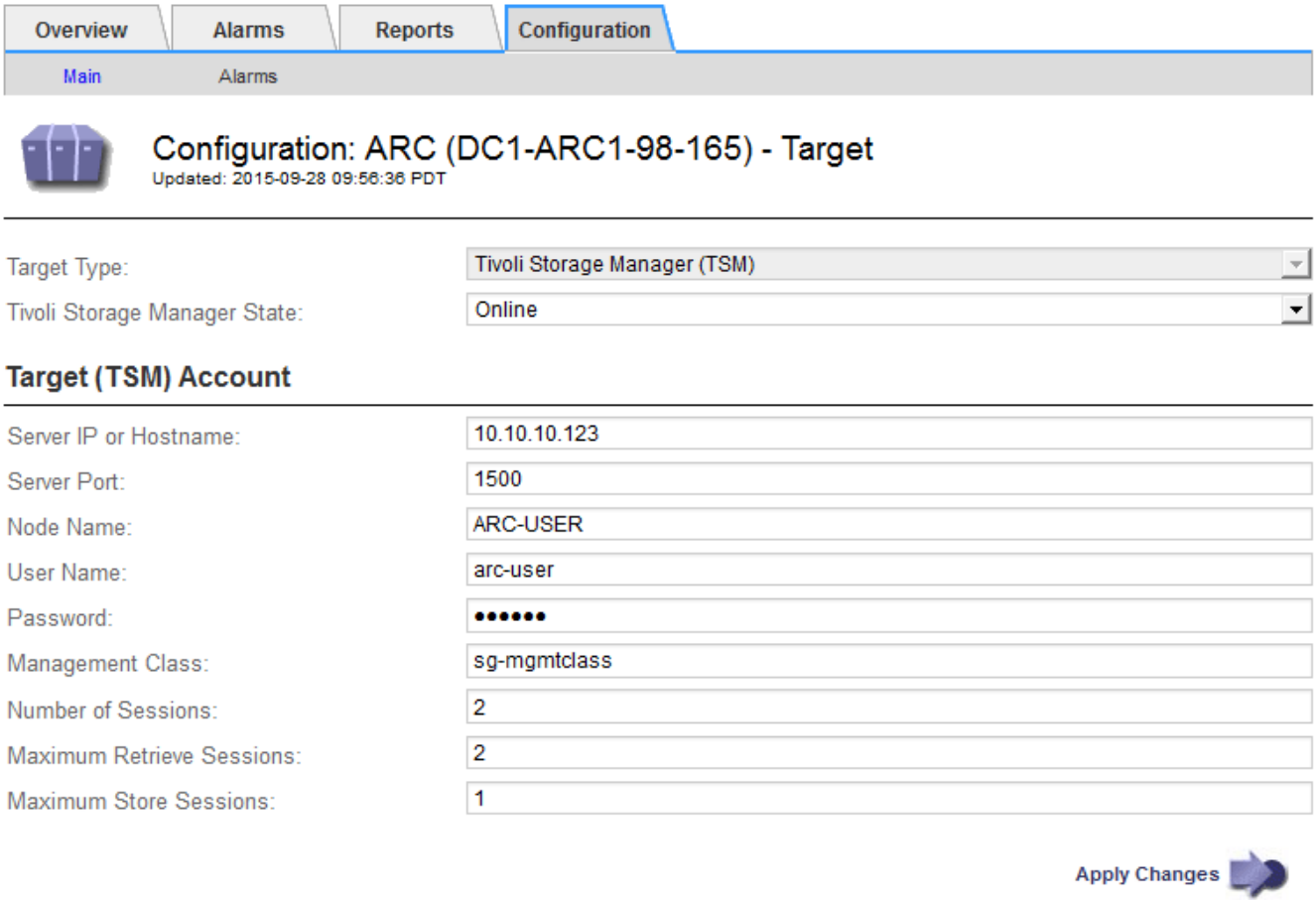
**Sobre esta tarefa**

Normalmente, o número de sessões simultâneas que o Archive Node tem aberto ao servidor middleware TSM é definido para o número de unidades de fita que o servidor TSM dedicou ao Archive Node. Uma unidade de fita é alocada para armazenamento enquanto o resto é alocado para recuperação. No entanto, em situações em que um nó de armazenamento está sendo reconstruído a partir de cópias do nó de arquivo ou o nó de arquivo está operando no modo somente leitura, você pode otimizar o desempenho do servidor TSM definindo o número máximo de sessões de recuperação para ser o mesmo que o número de sessões simultâneas. O resultado é que todas as unidades podem ser usadas simultaneamente para recuperação e, no máximo, uma dessas unidades também pode ser usada para armazenamento, se aplicável.

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.

3. Selecione **Configuração** > **Principal**.
4. Altere **sessões de recuperação máxima** para ser o mesmo que **número de sessões**.




5. Clique em **aplicar alterações**.

#### Configurar o estado de arquivo e contadores para TSM

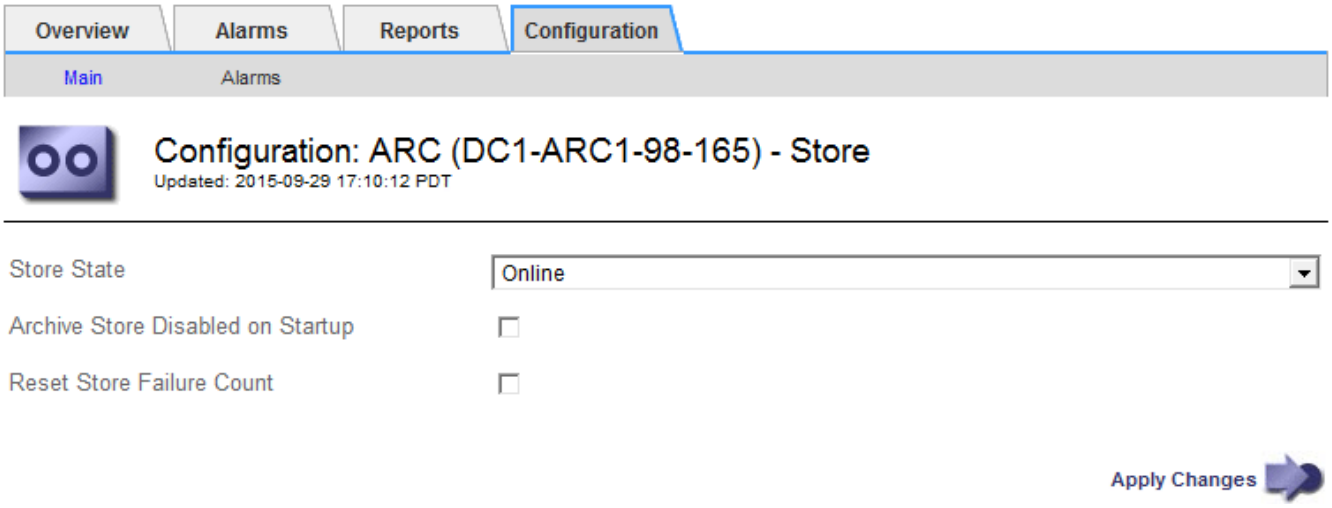
Se o seu Archive Node se conetar a um servidor middleware TSM, você poderá configurar o estado de armazenamento de arquivo de um Archive Node para Online ou Offline. Você também pode desativar o armazenamento de arquivos quando o nó de arquivo é iniciado pela primeira vez ou redefinir a contagem de falhas sendo rastreada para o alarme associado.

**O que você vai precisar**

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

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.




4. Modifique as seguintes definições, conforme necessário:
   - Estado da loja: Defina o estado do componente para:
     - On-line: O Archive Node está disponível para processar dados de objetos para armazenamento no sistema de armazenamento de arquivamento.
     - Offline: O nó de arquivo não está disponível para processar dados de objeto para armazenamento no sistema de armazenamento de arquivo.
   - Archive Store Disabled on Startup (armazenamento de arquivo desativado na inicialização): Quando selecionado, o componente Archive Store (armazenamento de arquivo) permanece no estado Read-Only (somente leitura) quando reiniciado. Usado para desativar persistentemente o armazenamento para o sistema de armazenamento de arquivo visado. Útil quando o sistema de armazenamento de arquivos visado não consegue aceitar conteúdo.
   - Repor contagem de falhas de armazenamento: Reponha o contador para falhas de armazenamento. Isso pode ser usado para limpar o alarme ARVF (falha de armazenamento).
5. Clique em **aplicar alterações**.

**Informações relacionadas**

"Gerenciando um nó de arquivo quando o servidor TSM atinge a capacidade"

#### Gerenciando um nó de arquivo quando o servidor TSM atinge a capacidade

O servidor TSM não tem como notificar o nó de arquivo quando o banco de dados TSM ou o armazenamento de Mídia de arquivamento gerenciado pelo servidor TSM estiver próximo da capacidade. O nó de arquivo continua a aceitar dados de objeto para transferência para o servidor TSM depois que o servidor TSM parar de aceitar novo conteúdo. Este conteúdo não pode ser gravado em Mídia gerenciada pelo servidor TSM. Um alarme é acionado se isso acontecer. Esta situação pode ser evitada através do monitoramento proativo do servidor TSM.

**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**

Para evitar que o serviço ARC envie mais conteúdo para o servidor TSM, você pode colocar o nó de Arquivo

offline, colocando o componente **ARC** > **Store** offline. Este procedimento também pode ser útil na prevenção de alarmes quando o servidor TSM não estiver disponível para manutenção.

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Store**.
3. Selecione **Configuração** > **Principal**.


4. Altere **Estado de armazenamento** para `Offline`.
5. Selecione **Archive Store Disabled on Startup**.
6. Clique em **aplicar alterações**.

### Configurando o Archive Node para somente leitura se o middleware TSM atingir a capacidade

Se o servidor de middleware TSM visado atingir a capacidade, o nó de arquivo pode ser otimizado para executar apenas recuperações.

**O que você vai precisar**

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

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Target**.
3. Selecione **Configuração** > **Principal**.
4. Altere as sessões de recuperação máxima para ser igual ao número de sessões simultâneas listadas em número de sessões.
5. Altere o máximo de sessões de armazenamento para 0.

> Não é necessário alterar o máximo de sessões de armazenamento para 0 se o nó de arquivo for apenas leitura. As sessões de armazenamento não serão criadas.

6. Clique em **aplicar alterações**.

### Configurar as definições de recuperação do nó de arquivo

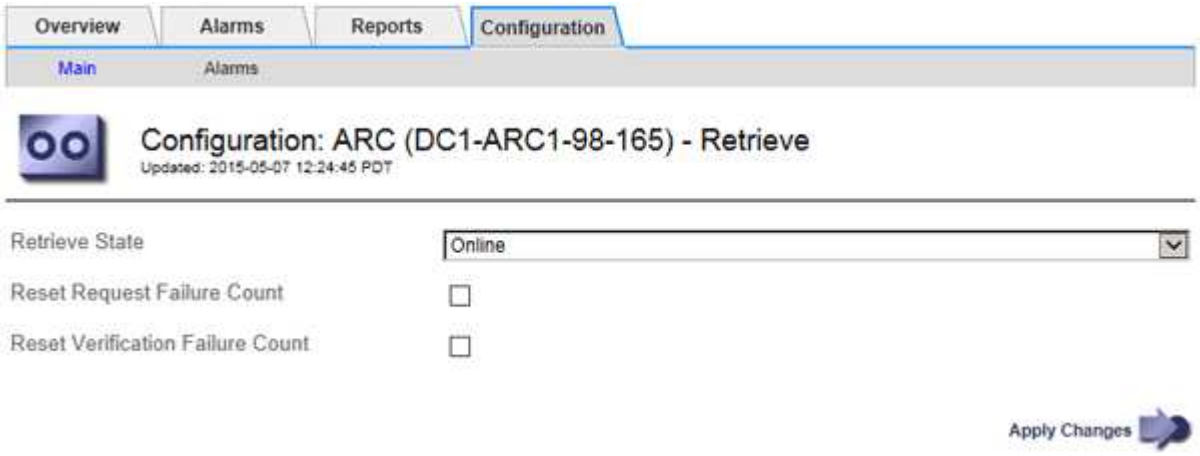
Você pode configurar as configurações de recuperação de um nó de arquivo para definir o estado como Online ou Offline, ou redefinir as contagens de falhas que estão sendo rastreadas para os alarmes associados.

#### O que você vai precisar

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

#### Passos

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione **Archive Node** > **ARC** > **Retrieve**.
3. Selecione **Configuração** > **Principal**.




4. Modifique as seguintes definições, conforme necessário:
   - **Retrieve State**: Defina o estado do componente para:
     - On-line: O nó de grade está disponível para recuperar dados de objeto do dispositivo de Mídia de arquivamento.
     - Offline: O nó de grade não está disponível para recuperar dados de objeto.
   - Reset Request Failures Count (Redefinir contagem de falhas de pedido): Selecione a caixa de verificação para repor o contador para falhas de pedido. Isso pode ser usado para limpar o alarme ARRF (falhas de solicitação).
   - Redefinir contagem de falhas de verificação: Marque a caixa de seleção para redefinir o contador para falhas de verificação em dados de objetos recuperados. Isso pode ser usado para limpar o alarme ARRV (falhas de verificação).
5. Clique em **aplicar alterações**.

### Configurando a replicação do Archive Node

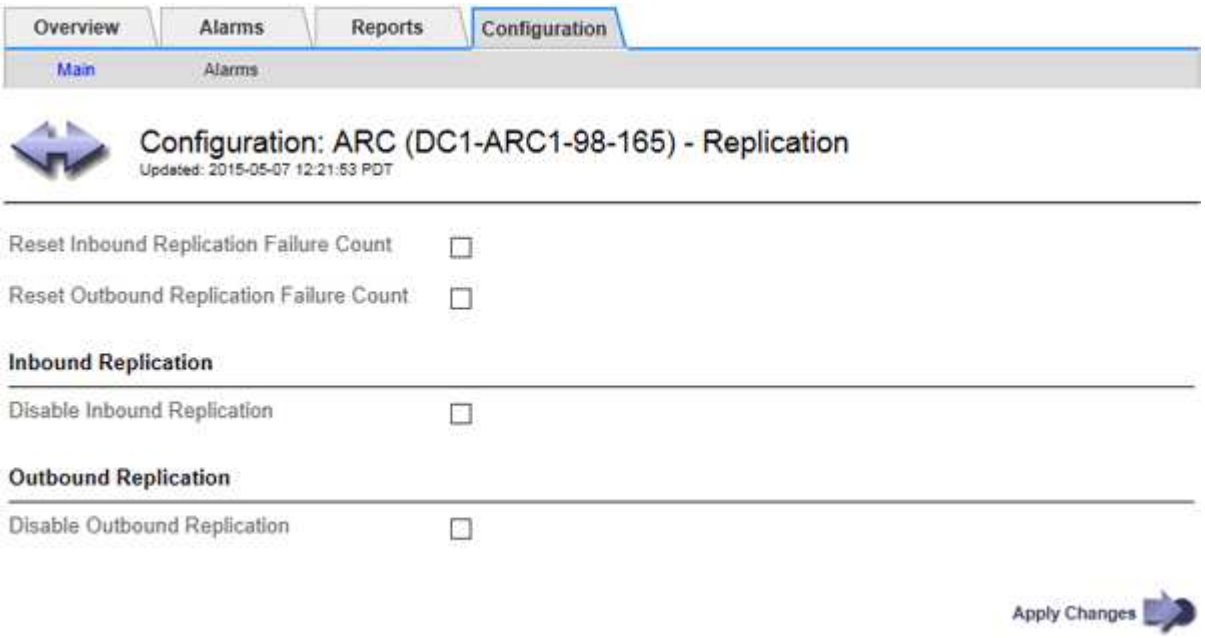
Você pode configurar as configurações de replicação para um nó de arquivo e desativar a replicação de entrada e saída ou redefinir as contagens de falha que estão sendo rastreadas para os alarmes associados.

#### O que você vai precisar

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

**Passos**

1. Selecione **Support** > **Tools** > **Grid Topology**.
2. Selecione ***Archive Node*** > **ARC** > **Replication**.
3. Selecione **Configuração** > **Principal**.




4. Modifique as seguintes definições, conforme necessário:
   - **Redefinir contagem de falhas de replicação de entrada**: Selecione para redefinir o contador para falhas de replicação de entrada. Isso pode ser usado para limpar o alarme RIRF (replicações embutidas — Failed).
   - **Redefinir contagem de falhas de replicação de saída**: Selecione para redefinir o contador para falhas de replicação de saída. Isso pode ser usado para limpar o alarme RORF (Outbound replicações — Failed).
   - **Desativar replicação de entrada**: Selecione para desativar a replicação de entrada como parte de um procedimento de manutenção ou teste. Deixe limpo durante o funcionamento normal.

     Quando a replicação de entrada é desativada, os dados de objeto podem ser recuperados do serviço ARC para replicação para outros locais no sistema StorageGRID, mas os objetos não podem ser replicados para este serviço ARC a partir de outros locais do sistema. O serviço ARC é apenas de leitura.

   - **Desativar replicação de saída**: Marque a caixa de seleção para desativar a replicação de saída (incluindo solicitações de conteúdo para recuperações HTTP) como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal.

     Quando a replicação de saída é desativada, os dados de objeto podem ser copiados para este serviço ARC para satisfazer as regras ILM, mas os dados de objeto não podem ser recuperados do serviço ARC para serem copiados para outros locais no sistema StorageGRID. O serviço ARC é apenas de escrita.

5. Clique em **aplicar alterações**.

## Definir alarmes personalizados para o nó de arquivo

Você deve estabelecer alarmes personalizados para os atributos ARQL e ARRL que são usados para monitorar a velocidade e eficiência da recuperação de dados de objetos do sistema de armazenamento de arquivos pelo nó Archive.

- ARQL: Comprimento médio da fila. O tempo médio, em microssegundos, em que os dados do objeto são enfileirados para recuperação do sistema de armazenamento de arquivamento.
- ARRL: Latência média da solicitação. O tempo médio, em microssegundos, necessário pelo nó de arquivo para recuperar dados de objetos do sistema de armazenamento de arquivamento.

Os valores aceitáveis para esses atributos dependem de como o sistema de armazenamento de arquivos é configurado e usado. (Vá para **ARC** > **Retrieve** > **Overview** > **Main**.) Os valores definidos para tempos limite de solicitação e o número de sessões disponibilizadas para solicitações de recuperação são particularmente influentes.

Depois que a integração estiver concluída, monitorize as recuperações de dados de objetos do nó de Arquivo para estabelecer valores para tempos de recuperação normais e comprimentos de fila. Em seguida, crie alarmes personalizados para ARQL e ARRL que serão acionados se surgir uma condição operacional anormal.

#### Informações relacionadas

"Monitorizar Resolução de problemas"

## Integração do Tivoli Storage Manager

Esta seção inclui as melhores práticas e informações de configuração para integrar um nó de arquivo com um servidor Tivoli Storage Manager (TSM), incluindo detalhes operacionais do nó de arquivo que afetam a configuração do servidor TSM.

- "Configuração e operação do nó de arquivamento"
- "Práticas recomendadas de configuração"
- "Concluir a configuração do nó de arquivo"

#### Configuração e operação do nó de arquivamento

Seu sistema StorageGRID gerencia o nó de arquivo como um local onde os objetos são armazenados indefinidamente e são sempre acessíveis.

Quando um objeto é ingerido, cópias são feitas em todos os locais necessários, incluindo nós de arquivo, com base nas regras de gerenciamento do ciclo de vida da informação (ILM) definidas para o seu sistema StorageGRID. O nó de arquivo atua como um cliente para um servidor TSM, e as bibliotecas de cliente TSM são instaladas no nó de arquivo pelo processo de instalação do software StorageGRID. Os dados do objeto direcionados para o nó de arquivo para armazenamento são salvos diretamente no servidor TSM à medida que são recebidos. O nó de arquivo não armazena os dados do objeto antes de salvá-los no servidor TSM, nem realiza agregação de objetos. No entanto, o nó de arquivo pode enviar várias cópias para o servidor TSM em uma única transação quando as taxas de dados são garantidas.

Depois que o nó de arquivo salva os dados do objeto no servidor TSM, os dados do objeto são gerenciados

pelo servidor TSM usando suas políticas de ciclo de vida/retenção. Essas políticas de retenção devem ser definidas para serem compatíveis com a operação do nó de arquivo. Ou seja, os dados de objeto salvos pelo nó de arquivo devem ser armazenados indefinidamente e devem sempre ser acessíveis pelo nó de arquivo, a menos que sejam excluídos pelo nó de arquivo.

Não há conexão entre as regras de ILM do sistema StorageGRID e as políticas de ciclo de vida/retenção do servidor TSM. Cada um opera independentemente do outro; no entanto, à medida que cada objeto é ingerido no sistema StorageGRID, você pode atribuir a ele uma classe de gerenciamento TSM. Essa classe de gerenciamento é passada para o servidor TSM junto com os dados do objeto. A atribuição de diferentes classes de gerenciamento a diferentes tipos de objetos permite configurar o servidor TSM para colocar dados de objetos em diferentes pools de armazenamento ou aplicar diferentes políticas de migração ou retenção, conforme necessário. Por exemplo, os objetos identificados como backups de banco de dados (conteúdo temporário que pode ser substituído por dados mais recentes) podem ser tratados de forma diferente dos dados da aplicação (conteúdo fixo que deve ser mantido indefinidamente).

O nó de arquivo pode ser integrado a um servidor TSM novo ou existente; ele não requer um servidor TSM dedicado. Os servidores TSM podem ser compartilhados com outros clientes, desde que o servidor TSM seja dimensionado adequadamente para a carga máxima esperada. O TSM deve ser instalado em um servidor ou máquina virtual separado do nó de arquivo.

É possível configurar mais de um nó de arquivo para gravar no mesmo servidor TSM; no entanto, esta configuração só é recomendada se os nós de arquivo gravarem conjuntos diferentes de dados no servidor TSM. A configuração de mais de um nó de arquivo para gravação no mesmo servidor TSM não é recomendada quando cada nó de arquivo grava cópias dos mesmos dados de objeto no arquivo. No último cenário, ambas as cópias estão sujeitas a um único ponto de falha (o servidor TSM) para o que é suposto ser cópias independentes e redundantes de dados de objeto.

Os nós de arquivamento não fazem uso do componente HSM (Hierarchical Storage Management) do TSM.

**Práticas recomendadas de configuração**

## Quando você está dimensionando e configurando seu servidor TSM, existem práticas recomendadas que você deve aplicar para otimizá-lo para trabalhar com o nó de Arquivo.

Ao dimensionar e configurar o servidor TSM, você deve considerar os seguintes fatores:

- Como o nó de arquivo não agrega objetos antes de salvá-los no servidor TSM, o banco de dados TSM deve ser dimensionado para conter referências a todos os objetos que serão gravados no nó de arquivo.
- O software Archive Node não pode tolerar a latência envolvida na gravação de objetos diretamente na fita ou em outra Mídia removível. Portanto, o servidor TSM deve ser configurado com um pool de armazenamento de disco para o armazenamento inicial de dados salvos pelo nó de arquivo sempre que Mídia removível for usada.
- Você deve configurar políticas de retenção de TSM para usar a retenção baseada em eventos. O nó de arquivo não suporta políticas de retenção de TSM baseadas na criação. Use as seguintes configurações recomendadas de retmin.0 e retver.0 na política de retenção (que indica que a retenção começa quando o nó de arquivamento aciona um evento de retenção e é mantido por 0 dias depois disso). No entanto, esses valores para retmin e retver são opcionais.

O pool de discos deve ser configurado para migrar dados para o pool de fitas (ou seja, o pool de fitas deve ser o NXTSTGPOOL do pool de discos). O pool de fitas não deve ser configurado como um pool de cópias do pool de discos com gravação simultânea em ambos os pools (ou seja, o pool de fitas não pode ser um COPYSTGPOOL para o pool de discos). Para criar cópias off-line das fitas que contêm dados do Archive

Node, configure o servidor TSM com um segundo pool de fitas que é um pool de cópias do pool de fitas usado para dados do Archive Node.

#### Concluir a configuração do nó de arquivo

O nó de arquivo não funciona depois de concluir o processo de instalação. Antes que o sistema StorageGRID possa salvar objetos no nó de arquivo TSM, você deve concluir a instalação e configuração do servidor TSM e configurar o nó de arquivo para se comunicar com o servidor TSM.

Para obter mais informações sobre como otimizar as sessões de recuperação e armazenamento do TSM, consulte informações sobre como gerenciar o armazenamento de arquivos.

- "Gerenciando nós de arquivamento"

Consulte a seguinte documentação da IBM, conforme necessário, enquanto prepara o servidor TSM para integração com o nó de arquivo em um sistema StorageGRID:

- "Guia de instalação e do usuário dos drivers de dispositivo de fita IBM"
- "Referência de programação de drivers de dispositivo de fita IBM"

##### Instalar um novo servidor TSM

Você pode integrar o nó de arquivo a um servidor TSM novo ou existente. Se você estiver instalando um novo servidor TSM, siga as instruções na documentação do TSM para concluir a instalação.

> Um nó de arquivo não pode ser co-hospedado com um servidor TSM.

##### Configurando o servidor TSM

Esta seção inclui instruções de exemplo para preparar um servidor TSM seguindo as práticas recomendadas do TSM.

As instruções a seguir o orientam durante o processo de:

- Definir um pool de armazenamento em disco e um pool de armazenamento em fita (se necessário) no servidor TSM
- Definir uma política de domínio que utilize a classe de gestão TSM para os dados guardados a partir do nó de arquivo e registar um nó para utilizar esta política de domínio

Estas instruções são fornecidas apenas para a sua orientação; não se destinam a substituir a documentação do TSM ou a fornecer instruções completas e abrangentes adequadas para todas as configurações. Instruções específicas de implantação devem ser fornecidas por um administrador do TSM que esteja familiarizado com seus requisitos detalhados e com o conjunto completo de documentação do TSM Server.

##### Definição de conjuntos de armazenamento em disco e fita TSM

O nó de arquivamento grava em um pool de armazenamento em disco. Para arquivar conteúdo em fita, você deve configurar o pool de armazenamento em disco para mover o conteúdo para um pool de armazenamento em fita.

**Sobre esta tarefa**

Para um servidor TSM, você deve definir um pool de armazenamento em fita e um pool de armazenamento em disco no Tivoli Storage Manager. Depois que o pool de discos for definido, crie um volume de disco e atribua-o ao pool de discos. Não é necessário um pool de fitas se o servidor TSM usar storage somente em disco.

Você deve concluir várias etapas em seu servidor TSM antes de criar um pool de armazenamento de fita. (Crie uma biblioteca de fitas e pelo menos uma unidade na biblioteca de fitas. Defina um caminho do servidor para a biblioteca e do servidor para as unidades e, em seguida, defina uma classe de dispositivo para as unidades.) Os detalhes dessas etapas podem variar dependendo da configuração de hardware e dos requisitos de armazenamento do site. Para obter mais informações, consulte a documentação do TSM.

O seguinte conjunto de instruções ilustra o processo. Você deve estar ciente de que os requisitos para o seu site podem ser diferentes, dependendo dos requisitos da sua implantação. Para obter detalhes de configuração e instruções, consulte a documentação do TSM.

Você deve fazer logon no servidor com Privileges administrativo e usar a ferramenta dsmadmc para executar os seguintes comandos.

**Passos**

1. Crie uma biblioteca de fitas.

   `define library tapelibrary libtype=scsi`

   ```
   `_tapelibrary_`Onde é escolhido um nome arbitrário para a biblioteca de fitas, e o valor de `libtype` pode variar dependendo do tipo de biblioteca de fitas.
   ```

2. Defina um caminho do servidor para a biblioteca de fitas.

   `define path servername tapelibrary srctype=server desttype=library device=lib-devicename`

   - *servername* É o nome do servidor TSM
   - *tapelibrary* é o nome da biblioteca de fitas que você definiu
   - *lib-devicename* é o nome do dispositivo para a biblioteca de fitas

3. Defina uma unidade para a biblioteca.

   `define drive tapelibrary drivename`

   - *drivename* é o nome que você deseja especificar para a unidade
   - *tapelibrary* é o nome da biblioteca de fitas que você definiu

     Você pode querer configurar uma unidade ou unidades adicionais, dependendo da configuração do hardware. (Por exemplo, se o servidor TSM estiver conetado a um switch Fibre Channel que tenha duas entradas de uma biblioteca de fitas, talvez você queira definir uma unidade para cada entrada.)

4. Defina um caminho do servidor para a unidade definida.

```
define path servername drivename srctype=server desttype=drive
library=tapelibrary device=drive-dname
```

- *drive-dname* é o nome do dispositivo para a unidade
- *tapelibrary* é o nome da biblioteca de fitas que você definiu

  Repita para cada unidade definida para a biblioteca de fitas, usando uma unidade *drivename* separada e *drive-dname* para cada unidade.

5. Defina uma classe de dispositivo para as unidades.

```
define devclass DeviceClassName devtype=lto library=tapelibrary
format=tapetype
```

- *DeviceClassName* é o nome da classe de dispositivo
- *lto* é o tipo de unidade conetada ao servidor
- *tapelibrary* é o nome da biblioteca de fitas que você definiu
- *tapetype* é o tipo de fita; por exemplo, ultrium3

6. Adicione volumes de fita ao inventário da biblioteca.

```
checkin libvolume tapelibrary
```

*tapelibrary* é o nome da biblioteca de fitas que você definiu.

7. Crie o pool de armazenamento de fita primário.

```
define stgpool SGWSTapePool DeviceClassName description=description
collocate=filespace maxscratch=XX
```

- *SGWSTapePool* É o nome do conjunto de armazenamento de fita do nó de arquivo. Você pode selecionar qualquer nome para o pool de armazenamento de fita (desde que o nome use as convenções de sintaxe esperadas pelo servidor TSM).
- *DeviceClassName* é o nome do nome da classe do dispositivo para a biblioteca de fitas.
- *description* É uma descrição do pool de armazenamento que pode ser exibido no servidor TSM usando o `query stgpool` comando. Por exemplo: "'conjunto de armazenamento de fita para o nó de arquivo.'"
- *collocate=filespace* Especifica que o servidor TSM deve gravar objetos do mesmo espaço de arquivo em uma única fita.
- XX é um dos seguintes:
  - O número de fitas vazias na biblioteca de fitas (caso o nó de arquivo seja o único aplicativo que usa a biblioteca).
  - O número de fitas alocadas para uso pelo sistema StorageGRID (nos casos em que a biblioteca de fitas é compartilhada).

8. Em um servidor TSM, crie um pool de armazenamento em disco. Na consola administrativa do servidor TSM, introduza

```
define stgpool SGWSDiskPool disk description=description
```

`maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high lowmig=percent_low`

- *SGWSDiskPool* É o nome do conjunto de discos do nó de arquivo. Você pode selecionar qualquer nome para o pool de armazenamento em disco (desde que o nome use as convenções de sintaxe esperadas pelo TSM).
- *description* É uma descrição do pool de armazenamento que pode ser exibido no servidor TSM usando o `query stgpool` comando. Por exemplo, ""conjunto de armazenamento em disco para o nó de arquivo".
- *maximum_file_size* força objetos maiores do que esse tamanho a serem gravados diretamente na fita, em vez de serem armazenados em cache no pool de discos. Recomenda-se definir *maximum_file_size* para 10 GB.
- *nextstgpool=SGWSTapePool* Refere o pool de armazenamento em disco ao pool de armazenamento em fita definido para o nó de arquivo.
- *percent_high* define o valor no qual o pool de discos começa a migrar seu conteúdo para o pool de fitas. Recomenda-se definir *percent_high* como 0 para que a migração de dados comece imediatamente
- *percent_low* define o valor no qual a migração para o conjunto de fitas pára. Recomenda-se definir *percent_low* como 0 para limpar o pool de discos.

9. Em um servidor TSM, crie um volume de disco (ou volumes) e atribua-o ao pool de discos.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* é o nome do pool de discos.
   - *volume_name* É o caminho completo para o local do volume (por exemplo, `/var/local/arc/stage6.dsm` ) no servidor TSM onde grava o conteúdo do pool de discos em preparação para transferência para fita.
   - *size* É o tamanho, em MB, do volume do disco.

     Por exemplo, para criar um único volume de disco de modo que o conteúdo de um pool de discos preencha uma única fita, defina o valor de tamanho como 200000 quando o volume da fita tiver uma capacidade de 200 GB.

     No entanto, pode ser desejável criar vários volumes de disco de um tamanho menor, já que o servidor TSM pode gravar em cada volume no pool de discos. Por exemplo, se o tamanho da fita for de 250 GB, crie 25 volumes de disco com um tamanho de 10 GB (10000) cada.

   O servidor TSM prealoca espaço no diretório para o volume de disco. Isso pode levar algum tempo para ser concluído (mais de três horas para um volume de disco de 200 GB).

#### Definir uma política de domínio e registar um nó

Você precisa definir uma política de domínio que use a classe de gerenciamento TSM para os dados salvos do nó de arquivamento e, em seguida, Registrar um nó para usar essa diretiva de domínio.

Os processos do nó de arquivamento podem vazar memória se a senha do cliente para o nó de arquivamento no Tivoli Storage Manager (TSM) expirar. Certifique-se de que o servidor TSM está configurado para que o nome de utilizador/palavra-passe do cliente para o nó de arquivo nunca expire.

Ao Registrar um nó no servidor TSM para o uso do nó de arquivo (ou atualizar um nó existente), você deve especificar o número de pontos de montagem que o nó pode usar para operações de gravação especificando o parâmetro MAXNUMMP para o comando DE NÓ DE REGISTRO. O número de pontos de montagem é normalmente equivalente ao número de cabeças de unidade de fita alocadas ao nó de arquivo. O número especificado para MAXNUMMP no servidor TSM deve ser pelo menos tão grande quanto o valor definido para **ARC** > **Target** > **Configuration** > **Main** > **Maximum Store Sessions** para o Archive Node, que é definido para um valor de 0 ou 1, já que as sessões de armazenamento simultâneas não são suportadas pelo Archive Node.

O valor de MAXSESSIONS definido para o servidor TSM controla o número máximo de sessões que podem ser abertas para o servidor TSM por todos os aplicativos clientes. O valor de MAXSESSIONS especificado no TSM deve ser pelo menos tão grande quanto o valor especificado para **ARC** > **Target** > **Configuration** > **Main** > **Number of Sessions** no Grid Manager para o Archive Node. O nó de arquivo cria simultaneamente, no máximo, uma sessão por ponto de montagem, mais um pequeno número (inferior a 5) de sessões adicionais.

O nó TSM atribuído ao nó de arquivo usa uma política de domínio personalizada `tsm-domain` . A `tsm-domain` política de domínio é uma versão modificada da política de domínio "sandard", configurada para gravar em fita e com o destino do arquivo definido como o pool de armazenamento do sistema StorageGRID (*`SGWSDiskPool`*).

Você deve fazer login no servidor TSM com Privileges administrativo e usar a ferramenta dsmadmc para criar e ativar a diretiva de domínio.

#### Criando e ativando a política de domínio

Você deve criar uma política de domínio e ativá-la para configurar o servidor TSM para salvar os dados enviados do nó de Arquivo.

**Passos**

1. Crie uma política de domínio.

   ```
   copy domain standard tsm-domain
   ```

2. Se você não estiver usando uma classe de gerenciamento existente, insira uma das seguintes opções:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   *`default`* é a classe de gerenciamento padrão para a implantação.

3. Crie um copygroup para o pool de armazenamento apropriado. Introduza (numa linha):

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

*default* É a classe de gerenciamento padrão para o nó de arquivo. Os valores de `retinit`, `retmin` e `retver` foram escolhidos para refletir o comportamento de retenção atualmente utilizado pelo nó de arquivo

> Não defina `retinit` para `retinit=create`. A configuração `retinit=create` impede que o nó de arquivo exclua conteúdo, uma vez que os eventos de retenção são usados para remover conteúdo do servidor TSM.

4. Atribua a classe de gerenciamento como padrão.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Defina o novo conjunto de políticas como ativo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignore o aviso "'no backup copy group'" que aparece quando você digita o comando Activate.

6. Registre um nó para usar o novo conjunto de políticas no servidor TSM. No servidor TSM, introduza (numa linha):

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   ARC-user e ARC-password são o mesmo nome de nó de cliente e palavra-passe definidos no nó de arquivo, e o valor de MAXNUMMP é definido para o número de unidades de fita reservadas para sessões de armazenamento de nó de arquivo.

> Por padrão, o Registro de um nó cria uma ID de usuário administrativo com autoridade de proprietário do cliente, com a senha definida para o nó.

# Migração de dados para o StorageGRID

## É possível migrar grandes quantidades de dados para o sistema StorageGRID e, simultaneamente, usar o sistema StorageGRID para operações diárias.

A seção a seguir é um guia para entender e Planejar uma migração de grandes quantidades de dados para o sistema StorageGRID. Ele não é um guia geral para a migração de dados e não inclui etapas detalhadas para a execução de uma migração. Siga as diretrizes e instruções nesta seção para garantir que os dados sejam migrados com eficiência para o sistema StorageGRID sem interferir nas operações diárias e que os dados migrados sejam tratados adequadamente pelo sistema StorageGRID.

- "Confirmar a capacidade do sistema StorageGRID"
- "Determinando a política de ILM para dados migrados"
- "Impacto da migração nas operações"
- "Agendamento da migração de dados"
- "Monitoramento da migração de dados"
- "Criação de notificações personalizadas para alarmes de migração"

## Confirmar a capacidade do sistema StorageGRID

Antes de migrar grandes quantidades de dados para o sistema StorageGRID, confirme se o sistema StorageGRID tem a capacidade de disco para lidar com o volume esperado.

Se o sistema StorageGRID incluir um nó de arquivo e uma cópia de objetos migrados tiver sido salva no armazenamento de dados nearline (como fita), verifique se o armazenamento do nó de arquivamento tem capacidade suficiente para o volume esperado de dados migrados.

Como parte da avaliação de capacidade, observe o perfil de dados dos objetos que você planeja migrar e calcule a quantidade de capacidade de disco necessária. Para obter detalhes sobre como monitorar a capacidade de disco do seu sistema StorageGRID, consulte as instruções para monitoramento e solução de problemas do StorageGRID.

**Informações relacionadas**

"Monitorizar Resolução de problemas"

"Gerenciando nós de storage"

## Determinando a política de ILM para dados migrados

A política ILM do sistema StorageGRID determina quantas cópias são feitas, os locais para os quais as cópias são armazenadas e por quanto tempo essas cópias são mantidas. Uma política ILM consiste em um conjunto de regras ILM que descrevem como filtrar objetos e gerenciar dados de objetos ao longo do tempo.

Dependendo de como os dados migrados são usados e de seus requisitos de dados migrados, talvez você queira definir regras exclusivas de ILM para dados migrados que são diferentes das regras de ILM usadas para operações diárias. Por exemplo, se houver requisitos regulatórios diferentes para o gerenciamento diário de dados do que os dados incluídos na migração, talvez você queira um número diferente de cópias dos dados migrados em um nível diferente de storage.

Você pode configurar regras que se aplicam exclusivamente aos dados migrados se for possível distinguir de forma exclusiva entre dados migrados e dados de objetos salvos de operações diárias.

Se você puder distinguir de forma confiável entre os tipos de dados usando um dos critérios de metadados, use esses critérios para definir uma regra de ILM que se aplica apenas aos dados migrados.

Antes de iniciar a migração de dados, certifique-se de que compreende a política de ILM do sistema StorageGRID e de que forma será aplicada aos dados migrados e de que fez e testou quaisquer alterações à política ILM.

Uma política de ILM que foi incorretamente especificada pode causar perda de dados irrecuperável. Revise cuidadosamente todas as alterações feitas em uma política ILM antes de ativá-la para garantir que a política funcionará conforme pretendido.

**Informações relacionadas**

"Gerenciar objetos com ILM"

## Impacto da migração nas operações

O sistema StorageGRID foi desenvolvido para fornecer operações eficientes de storage e recuperação de objetos, além de fornecer excelente proteção contra a perda de dados por meio da criação otimizada de cópias redundantes de dados de objetos e metadados.

No entanto, a migração de dados deve ser cuidadosamente gerenciada de acordo com as instruções deste capítulo para evitar ter impactos nas operações diárias do sistema ou, em casos extremos, colocar os dados em risco de perda em caso de falha no sistema StorageGRID.

A migração de grandes quantidades de dados coloca carga adicional no sistema. Quando o sistema StorageGRID está muito carregado, ele responde mais lentamente às solicitações para armazenar e recuperar objetos. Isso pode interferir com as solicitações de armazenamento e recuperação que são parte integrante das operações diárias. A migração também pode causar outros problemas operacionais. Por exemplo, quando um nó de armazenamento está próximo da capacidade, a carga intermitente pesada devido à ingestão de lote pode fazer com que o nó de armazenamento alterne entre somente leitura e leitura-gravação, gerando notificações.

Se o carregamento pesado persistir, as filas podem se desenvolver para várias operações que o sistema StorageGRID deve executar para garantir a redundância total dos dados e metadados do objeto.

A migração de dados deve ser cuidadosamente gerenciada de acordo com as diretrizes deste documento para garantir o funcionamento seguro e eficiente do sistema StorageGRID durante a migração. Ao migrar dados, ingira objetos em lotes ou controle continuamente a ingestão. Em seguida, monitore continuamente o sistema StorageGRID para garantir que vários valores de atributo não sejam excedidos.

## Agendamento da migração de dados

Evite migrar dados durante o horário operacional principal. Limite a migração de dados para noites, fins de semana e outras ocasiões em que o uso do sistema é baixo.

Se possível, não programe a migração de dados durante períodos de alta atividade. No entanto, se não for prático evitar completamente o período de atividade elevada, é seguro prosseguir desde que monitorize de perto os atributos relevantes e tome medidas se excederem os valores aceitáveis.

**Informações relacionadas**

"Monitoramento da migração de dados"

## Monitoramento da migração de dados

A migração de dados deve ser monitorada e ajustada conforme necessário para garantir que os dados sejam colocados de acordo com a política de ILM dentro do prazo exigido.

Esta tabela lista os atributos que você deve monitorar durante a migração de dados e os problemas que eles representam.

Se você usar políticas de classificação de tráfego com limites de taxa para reduzir a ingestão, poderá monitorar a taxa observada em conjunto com as estatísticas descritas na tabela a seguir e reduzir os limites, se necessário.

| Monitorar | Descrição |
| --- | --- |
| Número de objetos aguardando avaliação ILM | 1. Selecione **Support** > **Tools** > **Grid Topology**.<br>2. Selecione ***deployment*** > **Overview** > **Main**.<br>3. Na seção ILM Activity, monitore o número de objetos mostrados para os seguintes atributos:<br>◦ **Aguardando - todos (XQUZ)**: O número total de objetos aguardando avaliação ILM.<br>◦ **Aguardando - Cliente (XCQZ)**: O número total de objetos aguardando avaliação ILM das operações do cliente (por exemplo, ingest).<br>4. Se o número de objetos mostrados para qualquer um desses atributos exceder 100.000, diminua a taxa de ingestão de objetos para reduzir a carga no sistema StorageGRID. |
| Capacidade de armazenamento do sistema de arquivamento direcionado | Se a política de ILM salvar uma cópia dos dados migrados para um sistema de armazenamento de arquivamento de destino (fita ou nuvem), monitore a capacidade do sistema de armazenamento de arquivamento de destino para garantir que haja capacidade suficiente para os dados migrados. |
| **Archive Node** > **ARC** > **Store** | Se um alarme para o atributo **Store Failures (ARVF)** for acionado, o sistema de armazenamento de arquivos alvo pode ter atingido a capacidade. Verifique o sistema de armazenamento de arquivos alvo e resolva quaisquer problemas que acionaram um alarme. |

## Criação de notificações personalizadas para alarmes de migração

Você pode querer que o StorageGRID envie notificações de alerta ou notificações de alarme (sistema legado) para o administrador do sistema responsável pelo monitoramento da migração se certos valores excederem os limites recomendados.

**O que você vai precisar**

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.
- Você deve ter configurado configurações de e-mail para notificações de alerta (ou alarme).

**Passos**

1. Crie uma regra de alerta personalizada ou um alarme personalizado global para cada métrica ou atributo StorageGRID do Prometheus que você deseja monitorar durante a migração de dados.

   Os alertas são acionados com base nos valores métricos Prometheus. Os alarmes são acionados com base em valores de atributo. Consulte as instruções para monitoramento e solução de problemas do StorageGRID para obter mais informações.

2. Desative a regra de alerta personalizado ou o alarme personalizado global após a conclusão da migração de dados.

Observe que os alarmes personalizados globais substituem os alarmes padrão.

**Informações relacionadas**

"Monitorizar Resolução de problemas"

## Informações sobre direitos autorais



## Informações sobre marcas comerciais