



Administrar o StorageGRID

StorageGRID

NetApp
October 03, 2025

Índice

Administrar o StorageGRID	1
Administre o StorageGRID: Visão geral	1
Sobre estas instruções	1
Antes de começar	1
Comece a usar o StorageGRID	1
Requisitos do navegador da Web	1
Faça login no Gerenciador de Grade	1
Saia do Grid Manager	5
Altere a sua palavra-passe	6
Altere o tempo limite da sessão do navegador	7
Veja as informações da licença do StorageGRID	8
Atualizar informações de licença do StorageGRID	9
Use a API	9
Controle o acesso ao StorageGRID	29
Altere a frase-passe de provisionamento	29
Altere as senhas do console do nó	31
Controle o acesso através de firewalls	33
Use a federação de identidade	34
Gerenciar grupos de administradores	39
Desative recursos com a API	45
Gerenciar usuários	47
Usar logon único (SSO)	49
Gerir as definições de segurança	77
Gerenciar certificados	77
Configurar servidores de gerenciamento de chaves	109
Gerenciar configurações de proxy	139
Gerenciar redes de clientes não confiáveis	142
Gerenciar locatários	144
Gerenciar locatários	144
Crie uma conta de locatário	146
Altere a senha para o usuário raiz local do locatário	151
Editar conta de locatário	152
Eliminar conta de inquilino	155
Gerenciar serviços de plataforma	155
Gerenciar S3 Selecione para contas de inquilino	164
Configurar conexões de cliente S3 e Swift	165
Sobre as conexões de clientes S3 e Swift	165
Resumo: Endereços IP e portas para conexões de clientes	166
Configurar interfaces VLAN	168
Gerenciar grupos de alta disponibilidade	172
Gerenciar o balanceamento de carga	184
Configure os nomes de domínio de endpoint da API S3	195
Ativar HTTP para comunicações de cliente	197

Controle quais operações do cliente são permitidas	198
Gerencie redes e conexões	199
Diretrizes para redes StorageGRID	199
Ver endereços IP	200
Cifras suportadas para conexões TLS de saída	201
Alterar a encriptação de transferência de rede	202
Gerenciar políticas de classificação de tráfego	203
Gerenciar custos de link	216
Use o AutoSupport	219
O que é o AutoSupport?	219
Configurar o AutoSupport	220
Acione manualmente uma mensagem AutoSupport	226
Solucionar problemas de mensagens do AutoSupport	226
Envie mensagens AutoSupport do e-Series através do StorageGRID	228
Gerenciar nós de storage	232
Sobre o gerenciamento de nós de storage	232
O que é um nó de storage?	232
Gerenciar opções de armazenamento	236
Gerenciar o storage de metadados de objetos	241
Configure as configurações globais para objetos armazenados	248
Configurações do nó de storage	251
Gerencie nós de storage completos	256
Gerenciar nós de administração	256
O que é um nó Admin	256
Use vários nós de administração	257
Identifique o nó de administração principal	258
Selecione um remetente preferido	259
Exibir status de notificação e filas	260
Como os nós de administração mostram alarmes reconhecidos (sistema legado)	261
Configurar acesso de cliente de auditoria	262
Gerenciar nós de arquivamento	279
O que é um nó de arquivo	279
Arquive para a nuvem por meio da API S3	280
Arquive para fita através do middleware TSM	287
Configurar as definições de recuperação do nó de arquivo	292
Configurar a replicação do nó de arquivo	293
Definir alarmes personalizados para o nó de arquivo	295
Integre o Tivoli Storage Manager	295
Migrar dados para o StorageGRID	302
Confirme a capacidade do sistema StorageGRID	302
Determine a política de ILM para dados migrados	302
Impacto da migração nas operações	303
Agendar e monitorar a migração de dados	303

Administrar o StorageGRID

Administre o StorageGRID: Visão geral

Use estas instruções para configurar e administrar um sistema StorageGRID.

Sobre estas instruções

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.

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

Antes de começar

- 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.

Comece a usar o StorageGRID

Requisitos do navegador da Web

Você deve usar um navegador da Web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	96
Microsoft Edge	96
Mozilla Firefox	94

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

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Faça login no Gerenciador de Grade

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

- Você tem suas credenciais de login.
- Você tem o URL para o Gerenciador de Grade.
- Você está usando um [navegador da web suportado](#).
- Os cookies são ativados no seu navegador.
- Você tem 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 conectará 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 a interface principal 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/
```

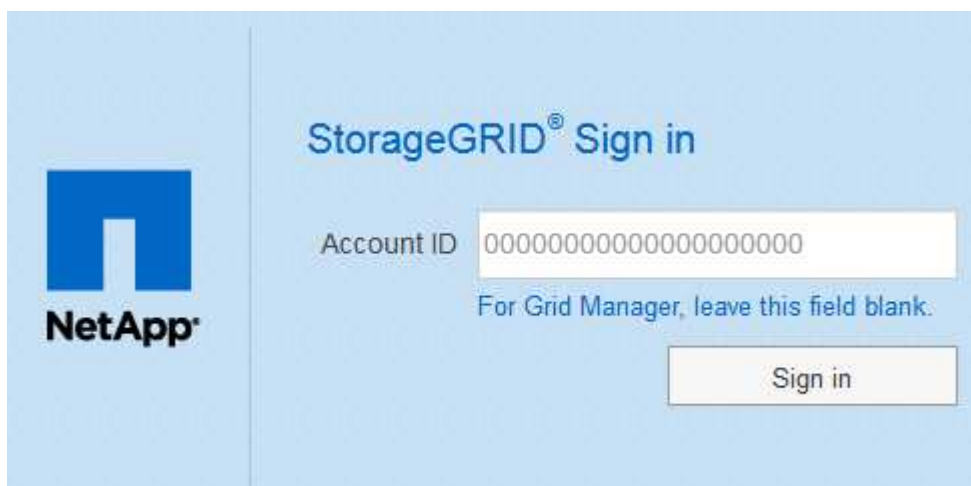
3. Se for solicitado um alerta de segurança, instale o certificado usando o assistente de instalação do navegador ([Sobre certificados de segurança](#) consulte).
4. Entre no Gerenciador de Grade:
 - Se o logon único (SSO) não estiver sendo usado para seu sistema StorageGRID:

- i. Insira seu nome de usuário e senha para o Gerenciador de Grade.
- ii. Selecione **entrar**.



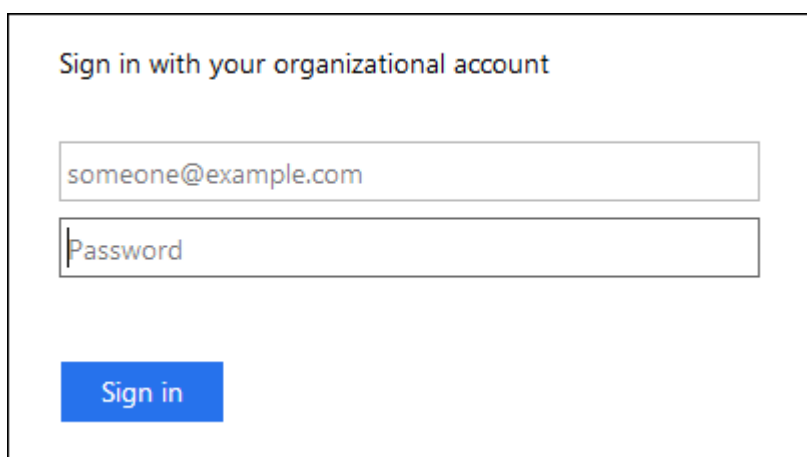
The image shows the StorageGRID Grid Manager login page. On the left is the NetApp logo. On the right, the title "StorageGRID® Grid Manager" is displayed. Below the title are two input fields: "Username" and "Password". A "Sign in" button is located at the bottom right of the form area.

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



The image shows the StorageGRID Sign in page. On the left is the NetApp logo. On the right, the title "StorageGRID® Sign in" is displayed. Below the title is an "Account ID" input field containing a series of zeros. Below this field is the text "For Grid Manager, leave this field blank." A "Sign in" button is located at the bottom right of the form area.

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

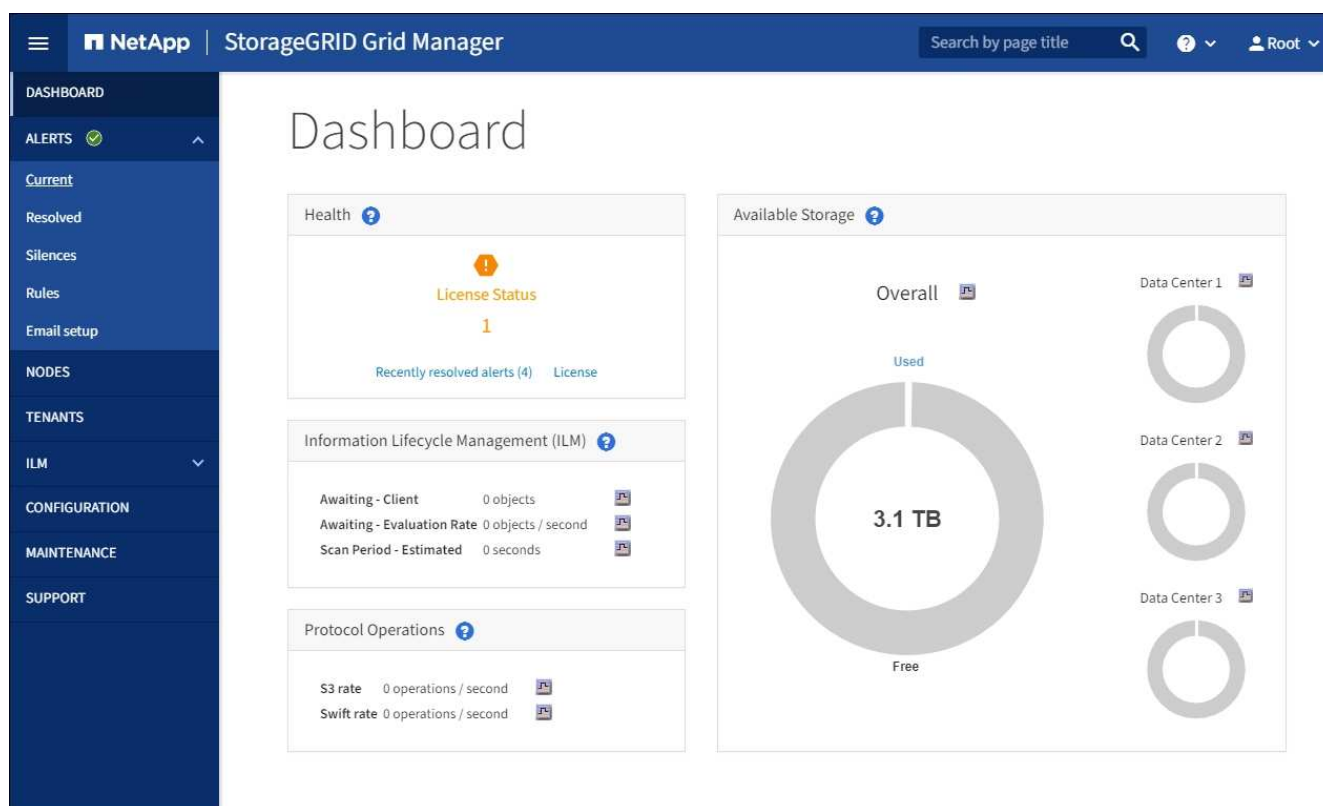


The image shows a login form for an organizational account. The title is "Sign in with your organizational account". Below the title are two input fields: one for an email address (containing "someone@example.com") and one for a password (containing "Password"). A blue "Sign in" button is located at the bottom left of the form area.

- 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 selecione **entrar**.
 - Selecione **Gerenciador de Grade** se aparecer na lista de contas recentes e selecione **entrar**.



- ii. Inicie sessão com as suas credenciais SSO padrão na página de início de sessão SSO da sua organização. Quando você estiver conectado, a página inicial do Gerenciador de Grade será exibida, que inclui o Painel de Controle. Para saber quais informações são fornecidas, [Veja o Dashboard](#) consulte .



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

Opção	Passos
SSO não ativado	<p>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.</p> <p>b. Insira seu nome de usuário e senha para o Gerenciador de Grade.</p> <p>c. Selecione entrar.</p>
SSO ativado	<p>Na barra de endereços do navegador, insira o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração.</p> <p>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.</p> <p>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.</p>

Informações relacionadas

- [Controle o acesso através de firewalls](#)
- [Configurar o logon único](#)
- [Gerenciar grupos de administradores](#)
- [Gerenciar grupos de alta disponibilidade](#)
- [Use uma conta de locatário](#)
- [Monitorar e solucionar problemas](#)

Saia do Grid Manager

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. Selecione seu nome de usuário no canto superior direito.



2. Selecione **Sair**.

Opção	Descrição
SSO não em uso	<p>Você está desconetado do Admin Node.</p> <p>A página de login do Gerenciador de Grade é exibida.</p> <p>Nota: se você tiver feito login em mais de um nó Admin, você deve sair de cada nó.</p>
SSO ativado	<p>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.</p> <p>Observação: se o SSO estiver ativado e você também estiver conectado ao Gerenciador do Locatário, você também deverá sair da conta do locatário para sair do SSO.</p>

Informações relacionadas

- [Configurar o logon único](#)
- [Use uma conta de locatário](#)

Altere 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

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** > **Change password**.
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 caracteres. As senhas diferenciam maiúsculas de minúsculas.

4. Volte a introduzir a nova palavra-passe.
5. Selecione **Guardar**.

Altere 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 selecionasse **Sair** manualmente. O usuário deve reinserir suas credenciais SSO para acessar o StorageGRID novamente. [Configurar o logon único](#) Consulte .



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 **CONFIGURATION** > **System** > **Display OPTIONS**.
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.



Display Options

Updated: 2017-03-09 20:38:53 MST

Current Sender

ADMIN-DC1-ADM1

Preferred Sender

ADMIN-DC1-ADM1

GUI Inactivity Timeout

900

Notification Suppress All



Apply Changes



3. Selecione **aplicar alterações**.

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

Veja as informações da 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

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, selecione o ícone de status da Licença ou o link **Licença**. Este link aparece somente se houver um problema com a licença.
- Selecione **MAINTENANCE > System > License**.

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.

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

Passos

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

O novo ficheiro de licença é validado e apresentado.

5. Selecione **Guardar**.

Use a API

Use 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.

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, [Use uma conta de locatário](#) consulte .
- `/private`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas. As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

Emitir solicitações de API

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.

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

O que você vai precisar

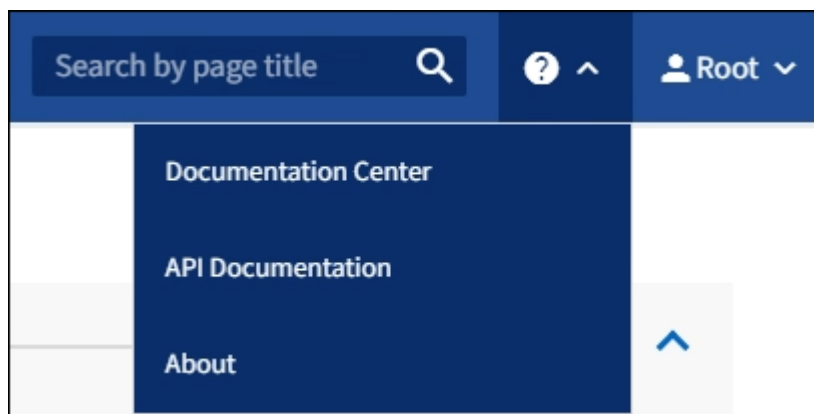
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.



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. No cabeçalho do Gerenciador de Grade, selecione o ícone de ajuda e selecione **Documentação da API**.



2. Para executar uma operação com a API privada, selecione **ir para a documentação da API privada** na página da API de gerenciamento do StorageGRID.

As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Selecione a operação desejada.

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

e DELETE.

4. 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.

groups Operations on groups

GET /grid/groups Lists Grid Administrator Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated
limit integer (query)	maximum number of results Default value : 25
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker) Available values : asc, desc

Responses Response content type: application/json

Code	Description
200	successfully retrieved

Example Value | Model

```
{
  "responseTime": "2021-03-29T14:22:19.673Z",
  "status": "success",
  "apiVersion": "3.3",
  "deprecated": false,
  "data": [
    {
      "displayName": "Developers",

```

5. 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.
6. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.
7. Selecione **Experimente**.

8. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
9. Selecione **Executar**.
10. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API Grid Management

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



Esta lista inclui apenas as operações disponíveis na API pública.

- *** 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-details* — operações em detalhes do nó.
- **Node-health** — operações no status de integridade do nó.
- **ntp-servers** — 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.

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"
```

Determine 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
  ]
}
```

Especifique 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
```

Proteger contra falsificação de solicitação entre locais (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 conectado.

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.

Use a API se o logon único estiver ativado

Use a API se o logon único estiver ativado (ative Directory)

Se você tiver [Logon único configurado e habilitado \(SSO\)](#) e usar o ative Directory como provedor SSO, deverá emitir uma série de solicitações de API para obter um token de autenticação válido para a API de Gerenciamento de Grade ou para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

Estas instruções se aplicam se você estiver usando o ative Directory como provedor de identidade SSO.

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: `A valid SubjectConfirmation was not found on this Response.`



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: `Unsupported SAML version.`

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 método SSO. Introduza ADFS ou adfs.
- O nome de usuário SSO

- O domínio onde o StorageGRID está instalado
- O endereço para StorageGRID
- O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário.

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

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

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

3. Se você quiser usar solicitações curl, use o procedimento a seguir.
 - a. Declare as variáveis necessárias para iniciar sessão.

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



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

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

Este exemplo mostra uma SOLICITAÇÃO POST para um URL de autenticação assinada para TENANTACCOUNTID. Os resultados serão passados para `python -m json.tool remove` 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=fZHRTToMwFIZfhh...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=
$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --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=fZHRT0MwFIZfhh...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
XfXVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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="PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />

```

- i. Salve o SAMLResponse do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...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.

Saia 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. Estas instruções se aplicam se você estiver usando o ativo Directory como provedor de identidade SSO

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%3D",
  "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=fZDNboMwEIRfhZ...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
```

Use a API se o logon único estiver habilitado (Azure)

Se você tiver [Logon único configurado e habilitado \(SSO\)](#) e usar o Azure como provedor SSO, você pode usar dois scripts de exemplo para obter um token de autenticação válido para a API de Gerenciamento de Grade ou a API de Gerenciamento do locatário.

Inicie sessão na API se o início de sessão único do Azure estiver ativado

Estas instruções se aplicam se você estiver usando o Azure como provedor de identidade SSO

O que você vai precisar

- Você sabe o endereço de e-mail SSO e a senha de 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 os seguintes scripts de exemplo:

- O `storagegrid-ssoauth-azure.py` script Python
- O `storagegrid-ssoauth-azure.js` script Node.js

Ambos os scripts estão localizados no diretório arquivos de instalação do StorageGRID (`./rpms`` para Linux ou CentOS, para Ubuntu ou Debian, `./debs` e `./vsphere` para VMware).

Para escrever sua própria integração com a API do Azure, consulte o `storagegrid-ssoauth-azure.py` script. O script Python faz duas solicitações diretamente ao StorageGRID (primeiro para obter o SAMLRequest e depois para obter o token de autorização), e também chama o script Node.js para interagir com o Azure para executar as operações SSO.

As operações SSO podem ser executadas usando uma série de solicitações de API, mas isso não é simples. O módulo Puppeteer Node.js é usado para raspar a interface SSO do Azure.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version`.

Passos

1. Instale as dependências necessárias, da seguinte forma:
 - a. Instale o Node.js ("<https://nodejs.org/en/download/>" consulte).
 - b. Instale os módulos Node.js necessários (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passe o script Python para o interpretador Python para executar o script.

O script Python chamará então o script Node.js correspondente para executar as interações SSO do Azure.

3. Quando solicitado, insira valores para os seguintes argumentos (ou passe-os usando parâmetros):
 - O endereço de e-mail SSO usado para entrar no Azure
 - O endereço para StorageGRID
 - O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário

4. Quando solicitado, insira a senha e esteja preparado para fornecer uma autorização de MFA ao Azure, se solicitado.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****

StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



O script assume que o MFA é feito usando o Microsoft Authenticator. Talvez seja necessário modificar o script para dar suporte a outras formas de MFA (como inserir um código recebido por mensagem de texto).

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.

Use a API se o logon único estiver ativado (PingFederate)

Se você tem [Logon único configurado e habilitado \(SSO\)](#) e usa o PingFederate como provedor SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de Gerenciamento de Grade ou para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

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: `A valid SubjectConfirmation was not found on this Response.`



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: `Unsupported SAML version.`

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 método SSO. Você pode inserir qualquer variação de "pingfederate" (PINGFEDERATE, pingfederate, e assim por diante).
- O nome de usuário SSO
- O domínio onde o StorageGRID está instalado. Este campo não é usado para PingFederate. Você pode deixá-lo em branco ou inserir qualquer valor.
- O endereço para StorageGRID
- O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário.

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

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

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

3. Se você quiser usar solicitações `curl`, use o procedimento a seguir.
 - a. Declare as variáveis necessárias para iniciar sessão.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.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 uma 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://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

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

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Exporte a resposta e o cookie e ecoe a resposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

- e. Exporte o valor 'pf.adapterId' e ecoe a resposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

- f. Exporte o valor 'href' (remova a barra à direita /) e faça eco da resposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exportar o valor "ação":

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Enviar cookies juntamente com credenciais:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

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.

Saia 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. Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

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://my-ping-
url/ldap/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2021-10-12T22:20:30.839Z",
  "status": "success"
}
```

2. Salve o URL de logout.

```
export LOGOUT_REQUEST='https://my-ping-
url/ldap/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...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: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

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
```

Controle o acesso ao StorageGRID

Altere a frase-passe 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 senha também é necessária para baixar backups do pacote de recuperação que incluem informações de topologia de grade, senhas de console de nó de grade e chaves de criptografia para o sistema StorageGRID.

O que você vai precisar

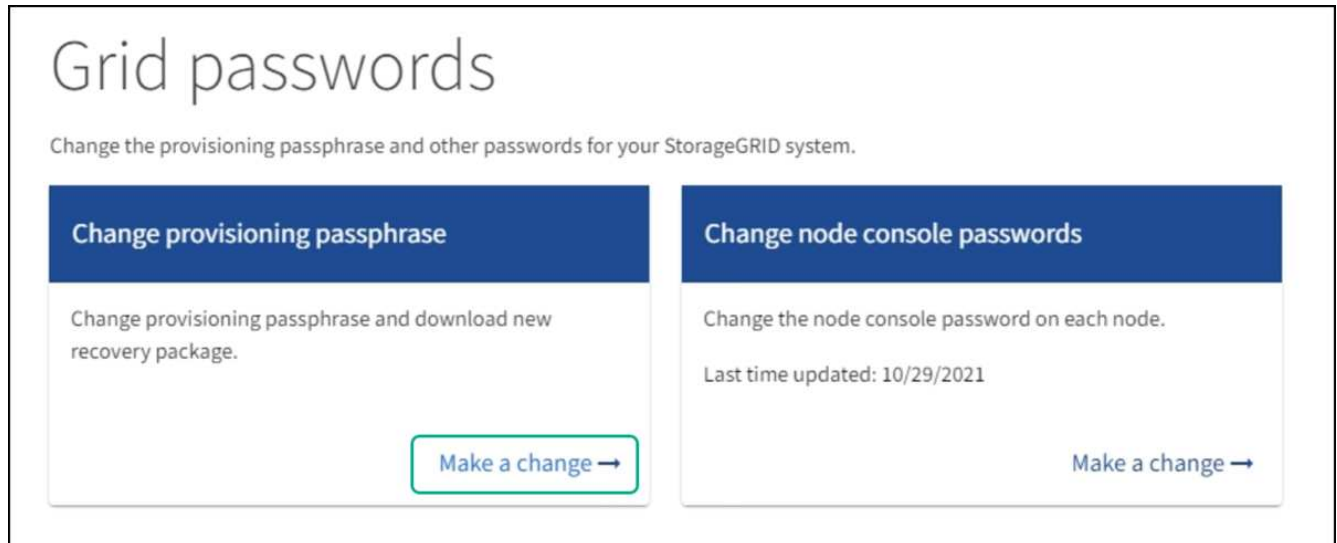
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de Manutenção ou Acesso root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

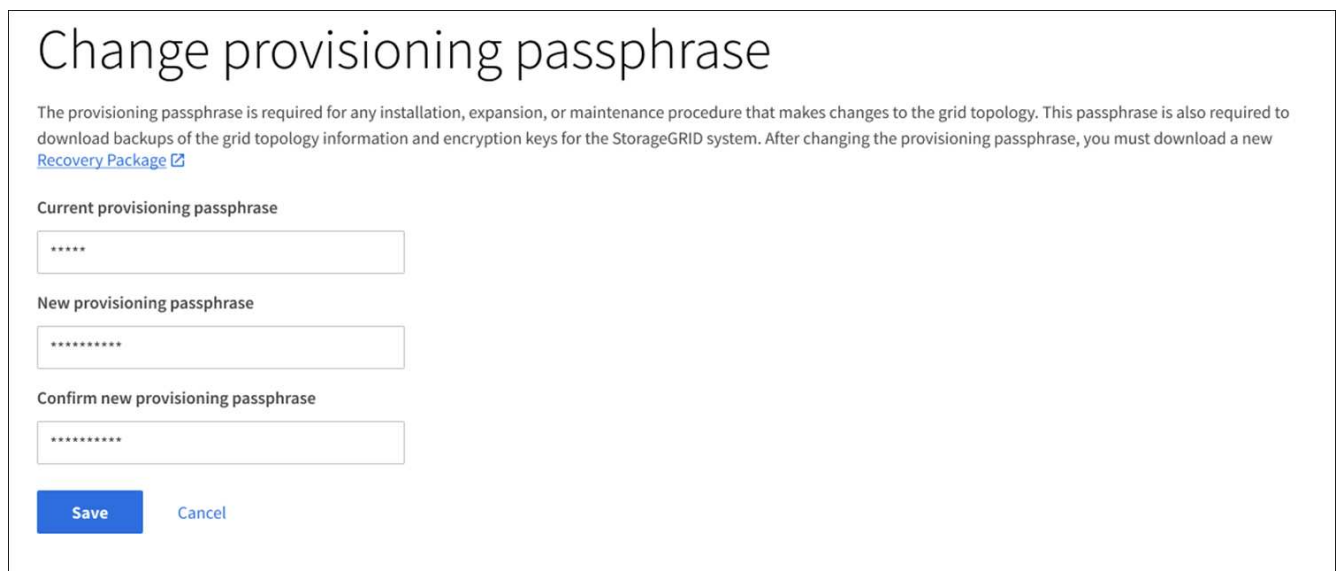
A frase-passe de provisionamento é necessária para muitos procedimentos de instalação e manutenção, e para [Transferir o pacote de recuperação](#). A senha de provisionamento não está listada no `Passwords.txt` arquivo. Certifique-se de documentar a senha de provisionamento e mantê-la em um local seguro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

Passos

1. Selecione **CONFIGURATION > access control> Grid passwords**.



2. Selecione **Faça uma alteração** em **Change Provisioning passphrase**.



3. Introduza a sua frase-passe de aprovisionamento atual.
4. Introduza a nova frase-passe. A frase-passe deve conter pelo menos 8 e não mais de 32 caracteres. As senhas são sensíveis a maiúsculas e minúsculas.
5. Armazene a nova senha de provisionamento em um local seguro. É necessário para procedimentos de instalação, expansão e manutenção.
6. Digite novamente a nova senha e selecione **Salvar**.

O sistema exibe um banner verde de sucesso quando a alteração da senha de provisionamento estiver concluída.

Configuration > Grid passwords > Change provisioning passphrase

Success
Provisioning passphrase changed successfully

Change provisioning passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to [download backups of the grid topology information and encryption keys for the StorageGRID system](#). After changing the provisioning passphrase, you must download a new [Recovery Package](#).

Current provisioning passphrase

New provisioning passphrase

Confirm new provisioning passphrase

Save Cancel

7. Selecione **Pacote de recuperação**.

8. Insira a nova senha de provisionamento para baixar o novo Pacote de recuperação.



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.

Altere as senhas do console do nó

Cada nó na sua grade tem uma senha exclusiva do console de nó, que você precisa fazer login no nó. Use estas etapas para alterar cada senha exclusiva do console de nó para cada nó na grade.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem a permissão Manutenção ou Acesso root.
- Você tem a senha de provisionamento atual.

Sobre esta tarefa

Use a senha do console do nó para fazer login em um nó como "admin" usando SSH, ou para o usuário raiz em uma conexão VM/console físico. O processo de alteração de senha do console do nó cria novas senhas para cada nó na grade e armazena as senhas em um arquivo atualizado `Passwords.txt` no Pacote de recuperação. As senhas são listadas na coluna Senha no `Passwords.txt` arquivo.



Existem senhas de acesso SSH separadas para as chaves SSH usadas para comunicação entre nós. As senhas de acesso SSH não são alteradas por este procedimento.

Acesse o assistente

Passos

1. Selecione **CONFIGURATION > Access control > Grid passwords**.

2. Em **alterar senhas de console de nó**, selecione **fazer uma alteração**.

Introduza a frase-passe de aprovisionamento

Passos

1. Introduza a frase-passe de aprovisionamento da grelha.
2. Selecione **continuar**.

Faça o download do pacote de recuperação atual

Antes de alterar as senhas do console do nó, baixe o Pacote de recuperação atual. Você pode usar as senhas neste arquivo se o processo de alteração de senha falhar em qualquer nó.

Passos

1. Selecione **Baixar pacote de recuperação**.
2. Copie o arquivo do pacote de recuperação (.zip) para dois locais seguros, seguros e separados.



O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

3. Selecione **continuar**.
4. Quando a caixa de diálogo de confirmação for exibida, selecione **Sim** se estiver pronto para começar a alterar as senhas do console do nó.

Não é possível cancelar este processo após o início.

Altere as senhas do console do nó

Quando o processo de senha do console do nó é iniciado, um novo Pacote de recuperação é gerado que inclui as novas senhas. Em seguida, as senhas são atualizadas em cada nó.

Passos

1. Aguarde que o novo pacote de recuperação seja gerado, o que pode levar alguns minutos.
2. Selecione **Transferir novo pacote de recuperação**.
3. Quando o download for concluído:
 - a. Abra o .zip ficheiro.
 - b. Confirme se você pode acessar o conteúdo, incluindo o Passwords.txt arquivo, que contém as novas senhas do console do nó.
 - c. Copie o novo arquivo do pacote de recuperação (.zip) para dois locais seguros, seguros e separados.



Não substituir o pacote de recuperação antigo.

O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

4. Marque a caixa de seleção para indicar que você baixou o novo Pacote de recuperação e verificou o conteúdo.

5. Selecione **alterar senhas do console de nós** e aguarde que todos os nós sejam atualizados com as novas senhas. Isso pode levar alguns minutos.

Se as senhas forem alteradas para todos os nós, um banner verde de sucesso será exibido. Vá para a próxima etapa.

Se houver um erro durante o processo de atualização, uma mensagem de banner lista o número de nós que não conseguiram alterar suas senhas. O sistema irá tentar novamente automaticamente o processo em qualquer nó que não tenha a sua palavra-passe alterada. Se o processo terminar com alguns nós ainda não tendo uma senha alterada, o botão **Repetir** será exibido.

Se a atualização da palavra-passe tiver falhado para um ou mais nós:

- a. Reveja as mensagens de erro listadas na tabela.
- b. Resolva os problemas.
- c. Selecione **Repetir**.



A tentativa de novo altera apenas as senhas do console do nó nos nós que falharam durante tentativas anteriores de alteração de senha.

6. Depois que as senhas do console do nó tiverem sido alteradas para todos os nós, exclua o [Primeiro pacote de recuperação que você baixou](#).
7. Opcionalmente, use o link **Recovery package** para baixar uma cópia adicional do novo Recovery Package.

Controle o acesso através de firewalls

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

Controle 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 conectar 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. Nota: a porta 443 também é usada para algum tráfego interno.

Porta	Descrição	Se a porta estiver aberta...
8443	Porta restrita do Gerenciador de Grade em nós de administração	<ul style="list-style-type: none"> Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador de Grade e a API de Gerenciamento de Grade usando HTTPS. 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. As solicitações de conteúdo interno serão rejeitadas.
9443	Porta restrita do Gerenciador de inquilinos em nós de administração	<ul style="list-style-type: none"> Navegadores da Web e clientes de API de gerenciamento podem acessar o Gerenciador do locatário e a API de gerenciamento do locatário usando HTTPS. Navegadores da Web e clientes de API de gerenciamento não podem acessar o Gerenciador de Grade ou a API de Gerenciamento de Grade. 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

- [Faça login no Gerenciador de Grade](#)
- [Crie uma conta de locatário](#)
- [Comunicações externas](#)

Use 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.

Configure a federação de identidade para o Grid Manager

Você pode configurar a federação de identidade no Gerenciador de Grade se quiser que os grupos de administração e usuários sejam gerenciados em outro sistema, como [ativo Directory](#), [Azure ativo Directory \(Azure AD\)](#), [OpenLDAP](#) ou [Oracle Directory Server](#).

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

- Você está usando o ativo Directory, o Azure AD, o OpenLDAP ou o Oracle Directory Server como provedor de identidade.



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

- Se você pretende usar o OpenLDAP, você deve configurar o servidor OpenLDAP. [Diretrizes para configurar um servidor OpenLDAP](#)Consulte .
- Se você planeja habilitar o logon único (SSO), revisou o [requisitos para o uso de logon único](#).
- Se você planeja usar TLS (Transport Layer Security) para comunicações com o servidor LDAP, o provedor de identidade está usando TLS 1,2 ou 1,3. [Cifras suportadas para conexões TLS de saída](#)Consulte .

Sobre esta tarefa

Você pode configurar uma fonte de identidade para o Gerenciador de Grade se quiser importar grupos de outro sistema, como ativo Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Você pode importar os seguintes tipos de grupos:

- 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. [Crie uma conta de locatário](#)Consulte e [Use uma conta de locatário](#) para obter detalhes.

Introduza a configuração

1. Selecione **CONFIGURATION > access control > Identity Federation**.
2. Selecione **Ativar federação de identidade**.
3. Na secção tipo de serviço LDAP, selecione o tipo de serviço LDAP que pretende configurar.

Ldap service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
------------------	-------	----------	-------

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. Caso contrário, vá para a próxima etapa.
 - **Nome exclusivo do usuário:** O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente `sAMAccountName` ao ativo 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 ativo 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 `Active 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 `Active 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. Para todos os tipos de serviço LDAP, introduza as informações de ligação de rede e servidor LDAP necessárias na secção Configurar servidor LDAP.

- **Nome de host:** O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
- **Port:** A porta usada para se conectar 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 conectará ao servidor LDAP.

No `Active 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`
 - **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl`, E `userPrincipalName`
 - **Azure:** `accountEnabled` E `userPrincipalName`
- **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 `Active 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 da base de usuários** a que pertencem.

- **Bind username format** (opcional): O padrão de username padrão StorageGRID deve ser usado se o padrão não puder ser determinado automaticamente.

É recomendado fornecer **Bind username format** porque pode permitir que os usuários façam login se o StorageGRID não conseguir vincular-se à conta de serviço.

Introduza um destes padrões:

- **Padrão UserPrincipalName (ative Directory e Azure):** [USERNAME]@example.com
- * Padrão de nome de logon de nível inferior (ative Directory e Azure)*: example\[USERNAME]
- * Padrão de nome distinto *: CN=[USERNAME], CN=Users, DC=example, DC=com

Inclua [USERNAME] exatamente como escrito.

6. Na seção Transport Layer Security (TLS), selecione uma configuração de segurança.

- **Use STARTTLS:** Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para active Directory, OpenLDAP ou outro, mas esta opção não é suportada para o Azure.
- **Use LDAPS:** A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar essa opção para o Azure.
- **Não use TLS:** O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será protegido. Esta opção não é suportada para o Azure.



O uso da opção **não usar TLS** não é suportado se o servidor do active 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 de grade 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.

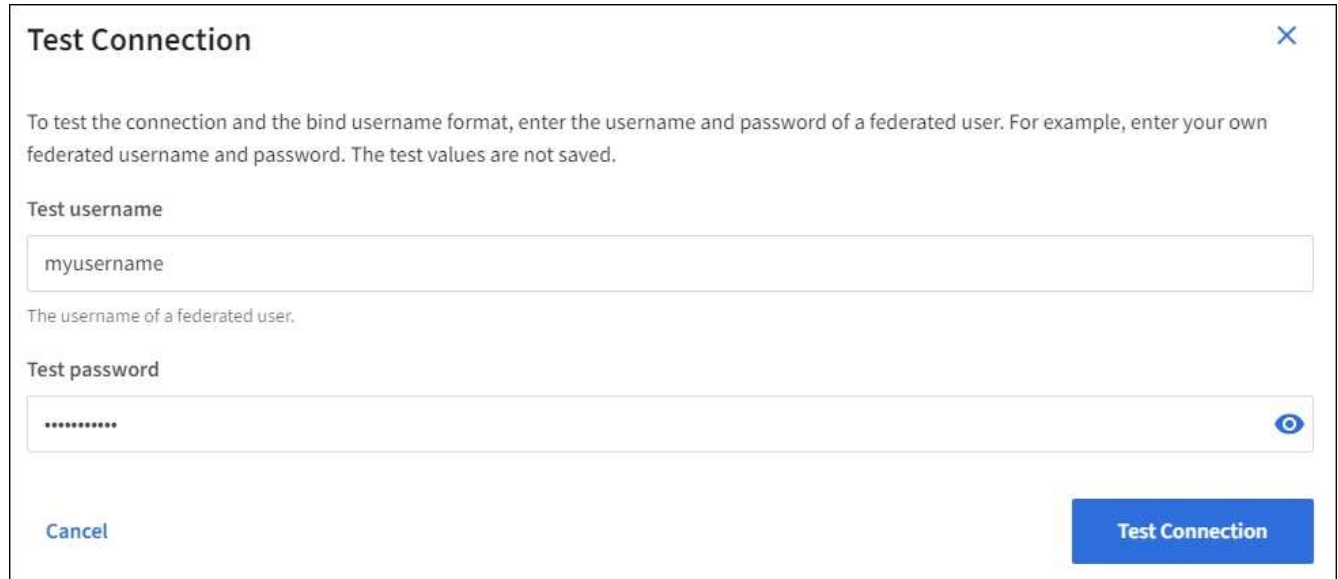
Teste a conexão e salve a configuração

Depois de introduzir todos os valores, tem de testar a ligação antes de poder guardar a configuração. O StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato de nome de usuário de vinculação, se você tiver fornecido uma.

1. Selecione **Test Connection**.
2. Se você não forneceu um formato de nome de usuário do BIND:
 - Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
 - Uma mensagem ""test Connection could not be established"" (não foi possível estabelecer ligação) é apresentada se as definições de ligação forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você tiver fornecido um formato de nome de usuário do BIND, insira o nome de usuário e a senha de

um usuário federado válido.

Por exemplo, insira seu próprio nome de usuário e senha. Não inclua caracteres especiais no nome de usuário, como em ou /.



- Uma mensagem ""Teste de conexão bem-sucedida"" aparece se as configurações de conexão forem válidas. Selecione **Save** (Guardar) para guardar a configuração.
- Uma mensagem de erro é exibida se as configurações de conexão, o formato de nome de usuário de ligação ou o nome de usuário de teste e a senha forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar 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.

Passos

1. Vá para a página de federação de identidade.
2. Selecione **servidor de sincronização** na parte superior da página.

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.

Desativar 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.

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 conectados 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 **habilitado** ou **modo Sandbox**. O status SSO na página de logon único deve ser **Desabilitado** antes de desativar a federação de identidade. [Desative o logon único](#) Consulte .

Passos

1. Vá para a página de federação de identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

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.



Para fontes de identidade que não são ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso S3 aos usuários que estão desativados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 para o usuário e remova o usuário de todos os grupos.

Sobreposições de Memberof e refint

As sobreposições membranadas e refinadas devem ser ativadas. Para obter mais informações, consulte as instruções para a manutenção da associação de grupo reverso no "[Documentação do OpenLDAP: Guia do administrador da versão 2,4](#)".

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 "[Documentação do OpenLDAP: Guia do administrador da versão 2,4](#)".

Gerenciar 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.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- Se você pretende importar um grupo federado, você configurou a federação de identidade e o grupo federado já existe na origem de identidade configurada.

Crie um grupo 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.

Acesse o assistente

1. Selecione **CONFIGURATION > Access Control > Admin Groups**.
2. Selecione **criar grupo**.

Escolha um tipo de grupo

Você pode criar um grupo local ou importar um grupo federado.

- Crie um grupo local se quiser atribuir permissões a usuários locais.
- Crie um grupo federado para importar usuários da origem da identidade.

Grupo local

1. Selecione **local group**.
2. Introduza um nome de apresentação para o grupo, que pode atualizar posteriormente, conforme necessário. Por exemplo, "usuários de Manutenção" ou "Administradores de ILM."
3. Introduza um nome exclusivo para o grupo, que não pode atualizar mais tarde.
4. Selecione **continuar**.

Grupo federado

1. Selecione **Federated Group**.
2. Introduza o nome do grupo que pretende importar, exatamente como aparece na origem de identidade configurada.
 - Para o Active Directory e Azure, use o sAMAccountName.
 - Para OpenLDAP, use o CN (Nome Comum).
 - Para outro LDAP, use o nome exclusivo apropriado para o servidor LDAP.
3. Selecione **continuar**.

Gerenciar permissões de grupo

1. 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.

2. Selecione um ou mais [Permissões de grupo](#).

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

3. Se estiver criando um grupo local, selecione **continuar**. Se você estiver criando um grupo federado, selecione **criar grupo** e **concluir**.

Adicionar utilizadores (apenas grupos locais)

1. Opcionalmente, selecione um ou mais usuários locais para este grupo.


Se ainda não tiver criado utilizadores locais, pode guardar o grupo sem adicionar utilizadores. Pode adicionar este grupo ao utilizador na página utilizadores. [Gerenciar usuários](#) Consulte para obter detalhes.

2. Selecione **criar grupo** e **concluir**.

Exibir e editar grupos de administração

Você pode exibir detalhes de grupos existentes, modificar um grupo ou duplicar um grupo.

- Para exibir informações básicas de todos os grupos, revise a tabela na página grupos.
- Para exibir todos os detalhes de um grupo específico ou editar um grupo, use o menu **ações** ou a página de detalhes.

Tarefa	Menu ações	Página de detalhes
Ver detalhes do grupo	a. Marque a caixa de seleção do grupo. b. Selecione ações > Exibir detalhes do grupo .	Selecione o nome do grupo na tabela.
Editar nome de exibição (apenas grupos locais)	a. Marque a caixa de seleção do grupo. b. Selecione ações > Editar nome do grupo . c. Introduza o novo nome. d. Selecione Salvar alterações .	a. Selecione o nome do grupo para exibir os detalhes. b. Selecione o ícone de edição  . c. Introduza o novo nome. d. Selecione Salvar alterações .

Tarefa	Menu ações	Página de detalhes
Editar o modo de acesso ou permissões	a. Marque a caixa de seleção do grupo. b. Selecione ações > Exibir detalhes do grupo . c. Opcionalmente, altere o modo de acesso do grupo. d. Opcionalmente, selecione ou Permissões de grupo desmarque . e. Selecione Salvar alterações .	a. Selecione o nome do grupo para exibir os detalhes. b. Opcionalmente, altere o modo de acesso do grupo. c. Opcionalmente, selecione ou Permissões de grupo desmarque . d. Selecione Salvar alterações .

Duplicar um grupo

1. Marque a caixa de seleção do grupo.
2. Selecione **ações > grupo duplicado**.
3. Conclua o assistente de grupo duplicado.

Eliminar um grupo

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 todos os usuários do grupo, mas não exclui os usuários.

1. Na página grupos, marque a caixa de seleção para cada grupo que deseja remover.
2. Selecione **ações > Excluir grupo**.
3. Selecione **Excluir grupos**.

Permissões de grupo

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 ou na API de Gerenciamento 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

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.

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 **Root Access**.

Acesso à raiz

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

Reconhecer alarmes (legado)

Esta permissão fornece acesso para reconhecer e responder a alarmes (sistema legado). Todos os usuários conectados 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.

Altere a senha raiz do locatário

Essa permissão fornece acesso à opção **alterar senha de root** na página de locatários, permitindo que você controle quem pode alterar a senha para o usuário raiz local do locatário. Essa permissão também é usada para migrar chaves S3 quando o recurso de importação de chaves S3 estiver ativado. Os usuários que não têm essa permissão não podem ver a opção **alterar senha de root**.



Para conceder acesso à página de locatários, que contém a opção **alterar senha de root**, atribua também a permissão **Contas de locatário**.

Configuração da página de topologia de grade

Esta permissão fornece acesso às guias Configuração na página **SUPPORT > Tools > Grid topology**.

ILM

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

- Regras
- Políticas
- Codificação de apagamento
- Regiões
- Pools de armazenamento



Os usuários devem ter as permissões **outras configurações de grade** e **Configuração de página de topologia de grade** para gerenciar as notas de armazenamento.

Manutenção

Os usuários devem ter a permissão Manutenção para usar estas opções:

- **CONFIGURAÇÃO > controle de acesso:**

- Senhas de grade

- **MANUTENÇÃO > tarefas:**

- Descomissionar
- Expansão
- Verificação de existência do objeto
- Recuperação

- **MANUTENÇÃO > sistema:**

- Pacote de recuperação
- Atualização de software

- **SUORTE > Ferramentas:**

- Registos

Os utilizadores que não têm a permissão Manutenção podem ver, mas não editar, estas páginas:

- **MANUTENÇÃO > rede:**

- Servidores DNS
- Rede de rede
- Servidores NTP

- **MANUTENÇÃO > sistema:**

- Licença

- **CONFIGURAÇÃO > Segurança:**

- Certificados
- Nomes de domínio

- **CONFIGURAÇÃO > Monitoramento:**

- Servidor de auditoria e syslog

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.

Consulta de métricas

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

Pesquisa de metadados de objetos

Esta permissão fornece acesso à página **ILM > Object metadata lookup**.

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 **Grid topology page Configuration**.

- **ILM:**
 - Classes de armazenamento
- **CONFIGURAÇÃO > rede:**
 - Custo da ligação
- **CONFIGURAÇÃO > sistema:**
 - Opções de visualização
 - Opções de grelha
 - Opções de armazenamento
- **SUPORTE > Alarmes (legado):**
 - Eventos personalizados
 - Alarmes globais
 - Configuração de e-mail legado

Administrador do dispositivo de storage

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

Contas de inquilino

Essa permissão fornece acesso à página de locatários, onde você pode criar, editar e remover contas de locatários. Essa permissão também permite que os usuários visualizem as políticas de classificação de tráfego existentes.

Desative recursos com a API

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. Desativar um recurso é a única maneira de impedir que o usuário root ou usuários que pertencem a grupos de administração com permissão **root Access** 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 **alterar senha de root do locatário** no Gerenciador de Grade (tanto a UI quanto a API), a empresa A pode garantir que nenhum usuário Admin - incluindo o usuário raiz e os usuários pertencentes a grupos com a permissão **acesso root** - pode alterar a senha para o usuário raiz de qualquer conta de locatário.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade. [Use a API de gerenciamento de grade](#) Consulte .
2. Localize o endpoint *Deactivate Features*
3. Para desativar um recurso, como alterar a 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 * alterar senha de root do locatário * não aparece mais na interface do usuário, e qualquer solicitação de API que tente alterar a senha de raiz de um locatário falhará com "403 Forbidden."

Reativar 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.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade.
2. Localize o endpoint *Deactivate Features*
3. Para reativar todos os recursos, envie um corpo para a API assim:

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

Quando essa solicitação estiver concluída, todos os recursos, incluindo o recurso alterar senha de root do locatário, são reativados. A permissão de gerenciamento **alterar senha de root do locatário** agora aparece na interface do usuário, e qualquer solicitação de API que tente alterar a senha de root de um locatário terá êxito, assumindo que o usuário tenha a permissão de gerenciamento **acesso root** ou **alterar senha de root 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 raiz do locatário e continuar a desativar o recurso de reconhecimento de alarme, envie esta SOLICITAÇÃO PUT:

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

Gerenciar usuários

Você pode exibir usuários locais e federados. Você também 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 que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

Crie um usuário local

Você pode criar um ou mais usuários locais e atribuir cada usuário a um ou mais grupos locais. As permissões do grupo controlam quais recursos do Gerenciador de Grade e da API de Gerenciamento de Grade o usuário pode acessar.

Você pode criar somente usuários locais. Use a fonte de identidade externa para gerenciar usuários e grupos federados.

O Gerenciador de Grade inclui um usuário local predefinido, chamado "root". Você não pode remover o usuário raiz.



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

Acesse o assistente

1. Selecione **CONFIGURATION > Access Control > Admin Users**.
2. Selecione **criar usuário**.

Introduza as credenciais do utilizador

1. Introduza o nome completo do utilizador, um nome de utilizador exclusivo e uma palavra-passe.
2. Opcionalmente, selecione **Sim** se esse usuário não tiver acesso ao Gerenciador de Grade ou à API de Gerenciamento de Grade.
3. Selecione **continuar**.

Atribuir a grupos

1. Opcionalmente, atribua o usuário a um ou mais grupos para determinar as permissões do usuário.

Se ainda não tiver criado grupos, pode guardar o utilizador sem selecionar grupos. Você pode adicionar esse usuário a um grupo na página grupos.

Se um usuário pertencer a vários grupos, as permissões serão cumulativas. [Gerenciar grupos de administradores](#) Consulte para obter detalhes.

2. Selecione **Create user** e selecione **Finish**.

Ver e editar utilizadores locais

Você pode exibir detalhes de usuários locais e federados existentes. Você pode modificar um usuário local para alterar o nome completo, a senha ou a associação de grupo do usuário. Você também pode impedir temporariamente que um usuário acesse o Gerenciador de Grade e a API de Gerenciamento de Grade.


Só pode editar utilizadores locais. Use a fonte de identidade externa para gerenciar usuários federados.

- Para exibir informações básicas para todos os usuários locais e federados, revise a tabela na página usuários.
- Para visualizar todos os detalhes de um usuário específico, editar um usuário local ou alterar a senha de um usuário local, use o menu **ações** ou a página de detalhes.

Todas as edições são aplicadas na próxima vez que o usuário sair e, em seguida, voltar a entrar no Gerenciador de Grade.



Os usuários locais podem alterar suas próprias senhas usando a opção **alterar senha** no banner do Gerenciador de Grade.

Tarefa	Menu ações	Página de detalhes
Ver detalhes do utilizador	<ol style="list-style-type: none">Selecione a caixa de verificação para o utilizador.Selecione ações > Exibir detalhes do usuário.	Selecione o nome do usuário na tabela.
Editar nome completo (somente usuários locais)	<ol style="list-style-type: none">Selecione a caixa de verificação para o utilizador.Selecione ações > Editar nome completo.Introduza o novo nome.Selecione Salvar alterações.	<ol style="list-style-type: none">Selecione o nome do usuário para exibir os detalhes.Selecione o ícone de edição .Introduza o novo nome.Selecione Salvar alterações.
Negar ou permitir acesso à StorageGRID	<ol style="list-style-type: none">Selecione a caixa de verificação para o utilizador.Selecione ações > Exibir detalhes do usuário.Selecione a guia Acesso.Selecione Sim para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, ou selecione não para permitir que o usuário faça login.Selecione Salvar alterações.	<ol style="list-style-type: none">Selecione o nome do usuário para exibir os detalhes.Selecione a guia Acesso.Selecione Sim para impedir que o usuário faça login no Gerenciador de Grade ou na API de Gerenciamento de Grade, ou selecione não para permitir que o usuário faça login.Selecione Salvar alterações.

Tarefa	Menu ações	Página de detalhes
Alterar palavra-passe (apenas utilizadores locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione ações > Exibir detalhes do usuário . c. Selecione a guia Senha. d. Introduza uma nova palavra-passe. e. Selecione alterar palavra-passe .	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Senha. c. Introduza uma nova palavra-passe. d. Selecione alterar palavra-passe .
Alterar grupos (somente usuários locais)	a. Selecione a caixa de verificação para o utilizador. b. Selecione ações > Exibir detalhes do usuário . c. Selecione a guia grupos. d. Opcionalmente, selecione o link após um nome de grupo para exibir os detalhes do grupo em uma nova guia do navegador. e. Selecione Editar grupos para selecionar grupos diferentes. f. Selecione Salvar alterações .	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia grupos. c. Opcionalmente, selecione o link após um nome de grupo para exibir os detalhes do grupo em uma nova guia do navegador. d. Selecione Editar grupos para selecionar grupos diferentes. e. Selecione Salvar alterações .

Duplicar um usuário

Você pode duplicar um usuário existente para criar um novo usuário com as mesmas permissões.

1. Selecione a caixa de verificação para o utilizador.
2. Selecione **ações > usuário duplicado**.
3. Conclua o assistente de usuário duplicado.

Eliminar um utilizador

Você pode excluir um usuário local para remover permanentemente esse usuário do sistema.



Não é possível eliminar o utilizador raiz.

1. Na página usuários, marque a caixa de seleção para cada usuário que deseja remover.
2. Selecione **ações > Excluir usuário**.
3. Selecione **Eliminar utilizador**.

Usar logon único (SSO)

Configurar o 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. Os utilizadores locais não podem iniciar sessão no StorageGRID.

Como o single sign-on funciona

O sistema StorageGRID suporta logon único (SSO) usando o padrão de linguagem de marcação de asserção de Segurança 2,0 (SAML 2,0).

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

Inicie sessão quando o SSO estiver ativado

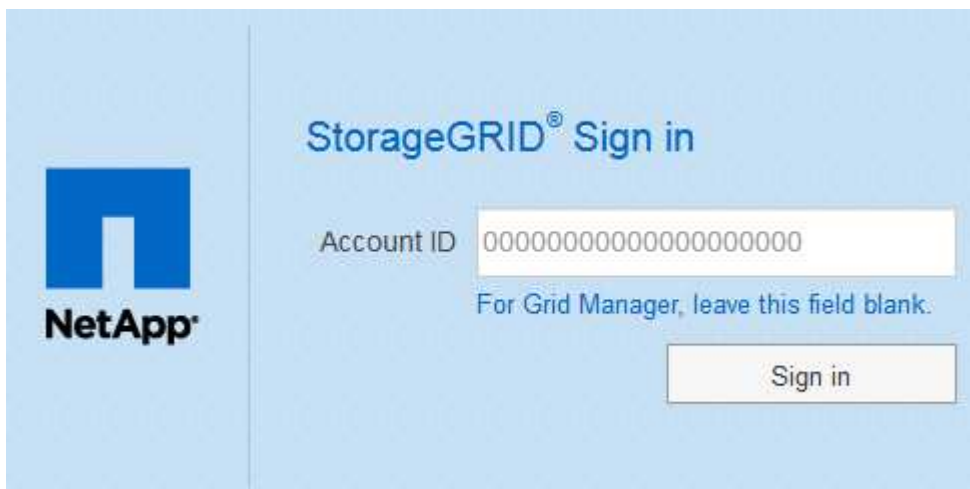
Quando o SSO está ativado e você entra no StorageGRID, você é redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

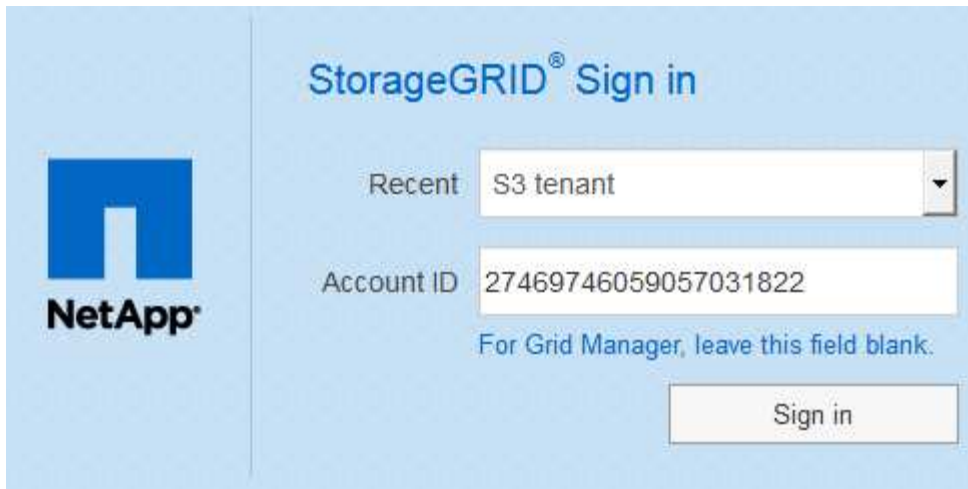
1. Insira o nome de domínio totalmente qualificado ou o endereço IP de qualquer nó de administrador do StorageGRID em um navegador da Web.

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:

A screenshot of the StorageGRID Sign in page. On the left is the NetApp logo. The main area has the title 'StorageGRID® Sign in'. Below it is a text input field labeled 'Account ID' containing a long string of zeros. Underneath the field is the text 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.

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



The image shows the StorageGRID Sign in page. On the left is the NetApp logo. On the right, the title 'StorageGRID® Sign in' is at the top. Below it is a 'Recent' dropdown menu showing 'S3 tenant'. Underneath is an 'Account ID' text box containing '27469746059057031822'. A note below the text box says 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.



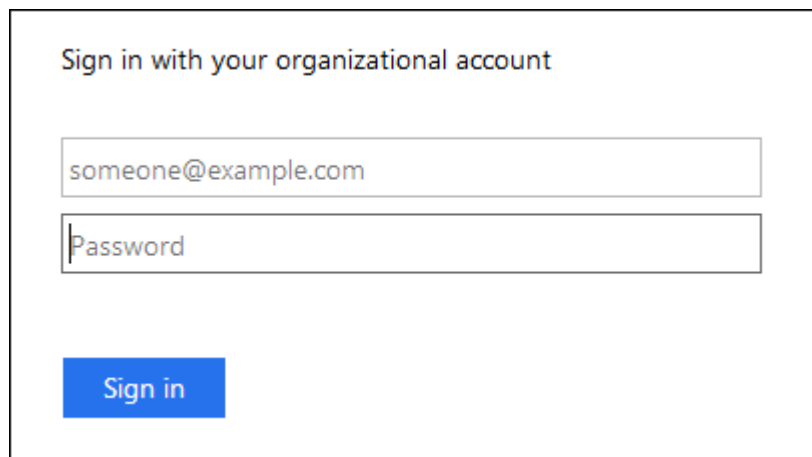
A página de login do StorageGRID não é exibida quando você insere o URL completo de uma conta de locatário (ou seja, um nome de domínio totalmente qualificado ou endereço IP seguido de `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO da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

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

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

3. Selecione **entrar**

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



The image shows a 'Sign in with your organizational account' page. It has a title at the top. Below it are two text input fields: the first contains 'someone@example.com' and the second is labeled 'Password'. At the bottom left is a blue 'Sign in' button.

4. Faça login com suas credenciais SSO.

Se suas credenciais SSO estiverem corretas:

- O provedor de identidade (IDP) fornece uma resposta de autenticação ao StorageGRID.
- O StorageGRID valida a resposta de autenticação.
- Se a resposta for válida e você pertencer a um grupo federado com permissões de acesso ao StorageGRID, você estará conectado ao Gerenciador de Grade ou ao Gerenciador de Locatário,

dependendo da conta selecionada.



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

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

Você não precisa reinserir suas credenciais SSO.

Sair quando o SSO estiver ativado

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

Passos

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

É apresentada a página de início de sessão do StorageGRID. A lista suspensa **Recent Accounts** (Contas recentes) é atualizada para incluir o **Grid Manager** ou o nome do locatário, para que você possa acessar essas interfaces de usuário mais rapidamente no futuro.

Se você estiver conectado a...	E você sai de...	Você está logado fora de...
Grid Manager em um ou mais nós de administração	Grid Manager em qualquer nó de administração	Grid Manager em todos os nós de administração Observação: se você usar o Azure para SSO, pode levar alguns minutos para ser desconectado de todos os nós de administração.
Gerenciador de locatários em um ou mais nós de administração	Gerente de locatário em qualquer nó de administrador	Gerenciador de locatários em todos os nós de administração
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Apenas o Grid Manager. Você também deve sair do Gerenciador do Locatário para sair do SSO.



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

Requisitos para o uso de logon único

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

Requisitos do provedor de identidade

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

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

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

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Active Directory	<ul style="list-style-type: none">• Active Directory• Azure• PingFederate
Azure	Azure

Requisitos do AD FS

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

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



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.

Requisitos adicionais

- Transport Layer Security (TLS) 1,2 ou 1,3
- Microsoft .NET Framework, versão 3.5.1 ou superior

Requisitos de certificado do servidor

Por padrão, o StorageGRID usa um certificado 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 confiança de parte confiável (AD FS), aplicativos empresariais (Azure) ou conexões de provedor de serviços (PingFederate) para StorageGRID, você usa o certificado de servidor como o certificado de assinatura para solicitações StorageGRID.

Se ainda não [configurado um certificado personalizado para a interface de gerenciamento](#) fez, 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 partes dependentes do StorageGRID, aplicativos empresariais ou conexões SP.



O uso do certificado de servidor padrão de um nó de administrador em uma conexão de confiança de parte confiável, aplicativo empresarial ou SP não é recomendado. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de iniciar sessão no nó recuperado, tem de atualizar a confiança de parte fidedigna, a aplicação empresarial ou a ligação SP 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.

Requisitos portuários

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 autenticuem com logon único. [Controle o acesso através de firewalls](#) Consulte.

Confirme se os 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- Você já configurou a federação de identidade.

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 **GERENCIAMENTO DE ACESSO > federação de identidade**.
 - 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 selecione **Salvar**.
2. Confirme se um usuário federado pode acessar o Gerenciador de Grade:
 - a. No Gerenciador de Grade, selecione **CONFIGURATION > Access Control > Admin Groups**.
 - 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 selecione **ações > Editar**.
 - c. Na guia Inserir detalhes, selecione **continuar**.
 - d. Se a caixa de seleção **Use own Identity source** estiver selecionada, desmarque a caixa e selecione **Save**.

Edit the tenant

Enter details ————— 2 Select permissions

Select permissions

Select the permissions for this tenant account.

☐ Allow platform services ?

☐ Use own identity source ?

☐ Allow S3 Select ?

É apresentada a página do locatário.

- a. Selecione a conta de locatário, selecione **entrar** e faça login na conta de locatário como usuário raiz local.
- b. No Gerenciador do Locatário, selecione **GERENCIAMENTO 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](#)
- [Gerenciar grupos de administradores](#)
- [Use uma conta de locatário](#)

Use o modo sandbox

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

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- Você configurou a federação de identidade para o seu sistema StorageGRID.
- Para a federação de identidade **tipo de serviço LDAP**, você selecionou o ativo Directory ou o Azure, com base no provedor de identidade SSO que você planeja usar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Ativo Directory	<ul style="list-style-type: none">• Ativo Directory• Azure• PingFederate
Azure	Azure

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 provedor de identidade SSO. Por sua vez, o provedor de identidade SSO envia uma resposta de autenticação de volta ao StorageGRID, indicando se a solicitação de autenticação foi bem-sucedida. Para solicitações bem-sucedidas:

- A resposta do ativo Directory ou PingFederate inclui um identificador universal único (UUID) para o usuário.
- A resposta do Azure inclui um Nome Principal de Usuário (UPN).

Para permitir que o StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre solicitações de autenticação de usuário, você deve configurar certas configurações no StorageGRID. Em seguida, você deve usar o software do provedor de identidade SSO para criar uma confiança de parte confiável (AD FS), aplicativo empresarial (Azure) ou provedor de serviços (PingFederate) para cada nó de administração. 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. Quando você está usando o modo sandbox, os usuários não podem entrar usando SSO.

Acesse o modo sandbox

1. Selecione **CONFIGURATION > access control > Single sign-on**.

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

Single Sign-on

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

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Se as opções de Status SSO não forem exibidas, confirme se você configurou o provedor de identidade como a origem de identidade federada. [Requisitos para o uso de logon único](#) Consulte .

2. Selecione **Sandbox Mode**.

A seção Provedor de identidade é exibida.

Insira os detalhes do provedor de identidade

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

Active Directory

1. Digite o nome do serviço **Federation** para o provedor de identidade, exatamente como aparece no Active Directory Federation Service (AD FS).



Para localizar o nome do serviço de federação, vá para Gerenciador do Windows Server. 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.

2. Especifique qual certificado TLS será usado 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 o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.
 - **Não use TLS:** Não use um certificado TLS para proteger a conexão.
3. Na seção parte dependente, especifique o **identificador de parte dependente** para StorageGRID. Esse valor controla o nome que você usa para cada confiança de parte confiável no AD FS.
 - 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 mostra o identificador de parte confiável para cada nó Admin em seu sistema, com base no nome do host do nó.



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.

4. Selecione **Guardar**.

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



Azure

1. Especifique qual certificado TLS será usado 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 o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

- **Não use TLS:** Não use um certificado TLS para proteger a conexão.
2. Na seção aplicativo empresarial, especifique o **Nome do aplicativo empresarial** para StorageGRID. Esse valor controla o nome que você usa para cada aplicativo corporativo no Azure AD.
 - 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 mostra um nome de aplicativo corporativo para cada nó Admin em seu sistema, com base no nome do host do nó.



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

3. Siga as etapas em [Crie aplicativos empresariais no Azure AD](#) para criar um aplicativo corporativo para cada nó de administração listado na tabela.
4. No Azure AD, copie o URL de metadados da federação para cada aplicativo corporativo. Em seguida, cole esse URL no campo **URL de metadados de Federação** correspondente no StorageGRID.
5. Depois de copiar e colar um URL de metadados de federação para todos os nós de administração, selecione **Salvar**.

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



PingFederate

1. Especifique qual certificado TLS será usado 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 o texto do certificado personalizado e cole-o na caixa de texto **certificado CA**.

 - **Não use TLS:** Não use um certificado TLS para proteger a conexão.
2. Na seção Fornecedor de Serviços (SP), especifique o **ID de conexão SP** para StorageGRID. Esse valor controla o nome que você usa para cada conexão SP no PingFederate.
 - 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 mostra o ID de conexão do SP para cada nó de administrador no sistema, com base no nome do host do nó.



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

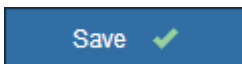
3. Especifique o URL de metadados de federação para cada nó Admin no campo **URL de metadados de Federação**.

Use o seguinte formato:

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

4. Selecione **Guardar**.

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



Configurar trusts de terceiros confiáveis, aplicativos empresariais ou conexões SP

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

O StorageGRID pode permanecer no modo sandbox enquanto necessário. No entanto, quando **modo Sandbox** está selecionado na página de logon único, o SSO é desativado para todos os usuários do StorageGRID. Somente usuários locais podem fazer login.

Siga estas etapas para configurar as trusts de parte confiável (ative Directory), aplicativos empresariais completos (Azure) ou configurar conexões SP (PingFederate).

Active Directory

1. Vá para Serviços de Federação do Active Directory (AD FS).
2. Crie uma ou mais confiança de parte confiáveis para o StorageGRID, usando cada identificador de parte confiável mostrado na tabela na página de logon único do StorageGRID.

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

Para obter instruções, vá [Criar confiança de parte confiável no AD FS](#) para .

Azure

1. Na página de logon único para o nó Admin ao qual você está conectado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
 - a. Faça login no nó.
 - b. Selecione **CONFIGURATION > access control > Single sign-on**.
 - c. Baixe e salve os metadados SAML para esse nó.
3. Vá para o Portal do Azure.
4. Siga as etapas em [Crie aplicativos empresariais no Azure AD](#) para carregar o arquivo de metadados SAML para cada nó Admin em seu aplicativo corporativo do Azure correspondente.

PingFederate

1. Na página de logon único para o nó Admin ao qual você está conectado atualmente, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para qualquer outro nó Admin na sua grade, repita estas etapas:
 - a. Faça login no nó.
 - b. Selecione **CONFIGURATION > access control > Single sign-on**.
 - c. Baixe e salve os metadados SAML para esse nó.
3. Vá para PingFederate.
4. [Crie uma ou mais conexões de provedor de serviços \(SP\) para o StorageGRID](#). Use o ID de conexão do SP para cada nó de administrador (mostrado na tabela na página de logon único do StorageGRID) e os metadados SAML que você baixou para esse nó de administrador.

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

Testar conexões SSO

Antes de aplicar o uso de logon único para todo o sistema StorageGRID, você deve confirmar que o logon único e o logout único estão configurados corretamente para cada nó de administração.

Active Directory

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

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

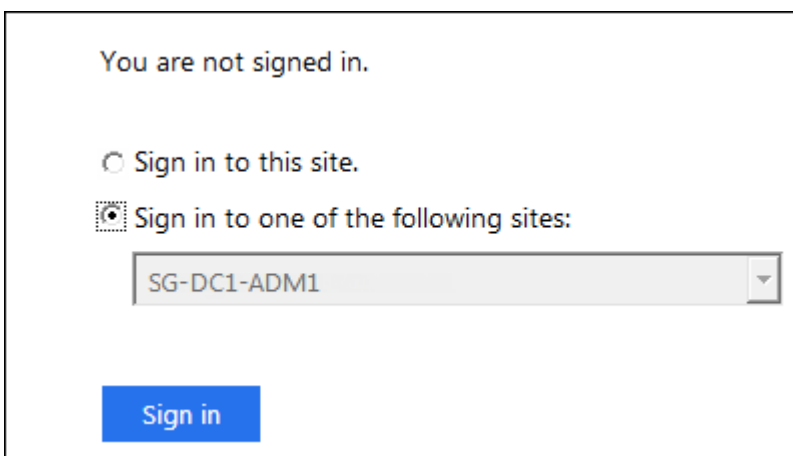
Sandbox mode

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

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

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

2. Selecione o link ou copie e cole o URL em um navegador para acessar a página de login do provedor de identidade.
3. 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 selecione **entrar**.



4. 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.
5. Repita estas etapas para verificar a conexão SSO para cada nó Admin na grade.

Azure

1. Vá para a página de logon único no portal do Azure.
2. Selecione **Teste este aplicativo**.
3. Insira as credenciais de um usuário federado.
 - 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.
4. Repita estas etapas para verificar a conexão SSO para cada nó Admin na grade.

PingFederate

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

Selecione e teste um link de cada vez.

Sandbox mode

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

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Insira as credenciais de um usuário federado.
 - 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.
3. Selecione o próximo link para verificar a conexão SSO para cada nó Admin na grade.

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

Ative o logon único

Quando você confirmar que pode usar o SSO para fazer login em cada nó de administrador, você pode ativar o SSO para todo o seu sistema StorageGRID.



Quando o SSO está ativado, todos os usuários devem usar o SSO para acessar o Gerenciador de Grade, o Gerenciador de Locatário, a API de Gerenciamento de Grade e a API de Gerenciamento de Locatário. Os usuários locais não podem mais acessar o StorageGRID.

1. Selecione **CONFIGURATION > access control > Single sign-on**.
2. Altere o Status SSO para **Enabled**.
3. Selecione **Guardar**.
4. Reveja a mensagem de aviso e selecione **OK**.

O início de sessão único está agora ativado.



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

Criar confiança de parte confiável no AD FS

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

O que você vai precisar

- Você configurou o logon único para o StorageGRID e selecionou **AD FS** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. [Use o modo sandbox](#) Consulte .
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador de entidade dependente para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos nós de administração na página de logon único do StorageGRID.



Você deve criar uma 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.
- Se você estiver criando a confiança de parte confiável manualmente, 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.

Sobre esta tarefa

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

Crie 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.

Passos

1. No menu Iniciar do Windows, selecione o ícone do PowerShell com o botão direito 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. Selecione **aplicar** e **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. Selecione **Adicionar regra**.
- d. Na página Seleccionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **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 **active 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. Selecione **Finish** e **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, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. [Use o modo Sandbox](#) Consulte para obter instruções.

Crie 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.

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas e Gerenciamento do AD FS**.
2. Em ações, selecione **Adicionar confiança de parte dependente**.
3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **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. Selecione **Adicionar regra**:
 - c. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **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 **active 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. Selecione **Finish** e **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, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. [Use o modo Sandbox](#) Consulte para obter instruções.

Crie uma confiança de parte confiável manualmente

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

Passos

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

2. Em ações, selecione **Adicionar confiança de parte dependente**.

3. Na página de boas-vindas, escolha **reconhecimento de reclamações** e selecione **Iniciar**.

4. Selecione **Digite os dados sobre a parte que depende manualmente** e selecione **Next**.

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, selecione **Adicionar regra**:

- a. Na página Selecionar modelo de regra, selecione **Enviar atributos LDAP como reivindicações** na lista e selecione **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 **ativo 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. Selecione **Finish** e **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. Selecione **Adicionar 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. Selecione **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. Selecione **aplicar** e **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, retorne ao StorageGRID e teste todas as confianças de terceiros confiáveis para confirmar que elas estão configuradas corretamente. [Use o modo sandbox](#) Consulte para obter instruções.

Crie aplicativos empresariais no Azure AD

Você usa o Azure AD para criar um aplicativo corporativo para cada nó de administrador no sistema.

O que você vai precisar

- Você começou a configurar o logon único para o StorageGRID e selecionou **Azure** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. [Use o modo sandbox](#) Consulte .
- Você tem o **Nome do aplicativo Enterprise** para cada nó Admin no seu sistema. Você pode copiar esses valores da tabela de detalhes do nó de administrador na página de logon único do StorageGRID.



Você deve criar um aplicativo empresarial para cada nó de administração no sistema StorageGRID. Ter um aplicativo corporativo 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 aplicativos empresariais no Azure active Directory.
- Você tem uma conta do Azure com uma assinatura ativa.
- Você tem uma das seguintes funções na conta do Azure: Administrador Global, Administrador de aplicativos em nuvem, Administrador de aplicativos ou proprietário do responsável do serviço.

Acesse o Azure AD

1. Inicie sessão no "[Portal do Azure](#)".
2. Navegue até "[Azure active Directory](#)".
3. "[Aplicações empresariais](#)"Selecione .

Crie aplicativos empresariais e salve a configuração SSO do StorageGRID

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

1. Repita as etapas a seguir para cada nó Admin.
 - a. No painel aplicativos do Azure Enterprise, selecione **novo aplicativo**.
 - b. Selecione **Crie seu próprio aplicativo**.
 - c. Para o nome, insira o **Nome do aplicativo da empresa** que você copiou da tabela de detalhes do nó de administrador na página de logon único do StorageGRID.
 - d. Deixe o botão de opção **integrar qualquer outro aplicativo que você não encontrar na galeria (não galeria)** selecionado.
 - e. Selecione **criar**.
 - f. Selecione o link **Get Started** no **2. Configure a caixa Single Sign On** (Início de sessão único) ou selecione o link **Single Sign-On** (Início de sessão único) na margem esquerda.
 - g. Selecione a caixa **SAML**.
 - h. Copie o URL de metadados de Federação de aplicativos*, que você pode encontrar em **Etapa 3 certificado de assinatura SAML**.
 - i. Vá para a página de logon único do StorageGRID e cole o URL no campo **URL de metadados da Federação** que corresponde ao nome do aplicativo **empresa** que você usou.
2. Depois de colar um URL de metadados de federação para cada nó de administrador e fazer todas as outras alterações necessárias na configuração SSO, selecione **Salvar** na página de logon único do StorageGRID.

Faça o download dos metadados SAML para cada nó de administração

Depois que a configuração SSO for salva, você pode baixar um arquivo de metadados SAML para cada nó de administrador no sistema StorageGRID.

Repita estas etapas para cada nó Admin:

1. Inicie sessão no StorageGRID a partir do nó de administração.
2. Selecione **CONFIGURATION > access control > Single sign-on**.
3. Selecione o botão para baixar os metadados SAML para esse nó Admin.
4. Salve o arquivo, que você carregará no Azure AD.

Carregue metadados SAML para cada aplicação empresarial

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

1. Retorne ao Portal do Azure.
2. Repita estes passos para cada aplicação empresarial:



Talvez seja necessário atualizar a página aplicativos empresariais para ver os aplicativos adicionados anteriormente na lista.

- a. Vá para a página Propriedades do aplicativo corporativo.
- b. Defina **atribuição necessária** como **não** (a menos que você queira configurar atribuições separadamente).
- c. Acesse a página de início de sessão único.

- d. Conclua a configuração SAML.
 - e. Selecione o botão **Upload metadata file** e selecione o arquivo de metadados SAML que você baixou para o Admin Node correspondente.
 - f. Depois que o arquivo for carregado, selecione **Save** e, em seguida, selecione **X** para fechar o painel. Você será retornado à página Configurar logon único com SAML.
3. Siga os passos em [Use o modo sandbox](#) para testar cada aplicação.

Crie conexões de provedor de serviços (SP) no PingFederate

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

O que você vai precisar

- Você configurou o logon único para o StorageGRID e selecionou **Ping federate** como o tipo SSO.
- **O modo Sandbox** está selecionado na página de logon único no Gerenciador de Grade. [Use o modo sandbox](#) Consulte .
- Você tem o **ID de conexão SP** para cada nó de administrador no sistema. Você pode encontrar esses valores na tabela de detalhes dos nós de administração na página de logon único do StorageGRID.
- Você baixou os **metadados SAML** para cada nó Admin no seu sistema.
- Você tem experiência em criar conexões SP no servidor PingFederate.
- Você tem o "[Guia de referência do administrador](#)" para PingFederate Server. A documentação do PingFederate fornece instruções detalhadas passo a passo e explicações.
- Você tem a permissão Admin para PingFederate Server.

Sobre esta tarefa

Estas instruções resumem como configurar o PingFederate Server versão 10,3 como um provedor SSO para o StorageGRID. Se você estiver usando outra versão do PingFederate, talvez seja necessário adaptar essas instruções. Consulte a documentação do PingFederate Server para obter instruções detalhadas sobre o seu lançamento.

Complete pré-requisitos no PingFederate

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

Criar armazenamento de dados

Se você ainda não o fez, crie um armazenamento de dados para conectar o PingFederate ao servidor LDAP do AD FS. Use os valores usados [configurando a federação de identidade](#) no StorageGRID.

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

Criar validador de credenciais de senha

Se você ainda não o fez, crie um validador de credenciais de senha.

- **Type:** LDAP Username Password Credential Validator
- **Armazenamento de dados:** Selecione o armazenamento de dados que você criou.
- **Base de pesquisa:** Insira informações do LDAP (por exemplo,
- **Filtro de pesquisa:** SAMAccountName
- **Escopo:** Subárvore

Criar instância de adaptador IDP

Se você ainda não o fez, crie uma instância de adaptador IDP.

1. Acesse a **Autenticação > integração > adaptadores IDP**.
2. Selecione **criar nova instância**.
3. Na guia tipo, selecione **HTML form IDP Adapter**.
4. Na guia adaptador IDP, selecione **Adicionar uma nova linha a 'Validadores de credenciais'**.
5. Selecione o [validador de credenciais de senha](#) que você criou.
6. Na guia Adapter Attributes (atributos do adaptador), selecione o atributo **username** para **pseudônimo**.
7. Selecione **Guardar**.

Criar ou importar certificado de assinatura[[certificado de assinatura]]

Se ainda não o fez, crie ou importe o certificado de assinatura.

1. Acesse a **Security > Signing & Decryption Keys & Certificates**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP no PingFederate

Quando você cria uma conexão SP no PingFederate, importa os metadados SAML que você baixou do StorageGRID para o nó Admin. O arquivo de metadados contém muitos dos valores específicos que você precisa.



Você deve criar uma conexão SP para cada nó de administração no sistema StorageGRID, para que os usuários possam fazer login e sair com segurança de qualquer nó. Use estas instruções para criar a primeira conexão SP. Em seguida, acesse a [Crie conexões SP adicionais](#) para criar quaisquer ligações adicionais de que necessita.

Escolha o tipo de conexão SP

1. Acesse a **aplicações > integração > ligações SP**.
2. Selecione **criar conexão**.
3. Selecione **não utilize um modelo para esta ligação**.
4. Selecione **Browser SSO Profiles** e **SAML 2,0** como protocolo.

Importar metadados do SP

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

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

4. Selecione **seguinte**.

Configure o SSO do navegador IDP

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia perfis SAML, selecione as opções **SSO iniciado por SP**, **SLO inicial por SP**, **SSO iniciado por IDP** e **SLO iniciado por IDP**.
3. Selecione **seguinte**.
4. Na guia Assertion Lifetime, não faça alterações.
5. Na guia criação de asserções, selecione **Configurar criação de asserções**.
 - a. Na guia Mapeamento de identidade, selecione **Standard**.
 - b. Na guia Contrato de Atributo, use o **SAML_SUBJECT** como Contrato de Atributo e o formato de nome não especificado que foi importado.
6. Para estender o contrato, selecione **Excluir** para remover `urn:oid o`, que não é usado.

Instância do adaptador de mapa

1. Na guia Mapeamento de origem de autenticação, selecione **Mapear nova instância de adaptador**.
2. Na guia instância do adaptador, selecione o **instância do adaptador** que você criou.
3. Na guia método de mapeamento, selecione **recuperar atributos adicionais de um armazenamento de dados**.
4. Na guia origem do atributo e Pesquisa de usuário, selecione **Adicionar origem do atributo**.
5. Na guia armazenamento de dados, forneça uma descrição e selecione o **armazenamento de dados** que você adicionou.
6. Na guia Pesquisa de diretório LDAP:
 - Digite o **DN base**, que deve corresponder exatamente ao valor inserido no StorageGRID para o servidor LDAP.
 - Para o escopo de pesquisa, selecione **subtree**.
 - Para a classe de objeto raiz, procure o atributo **objectGUID** e adicione-o.
7. Na guia tipos de codificação de atributos binários LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia filtro LDAP, digite **sAMAccountName**.
9. Na guia execução de contrato de atributo, selecione **LDAP (attribute)** na lista suspensa origem e selecione **objectGUID** na lista suspensa valor.
10. Revise e salve a fonte do atributo.

11. Na guia origem do atributo de salvamento de falha, selecione **Abortar a transação SSO**.
12. Reveja o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configure as definições do protocolo

1. Na guia **conexão SP > SSO do navegador > Configurações do protocolo**, selecione **Configurar configurações do protocolo**.
2. Na guia URL do Serviço ao Consumidor de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para vinculação e `/api/saml-response` URL do ponto final).
3. Na guia URLs de serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para vinculação e `/api/saml-logout` para URL de ponto final).
4. Na guia Allowable SAML Bindings (ligações SAML permitidas), desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são obrigatórios.
5. Na guia Política de assinatura, deixe as caixas de seleção **Require Authn Requests to be signed** e **Always Sign Assertion** selecionadas.
6. Na guia Diretiva de criptografia, selecione **nenhum**.
7. Reveja o resumo e selecione **Concluído** para guardar as definições do protocolo.
8. Revise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

1. Na guia conexão SP, selecione **credenciais**.
2. Na guia credenciais, selecione **Configurar credenciais**.
3. Selecione o [certificado de assinatura](#) que você criou ou importou.
4. Selecione **Next** para ir para **Manage Signature Verification Settings**.
 - a. Na guia Trust Model (modelo de confiança), selecione **Unanchored** (sem ancoragem).
 - b. Na guia certificado de verificação de assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID.
5. Reveja os ecrãs de resumo e selecione **Guardar** para guardar a ligação SP.

Crie conexões SP adicionais

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



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

1. Selecione **Ação > Copiar** para criar uma cópia da conexão SP inicial para cada nó de administração adicional.
2. Introduza a ID da ligação e o nome da ligação para a cópia e selecione **Guardar**.
3. Escolha o arquivo de metadados correspondente ao nó Admin:
 - a. Selecione **Ação > Atualizar com metadados**.

- b. Selecione **escolha Arquivo** e carregue os metadados.
 - c. Selecione **seguinte**.
 - d. Selecione **Guardar**.
4. Resolva o erro devido ao atributo não utilizado:
 - a. Selecione a nova ligação.
 - b. Selecione **Configure Browser SSO > Configure Assertion creation > Attribute Contract**.
 - c. Exclua a entrada para **urn:oid**.
 - d. Selecione **Guardar**.

Desative o 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

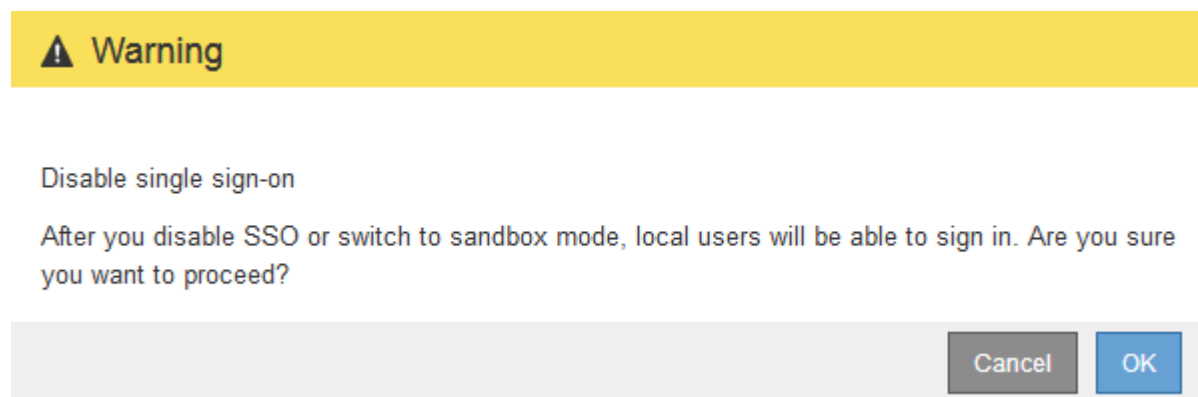
Passos

1. Selecione **CONFIGURATION > access control > Single sign-on**.

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

2. Selecione a opção **Disabled** (Desativado).
3. Selecione **Guardar**.

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



4. Selecione **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.

Desative e reative 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 tem permissões de acesso específicas.
- Você tem o `Passwords.txt` arquivo.
- Você sabe 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:

- Introduza o seguinte comando: `ssh admin@Admin_Node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- 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:

- Selecione **CONFIGURATION > access control > Single sign-on**.
- Altere as configurações de SSO incorretas ou desatualizadas.
- Selecione **Guardar**.

Selecionar **Save** na página Single Sign-On (Início de sessão único) reativa automaticamente o SSO para toda a grelha.

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. Selecione **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.

Gerir as definições de segurança

Gerenciar certificados

Sobre certificados de segurança

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 conecta 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).

- Certificado padrão de CA de grade*

O StorageGRID inclui uma autoridade de certificação (CA) integrada que gera um certificado interno da CA de grade durante a instalação do sistema. O certificado de CA de grade é usado, por padrão, para proteger o

tráfego interno do StorageGRID. Uma autoridade de certificação externa (CA) pode emitir certificados personalizados que são totalmente compatíveis com as políticas de segurança de informações da sua organização. Embora seja possível usar o certificado da CA de Grade 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 aos [diretrizes de endurecimento do sistema](#) certificados do servidor para.
- 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.

Acesse certificados de segurança

Você pode acessar informações sobre todos os certificados do StorageGRID em um único local, juntamente com links para o fluxo de trabalho de configuração de cada certificado.

1. No Gerenciador de Grade, selecione **CONFIGURATON > Segurança > certificados**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

GlobalGrid CAClientLoad balancer endpointsTenantsOther

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type	Expiration date
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Selecione uma guia na página certificados para obter informações sobre cada categoria de certificado e para acessar as configurações de certificado. Você só pode acessar uma guia se tiver a permissão apropriada.

- * Global*: Protege o acesso à StorageGRID de navegadores da web e clientes de API externos.
- * Grade CA*: Protege o tráfego interno do StorageGRID.
- **Cliente**: Protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
- * Terminais de balanceador de carga*: Protege conexões entre clientes S3 e Swift e o balanceador de carga StorageGRID.
- * Inquilinos*: Protege conexões com servidores de federação de identidade ou de endpoints de serviço de plataforma para recursos de armazenamento S3.
- **Outros**: Protege conexões StorageGRID que exigem certificados específicos.

Cada guia é descrito abaixo com links para detalhes adicionais do certificado.

Global

Os certificados globais protegem o acesso à StorageGRID a partir de navegadores da Web e clientes externos da API S3 e Swift. Dois certificados globais são inicialmente gerados pela autoridade de certificação StorageGRID durante a instalação. A prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa.

- [Certificado de interface de gerenciamento](#): Protege as conexões do navegador da Web do cliente às interfaces de gerenciamento do StorageGRID.
- [Certificado API S3 e Swift](#): Protege as conexões da API do cliente aos nós de storage, nós de administração e nós de gateway, que os aplicativos clientes S3 e Swift usam para carregar e baixar dados de objetos.

As informações sobre os certificados globais instalados incluem:

- **Nome**: Nome do certificado com link para gerenciar o certificado.
- **Descrição**
- **Tipo**: Personalizado ou padrão. Você deve sempre usar um certificado personalizado para melhorar a segurança da grade.
- **Data de expiração**: Se estiver usando o certificado padrão, nenhuma data de expiração será exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
 - [Substitua o certificado padrão da interface de gerenciamento gerado pelo StorageGRID](#) Usado para conexões do Grid Manager e do Tenant Manager.
 - [Substitua o certificado API S3 e Swift](#) Usado para conexões de nó de armazenamento, serviço CLB (obsoleto) e terminais de balanceador de carga (opcional).
- [Restaure o certificado padrão da interface de gerenciamento](#).
- [Restaure o certificado padrão da API S3 e Swift](#).
- [Use um script para gerar um novo certificado de interface de gerenciamento autoassinado](#).
- Copie ou transfira a [certificado de interface de gerenciamento](#) ou [Certificado API S3 e Swift](#).

CA da grelha

O [Certificado CA de grade](#), gerado pela autoridade de certificação StorageGRID durante a instalação do StorageGRID, protege todo o tráfego interno do StorageGRID.

As informações do certificado incluem a data de validade do certificado e o conteúdo do certificado.

Você pode [Copie ou baixe o certificado da CA de Grade](#), mas não pode alterá-lo.

Cliente

[Certificados de cliente](#), Gerado por uma autoridade de certificação externa, proteja as conexões entre ferramentas de monitoramento externas e o banco de dados do StorageGRID Prometheus.

A tabela de certificados tem uma linha para cada certificado de cliente configurado e indica se o certificado pode ser usado para acesso ao banco de dados Prometheus, juntamente com a data de validade do certificado.

Você pode:

- [Carregue ou gere um novo certificado de cliente.](#)
- Selecione um nome de certificado para exibir os detalhes do certificado onde você pode:
 - [Altere o nome do certificado do cliente.](#)
 - [Defina a permissão de acesso Prometheus.](#)
 - [Carregue e substitua o certificado do cliente.](#)
 - [Copie ou baixe o certificado do cliente.](#)
 - [Remova o certificado do cliente.](#)
- Selecione **ações** para rapidamente [editar](#), [fixe](#), ou [retire](#) um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los ao mesmo tempo usando **ações** > **Remover**.

Pontos de extremidade do balanceador de carga

[Certificados de terminais do balanceador de carga](#), Que você carrega ou gera, proteja as conexões entre clientes S3 e Swift e o serviço de balanceamento de carga StorageGRID em nós de gateway e nós de administração.

A tabela de endpoint do balanceador de carga tem uma linha para cada endpoint do balanceador de carga configurado e indica se o certificado global S3 e Swift API ou um certificado de endpoint do balanceador de carga personalizado está sendo usado para o endpoint. A data de validade de cada certificado também é exibida.



As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- [Selecione um nome de endpoint para abrir uma guia do navegador com informações sobre o endpoint do balanceador de carga, incluindo os detalhes do certificado.](#)
- [Especifique um certificado de endpoint do balanceador de carga para o FabricPool.](#)
- [Use o certificado global S3 e Swift API](#) em vez de gerar um novo certificado de endpoint do balanceador de carga.

Inquilinos

Os locatários podem usar [certificados de servidor de federação de identidade](#) ou [certificados de endpoint de serviço de plataforma](#) proteger suas conexões com o StorageGRID.

A tabela de locatário tem uma linha para cada locatário e indica se cada locatário tem permissão para usar sua própria fonte de identidade ou serviços de plataforma.

Você pode:

- [Selecione um nome de locatário para iniciar sessão no Gestor de inquilinos](#)
- [Selecione um nome de locatário para exibir os detalhes da federação de identidade do locatário](#)
- [Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma do locatário](#)
- [Especifique um certificado de endpoint de serviço de plataforma durante a criação do endpoint](#)

Outros

O StorageGRID usa outros certificados de segurança para fins específicos. Estes certificados são listados pelo seu nome funcional. Outros certificados de segurança incluem:

- [Certificados de federação de identidade](#)
- [Certificados do Cloud Storage Pool](#)
- [Certificados de servidor de gerenciamento de chaves \(KMS\)](#)
- [Certificados de logon único](#)
- [Certificados de notificação de alerta por e-mail](#)
- [Certificados de servidor syslog externos](#)

As informações indicam o tipo de certificado que uma função utiliza e as datas de expiração do certificado do servidor e do cliente, conforme aplicável. A seleção de um nome de função abre uma guia do navegador onde você pode exibir e editar os detalhes do certificado.



Você só pode exibir e acessar informações de outros certificados se tiver a permissão apropriada.

Você pode:

- [Exibir e editar um certificado de federação de identidade](#)
- [Carregar certificados de servidor de gerenciamento de chaves \(KMS\) e cliente](#)
- [Especifique um certificado do Cloud Storage Pool para S3, C2S S3 ou Azure](#)
- [Especifique manualmente um certificado SSO para confiança de parte confiável](#)
- [Especifique um certificado para notificações por e-mail de alerta](#)
- [Especifique um certificado de servidor syslog externo](#)

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para artigos que contêm instruções de implementação.

Certificado de interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	<p>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.</p> <p>Este certificado também autentica as conexões da API de Gerenciamento de Grade e da API de Gerenciamento do locatário.</p> <p>Pode utilizar o certificado predefinido criado durante a instalação ou carregar um certificado personalizado.</p>	CONFIGURATION > Security > Certificates , selecione a guia Global e, em seguida, selecione Management interface certificate	Configurar certificados de interface de gerenciamento

Certificado API S3 e Swift

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras de clientes S3 ou Swift a um nó de armazenamento, ao serviço CLB (Connection Load Balancer) obsoleto em um nó de gateway e terminais de balanceador de carga (opcional).	CONFIGURATION > Security > Certificates , selecione a guia Global e, em seguida, selecione S3 e Swift API certificate	Configure os certificados API S3 e Swift

Certificado CA de grade

Consulte [Descrição do certificado da CA de Grade padrão](#).

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	<p>Instalado em cada cliente, permitindo que o StorageGRID autentique o acesso de cliente externo.</p> <ul style="list-style-type: none"> • Permite que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas. 	CONFIGURATION > Security > Certificates e selecione a guia Client	Configurar certificados de cliente

Certificado de ponto final do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	<p>Autentica a conexão entre clientes S3 ou Swift e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração. Você pode fazer upload ou gerar um certificado de balanceador de carga ao configurar um endpoint de balanceador de carga. Os aplicativos clientes usam o certificado do balanceador de carga ao se conectar ao StorageGRID para salvar e recuperar dados de objeto.</p> <p>Você também pode usar uma versão personalizada do certificado global Certificado API S3 e Swift para autenticar conexões com o serviço Load Balancer. Se o certificado global for usado para autenticar conexões do balanceador de carga, você não precisará carregar ou gerar um certificado separado para cada ponto de extremidade do balanceador de carga.</p> <p>Nota: o certificado usado para autenticação do balanceador de carga é o certificado mais usado durante a operação normal do StorageGRID.</p>	CONFIGURATION > Network > Load balancer endpoints	<ul style="list-style-type: none"> • Configurar pontos de extremidade do balanceador de carga • Crie um ponto de extremidade do balanceador de carga para o FabricPool

Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre o StorageGRID e um provedor de identidade externo, como ative Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, que permite que grupos de administração e usuários sejam gerenciados por um sistema externo.	CONFIGURATION > Access Control > Identity Federation	Use a federação de identidade

Certificado de endpoint de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
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	Criar endpoint de serviços de plataforma Editar endpoint de serviços de plataforma

Certificado de endpoint do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um pool de storage de nuvem do StorageGRID para um local de storage externo, como o S3 Glacier ou o storage Microsoft Azure Blob. Um certificado diferente é necessário para cada tipo de provedor de nuvem.	ILM > conjuntos de armazenamento	Crie um pool de storage em nuvem

Certificado de servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
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.	CONFIGURATION > Security > Key Management Server	Adicionar servidor de gerenciamento de chaves (KMS)

Certificado de logon único (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como AD FS (Serviços de Federação do Active Directory) e StorageGRID usados para solicitações de logon único (SSO).	CONFIGURATION > access control > Single sign-on	Configurar o logon único

Certificado de notificação de alerta por e-mail

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	<p>Autentica a conexão entre um servidor de e-mail SMTP e o StorageGRID que é usado para notificações de alerta.</p> <ul style="list-style-type: none"> • Se as comunicações com o servidor SMTP exigirem TLS (Transport Layer Security), você deverá especificar o certificado CA do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação. 	ALERTAS > Configuração do e-mail	Configurar notificações por e-mail para alertas

Certificado de servidor syslog externo

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	<p>Autentica a conexão TLS ou RELP/TLS entre um servidor syslog externo que Registra eventos no StorageGRID.</p> <p>Nota: não é necessário um certificado de servidor syslog externo para conexões TCP, RELP/TCP e UDP a um servidor syslog externo.</p>	CONFIGURATION > Monitoring > Audit and syslog Server e selecione Configure External syslog Server	Configurar um servidor syslog externo

Exemplos de certificados

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 conecta 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.

Configurar certificados de servidor

Tipos de certificado de servidor suportados

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (algoritmo de assinatura digital de curva elíptica).

Para obter mais informações sobre como o StorageGRID protege conexões de clientes para a API REST, [Use S3](#) consulte ou [Use Swift](#).

Configurar certificados de interface de gerenciamento

Você pode substituir o certificado de interface de gerenciamento padrão por um único certificado personalizado que permite que os usuários acessem o Gerenciador de Grade e o Gerenciador do locatário sem encontrar avisos de segurança. Você também pode reverter para o certificado de interface de gerenciamento padrão ou gerar um novo.

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 interface de gerenciamento personalizado comum e uma chave privada correspondente.

Como um único certificado de interface de gerenciamento personalizado é usado para todos os nós de administração, você deve especificar o certificado como um certificado curinga ou multi-domínio se os clientes precisarem verificar o nome do host ao se conectar 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 de grade 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** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION > Security > Certificates** e observando a data de validade do certificado da interface de gerenciamento na guia Global.



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 de interface de gerenciamento personalizado expira.
- [reverter de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão](#) Você .

Adicione um certificado de interface de gerenciamento personalizado

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

Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor:** O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado:** O arquivo de chave privada de certificado de servidor personalizado (.key).



As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA:** Um único arquivo opcional 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.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: storagegrid_certificate.pem

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

Gerar certificado

Gere os ficheiros de certificado do servidor.



A prática recomendada para um ambiente de produção é usar um certificado de interface de gerenciamento personalizado assinado por uma autoridade de certificação externa.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

- **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
- **IP:** Um ou mais endereços IP a incluir no certificado.
- **Assunto:** X.509 Assunto ou nome distinto (DN) do proprietário do certificado.
- **Dias válidos:** Número de dias após a criação em que o certificado expira.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**. O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Gerenciador de Grade, Gerenciador de locatário, API do Gerenciador de Grade ou API do Gerenciador de Tenant.

5. Atualize a página para garantir que o navegador da Web seja atualizado.



Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página de certificado de interface de gerenciamento exibe informações detalhadas de certificado para os certificados que estão em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaurar o certificado padrão da interface de gerenciamento

Você pode reverter para o uso do certificado de interface de gerenciamento padrão para conexões do Gerenciador de Grade e do Gerenciador de Tenant.

Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione **Use default certificate** (usar certificado padrão).

Quando você restaura o certificado de interface de gerenciamento padrão, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado de interface de gerenciamento padrão é usado para todas as novas conexões de cliente subsequentes.

4. Atualize a página para garantir que o navegador da Web seja atualizado.

Use um script para gerar um novo certificado de interface de gerenciamento autoassinado

Se for necessária uma validação estrita do nome do host, você pode usar um script para gerar o certificado da interface de gerenciamento.

O que você vai precisar

- Você tem permissões de acesso específicas.
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

A melhor prática para um ambiente de produção é usar um certificado assinado por uma autoridade de certificação externa.

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 da interface de gerenciamento, que é usado pelo Gerenciador de Grade e pelo Gerenciador de Locatário.
- 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 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 720
```

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 **CONFIGURATION > Security > Certificates**

- c. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags DE INÍCIO e FIM.

Transfira ou copie o certificado da interface de gestão

Você pode salvar ou copiar o conteúdo do certificado da interface de gerenciamento para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **certificado de interface de gerenciamento**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA .pem. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Configure os certificados API S3 e Swift

Você pode substituir ou restaurar o certificado do servidor usado para conexões de cliente S3 ou Swift para nós de armazenamento, o serviço CLB (Connection Load Balancer) obsoleto em nós de Gateway ou para carregar pontos de extremidade do balanceador. 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 conectar 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, você também pode precisar instalar o certificado de CA de Grade no cliente API S3 ou Swift que você usará 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 global Server certificate for S3 and Swift API** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION > Security > Certificates** e observando a data de expiração do certificado API S3 e Swift na guia Global.

Você pode fazer upload ou gerar um certificado personalizado de API S3 e Swift.

Adicione um certificado personalizado de API S3 e Swift

Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os ficheiros de certificado do servidor necessários.

a. Selecione **carregar certificado**.

b. Carregue os ficheiros de certificado do servidor necessários:

- **Certificado de servidor:** O arquivo de certificado de servidor personalizado (codificado PEM).
- **Chave privada de certificado:** O arquivo de chave privada de certificado de servidor personalizado (.key).



As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA:** Um único arquivo opcional contendo os certificados de cada autoridade de certificação de emissão intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados em ordem de cadeia de certificados.
- c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado personalizado da API S3 e Swift que foi carregado. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.

- Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Guardar**.

O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

Gerar certificado

Gere os ficheiros de certificado do servidor.

a. Selecione **Generate certificate** (gerar certificado).

b. Especifique as informações do certificado:

- **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
- **IP:** Um ou mais endereços IP a incluir no certificado.
- **Assunto:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
- **Dias válidos:** Número de dias após a criação em que o certificado expira.

c. Selecione **Generate**.

d. Selecione **Detalhes do certificado** para exibir os metadados e o PEM para o certificado personalizado da API S3 e Swift que foi gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **Guardar**.

O certificado de servidor personalizado é usado para novas conexões de cliente S3 e Swift subsequentes.

5. Selecione uma guia para exibir metadados para o certificado padrão do servidor StorageGRID, um certificado assinado pela CA que foi carregado ou um certificado personalizado que foi gerado.



Depois de carregar ou gerar um novo certificado, aguarde até um dia para que os alertas de expiração de certificado relacionados sejam apagados.

6. Atualize a página para garantir que o navegador da Web seja atualizado.

7. Depois de adicionar um certificado personalizado de API S3 e Swift, a página de certificado de API S3 e Swift exibe informações detalhadas de certificado para o certificado personalizado de API S3 e Swift que está em uso. Você pode baixar ou copiar o PEM do certificado conforme necessário.

Restaure o certificado padrão da API S3 e Swift

Você pode reverter para o uso do certificado padrão S3 e Swift API para conexões de clientes S3 e Swift para nós de armazenamento e para o serviço CLB obsoleto em nós de Gateway. No entanto, você não pode usar o certificado padrão S3 e Swift API para um endpoint de balanceador de carga.

Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione **Use default certificate** (usar certificado padrão).

Quando você restaura a versão padrão do certificado global S3 e Swift API, os arquivos de certificado de servidor personalizado configurados são excluídos e não podem ser recuperados do sistema. O certificado padrão da API S3 e Swift será usado para novas conexões de cliente S3 e Swift subsequentes para nós de armazenamento e para o serviço CLB obsoleto em nós de Gateway.

4. Selecione **OK** para confirmar o aviso e restaurar o certificado padrão da API S3 e Swift.

Se você tiver permissão de acesso root e o certificado personalizado S3 e Swift API foi usado para conexões de endpoint do balanceador de carga, uma lista será exibida de endpoints do balanceador de carga que não estarão mais acessíveis usando o certificado padrão S3 e Swift API. Acesse a [Configurar pontos de extremidade do balanceador de carga](#) para editar ou remover os endpoints afetados.

5. Atualize a página para garantir que o navegador da Web seja atualizado.

Faça o download ou copie o certificado API S3 e Swift

Você pode salvar ou copiar o conteúdo do certificado S3 e Swift API para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION > Security > Certificates**.
2. Na guia **Global**, selecione **S3 e Swift API certificate**.
3. Selecione a guia **Server** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Transfira o ficheiro de certificado ou o pacote CA

Baixe o certificado ou o arquivo do pacote CA .pem. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Baixar certificado** ou **Baixar pacote CA**.

Se você estiver baixando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão baixados como um único arquivo.

- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

Copie o texto do certificado para colar em outro lugar. Se você estiver usando um pacote CA opcional, cada certificado no pacote será exibido em sua própria subguia.

- a. Selecione **Copiar certificado PEM** ou **Copiar pacote CA PEM**.

Se você estiver copiando um pacote de CA, todos os certificados nas guias secundárias do pacote de CA serão copiados juntos.

- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Informações relacionadas

- [Use S3](#)
- [Use Swift](#)
- [Configure os nomes de domínio de endpoint da API S3](#)

Copie o certificado da CA de Grade

O StorageGRID usa uma autoridade de certificação interna (CA) para proteger o tráfego interno. Este certificado não muda se você carregar seus próprios certificados.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Grid CA**.
2. Na seção **Certificate PEM**, baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado .pem.

- a. Selecione **Baixar certificado**.
- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado PEM

Copie o texto do certificado para colar em outro lugar.

- a. Selecione **Copiar certificado PEM**.
- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Configurar 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 tem permissões de acesso específicas.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Sobre esta tarefa

Ao criar um endpoint de 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, [Configurar o StorageGRID para FabricPool](#) consulte .



O serviço CLB (Connection Load Balancer) separado nos nós de gateway está obsoleto e não é 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 opcional da 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.

Configurar certificados de cliente

Os certificados de cliente permitem que clientes externos autorizados acessem o banco de dados do StorageGRID Prometheus, fornecendo uma maneira segura para que ferramentas externas monitorem 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.

Consulte as informações sobre [uso geral do certificado de segurança](#) e [configurando certificados de servidor personalizados](#).



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **expiração de certificados de cliente configurados na página certificados** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **CONFIGURATION > Security > Certificates** e observando a data de validade do certificado do cliente na guia Client.



Se você estiver usando um servidor de gerenciamento de chaves (KMS) para proteger os dados em nós de dispositivo especialmente configurados, consulte as informações específicas sobre [Carregar um certificado de cliente KMS](#) .

O que você vai precisar

- Você tem permissão de acesso root.

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Para configurar um certificado de cliente:
 - Você tem o endereço IP ou o nome de domínio do nó Admin.
 - Se tiver configurado o certificado da interface de gerenciamento do StorageGRID, você terá a CA, o certificado do cliente e a chave privada usadas para configurar o certificado da interface de gerenciamento.
 - Para carregar o seu próprio certificado, a chave privada do certificado está disponível no seu computador local.
 - A chave privada deve ter sido salva ou gravada no momento em que foi criada. Se você não tiver a chave privada original, você deve criar uma nova.
- Para editar um certificado de cliente:
 - Você tem o endereço IP ou o nome de domínio do nó Admin.
 - Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no computador local.

Adicionar certificados de cliente

Siga o procedimento para o seu cenário para adicionar um certificado de cliente:

- [Certificado de interface de gerenciamento já configurado](#)
- [Certificado de cliente emitido pela CA](#)
- [Certificado gerado pelo Grid Manager](#)

Certificado de interface de gerenciamento já configurado

Use este procedimento para adicionar um certificado de cliente se um certificado de interface de gerenciamento já estiver configurado usando uma CA fornecida pelo cliente, um certificado de cliente e uma chave privada.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.
5. Na seção **tipo de certificado**, carregue o arquivo de certificado da interface de gerenciamento .pem.
 - a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
 - b. Carregar o ficheiro de certificado da interface de gestão (.pem).
 - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
 - Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
 - c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

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

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 Auth** e com **CA Cert**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole

- A interface de gerenciamento certificado CA para **CA Cert**
- O certificado de cliente para **Cert de cliente**
- A chave privada para **chave do cliente**

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

Servername deve corresponder ao nome de domínio como aparece no certificado da 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 o [Instruções para monitorar o StorageGRID](#).

Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use um certificado de cliente emitido pela CA e uma chave privada.

Passos

1. Execute as etapas para [configurar um certificado de interface de gerenciamento](#).
2. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
3. Selecione **Adicionar**.
4. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.
6. Na seção **tipo de certificado**, carregue o certificado do cliente, a chave privada e os arquivos do pacote CA .pem:
 - a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
 - b. Carregar ficheiros de certificado de cliente, chave privada e pacote CA (.pem).
 - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

Os novos certificados aparecem na guia **Cliente**.

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

- 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 Auth** e **com CA Cert**.

- d. Em Detalhes de autenticação TLS/SSL, copie e cole

- A interface de gerenciamento certificado CA para **CA Cert**
- O certificado de cliente para **Cert de cliente**
- A chave privada para **chave do cliente**

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

Servername deve corresponder ao nome de domínio como aparece no certificado da 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 o [Instruções para monitorar o StorageGRID](#).

Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para Prometheus que use a função gerar certificado no Gerenciador de Grade.

Passos

1. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione **Adicionar**.
3. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.
5. Na seção **tipo de certificado**, selecione **gerar certificado**.
6. Especifique as informações do certificado:

- **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados do nó de administrador a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
- **IP:** Um ou mais endereços IP de nó de administrador a incluir no certificado.
- **Assunto:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.

7. Selecione **Generate**.

8. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.



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

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

Especifique o nome do arquivo de chave privada e o local de download.

9. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

10. No Gerenciador de Grade, selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Global**.

11. Selecione **certificado de interface de gestão**.

12. Selecione **usar certificado personalizado**.

13. Carregue os arquivos `certificate.pem` e `private_key.pem` da [detalhes do certificado do cliente](#) etapa. Não há necessidade de carregar o pacote CA.

- Selecione **carregar certificado** e, em seguida, selecione **continuar**.
- Carregar cada ficheiro de certificado (`.pem`).
- Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

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

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

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

- 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 Auth** e com **CA Cert**.

d. Em Detalhes de autenticação TLS/SSL, copie e cole

- O certificado de cliente de interface de gerenciamento para **CA Cert** e **Client Cert**
- A chave privada para **chave do cliente**

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

Servername deve corresponder ao nome de domínio como aparece no certificado da 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 o [Instruções para monitorar o StorageGRID](#).

Editar certificados de cliente

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

Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.

As datas de expiração do certificado e as permissões de acesso Prometheus estão 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 certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione **Editar nome e permissão**
4. Introduza um nome de certificado que contenha, no mínimo, 1 e no máximo, 32 caracteres.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externo, selecione **permitir Prometheus**.
6. Selecione **continuar** para salvar o certificado no Gerenciador de Grade.

O certificado atualizado é exibido na guia Cliente.

Anexar novo certificado de cliente

Você pode carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.

As datas de expiração do certificado e as permissões de acesso Prometheus estão 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 certificado que pretende editar.
3. Selecione **Editar** e, em seguida, selecione uma opção de edição.

Carregar certificado

Copie o texto do certificado para colar em outro lugar.

- a. Selecione **carregar certificado** e, em seguida, selecione **continuar**.
- b. Carregue o nome do certificado do cliente (.pem).

Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: storagegrid_certificate.pem

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- c. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

- a. Selecione **Generate certificate** (gerar certificado).
- b. Especifique as informações do certificado:

- **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um * como um curinga para representar vários nomes de domínio.
- **IP:** Um ou mais endereços IP a incluir no certificado.
- **Assunto:** X,509 Assunto ou nome distinto (DN) do proprietário do certificado.
- **Dias válidos:** Número de dias após a criação em que o certificado expira.

- c. Selecione **Generate**.

- d. Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.



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

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: storagegrid_certificate.pem

- Selecione **Copiar chave privada** para copiar a chave privada do certificado para colar em outro lugar.
- Selecione **Download private key** para salvar a chave privada como um arquivo.

Especifique o nome do arquivo de chave privada e o local de download.

e. Selecione **criar** para salvar o certificado no Gerenciador de Grade.

O novo certificado é exibido na guia Cliente.

Baixe ou copie certificados de cliente

Você pode baixar ou copiar um certificado de cliente para uso em outro lugar.

Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende copiar ou transferir.
3. Baixe ou copie o certificado.

Transfira o ficheiro de certificado

Transfira o ficheiro de certificado .pem.

- a. Selecione **Baixar certificado**.
- b. Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie o texto do certificado para colar em outro lugar.

- a. Selecione **Copiar certificado PEM**.
- b. Cole o certificado copiado em um editor de texto.
- c. Salve o arquivo de texto com a extensão .pem.

Por exemplo: `storagegrid_certificate.pem`

Remover certificados de cliente

Se você não precisar mais de um certificado de cliente administrador, poderá removê-lo.

Passos

1. Selecione **CONFIGURATION > Security > Certificates** e, em seguida, selecione a guia **Client**.
2. Selecione o certificado que pretende remover.

3. Selecione **Delete** e confirme.



Para remover até 10 certificados, selecione cada certificado a ser removido na guia Cliente e selecione **ações > Excluir**.

Depois que um certificado é removido, os clientes que usaram o certificado devem especificar um novo certificado de cliente para acessar o banco de dados do StorageGRID Prometheus.

Configurar servidores de gerenciamento de chaves

Configurar servidores de gerenciamento de chaves: Visão geral

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.

Reveja 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	Você configura um servidor de gerenciamento de chaves para o site StorageGRID (CONFIGURATION > Security > Key Management Server) e habilita a criptografia de nó para o dispositivo. Em seguida, um nó de dispositivo se conecta 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.	<p>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.</p> <div>  <p>O gerenciamento de chaves de criptografia com um KMS só é compatível com nós de storage e dispositivos de serviços.</p> </div>
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 acessar aos dados nas unidades seguras.	<p>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.</p> <ul style="list-style-type: none"> • SG6000 dispositivos de armazenamento • SG5700 dispositivos de armazenamento • 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 > 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.	<p>Dados de objeto S3 e Swift recém-ingetidos.</p> <p>Os objetos armazenados existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <ul style="list-style-type: none"> • Configurar 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.	<p>Somente dados de objeto S3 recém-ingeridos.</p> <p>A criptografia deve ser especificada para o intervalo. Os objetos bucket existentes não são criptografados. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <ul style="list-style-type: none"> • Use S3
Criptografia do lado do servidor de objetos S3 (SSE)	Você emite uma solicitação S3 para armazenar um objeto e incluir o <code>x-amz-server-side-encryption</code> cabeçalho da solicitação.	<p>Somente dados de objeto S3 recém-ingeridos.</p> <p>A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <p>StorageGRID gerencia as chaves.</p> <ul style="list-style-type: none"> • Use S3
Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C)	<p>Você emite uma solicitação S3 para armazenar um objeto e incluir três cabeçalhos de solicitação.</p> <ul style="list-style-type: none"> • <code>x-amz-server-side-encryption-customer-algorithm</code> • <code>x-amz-server-side-encryption-customer-key</code> • <code>x-amz-server-side-encryption-customer-key-MD5</code> 	<p>Somente dados de objeto S3 recém-ingeridos.</p> <p>A criptografia deve ser especificada para o objeto. Os metadados de objetos e outros dados confidenciais não são criptografados.</p> <p>As chaves são gerenciadas fora do StorageGRID.</p> <ul style="list-style-type: none"> • Use S3

Opção de criptografia	Como funciona	Aplica-se a
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.	<p>Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou datastore seja criptografado.</p> <p>Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.</p>
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.	<p>Somente dados e metadados de objetos (os dados de configuração do sistema não são criptografados).</p> <p>Um método de criptografia externo fornece controle mais rigoroso sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.</p> <ul style="list-style-type: none"> • "Amazon Simple Storage Service - Guia do desenvolvedor: Protegendo dados usando criptografia do lado do cliente"

Use 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 autcriptografia 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.

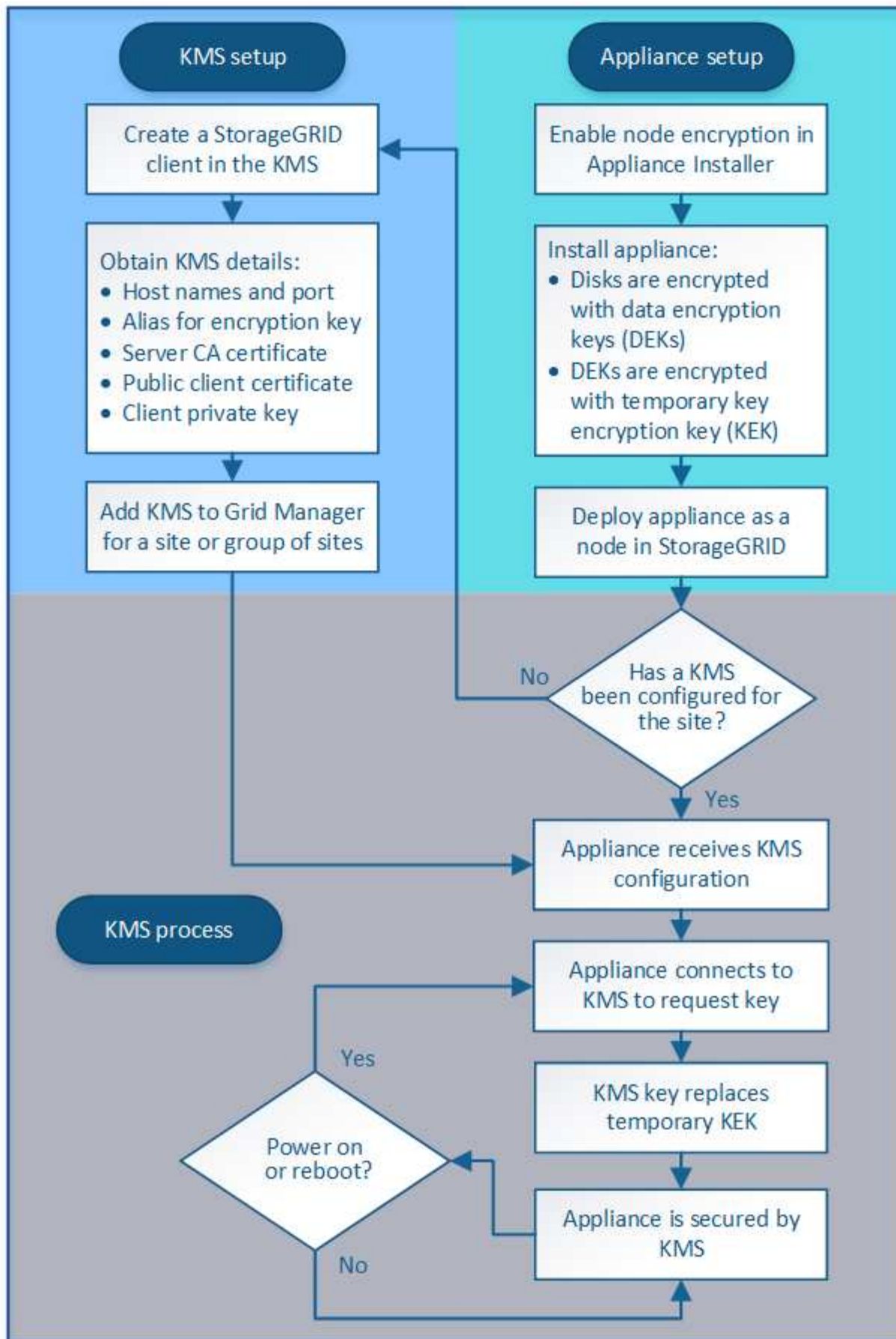
Se apenas uma pequena parte de seus objetos exigir criptografia, considere controlar a criptografia no intervalo ou no nível de objeto individual. Ativar vários níveis de criptografia tem um custo de desempenho adicional.

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.

Configurar 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.	Configure o StorageGRID como um cliente no KMS
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	Configure 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)

Configure 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 conectar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

Para obter detalhes, consulte o seguinte:

- [Aparelhos de serviços SG100 e 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 conectar 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 conectarem 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 reconecta 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 nos mecanismos de contêiner 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 localitários. 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.

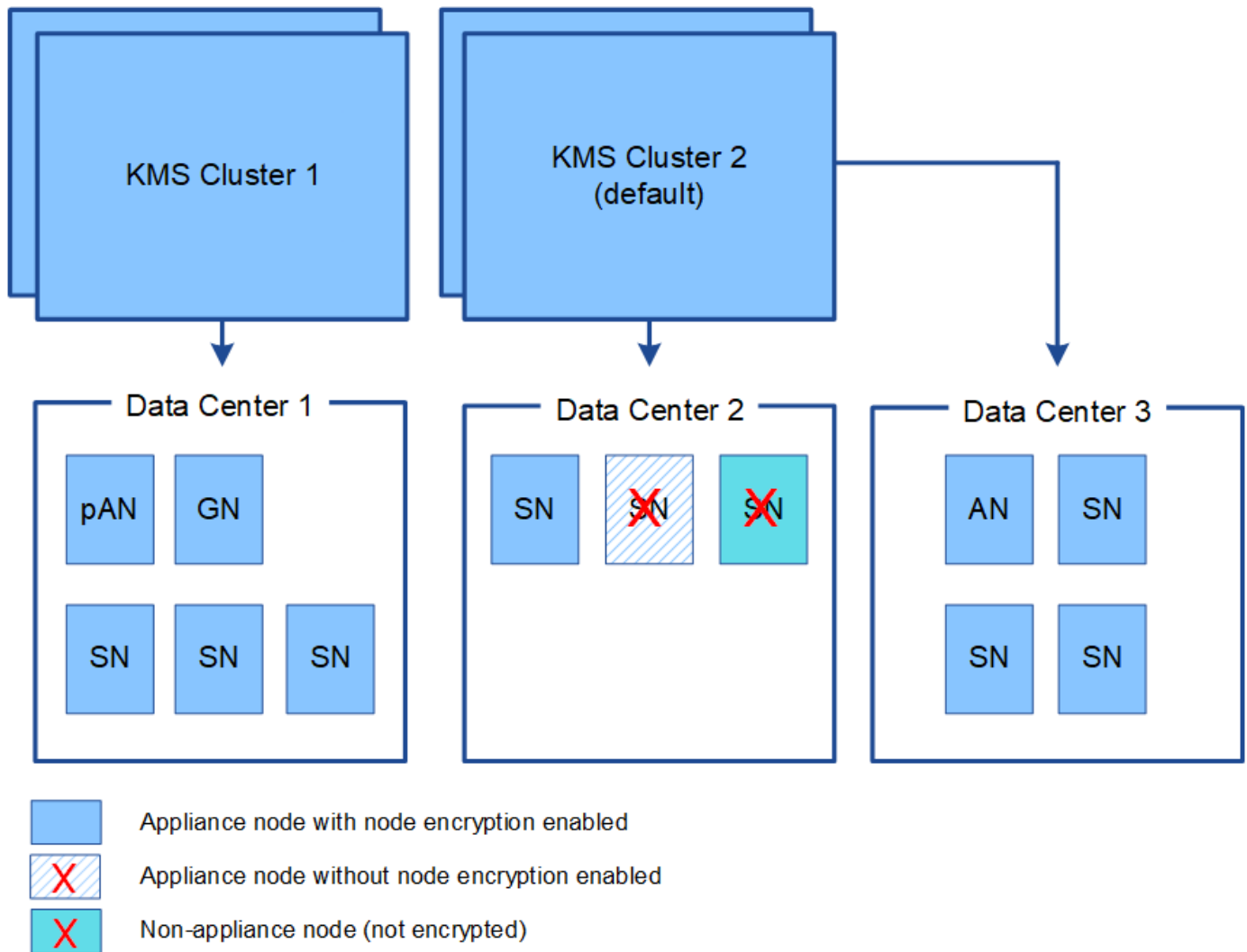
Quanto servidores de gerenciamento de chaves eu preciso?

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.

Informações relacionadas

- [Aparelhos de serviços SG100 e SG1000](#)
- [SG6000 dispositivos de armazenamento](#)
- [SG5700 dispositivos de armazenamento](#)
- [SG5600 dispositivos de armazenamento](#)

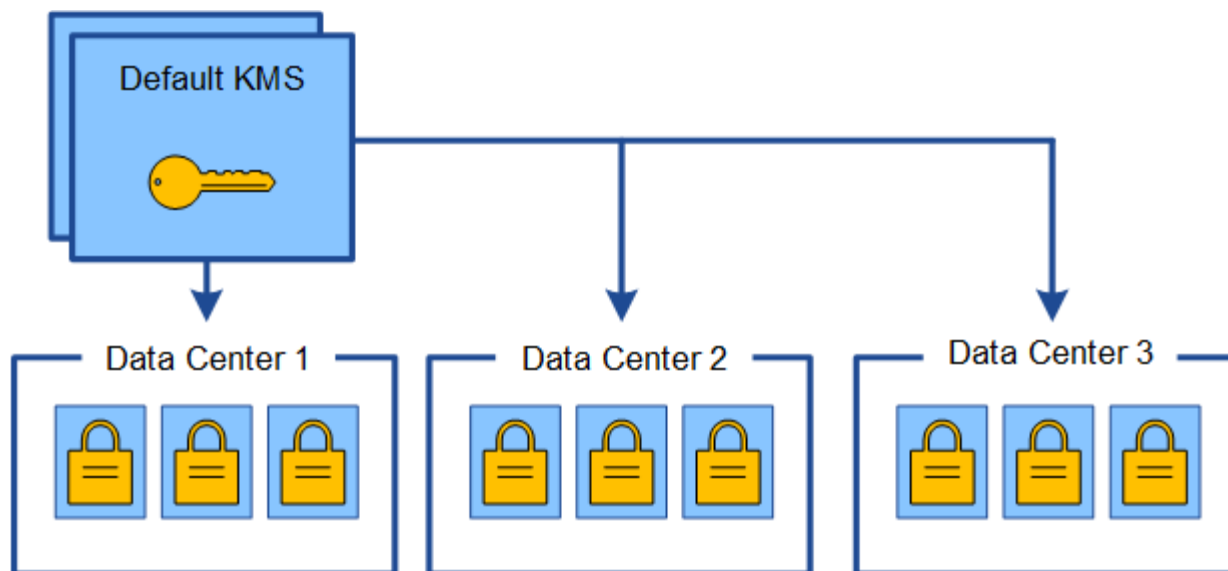
Considerações para alterar o KMS para um site

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.

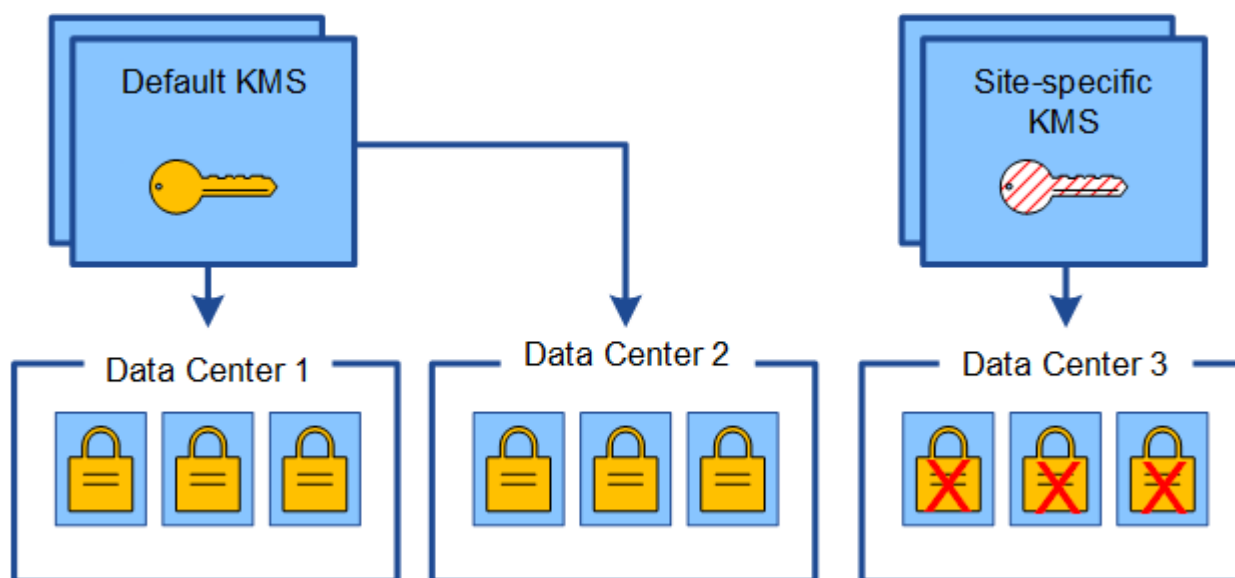
Se você alterar o KMS usado para um site, você deve garantir que os nós de dispositivo criptografados anteriormente nesse local possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, talvez seja necessário copiar a versão atual da chave de criptografia do KMS original para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

Por exemplo:

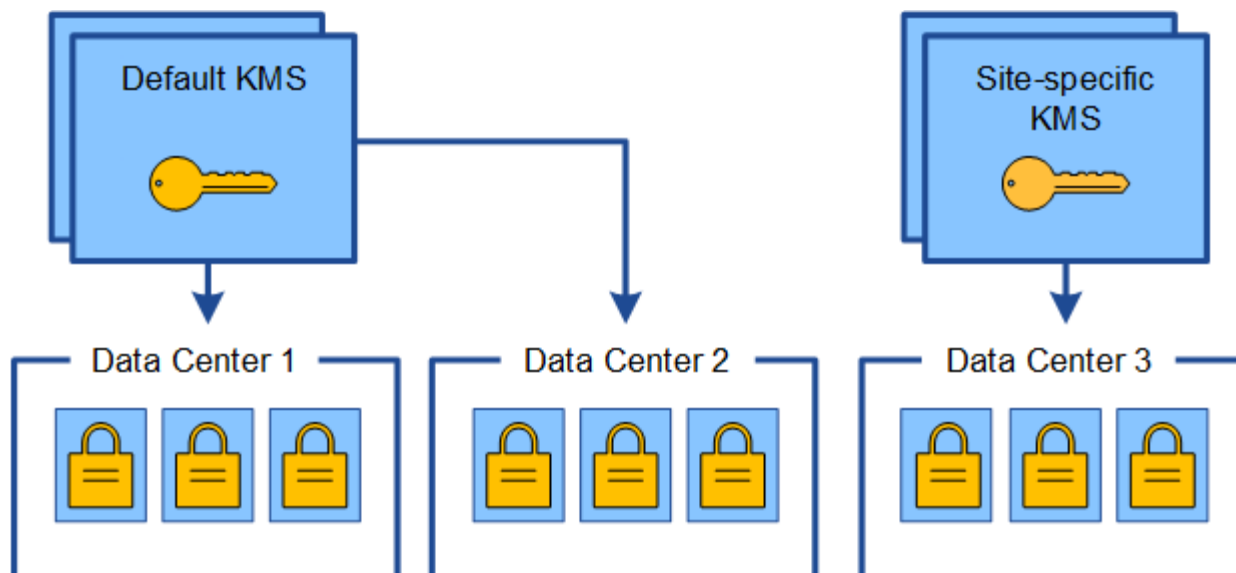
1. Você configura inicialmente um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de dispositivo que têm a configuração **Node Encryption** ativada conetam-se ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar 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.	<p>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.</p> <p>Editar um servidor de gerenciamento de chaves (KMS)</p>
Você tem um KMS padrão e adiciona um novo site em uma expansão. Você não deseja usar o KMS padrão para o novo site.	<ol style="list-style-type: none"> 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. 2. Usando o Gerenciador de Grade, adicione o novo KMS e selecione o site. <p>Adicionar um servidor de gerenciamento de chaves (KMS)</p>

Caso de uso para alterar o KMS de um site	Passos necessários
Você quer que o KMS para um site use um servidor diferente.	<ol style="list-style-type: none"> 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. 2. Usando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome de host ou endereço IP. <p>Adicionar um servidor de gerenciamento de chaves (KMS)</p>

Configure 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 conectará.



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

- Você revisou o [considerações e requisitos para usar um servidor de gerenciamento de chaves](#).
- Você tem [Configurado o StorageGRID como um cliente no KMS](#), e você tem as informações necessárias para cada cluster KMS ou KMS.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

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](#) Consulte para obter detalhes.

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 **CONFIGURATION > Security > Key Management Server**.

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

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

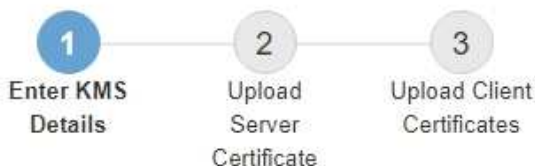
KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
------------------	----------	------------------	----------	--------------------

No key management servers have been configured. Select **Create**.

2. Selecione **criar**.

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

Add a Key Management Server



Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name	<input type="text"/>
Key Name	<input type="text"/>
Manages keys for	-- Choose One --
Port	<input type="text" value="5696"/>
Hostname	<input type="text"/>

+

Cancel

Next

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 caracteres.

Campo	Descrição
Nome da chave	O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres.
Gere as chaves para	<p>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.</p> <ul style="list-style-type: none"> • Selecione um site se este KMS gerenciará chaves de criptografia para os nós do dispositivo em um local específico. • 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. <p>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.</p>
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	<p>O nome de domínio ou endereço IP totalmente qualificado para o KMS.</p> <p>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 conectar ao KMS ou a todos os servidores em um cluster KMS.</p>

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**.

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.

Add a Key Management Server

1

2

3

Enter KMS
Details

Upload
Server
Certificate

Upload Client
Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ?

Browse

Cancel

Back

Next

2. Carregue o ficheiro de certificado.

Os metadados do certificado do servidor são exibidos.

Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ

Browse

k170vCA.pem

Server Certificate Metadata

Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79

Cancel

Back

Next



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

3. Selecione **seguinte**.

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.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

Client Certificate Private Key ?

Browse

Cancel

Back

Save

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.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Cancel

Back

Save

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**.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

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.

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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

Ver 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 **CONFIGURATION > Security > Key Management Server**.

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.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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	<p>O site StorageGRID associado ao KMS.</p> <p>Este campo exibe o nome de um site StorageGRID específico ou sites não gerenciados por outro KMS (KMS padrão).</p>
Nome do anfitrião	<p>O nome de domínio totalmente qualificado ou endereço IP do KMS.</p> <p>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.</p> <p>Por exemplo: 10.10.10.10 and 10.10.10.11 Ou 10.10.10.10 and 2 others.</p> <p>Para exibir todos os nomes de host em um cluster, selecione um KMS e, em seguida, selecione Editar.</p>
Estado do certificado	<p>Estado atual do certificado do servidor, do certificado da CA opcional e do certificado do cliente: Válido, expirado, próximo da expiração ou desconhecido.</p> <p>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.</p>

- 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.

- 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.

Exibir 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 **CONFIGURATION > Security > Key Management Server**.

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.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

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

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

Node Name	Node Type	Site	KMS Display Name ?	Key UID ?	Status ?
SGA-010-096-104-67 	Storage Node	Data Center 1	Default KMS	41b0...5c57	✓ Connected to KMS (2021-03-12 10:59:32 MST)

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	<p>O nome descritivo do KMS usado para o nó.</p> <p>Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS.</p> <p>Adicionar um servidor de gerenciamento de chaves (KMS)</p>
UID da chave	<p>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.</p> <p>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.</p>
Estado	<p>O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conectado, 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.</p> <p>Observação: você deve atualizar seu navegador para ver os novos valores.</p>

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 desconectado 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 conectividade DE KMS
- Nome da chave de encriptação KMS não encontrado
- Falha na rotação da chave de CRIPTOGRAFIA KMS
- A chave KMS falhou ao descriptar um volume de aparelho
- KMS não está configurado

Consulte as ações recomendadas para esses alertas nas instruções do [Monitoramento e solução de problemas do StorageGRID](#).



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

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

- Você revisou o [considerações e requisitos para usar um servidor de gerenciamento de chaves](#).
- Se pretende atualizar o site selecionado para um KMS, analisou o [Considerações para alterar o KMS para um site](#).
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

Passos

1. Selecione **CONFIGURATION > Security > Key Management Server**.

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

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:


- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

<div> + Create Edit Remove </div>				
KMS Display Name [?]	Key Name [?]	Manages keys for [?]	Hostname [?]	Certificate Status [?]
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	<div> ✓ All certificates are valid </div>

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 caracteres.
Nome da chave	<p>O alias exato da chave para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres.</p> <p>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.</p> <div><p>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.</p><p>Considerações e requisitos para usar um servidor de gerenciamento de chaves</p></div>
Gere as chaves para	<p>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.</p> <p>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.</p>
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	<p>O nome de domínio ou endereço IP totalmente qualificado para o KMS.</p> <p>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 conectar ao KMS ou a todos os servidores em um cluster KMS.</p>

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.

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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

- Você revisou o [considerações e requisitos para usar um servidor de gerenciamento de chaves](#).
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

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 **CONFIGURATION > Security > Key Management Server**.

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

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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

⚠ Warning

Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

4. Selecione **OK**.

A configuração do KMS é removida.

Gerenciar configurações de proxy

Configure 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 tem permissões de acesso específicas.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

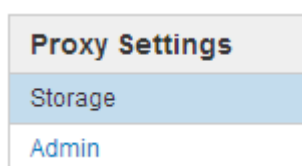
Sobre esta tarefa

Você pode configurar as configurações para um único proxy de armazenamento.

Passos

1. Selecione **CONFIGURATION > Security > Proxy settings**.

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.

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy ☒

Protocol ☐ HTTP ☐ SOCKS5

Hostname

Port (optional)

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 conectar 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. Selecione **Guardar**.

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 selecione **Salvar**.

Informações relacionadas

- [Rede e portas para serviços de plataforma](#)
- [Gerenciar objetos com ILM](#)

Configure as configurações do proxy Admin

Se você enviar mensagens AutoSupport usando HTTP ou HTTPS ([Configurar o AutoSupport](#) consulte), poderá configurar um servidor proxy não transparente entre nós de administração e o suporte técnico (AutoSupport).

O que você vai precisar

- Você tem permissões de acesso específicas.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Sobre esta tarefa

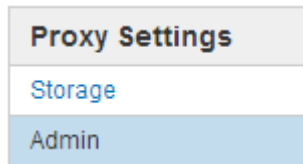
Você pode configurar as configurações para um único proxy Admin.

Passos

1. Selecione **CONFIGURATION > Security > Proxy settings**.

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).

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy ☒

Hostname

Port

Username (optional)

Password (optional)

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. Selecione **Guardar**.

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 selecione

Salvar.

Gerenciar redes de clientes não confiáveis

Gerenciar redes de clientes não confiáveis: Visão geral

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 no [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. [Configurar pontos de extremidade do balanceador de carga](#) Consulte .

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.

Especificar rede cliente do 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

- Você tem 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 **CONFIGURATION > Security > UnTrusted Client Networks**.

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

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network ☒ Trusted
Default ☐ Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	
Client Network untrusted on 0 nodes.		

Save

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. Selecione **Guardar**.

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.

Gerenciar locatários

Gerenciar 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.

O que são 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.

Criar e configurar 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.



Os valores de uso de storage de um locatário podem ficar desatualizados se os nós estiverem isolados de outros nós na grade. Os totais serão atualizados quando a conectividade de rede for restaurada.

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.

Configurar locatários do S3

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.

Configurar 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 autenticuem 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](#)

Crie uma conta de locatário

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

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. Se o StorageGRID não estiver usando logon único, 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.

O Gerenciador de Grade fornece um assistente que o leva pelas etapas para criar uma conta de locatário. As etapas variam de acordo com a [federação de identidade](#) configuração e [logon único](#) se a conta do Gerenciador de Grade que você usa para criar a conta de locatário pertence a um grupo de administração com a permissão de acesso root.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- 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 importou esse grupo federado para o Gerenciador de Grade. Você não precisa atribuir nenhuma permissão do Gerenciador de Grade a esse grupo de administradores. Consulte [instruções para gerenciar grupos de](#)

Passos

1. Selecione **TENANTS**.
2. Selecione **criar** e insira as seguintes informações para o locatário:
 - a. **Nome:** Insira um nome para a conta do locatário. Os nomes de inquilinos não precisam ser únicos. Quando a conta de locatário é criada, ela recebe um ID de conta numérico único.
 - b. **Descrição** (opcional): Insira uma descrição que o ajude a identificar o locatário.
 - c. **Tipo de cliente:** Selecione o tipo de cliente **S3** ou **Swift**.
 - d. **Cota de armazenamento** (opcional): Se você quiser que esse locatário tenha uma cota de armazenamento, insira um valor numérico para a cota e selecione as unidades corretas (GB, TB ou PB).

Create a tenant

1 Enter details — 2 Select permissions — 3 Define root access

Enter tenant details

Name ?

Description (optional) ?

Client type ?

☒ S3 ☐ Swift

Storage quota (optional) ?

GB ▾

Cancel Continue

3. Selecione **continuar** e configure o locatário S3 ou Swift.

S3 inquilino

Selecione as permissões apropriadas para o locatário. Algumas dessas permissões têm requisitos adicionais. Para obter detalhes, consulte a ajuda on-line para cada permissão.

- Permitir serviços de plataforma
- Usar a própria fonte de identidade (selecionável somente se o SSO não estiver sendo usado)
- Permitir seleção S3D ([Gerenciar S3](#) [Selecione para contas de inquilino](#) consulte)

Locatário rápido

Se o locatário usar sua própria fonte de identidade, selecione **Use own Identity source** (somente selecionável se o SSO não estiver sendo usado).

1. Selecione **continuar** e defina o acesso root para a conta de locatário.

Federação de identidade não configurada

1. Introduza uma palavra-passe para o utilizador raiz local.
2. Selecione **criar inquilino**.

SSO ativado

Quando o SSO está habilitado para StorageGRID, o locatário deve usar a origem de identidade que foi configurada para o Gerenciador de Grade. Nenhum usuário local pode entrar. Você especifica qual grupo federado tem permissão de acesso root para configurar a conta de locatário.

1. 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 selecionar o campo. Caso contrário, introduza o nome exclusivo do grupo.

2. Selecione **criar inquilino**.

SSO não ativado

1. Conclua as etapas descritas na tabela dependendo se o locatário gerenciará seus próprios grupos e usuários ou usará a origem de identidade configurada para o Gerenciador de Grade.

Se o inquilino vai...	Faça isso...
Gerencie seus próprios grupos e usuários	<ol style="list-style-type: none">a. Selecione Use own Identity source. Nota: Se esta caixa de verificação estiver selecionada e pretender utilizar a federação de identidade para grupos de inquilinos e utilizadores, o locatário deverá configurar a sua própria origem de identidade. Consulte instruções para o uso de contas de inquilino.b. Especifique uma senha para o usuário raiz local do locatário e selecione criar locatário.c. Selecione entrar como root para configurar o locatário ou selecione concluir para configurar o locatário mais tarde.
Use os grupos e usuários configurados para o Gerenciador de Grade	<ol style="list-style-type: none">a. Faça um ou ambos os procedimentos a seguir:<ul style="list-style-type: none">◦ Selecione um grupo federado existente no Gerenciador de Grade que deve ter a permissão de acesso raiz inicial para o locatário. Nota: Se você tiver permissões adequadas, os grupos federados existentes do Gerenciador de Grade serão listados quando você selecionar o campo. Caso contrário, introduza o nome exclusivo do grupo.◦ Especifique uma senha para o usuário raiz local do locatário.b. Selecione criar inquilino.

1. Para iniciar sessão no inquilino agora:

- Se você estiver acessando o Gerenciador de Grade em uma porta restrita, selecione **restrito** na tabela de locatário para saber mais sobre como acessar essa conta de locatário.

O URL do Gerenciador do Locatário tem este formato:

`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/`

- *FQDN_or_Admin_Node_IP* É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador
 - *port* é a porta somente locatário
 - *20-digit-account-id* É o ID exclusivo da conta do locatário
- Se você estiver acessando o Gerenciador de Grade na porta 443, mas não tiver definido uma senha para o usuário raiz local, na tabela locatários do Gerenciador de Grade, selecione **entrar** e insira as credenciais de um usuário no grupo federado de acesso raiz.
 - Se você estiver acessando o Gerenciador de Grade na porta 443 e definir uma senha para o usuário raiz local:
 - i. Selecione **entrar como root** para configurar o locatário agora.


Quando você faz login, os links são exibidos para configurar buckets ou contentores, federação de identidade, grupos e usuários.

Create a tenant

Enter details

Select permissions


Define root access







The tenant Tenant02 was created.

If you're ready to configure the tenant, select **Sign in as root**.

Sign in as root

 Signed in

You can now access the Tenant Manager to configure these settings:

- **Buckets**  : Create and manage buckets.
- **Identity federation**  : Configure an external identity source to use federated groups.
- **Groups**  : Manage groups and assign permissions.
- **Users**  : Manage local users and assign users to groups.

Finish

- i. Selecione os links para configurar a conta de locatário.

Cada link abre a página correspondente no Gerenciador do Locatário. Para concluir a página, consulte [instruções para o uso de contas de inquilino](#).

- ii. Caso contrário, selecione **Finish** para acessar o locatário mais tarde.

2. Para acessar o locatário mais tarde:

Se você estiver usando...	Faça um destes...
Porta 443	<ul style="list-style-type: none">• No Gerenciador de Grade, selecione TENANTS e Sign in à direita do nome do locatário.• Insira o URL do locatário em um navegador da Web: <code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code><ul style="list-style-type: none">◦ <i>FQDN_or_Admin_Node_IP</i> É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador◦ <i>20-digit-account-id</i> É o ID exclusivo da conta do locatário
Uma porta restrita	<ul style="list-style-type: none">• No Gerenciador de Grade, selecione TENANTS e restricted.• Insira o URL do locatário em um navegador da Web: <code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</code><ul style="list-style-type: none">◦ <i>FQDN_or_Admin_Node_IP</i> É um nome de domínio totalmente qualificado ou o endereço IP de um nó de administrador◦ <i>port</i> é a porta restrita somente para locatário◦ <i>20-digit-account-id</i> É o ID exclusivo da conta do locatário

Informações relacionadas

- [Controle o acesso através de firewalls](#)
- [Gerencie os serviços de plataforma para contas de inquilino S3](#)

Altere a senha para o usuário raiz local do 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

- Você tem 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**.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div><div></div></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div><div></div></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div><div></div></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div><div></div></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

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

O botão ações fica ativado.

3. Na lista suspensa **ações**, selecione **alterar senha de root**.
4. Introduza a nova palavra-passe para a conta de locatário.
5. Selecione **Guardar**.

Editar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

Passos

1. Selecione **TENANTS**.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Create

Export to CSV

Actions

Search tenants by name or ID

Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div><div></div></div> 10%	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div><div></div></div> 85%	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div><div></div></div> 50%	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div><div></div></div> 95%	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ 📄

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

Use a caixa de pesquisa para procurar uma conta de locatário por nome ou ID de locatário.

3. Na lista suspensa ações, selecione **Editar**.

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

Edit the tenant

1 Enter details

Select permissions

Enter tenant details

Name ?

Description (optional) ?

Client type ?

☒ S3 ☐ Swift

Storage quota (optional) ?

GB

Cancel

Continue

4. Altere os valores para estes campos conforme necessário:

- **Nome**
- **Descrição**
- **Tipo de cliente**
- **Cota de armazenamento**

5. Selecione **continuar**.

6. Selecione ou desmarque as permissões para a conta de locatário.

- Se você desabilitar **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.
- Altere a configuração da caixa de seleção **usa a própria origem de identidade** para determinar se a conta do 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.
- Ative ou desative **S3 Selezione** conforme necessário. [Gerenciar S3 Selezione para contas de inquilino](#) Consulte .

7. Selecione **Guardar**.

Informações relacionadas

- [Gerencie os serviços de plataforma para contas de inquilino S3](#)
- [Use uma conta de locatário](#)

Eliminar conta de inquilino

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 conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- 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.

Use a caixa de pesquisa para procurar uma conta de locatário por nome ou ID de locatário.

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

Gerenciar serviços de plataforma

Gerencie os serviços de plataforma para contas de inquilino 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.

O que são 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 da plataforma, esteja ciente das seguintes recomendações:

- 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.
- 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 pode resultar em desempenho mais lento do cliente S3.
- As solicitações para um endpoint que não pode ser concluído serão enfileiradas para um máximo de 500.000 solicitações. Esse limite é compartilhado igualmente entre locatários ativos. Novos inquilinos podem exceder temporariamente este limite de 500.000 para que os inquilinos recém-criados não sejam injustamente penalizados.

Informações relacionadas

- [Use uma conta de locatário](#)
- [Configure as configurações de proxy de armazenamento](#)
- [Monitorar e solucionar 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 [Configure as configurações de proxy de armazenamento](#) permitir que as mensagens sejam enviadas para endpoints externos, como um endpoint na Internet.

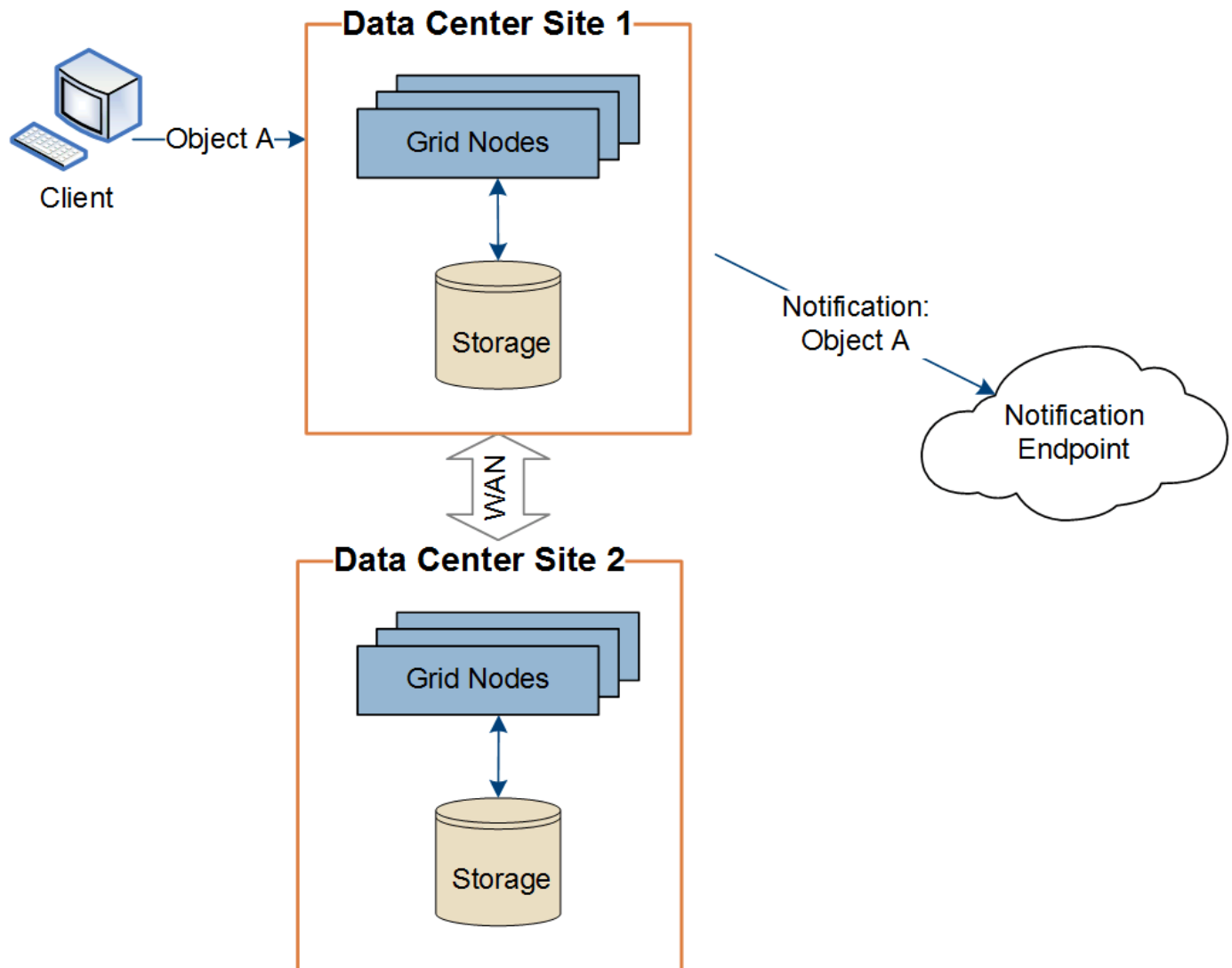
Informações relacionadas

- [Use uma conta de locatário](#)

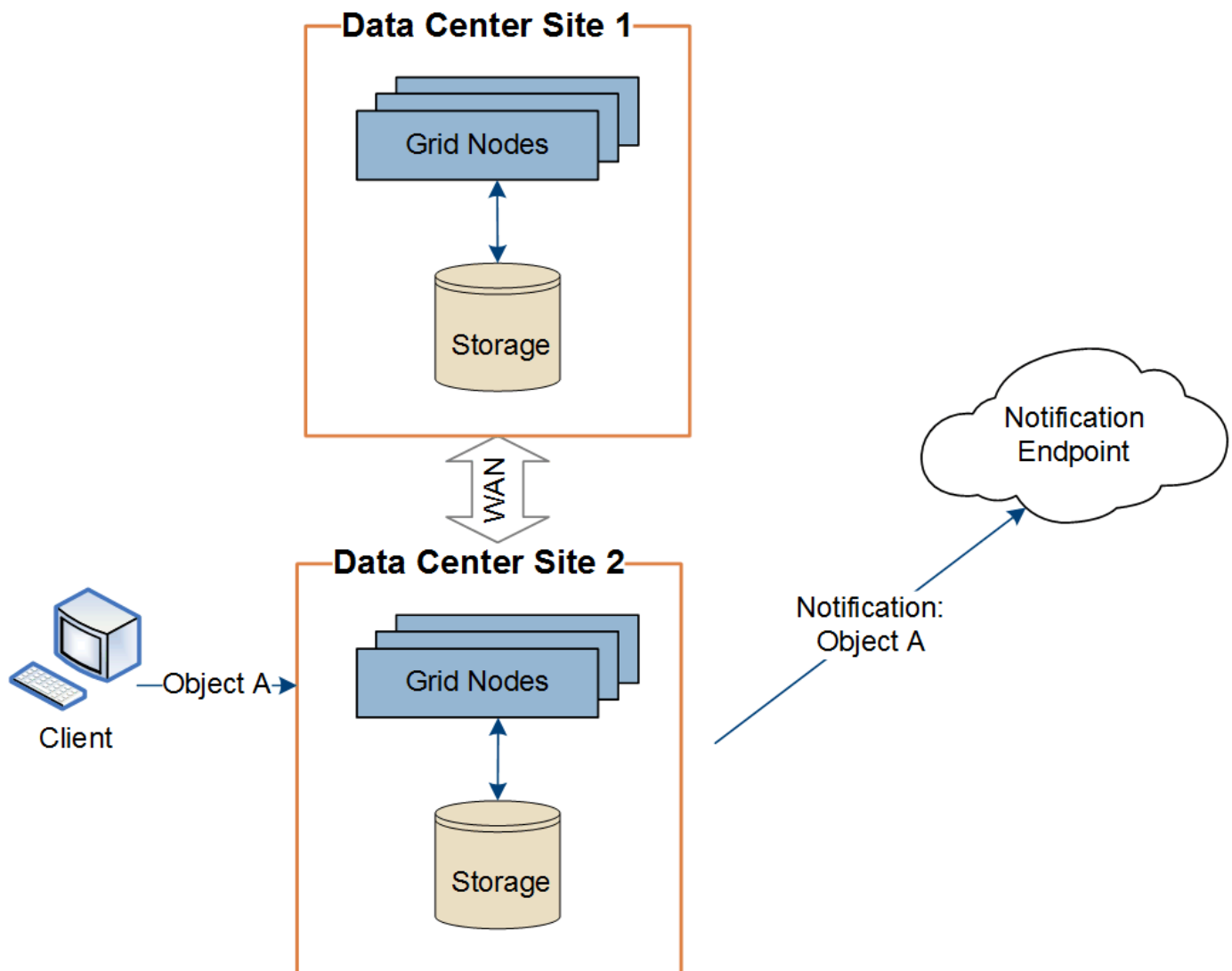
Entrega por local de mensagens de serviços de plataforma

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 conectando-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.

Solucionar problemas de serviços de 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.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.















One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name  	Last error  	Type  	URI  	URN  
<input type="checkbox"/>	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
<input type="checkbox"/>	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



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.

Determine 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 irrecuráveis

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 irrecuráveis. Por exemplo, um erro irrecurável ocorre se o endpoint for excluído.

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

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **site > node > SSM > Eventos**.
3. Veja o último evento na parte superior da tabela.

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

4. Siga as orientações fornecidas no conteúdo do alarme SMTT para corrigir o problema.
5. Selecione a guia **Configuração** para 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 irreversível, o alarme legado de Eventos totais (SMTT) será acionado no Grid Manager.

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.

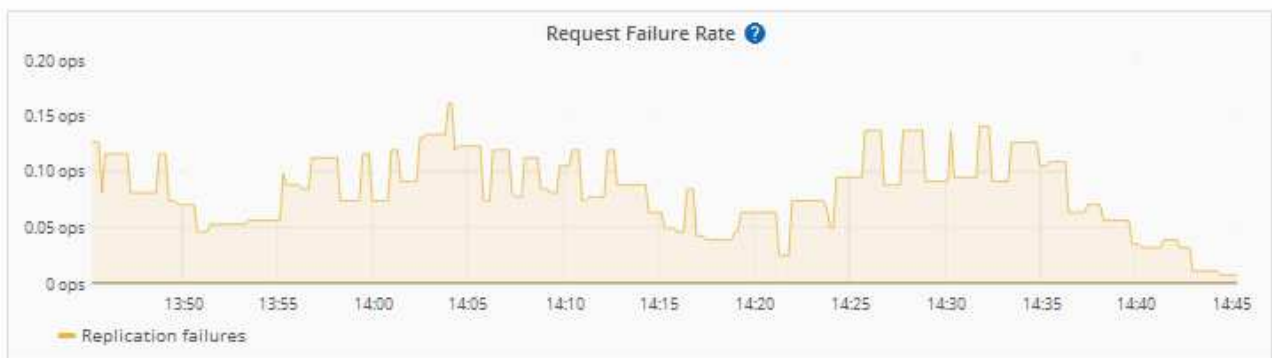
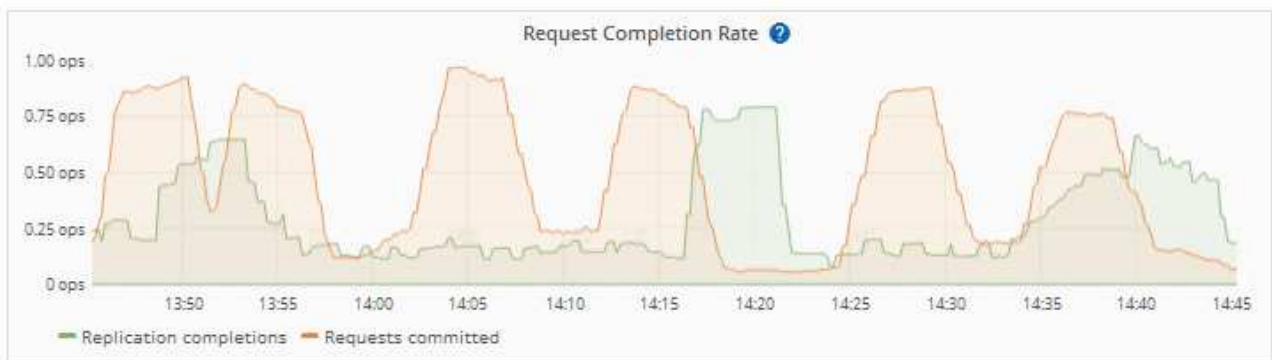
O único efeito visível é que as solicitações S3 recebidas demorarão mais tempo para serem executadas. Se você começar a detectar desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o backlog de solicitações continuar a crescer, as 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 **NODES**.
2. Selecione **síte > Serviços de Plataforma**.
3. Veja o gráfico de taxa de erro de solicitação.

[1 hour](#) [1 day](#) [1 week](#) [1 month](#) [Custom](#)

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 respectivos 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 [usando uma conta de locatário](#).

Informações relacionadas

- [Monitorar e solucionar problemas](#)
- [Configure as configurações de proxy de armazenamento](#)

Gerenciar S3 Selecione para contas de inquilino

Você pode permitir que certos locatários do S3 usem o S3 Select para emitir solicitações SelectObjectContent em objetos individuais.

S3 Select fornece uma maneira eficiente de pesquisar grandes quantidades de dados sem ter que implantar um banco de dados e recursos associados para habilitar pesquisas. Ele também reduz o custo e a latência da recuperação de dados.

O que é o S3 Select?

S3 Select permite que os clientes S3 usem as solicitações SelectObjectContent para filtrar e recuperar apenas os dados necessários de um objeto. A implementação do StorageGRID do S3 Select inclui um subconjunto de comandos e recursos do S3 Select.

Considerações e requisitos para usar o S3 Select

O StorageGRID requer o seguinte para consultas S3 Select:

- O objeto que você deseja consultar está em formato CSV ou é um arquivo compactado GZIP ou bzip2 contendo um arquivo formatado CSV.
- Aos locatários devem ser concedidos S3 Selecione a capacidade pelo administrador da grade. Selecione **permitir S3 Selecionar** quando [criando um locatário](#) ou [editando um locatário](#).
- A solicitação SelectObjectContent deve ser enviada para um [Ponto de extremidade do balanceador de carga StorageGRID](#). Os nós de administrador e gateway usados pelo endpoint devem ser SG100 ou SG1000 nós de dispositivo ou nós de software baseados em VMware.

Observe as seguintes limitações:

- Nós de balanceador de carga bare-metal não são compatíveis.
- As consultas não podem ser enviadas diretamente para nós de storage.
- As consultas enviadas através do serviço CLB obsoleto não são suportadas.



As solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Ative esse recurso somente quando necessário e somente para locatários confiáveis.

Consulte [Instruções para utilizar o S3 Select](#).

Configurar conexões de cliente S3 e Swift

Sobre as conexões de clientes S3 e Swift

Como administrador de grade, você gerencia as opções de configuração que controlam como os locatários S3 e Swift podem conectar 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 conectando-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 conectar 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:

- *** Interfaces VLAN*:** Você pode criar interfaces LAN virtual (VLAN) em nós de administração e nós de gateway para isolar e particionar o tráfego de clientes e locatários para segurança, flexibilidade e desempenho. Depois de criar uma interface VLAN, você a adiciona a um grupo de alta disponibilidade (HA).
- **Grupos de alta disponibilidade:** Você pode criar um grupo de HA das interfaces para 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.
- **Serviço de balanceamento de carga:** Você pode habilitar os clientes a usar 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 conectar usando pontos de extremidade do balanceador de carga.

Você também pode habilitar o uso de HTTP para clientes que se conectam 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 conectar 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 conectar usando o endereço IP virtual do grupo HA.

Sobre esta tarefa

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conectar 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 conecta	Endereço IP	Porta
Grupo HA	Balanceador de carga	Endereço IP virtual de um grupo HA	<ul style="list-style-type: none">• Porta de extremidade do balanceador de carga
Grupo HA	CLB Nota: o serviço CLB está obsoleto.	Endereço IP virtual de um grupo HA	Portas S3 padrão: <ul style="list-style-type: none">• HTTPS: 8082• HTTP: 8084 Portas Swift padrão: <ul style="list-style-type: none">• HTTPS:8083• HTTP:8085
Nó de administração	Balanceador de carga	Endereço IP do nó Admin	<ul style="list-style-type: none">• Porta de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	<ul style="list-style-type: none">• Porta de extremidade do balanceador de carga
Nó de gateway	CLB Nota: o serviço CLB está obsoleto.	Endereço IP do nó de gateway Nota: por padrão, as portas HTTP para CLB e LDR não estão ativadas.	Portas S3 padrão: <ul style="list-style-type: none">• HTTPS: 8082• HTTP: 8084 Portas Swift padrão: <ul style="list-style-type: none">• HTTPS:8083• HTTP:8085

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Nó de storage	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084 Portas Swift padrão: <ul style="list-style-type: none"> • HTTPS: 18083 • HTTP: 18085

Exemplos

Para conectar 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 conectar ao StorageGRID:

- `https://192.0.2.5:10443`

Para conectar 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 conectar ao StorageGRID:

- `https://192.0.2.6:10444`

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

Passos

1. Faça login no Gerenciador de Grade usando um [navegador da web suportado](#).
2. Para localizar o endereço IP de um nó de grade:
 - a. Selecione **NODES**.
 - b. Selecione o nó de administração, nó de gateway ou nó de armazenamento ao qual deseja se conectar.
 - c. Selecione a guia **Visão geral**.
 - d. Na seção informações do nó, observe os endereços IP do nó.
 - e. Selecione **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:

- Selecione **CONFIGURATION > Network > High Availability groups**.
- Na tabela, anote o endereço IP virtual do grupo HA.

4. Para localizar o número da porta de um endpoint do Load Balancer:

- Selecione **CONFIGURATION > Network > Load balancer endpoints**.

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

- Selecione um endpoint e selecione **Editar endpoint**.

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

- Confirme se o endpoint selecionado está configurado para uso com o protocolo correto (S3 ou Swift) e selecione **Cancelar**.
- 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.

Configurar interfaces VLAN

Você pode criar interfaces de LAN virtual (VLAN) em nós de administração e nós de gateway e usá-las em grupos de HA e pontos de extremidade do balanceador de carga para isolar e particionar o tráfego para obter segurança, flexibilidade e desempenho.

Considerações para interfaces VLAN

- Você cria uma interface VLAN inserindo um ID de VLAN e escolhendo uma interface pai em um ou mais nós.
- Uma interface pai deve ser configurada como uma interface de tronco no switch.
- Uma interface pai pode ser a rede de Grade (eth0), a rede de Cliente (eth2) ou uma interface de tronco adicional para a VM ou host bare-metal (por exemplo, ens256).
- Para cada interface VLAN, você pode selecionar apenas uma interface pai para um determinado nó. Por exemplo, você não pode usar a interface de rede de Grade e a interface de rede de cliente no mesmo nó de gateway que a interface pai para a mesma VLAN.
- Se a interface VLAN for para tráfego Admin Node, que inclui tráfego relacionado ao Grid Manager e ao Tenant Manager, selecione interfaces somente em Admin Nodes.

- Se a interface VLAN for para tráfego de clientes S3 ou Swift, selecione interfaces em nós de administração ou nós de gateway.
- Se você precisar adicionar interfaces de tronco, consulte o seguinte para obter detalhes:
 - **VMware (após a instalação do nó):** [VMware: Adicione interfaces de tronco ou acesso a um nó](#)
 - **RHEL ou CentOS (antes de instalar o nó):** [Criar arquivos de configuração de nó](#)
 - * Ubuntu ou Debian (antes de instalar o nó)*: [Criar arquivos de configuração de nó](#)
 - **RHEL, CentOS, Ubuntu ou Debian (após a instalação do nó):** [Linux: Adicione interfaces de tronco ou acesso a um nó](#)

Crie uma interface VLAN

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- Uma interface de tronco foi configurada na rede e conectada ao nó VM ou Linux. Você sabe o nome da interface do tronco.
- Você sabe o ID da VLAN que está configurando.

Sobre esta tarefa

O administrador da rede pode ter configurado uma ou mais interfaces de tronco e uma ou mais VLANs para segregar o tráfego de cliente ou administrador pertencente a diferentes aplicativos ou locatários. Cada VLAN é identificada por um ID numérico ou tag. Por exemplo, sua rede pode usar VLAN 100 para tráfego FabricPool e VLAN 200 para um aplicativo de arquivamento.

Você pode usar o Gerenciador de Grade para criar interfaces de VLAN que permitem que os clientes acessem o StorageGRID em uma VLAN específica. Ao criar interfaces VLAN, você especifica a ID da VLAN e seleciona interfaces pai (tronco) em um ou mais nós.

Acesse o assistente

1. Selecione **CONFIGURATION > Network > VLAN interfaces**.
2. Selecione **criar**.

Insira os detalhes das interfaces VLAN


1. Especifique o ID da VLAN na rede. Pode introduzir qualquer valor entre 1 e 4094.

Os IDs de VLAN não precisam ser exclusivos. Por exemplo, você pode usar VLAN ID 200 para tráfego de administrador em um local e o mesmo VLAN ID para tráfego de cliente em outro local. Você pode criar interfaces VLAN separadas com diferentes conjuntos de interfaces pai em cada local. No entanto, duas interfaces VLAN com o mesmo ID não podem compartilhar a mesma interface em um nó.


Se você especificar uma ID que já foi usada, uma mensagem será exibida. Você pode continuar criando outra interface de VLAN para o mesmo ID de VLAN ou pode selecionar **Cancelar** e editar a ID existente.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.

VLAN details

VLAN ID 

203

Description (optional) 

VLAN for S3 tenants. Uses Admin and Gateway Nodes at site 1.

60/64

Cancel Continue

3. Selecione **continuar**.

Escolha interfaces pai

A tabela lista as interfaces disponíveis para todos os nós de administração e nós de gateway em cada local da grade. As interfaces Admin Network (eth1) não podem ser usadas como interfaces pai e não são mostradas.







1. Selecione uma ou mais interfaces pai às quais anexar esta VLAN.

Por exemplo, você pode querer anexar uma VLAN à interface de rede de cliente (eth2) para um nó de gateway e um nó de administrador.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

Search...


	Site 	Node name 	Interface 	Description 	Node type 	Attached VLANs 
<input type="checkbox"/>	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
<input checked="" type="checkbox"/>	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
<input type="checkbox"/>	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
<input checked="" type="checkbox"/>	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
<input type="checkbox"/>	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

Previous Continue

2. Selecione **continuar**.

Confirme as definições

1. Revise a configuração e faça quaisquer alterações.
 - Se você precisar alterar a ID ou a descrição da VLAN, selecione **Digite os detalhes da VLAN** na parte superior da página.
 - Se você precisar alterar uma interface pai, selecione **escolha interfaces pai** na parte superior da página ou selecione **anterior**.
 - Se for necessário remover uma interface pai, selecione a lixeira .
2. Selecione **Guardar**.
3. Aguarde até 5 minutos para que a nova interface apareça como uma seleção na página grupos de alta disponibilidade e seja listada na tabela **interfaces de rede** para o nó (**NODES > parent interface node > Network**).

Editar uma interface VLAN

Ao editar uma interface VLAN, você pode fazer os seguintes tipos de alterações:

- Altere a ID ou a descrição da VLAN.
- Adicionar ou remover interfaces pai.

Por exemplo, você pode querer remover uma interface pai de uma interface VLAN se você planeja desativar o nó associado.

Observe o seguinte:

- Não é possível alterar um ID de VLAN se a interface de VLAN for usada em um grupo HA.
- Não é possível remover uma interface pai se essa interface pai for usada em um grupo HA.

Por exemplo, suponha que a VLAN 200 esteja conectada às interfaces pai nos nós A e B. se um grupo de HA usar a interface VLAN 200 para o nó A e a interface eth2 para o nó B, você poderá remover a interface pai não utilizada para o nó B, mas não poderá remover a interface pai usada para o nó A.

Passos

1. Selecione **CONFIGURATION > Network > VLAN interfaces**.
2. Marque a caixa de seleção da interface VLAN que deseja editar. Em seguida, selecione **ações > Editar**.
3. Opcionalmente, atualize o ID da VLAN ou a descrição. Em seguida, selecione **continuar**.

Não é possível atualizar um ID de VLAN se a VLAN for usada em um grupo HA.

4. Opcionalmente, marque ou desmarque as caixas de seleção para adicionar interfaces pai ou remover interfaces não utilizadas. Em seguida, selecione **continuar**.
5. Revise a configuração e faça quaisquer alterações.
6. Selecione **Guardar**.

Remova uma interface VLAN

Você pode remover uma ou mais interfaces VLAN.

Não é possível remover uma interface VLAN se ela for usada atualmente em um grupo HA. Você deve remover a interface VLAN do grupo HA antes de removê-la.

Para evitar quaisquer interrupções no tráfego do cliente, considere fazer um dos seguintes procedimentos:

- Adicione uma nova interface VLAN ao grupo HA antes de remover essa interface VLAN.
- Crie um novo grupo HA que não use essa interface VLAN.
- Se a interface VLAN que você deseja remover for atualmente a interface ativa, edite o grupo HA. Mova a interface VLAN que você deseja remover para a parte inferior da lista de prioridades. Aguarde até que a comunicação seja estabelecida na nova interface primária e remova a interface antiga do grupo HA. Finalmente, exclua a interface VLAN nesse nó.

Passos

1. Selecione **CONFIGURATION > Network > VLAN interfaces**.
2. Marque a caixa de seleção para cada interface VLAN que deseja remover. Em seguida, selecione **ações > Excluir**.
3. Selecione **Sim** para confirmar a sua seleção.

Todas as interfaces VLAN selecionadas são removidas. Um banner verde de sucesso aparece na página interfaces VLAN.

Gerenciar grupos de alta disponibilidade

Gerenciar grupos de alta disponibilidade (HA): Visão geral

Você pode agrupar as interfaces de rede de vários nós de administrador e gateway em um grupo de alta disponibilidade (HA). Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho.

O que é um grupo HA?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões de dados altamente disponíveis para clientes S3 e Swift ou para fornecer conexões altamente disponíveis para o Gerenciador de Grade e o Gerenciador de Tenant.

Cada grupo de HA fornece acesso aos serviços compartilhados nos nós selecionados.

- Grupos DE HA que incluem nós de gateway, nós de administração ou ambos fornecem conexões de dados altamente disponíveis para clientes S3 e Swift.
- Os GRUPOS DE HA que incluem apenas os nós de Admin fornecem conexões altamente disponíveis ao Gerenciador de Grade e ao Gerente do locatário.
- Um grupo de HA que inclui apenas dispositivos SG100 ou SG1000 e nós de software baseados em VMware pode fornecer conexões altamente disponíveis para [S3 inquilinos que usam S3 Selecto](#) . Os GRUPOS HA são recomendados ao usar S3 Select, mas não são necessários.

Como criar um grupo HA?

1. Você seleciona uma interface de rede para um ou mais nós de administrador ou nós de gateway. Você pode usar uma interface Grid Network (eth0), uma interface Client Network (eth2), uma interface VLAN ou uma interface de acesso que você adicionou ao nó.



Não é possível adicionar uma interface a um grupo HA se ele tiver um endereço IP atribuído pelo DHCP.

2. Você especifica uma interface para ser a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.
3. Você determina a ordem de prioridade para quaisquer interfaces de backup.
4. Você atribui um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos clientes podem usar qualquer um desses endereços VIP para se conectar ao StorageGRID.

Para obter instruções, [Configurar grupos de alta disponibilidade](#) consulte .

O que é a interface ativa?

Durante a operação normal, todos os endereços VIP do grupo HA são adicionados à interface principal, que é a primeira interface na ordem de prioridade. Enquanto a interface principal permanecer disponível, ela é usada quando os clientes se conectam a qualquer endereço VIP do grupo. Ou seja, durante a operação normal, a interface primária é a interface "ativa" para o grupo.

Da mesma forma, durante a operação normal, quaisquer interfaces de prioridade inferior para o grupo HA funcionam como interfaces de "backup". Essas interfaces de backup não são usadas a menos que a interface principal (atualmente ativa) fique indisponível.

Exibir o status atual do grupo de HA de um nó

Para ver se um nó está atribuído a um grupo de HA e determinar seu status atual, selecione **NÓS > node**.

Se a guia **Visão geral** incluir uma entrada para **grupos de HA**, o nó será atribuído aos grupos de HA listados. O valor após o nome do grupo é o status atual do nó no grupo HA:



- **Ativo:** O grupo HA está sendo hospedado neste nó.
- **Backup:** O grupo HA não está usando esse nó no momento; essa é uma interface de backup.
- **Stopped:** O grupo HA não pode ser hospedado neste nó porque o serviço de alta disponibilidade (keepalived) foi interrompido manualmente.
- **Falha:** O grupo HA não pode ser hospedado neste nó devido a um ou mais dos seguintes:
 - O serviço do Load Balancer (nginx-gw) não está sendo executado no nó.
 - A interface eth0 ou VIP do nó está inativa.
 - O nó está inativo.

Neste exemplo, o nó de administração principal foi adicionado a dois grupos de HA. Este nó é atualmente a interface ativa para o grupo de clientes administradores e uma interface de backup para o grupo de clientes FabricPool.

DC1-ADM1 (Primary Admin Node)

[Overview](#)
[Hardware](#)
[Network](#)
[Storage](#)
[Load balancer](#)
[Tasks](#)

Node information

Name:	DC1-ADM1
Type:	Primary Admin Node
ID:	ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state:	 Connected
Software version:	11.6.0 (build 20211207.1804.614bc17)
HA groups:	<div>Admin clients (Active)</div> <div>FabricPool clients (Backup)</div>
IP addresses:	<div>172.16.1.225 - eth0 (Grid Network)</div> <div>10.224.1.225 - eth1 (Admin Network)</div> <div>47.47.0.2, 47.47.1.225 - eth2 (Client Network)</div> <div>Show additional IP addresses </div>

O que acontece quando a interface ativa falha?

A interface que atualmente hospeda os endereços VIP é a interface ativa. Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP serão movidos para a primeira interface de backup disponível na ordem de prioridade. Se essa interface falhar, os endereços VIP passam para a próxima interface de backup disponível, e assim por diante.

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 conectividade 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.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos clientes tenham pouco impacto e possam confiar em comportamentos normais de repetição para continuar a operação.

Quando a falha é resolvida e uma interface de prioridade mais alta torna-se disponível novamente, os endereços VIP são movidos automaticamente para a interface de prioridade mais alta que está disponível.

Como os grupos HA são usados?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões altamente disponíveis ao StorageGRID para dados de objetos e para uso administrativo.

- 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	<ul style="list-style-type: none">• Nó de administração principal (primário)• Nós de administração não primários <p>Nota: o nó de administração principal deve ser a interface principal. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal.</p>
Acesso apenas ao Gestor do Locatário	<ul style="list-style-type: none">• Nós de administração primários ou não primários
Acesso ao cliente S3 ou Swift — Serviço de Load Balancer	<ul style="list-style-type: none">• Nós de administração• Nós de gateway
Acesso de cliente S3 para S3 Selezione	<ul style="list-style-type: none">• SG100 ou SG1000 aparelhos• Nós de software baseados em VMware <p>Nota: Os GRUPOS HA são recomendados ao usar o S3 Select, mas não são necessários.</p>

Objetivo do grupo HA	Adicione nós desse tipo ao grupo de HA
Acesso ao cliente S3 ou Swift — serviço CLB Nota: o serviço CLB está obsoleto.	<ul style="list-style-type: none"> Nós de gateway

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

Se um serviço do Grid Manager ou do Tenant Manager falhar, o failover do grupo HA não será acionado.

Se você estiver conectado ao Gerenciador de Grade ou ao Gerenciador de Locatário quando ocorrer failover, você será desconectado 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.

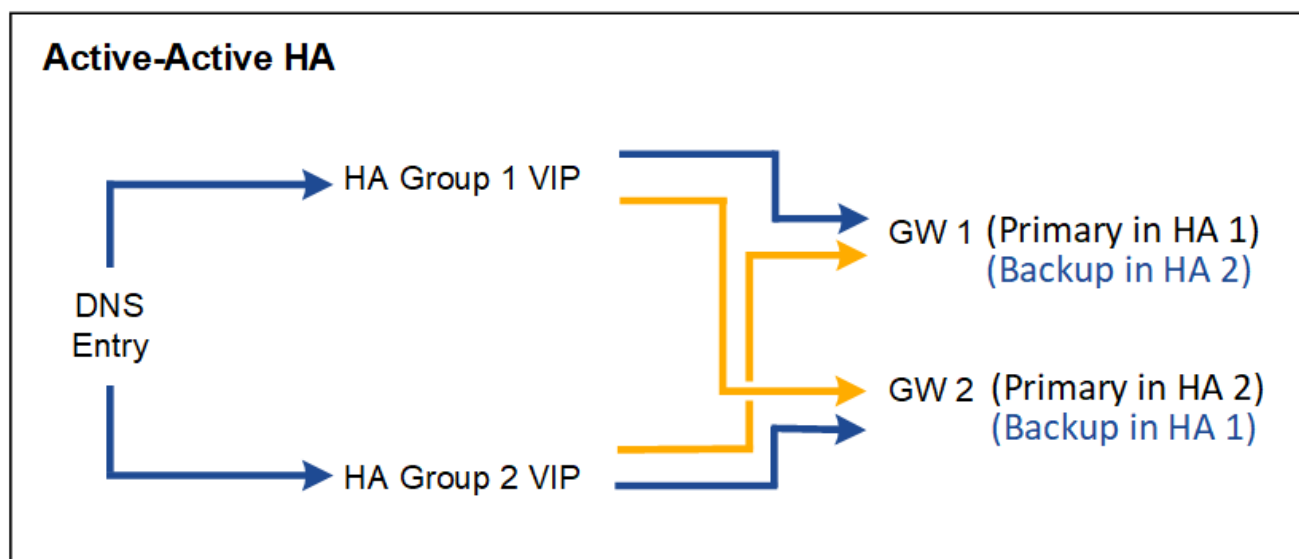
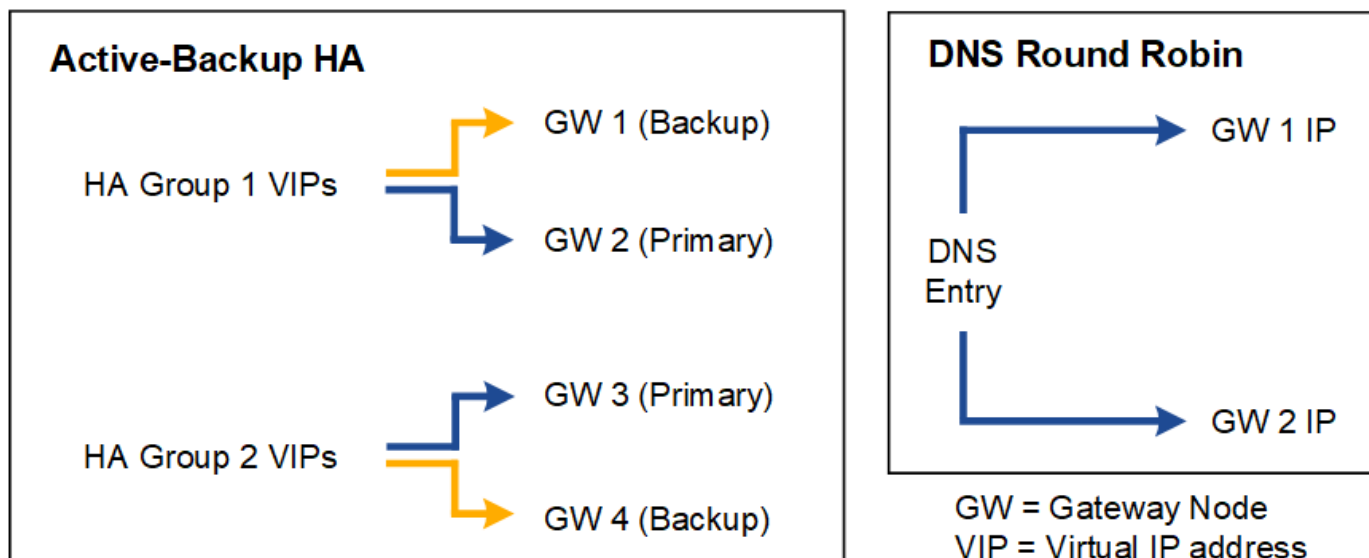


O serviço CLB está obsoleto.

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.

Nos diagramas, azul indica a interface principal no grupo HA e amarelo indica a interface de backup no grupo HA.



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

Configuração	Vantagens	Desvantagens
Active-Backup HA	<ul style="list-style-type: none"> Gerenciado pelo StorageGRID sem dependências externas. Failover rápido. 	<ul style="list-style-type: none"> Apenas um nó em um grupo de HA está ativo. Pelo menos um nó por grupo de HA ficará inativo.
DNS Round Robin	<ul style="list-style-type: none"> Maior taxa de transferência agregada. Sem hosts ociosos. 	<ul style="list-style-type: none"> Failover lento, que pode depender do comportamento do cliente. Requer configuração de hardware fora do StorageGRID. Precisa de uma verificação de integridade implementada pelo cliente.

Configuração	Vantagens	Desvantagens
Ha ativo-ativo	<ul style="list-style-type: none"> • O tráfego é distribuído em vários grupos de HA. • Alta taxa de transferência agregada que é dimensionada com o número de grupos de HA. • Failover rápido. 	<ul style="list-style-type: none"> • Mais complexo de configurar. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.

Configurar grupos de alta disponibilidade

Você pode configurar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- Se você planeja usar uma interface VLAN em um grupo HA, criou a interface VLAN. [Configurar interfaces VLAN](#) Consulte .
- Se você planeja usar uma interface de acesso para um nó em um grupo de HA, criou a interface:
 - **Red Hat Enterprise Linux ou CentOS (antes de instalar o nó):** [Criar arquivos de configuração de nó](#)
 - * Ubuntu ou Debian (antes de instalar o nó)*: [Criar arquivos de configuração de nó](#)
 - * Linux (após a instalação do nó)*: [Linux: Adicione interfaces de tronco ou acesso a um nó](#)
 - **VMware (após a instalação do nó):** [VMware: Adicione interfaces de tronco ou acesso a um nó](#)

Crie um grupo de alta disponibilidade

Ao criar um grupo de alta disponibilidade, você seleciona uma ou mais interfaces e as organiza por ordem de prioridade. Em seguida, atribua um ou mais endereços VIP ao grupo.

Uma interface deve ser incluída em um grupo de HA para um nó de gateway ou um nó de administrador. Um grupo de HA só pode usar uma interface para qualquer nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos de HA.

Acesse o assistente

1. Selecione **CONFIGURATION > Network > High Availability groups**.
2. Selecione **criar**.

Introduza os detalhes do grupo HA

1. Forneça um nome exclusivo para o grupo HA.

×

Create a high availability group

1 Enter details

2 Add interfaces

3 Prioritize interfaces

4 Enter IP addresses

Enter details for the HA group

HA group name

Description (optional)

- Opcionalmente, insira uma descrição para o grupo HA.
- Selecione **continuar**.

Adicionar interfaces ao grupo HA

- Selecione uma ou mais interfaces para adicionar a esse grupo de HA.

Use os cabeçalhos de coluna para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Search...

Total interface count: 4

Node	Interface	Site	IPv4 subnet	Node type
<input type="checkbox"/> DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
<input type="checkbox"/> DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth2	DC2	—	Admin Node

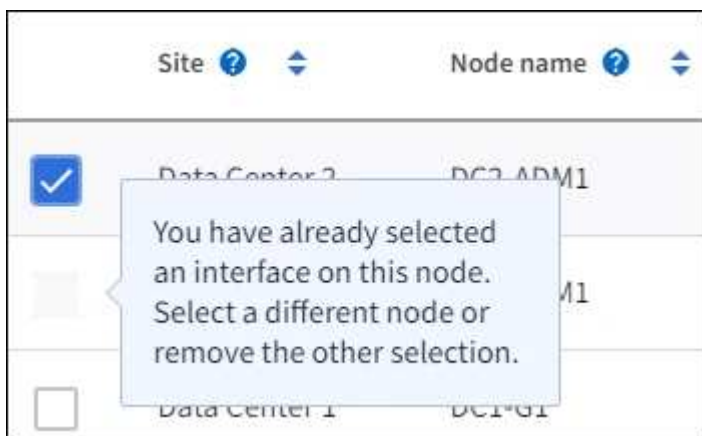
0 interfaces selected



Depois de criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

Diretrizes para a seleção de interfaces

- Você deve selecionar pelo menos uma interface.
- Você pode selecionar apenas uma interface para um nó.
- Se o grupo de HA for para proteção de HA dos serviços Admin Node, que incluem o Grid Manager e o Tenant Manager, selecione interfaces apenas em nós de administração.
- Se o grupo de HA for para proteção de HA de tráfego de cliente S3 ou Swift, selecione interfaces em nós de administração, nós de gateway ou ambos.
- Se o grupo HA for para proteção HA do serviço CLB obsoleto, selecione interfaces somente em nós de Gateway.
- Se você selecionar interfaces em diferentes tipos de nós, uma nota informativa será exibida. Lembre-se de que, se ocorrer um failover, os serviços fornecidos pelo nó ativo anteriormente podem não estar disponíveis no nó recém-ativo. Por exemplo, um nó de gateway de backup não pode fornecer proteção de HA dos serviços Admin Node. Da mesma forma, um nó Admin de backup não pode executar todos os procedimentos de manutenção que o nó Admin principal pode fornecer.
- Se não for possível selecionar uma interface, a caixa de verificação estará desativada. A dica da ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o seu valor de sub-rede ou gateway entrar em conflito com outra interface selecionada.
- Não é possível selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **continuar**.

Determine a ordem de prioridade

1. Determine a interface principal e todas as interfaces de backup (failover) para esse grupo de HA.

Arraste e solte linhas para alterar os valores na coluna **Priority Order**.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	⬆ DC1-ADM1-104-96	eth2	Primary Admin Node
2	⬆ DC2-ADM1-104-103	eth2	Admin Node



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

A primeira interface na lista é a interface principal. A interface principal é a interface ativa, a menos que ocorra uma falha.

Se o grupo de HA incluir mais de uma interface e a interface principal falhar, os endereços VIP serão movidos para a interface de maior prioridade disponível. Se essa interface falhar, os endereços VIP passam para a próxima interface de maior prioridade disponível, e assim por diante.

2. Selecione **continuar**.

Introduza endereços IP

1. No campo **Subnet CIDR**, especifique a sub-rede VIP na notação CIDR—um endereço IPv4 seguido de uma barra e o comprimento da sub-rede (0-32).

O endereço de rede não deve ter nenhum bit de host definido. Por exemplo, 192.16.0.0/22.



Se você usar um prefixo de 32 bits, o endereço de rede VIP também serve como endereço de gateway e endereço VIP.

Enter details for the HA group

Subnet CIDR ?

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ?

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ?

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

2. Opcionalmente, se algum cliente S3, Swift, administrativo ou inquilino acessar esses endereços VIP de uma sub-rede diferente, digite o **Endereço IP Gateway**. O endereço de gateway deve estar dentro da sub-rede VIP.

Os usuários de cliente e administrador usarão esse gateway para acessar os endereços IP virtuais.

3. Introduza um ou mais **endereços IP virtuais** para o grupo HA. Você pode adicionar até 10 endereços IP. Todos os VIPs devem estar dentro da sub-rede VIP.

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

4. Selecione **Create HA group** e selecione **Finish**.

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



Aguarde até 15 minutos para que as alterações em um grupo de HA sejam aplicadas a todos os nós.

Próximas etapas

Se você usar esse grupo de HA para balanceamento de carga, crie um ponto de extremidade do balanceador de carga para determinar a porta e o protocolo de rede e para anexar todos os certificados necessários. [Configurar pontos de extremidade do balanceador de carga](#)Consulte .

Edite um grupo de alta disponibilidade

Você pode editar um grupo de alta disponibilidade (HA) para alterar seu nome e descrição, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou atualizar endereços IP virtuais.

Por exemplo, talvez seja necessário editar um grupo de HA se desejar remover o nó associado a uma interface selecionada em um procedimento de desativação de site ou nó.

Passos

1. Selecione **CONFIGURATION > Network > High Availability groups**.

A página grupos de alta disponibilidade mostra todos os grupos de HA existentes.

High availability groups

[Learn more about HA groups](#)

You can group the network interfaces of multiple Admin and Gateway Nodes into a high availability (HA) group. If the active interface in the group fails, a backup interface can manage the workload.

Each HA group provides access to the shared services on the selected nodes. Select Gateway Nodes, Admin Nodes, or both for load balancing. Select Admin Nodes for management services. All interfaces in a group must be in the same subnet. You assign one or more virtual IP addresses (VIPs) to each group. Clients use these VIPs to connect to StorageGRID.

You cannot select an interface if it has a DHCP-assigned IP address.

Wait up to 15 minutes for changes to an HA group to be applied to all nodes.

Create

Actions ▾

Search...

Total HA groups count: 2

<input type="checkbox"/>	Name ? ▴ ▾	Description ? ▴ ▾	Virtual IP address ? ▴ ▾	Interfaces (in priority order) ? ▴ ▾
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

← Previous 1 Next →

2. Marque a caixa de seleção do grupo HA que deseja editar.
3. Siga um destes procedimentos, com base no que você deseja atualizar:
 - Selecione **ações > Editar endereço IP virtual** para adicionar ou remover endereços VIP.
 - Selecione **ações > Editar grupo HA** para atualizar o nome ou a descrição do grupo, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou remover endereços VIP.
4. Se você selecionou **Editar endereço IP virtual**:
 - a. Atualize os endereços IP virtuais do grupo HA.
 - b. Selecione **Guardar**.
 - c. Selecione **Finish**.
5. Se você selecionou **Edit HA group**:
 - a. Opcionalmente, atualize o nome ou a descrição do grupo.
 - b. Opcionalmente, selecione ou desmarque as caixas de seleção para adicionar ou remover interfaces.



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

- c. Opcionalmente, arraste e solte linhas para alterar a ordem de prioridade da interface principal e de quaisquer interfaces de backup para esse grupo de HA.
- d. Opcionalmente, atualize os endereços IP virtuais.
- e. Selecione **Save** e, em seguida, selecione **Finish**.



Aguarde até 15 minutos para que as alterações em um grupo de HA sejam aplicadas a todos os nós.

Remova um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) de cada vez. No entanto, não é possível remover um grupo de HA se ele estiver vinculado a um ou mais pontos de extremidade do balanceador de carga.

Para evitar interrupções do cliente, atualize quaisquer aplicativos de cliente S3 ou Swift afetados antes de remover um grupo HA. Atualize cada cliente para se conectar 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.

Passos

1. Selecione **CONFIGURATION > Network > High Availability groups**.
2. Marque a caixa de seleção para cada grupo de HA que deseja remover. Em seguida, selecione **ações > Remover grupo HA**.
3. Reveja a mensagem e selecione **Eliminar grupo HA** para confirmar a sua seleção.

Todos os grupos de HA selecionados são removidos. Um banner verde de sucesso aparece na página grupos de alta disponibilidade.

Gerenciar o balanceamento de carga

Gerenciar balanceamento de carga: Visão geral

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 equilibrar a carga de trabalho do cliente 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.

[Como funciona o balanceamento de carga - Serviço do Load Balancer](#) Consulte .

- Use o serviço CLB (Connection Load Balancer) obsoleto, que é instalado apenas em nós de Gateway. O serviço CLB fornece balanceamento de carga da camada 4 e suporta custos de link.

[Como funciona o balanceamento de carga - serviço CLB \(obsoleto\)](#) Consulte .

- 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 de rede (HTTP ou HTTPS), um tipo de cliente (S3 ou Swift) e um modo de ligação. Os endpoints HTTPS requerem um certificado de servidor. Os modos de vinculação permitem restringir a acessibilidade das portas de endpoint a:

- Os endereços IP virtuais (VIPs) de grupos específicos de alta disponibilidade (HA)
- Interfaces de rede específicas de nós específicos de Admin e Gateway

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 em [Remova os remaps 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.

Configurar pontos de extremidade do balanceador de carga

Os pontos de extremidade do balanceador de carga determinam as portas e os protocolos de rede S3 e os clientes Swift podem usar ao se conectar ao balanceador de carga StorageGRID nos nós de gateway e administrador.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- Se você remapeou anteriormente uma porta que pretende usar para o ponto de extremidade do balanceador de carga, você tem [removido o remapeamento da porta](#).
- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Os GRUPOS HA são recomendados, mas não são necessários. [Gerenciar grupos de alta disponibilidade](#) Consulte .
- Se o ponto final do balanceador de carga for usado [S3 inquilinos para S3 Select](#) pelo , ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente dispositivos SG100 ou SG1000 e nós de software baseados em VMware são permitidos para os pontos de extremidade do balanceador de carga usados para o S3 Select.
- Você configurou todas as interfaces VLAN que planeja usar. [Configurar interfaces VLAN](#) Consulte .
- Se você estiver criando um endpoint HTTPS (recomendado), você terá as informações para o certificado do servidor.



As alterações a um certificado de endpoint podem levar até 15 minutos para serem aplicadas a todos os nós.

- Para carregar um certificado, você precisa do certificado do servidor, da chave privada do certificado e, opcionalmente, de um pacote de CA.
- Para gerar um certificado, você precisa de todos os nomes de domínio e endereços IP que os clientes S3 ou Swift usarão para acessar o endpoint. Você também deve conhecer o assunto (Nome distinto).
- Se você quiser usar o certificado StorageGRID S3 e Swift API (que também pode ser usado para conexões diretamente aos nós de armazenamento), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. [Configure os certificados API S3 e Swift](#) Consulte .

O certificado 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, `*.storagegrid.example.com` usa o caractere curinga `*` para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`. [Configure os nomes de domínio de endpoint da API S3](#) Consulte .

Crie um ponto de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga especifica uma porta, um tipo de cliente (S3 ou Swift) e um protocolo de rede (HTTP ou HTTPS).

Acesse o assistente

1. Selecione **CONFIGURATION > Network > Load balancer endpoints**.
2. Selecione **criar**.

Introduza os detalhes do endpoint

- 1. Insira os detalhes do endpoint.

Create a load balancer endpoint

1 Enter endpoint details

2 Select binding mode

3 Attach certificate

Endpoint details

Name

Port

Enter an unused port or accept the suggested port.

10443

Client type

Select the type of client application that will use this endpoint.

S3

Swift

Network protocol

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

HTTPS (recommended)

HTTP

Cancel

Continue

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página pontos de extremidade do balanceador de carga.
Porta	<p>Os clientes de porta serão usados para se conectar ao serviço Load Balancer em nós de administração e nós de gateway.</p> <p>Aceite o número de porta sugerido ou insira qualquer porta externa que não seja usada por outro serviço de grade. Introduza um valor entre 1 e 65535.</p> <p>Se você digitar 80 ou 443, o endpoint será configurado somente em nós de Gateway. Essas portas são reservadas em nós de administração.</p> <p>Consulte Diretrizes de rede para obter informações sobre portas externas.</p>
Tipo de cliente	O tipo de aplicativo cliente que usará esse endpoint, S3 ou Swift .

Campo	Descrição
Protocolo de rede	<p>O protocolo de rede que os clientes utilizarão ao ligar a este ponto final.</p> <ul style="list-style-type: none"> • Selecione HTTPS para comunicação segura e criptografada TLS (recomendada). Você deve anexar um certificado de segurança antes de salvar o endpoint. • Selecione HTTP para comunicação menos segura e não criptografada. Use HTTP apenas para uma grade não-produção.

2. Selecione **continuar**.

Selecione o modo de encadernação

1. Selecione um modo de encadernação para o endpoint controlar como o endpoint é acessado.

Opção	Descrição
Global (predefinição)	<p>Os clientes podem acessar o endpoint usando um nome de domínio totalmente qualificado (FQDN), o endereço IP de qualquer nó de gateway ou nó de administrador ou o endereço IP virtual de qualquer grupo de HA em qualquer rede.</p> <p>Use a configuração Global (padrão), a menos que você precise restringir a acessibilidade deste endpoint.</p>
Interfaces de nós	<p>Os clientes devem usar o endereço IP de um nó e interface de rede selecionados para acessar esse endpoint.</p>
IPs virtuais de grupos de HA	<p>Os clientes devem usar um endereço IP virtual de um grupo de HA para acessar esse endpoint.</p> <p>Os endpoints com esse modo de encadernação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.</p> <p>Os endpoints com este modo podem usar o mesmo número de porta, desde que as interfaces selecionadas para os endpoints não se sobreponham.</p>



Se você usar a mesma porta para mais de um endpoint, um endpoint usando o modo **Virtual IPs de grupos de HA** substitui um endpoint usando o modo **Node interfaces**, que substitui um endpoint usando o modo **Global**.

2. Se você selecionou **interfaces de nó**, selecione uma ou mais interfaces de nó para cada nó de administrador ou nó de gateway que você deseja associar a esse ponto de extremidade.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☒ Node interfaces ☐ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search...

Total interface count: 3

<input type="checkbox"/>	Node	Node interface	Site	IP address	Node type
<input type="checkbox"/>	DC1-ADM1	eth0	Data Center 1	172.16.3.246 and 2 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth1	Data Center 1	10.224.3.246 and 5 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth2	Data Center 1	47.47.3.246 and 3 more	Primary Admin Node

3. Se você selecionou **IPs virtuais de grupos de HA**, selecione um ou mais grupos de HA.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☐ Node interfaces ☒ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search...

Q

Total interface count: 2

<input type="checkbox"/>	Name ?	Description ?	Virtual IP address ?	Interfaces (in priority order) ?
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

4. Se você estiver criando um endpoint **HTTP**, não será necessário anexar um certificado. Selecione **Create** para adicionar o novo ponto de extremidade do balanceador de carga. Em seguida, vá [Depois de terminar](#) para . Caso contrário, selecione **continuar** para anexar o certificado.

Anexar certificado

1. Se você estiver criando um endpoint **HTTPS**, selecione o tipo de certificado de segurança que deseja anexar ao endpoint.

O certificado protege as conexões entre clientes S3 e Swift e o serviço Load Balancer no nó Admin ou nos nós Gateway.

- * Carregar certificado*. Selecione esta opção se tiver certificados personalizados para carregar.
- **Gerar certificado**. Selecione esta opção se tiver os valores necessários para gerar um certificado personalizado.
- **Use o certificado StorageGRID S3 e Swift**. Selecione essa opção se quiser usar o certificado global S3 e Swift API, que também pode ser usado para conexões diretamente aos nós de storage.

Não é possível selecionar essa opção a menos que você tenha substituído o certificado padrão S3 e Swift API, assinado pela CA de grade, por um certificado personalizado assinado por uma autoridade de certificação externa. [Configure os certificados API S3 e Swift](#) Consulte .

2. Se você não estiver usando o certificado StorageGRID S3 e Swift, carregue ou gere o certificado.

Carregar certificado

- a. Selecione **carregar certificado**.
- b. Carregue os ficheiros de certificado do servidor necessários:
 - **Certificado do servidor:** O arquivo de certificado do servidor personalizado na codificação PEM.
 - **Chave privada de certificado:** O arquivo de chave privada de certificado de servidor personalizado (`.key`).



As chaves privadas EC devem ter 224 bits ou mais. As chaves privadas RSA devem ter 2048 bits ou mais.

- **Pacote CA:** Um único arquivo opcional 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.
- c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote opcional da CA, cada certificado será exibido em sua própria guia.
 - Selecione **Baixar certificado** para salvar o arquivo de certificado ou selecione **Baixar pacote de CA** para salvar o pacote de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** ou **Copiar pacote de CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- d. Selecione **criar**. O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 e Swift e o endpoint.

Gerar certificado

- a. Selecione **Generate certificate** (gerar certificado).
- b. Especifique as informações do certificado:
 - **Nome de domínio:** Um ou mais nomes de domínio totalmente qualificados a incluir no certificado. Use um `*` como um curinga para representar vários nomes de domínio.
 - **IP:** Um ou mais endereços IP a incluir no certificado.
 - **Assunto:** X.509 Assunto ou nome distinto (DN) do proprietário do certificado.
 - **Dias válidos:** Número de dias após a criação em que o certificado expira.
- c. Selecione **Generate**.
- d. Selecione **Detalhes do certificado** para ver os metadados do certificado gerado.

- Selecione **Transferir certificado** para guardar o ficheiro de certificado.

Especifique o nome do arquivo de certificado e o local de download. Salve o arquivo com a extensão `.pem`.

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copy Certificate PEM** para copiar o conteúdo do certificado para colar em outro lugar.

e. Selecione **criar**.

O ponto final do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 e Swift e este endpoint.

depois de terminar

1. Se você usar um sistema de nomes de domínio (DNS), verifique se o DNS inclui um Registro para associar o nome de domínio totalmente qualificado do StorageGRID a cada endereço IP que os clientes usarão para fazer conexões.

O endereço IP inserido no Registro DNS depende se você está usando um grupo HA de nós de balanceamento de carga:

- Se você tiver configurado um grupo HA, os clientes se conectarão aos endereços IP virtuais desse grupo HA.
- Se você não estiver usando um grupo de HA, os clientes se conectarão ao serviço do StorageGRID Load Balancer usando o endereço IP de qualquer nó de gateway ou nó de administrador.

Você também deve garantir que o Registro DNS faça referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes de curinga.

2. Forneça aos clientes S3 e Swift as informações necessárias para se conectar ao endpoint:

- Número da porta
- Nome de domínio ou endereço IP totalmente qualificado
- Todos os detalhes necessários do certificado

Visualize e edite pontos de extremidade do balanceador de carga


Você pode exibir detalhes dos endpoints existentes do balanceador de carga, incluindo os metadados do certificado para um endpoint seguro. Você também pode alterar o nome ou o modo de vinculação de um endpoint e atualizar quaisquer certificados associados.

Não é possível alterar o tipo de serviço (S3 ou Swift), a porta ou o protocolo (HTTP ou HTTPS).

- Para exibir informações básicas de todos os pontos de extremidade do balanceador de carga, revise a tabela na página pontos de extremidade do balanceador de carga.

<div>Create Actions Search...</div>						Total endpoints count: 1
<input type="checkbox"/>	Name ?	Port ?	Network protocol ?	Binding mode ?	Certificate expiration ?	
<input type="checkbox"/>	FabricPool endpoint	10443	HTTPS	Global	Oct 19th, 2022	

- Para exibir todos os detalhes sobre um endpoint específico, incluindo metadados de certificado, selecione o nome do endpoint na tabela.

FabricPool endpoint 

Port:10443

Client type:S3

Network protocol:HTTPS

Binding mode:Global

Endpoint ID:c2b6feb3-c567-449d-b717-4fed98c4a411

Remove


Binding Mode

Certificate

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode


Binding mode:Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Para editar um endpoint, use o menu **ações** na página terminais do balanceador de carga ou a página de detalhes de um endpoint específico.



Depois de editar um endpoint, você pode precisar esperar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu ações	Página de detalhes
Edite o nome do endpoint	<div>a. Marque a caixa de seleção do endpoint.</div> <div>b. Selecione ações > Editar nome do endpoint.</div> <div>c. Introduza o novo nome.</div> <div>d. Selecione Guardar.</div>	<div>a. Selecione o nome do endpoint para exibir os detalhes.</div> <div>b. Selecione o ícone de edição </div> <div>c. Introduza o novo nome.</div> <div>d. Selecione Guardar.</div>

Tarefa	Menu ações	Página de detalhes
Editar o modo de encadernação de endpoint	a. Marque a caixa de seleção do endpoint. b. Selecione actions > Edit endpoint binding mode c. Atualize o modo de encadernação conforme necessário. d. Selecione Salvar alterações .	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione Editar modo de encadernação . c. Atualize o modo de encadernação conforme necessário. d. Selecione Salvar alterações .
Editar certificado de endpoint	a. Marque a caixa de seleção do endpoint. b. Selecione ações > Editar certificado de endpoint . c. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. d. Selecione Salvar alterações .	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia certificado . c. Selecione Editar certificado . d. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3 e Swift, conforme necessário. e. Selecione Salvar alterações .

Remova os pontos finais do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **ações** ou remover um único endpoint da página de detalhes.



Para evitar interrupções do cliente, atualize os aplicativos de cliente S3 ou Swift afetados antes de remover um ponto de extremidade do balanceador de carga. Atualize cada cliente para se conectar usando uma porta atribuída a outro ponto de extremidade do balanceador de carga. Certifique-se de atualizar todas as informações de certificado necessárias também.

- Para remover um ou mais pontos finais:
 - Na página balanceador de carga, marque a caixa de seleção para cada ponto final que deseja remover.
 - Selecione **ações > Remover**.
 - Selecione **OK**.
- Para remover um endpoint da página de detalhes:
 - Na página Load balancer. Selecione o nome do endpoint.
 - Selecione **Remover** na página de detalhes.
 - Selecione **OK**.

Como funciona o balanceamento de carga - serviço CLB (obsoleto)

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, em seguida, expanda um Gateway Node até selecionar **CLB** e as opções abaixo dele.

The screenshot shows the 'Grid Topology' view on the left, with a tree structure of data centers and nodes. A blue box highlights the 'CLB' node under 'DC1-G1-98-161'. On the right, the 'Overview' tab is selected, showing a summary for 'DC1-G1-98-161' updated on 2015-10-27. Below this is a 'Storage Capacity' table.

Storage Capacity		
Storage Nodes Installed:	N/A	
Storage Nodes Readable:	N/A	
Storage Nodes Writable:	N/A	
Installed Storage Capacity:	N/A	
Used Storage Capacity:	N/A	
Used Storage Capacity for Data:	N/A	
Used Storage Capacity for Metadata:	N/A	
Usable Storage Capacity:	N/A	

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

- [Quais são os custos da ligação](#)
- [Atualizar custos de link](#)

Configure os 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 conectam.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- Você confirmou 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 fazer todas as seguintes ações:

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

Os clientes que usam conexões HTTPS (recomendadas) para a grade podem usar qualquer um destes certificados:

- Os clientes que se conectam a um ponto de extremidade do balanceador de carga podem usar um certificado personalizado para esse ponto de extremidade. Cada ponto de extremidade do balanceador de carga pode ser configurado para reconhecer nomes de domínio de endpoint diferentes.
- Os clientes que se conectam a um ponto de extremidade do balanceador de carga, diretamente a um nó de armazenamento, ou diretamente ao serviço CLB obsoleto em um nó de gateway podem personalizar o certificado global S3 e Swift API para incluir todos os nomes de domínio de endpoint necessários.

Passos

1. Selecione **CONFIGURATION > Network > Domain Names**.

A página nomes de domínio do endpoint é exibida.

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: `s3.example.com`, `s3.example.co.uk`, `s3-east.example.com`

Endpoint 1	<input type="text" value="s3.example.com"/>	✕
Endpoint 2	<input type="text"/>	+ ✕

2. Digite a lista de nomes de domínio de endpoint da API S3 nos campos **Endpoint**. Utilize o **+** ícone para adicionar campos adicionais.

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

3. Selecione **Guardar**.
4. Certifique-se de que os certificados de servidor que os clientes utilizam correspondem aos nomes de domínio de endpoint necessários.

- Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que use seu próprio certificado, atualize o certificado associado ao ponto de extremidade.
 - Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que use o certificado global S3 e Swift API, diretamente aos nós de armazenamento ou ao serviço CLB nos nós de Gateway, atualize o certificado global S3 e Swift API.
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](#)
- [Ver endereços IP](#)
- [Configurar grupos de alta disponibilidade](#)
- [Configure os certificados API S3 e Swift](#)
- [Configurar pontos de extremidade do balanceador de carga](#)

Ativar HTTP para comunicações de 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 conectam 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 conectar 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 **CONFIGURATION > System > Grid options**.
2. Na seção Opções de rede, marque a caixa de seleção **Ativar conexão HTTP**.

Network Options



3. Selecione **Guardar**.

Informações relacionadas

- [Configurar pontos de extremidade do balanceador de carga](#)
- [Use S3](#)
- [Use Swift](#)

Controle 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 **CONFIGURATION > System > Grid options**.
2. Na seção Opções de rede, marque a caixa de seleção **impedir modificação de cliente**.

Network Options



Prevent Client Modification ☒

Enable HTTP Connection ☐

Network Transfer Encryption ☐ AES128-SHA ☒ AES256-SHA

3. Selecione **Guardar**.

Gerencie redes e conexões

Diretrizes para redes StorageGRID

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

[Configurar conexões de cliente S3 e Swift](#) Consulte para saber como conectar clientes S3 ou Swift.

Redes StorageGRID predefinidas

Por padrão, o StorageGRID oferece suporte a 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 obter mais informações sobre a topologia de rede, [Diretrizes de rede](#) consulte .

Rede de rede

Obrigatório. A rede de grade é usada para todo o tráfego interno do StorageGRID. Ele fornece conectividade 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 conectado 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.

Interfaces opcionais

Opcionalmente, você pode adicionar interfaces extras a um nó. Por exemplo, você pode querer adicionar uma interface de tronco a um nó Admin ou Gateway, para que você possa usar [Interfaces VLAN](#) para segregar o tráfego pertencente a diferentes aplicativos ou locatários. Ou, talvez você queira adicionar uma interface de acesso a ser usada em um [Grupo de alta disponibilidade \(HA\)](#).

Para adicionar interfaces de tronco ou acesso, consulte o seguinte:

- **VMware (após a instalação do nó):** [VMware: Adicione interfaces de tronco ou acesso a um nó](#)
- **RHEL ou CentOS (antes de instalar o nó):** [Criar arquivos de configuração de nó](#)
- * Ubuntu ou Debian (antes de instalar o nó)*: [Criar arquivos de configuração de nó](#)
- **RHEL, CentOS, Ubuntu ou Debian (após a instalação do nó):** [Linux: Adicione interfaces de tronco ou acesso a um nó](#)

Ver 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).

Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, [Recuperar e manter](#) consulte .

Passos

- 1. Selecione **NODES > grid node > Visão geral**.
- 2. Selecione **Mostrar mais** à direita do título dos endereços IP.

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

DC2-SGA-010-096-106-021 (Storage Node) [✕](#)

OverviewHardwareNetworkStorageObjectsILMTasks

Node information ?

Name:DC2-SGA-010-096-106-021

Type:Storage Node

ID:f0890e03-4c72-401f-ae92-245511a38e51

Connection state:

✓

Connected

Storage used:

Object data7% ?

Object metadata5% ?

Software version:11.6.0 (build 20210915.1941.afce2d9)

IP addresses:10.96.106.21 - eth0 (Grid Network)

Hide additional IP addresses ^

Interface	IP address
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name	Severity ?	Time triggered	Current values
ILM placement unachievable	<div><div>!</div>Major</div>	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

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.

201

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

Alterar a 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 controle entre nós de grade. Esta definição não afeta a encriptação de dados.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 **CONFIGURATION > System > Grid options**.
2. Na seção Opções de rede, altere criptografia de transferência de rede para **AES128-SHA** ou **AES256-SHA** (padrão).

Network Options



3. Selecione **Guardar**.

Gerenciar políticas de classificação de tráfego

Gerenciar 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 correspondentes

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.

Limitação de tráfego

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

Os valores-limite são impostos 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.



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 impacto menor no desempenho adicional no tráfego não limitado.

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.

Use 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 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 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 Largura de banda de 1 GB/seg (8 Gbps)	dólares por mês

Crie políticas de classificação de tráfego

Você cria políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por intervalo, localatário, 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.
- Você criou todos os pontos de extremidade do balanceador de carga que deseja corresponder.
- Você criou quaisquer inquilinos que você deseja combinar.

Passos

1. Selecione **CONFIGURATION > Network > Traffic Classification**.

É apresentada a página políticas de classificação de tráfego.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create
Edit
Remove
Metrics

Name	Description	ID
No policies found.		

2. Selecione **criar**.

É apresentada a caixa de diálogo criar política de classificação de tráfego.

Create Traffic Classification Policy

Policy

Name ⓘ

Description

Matching Rules

Traffic that matches any rule is included in the policy.

+ Create

✎ Edit

✕ Remove

Type	Inverse Match	Match Value
------	---------------	-------------

No matching rules found.

Limits (Optional)

+ Create

✎ Edit

✕ Remove

Type	Value	Units
------	-------	-------

No limits found.

Cancel

Save

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. Selecione **criar** na seção **regras correspondentes**.

A caixa de diálogo criar regra de correspondência é exibida.

Create Matching Rule

Matching Rules

Type ⓘ -- Choose One -- ▾

Match Value ⓘ Choose type before providing match value

Inverse Match ⓘ ☐

Cancel Apply

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. [Configurar pontos de extremidade do balanceador de carga](#) Consulte .
 - 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. Selecione **aplicar**.

A regra é criada e está listada na tabela regras correspondentes.

+ Create
Edit
Remove

Type	Inverse Match	Match Value
Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

+ Create
Edit
Remove

Type	Value	Type	Units
No limits found.			

Cancel
Save

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. Selecione **criar** na seção **limites**.

A caixa de diálogo criar limite é exibida.

Create Limit

Limits (Optional)

Type
-- Choose One --

Aggregate rate limits in use. Per-request rate limits are not available.

Value

Cancel
Apply

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 impacto 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. Selecione **aplicar**.

O limite é criado e é listado na tabela limites.

+ Create
Edit
Remove

Type	Inverse Match	Match Value
<input checked="" type="radio"/> Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

+ Create
Edit
Remove

Type	Value	Units
<input checked="" type="radio"/> Aggregate Bandwidth Out	10000000000	Bytes/Second

Displaying 1 limit.

Cancel Save

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, selecione **Salvar**.

A política é guardada e está listada na tabela políticas de classificação de tráfego.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit Remove Metrics		
Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

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. [Exibir métricas de tráfego de rede](#)Consulte .

Edite 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

Passos

1. Selecione **CONFIGURATION > Network > Traffic Classification**.

A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create

Edit

Remove

Metrics

	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

2. Selecione o botão de opção à esquerda da política que pretende editar.
3. Selecione **Editar**.

A caixa de diálogo Editar diretiva de classificação de tráfego é exibida.

Edit Traffic Classification Policy "Fabric Pools"

Policy

Name

Fabric Pools

Description (optional)

Monitor Fabric Pools

Matching Rules

Traffic that matches any rule is included in the policy.

+ Create Edit Remove

Type	Inverse Match	Match Value
<input checked="" type="checkbox"/> CIDR		10.10.152.0/24

Displaying 1 matching rule.

Limits (Optional)

+ Create Edit Remove

Type	Value	Units
------	-------	-------

No limits found.

Cancel

Save

4. Crie, edite ou remova regras e limites correspondentes conforme necessário.
 - a. Para criar uma regra ou limite correspondente, selecione **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, selecione **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 selecione **Remover**. Em seguida, selecione **OK** para confirmar que deseja remover a regra ou limite.
5. Quando terminar de criar ou editar uma regra ou um limite, selecione **aplicar**.
6. Quando terminar de editar a política, selecione **Guardar**.

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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

Passos

1. Selecione **CONFIGURATION > Network > Traffic Classification**.

A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create ✎ Edit ✕ Remove 📊 Metrics			
	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdbc894b
Displaying 2 traffic classification policies.			

2. Selecione o botão de opção à esquerda da política que pretende eliminar.
3. Selecione **Remover**.

É apresentada uma caixa de diálogo Aviso.



4. Selecione **OK** para confirmar que deseja excluir a política.

A política é eliminada.

Exibir 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root ou a permissão Contas do Locatário.

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 **CONFIGURATION > Network > Traffic Classification**.

A página políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create

Edit

Remove

Metrics

	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.



Os botões **criar**, **Editar** e **Remover** serão desativados se você tiver a permissão Contas do locatário, mas não tiver a permissão de acesso root.

- 2. Selecione o botão de opção à esquerda da política para a qual deseja exibir as métricas.
- 3. Selecione **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.

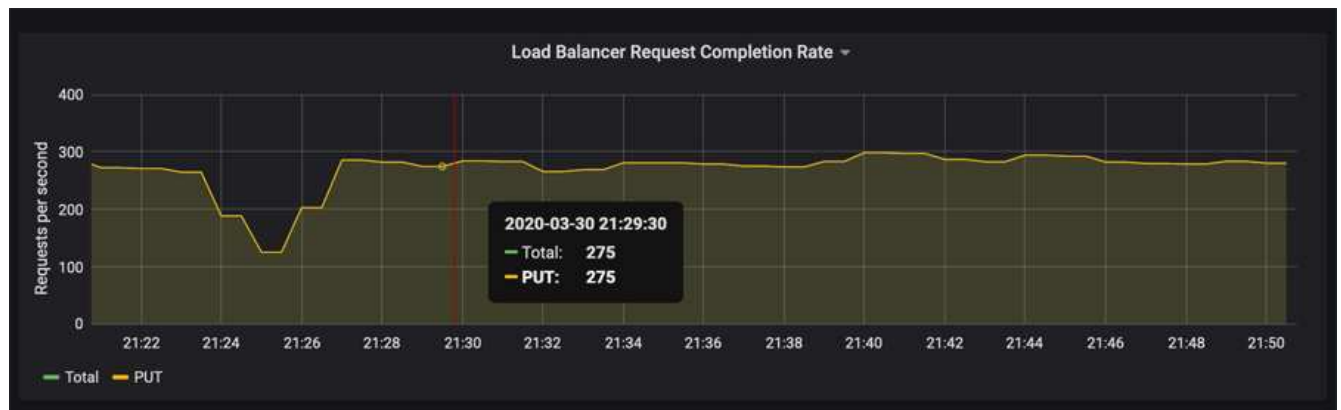
Você pode selecionar outras políticas para exibir usando a lista suspensa **policy**.



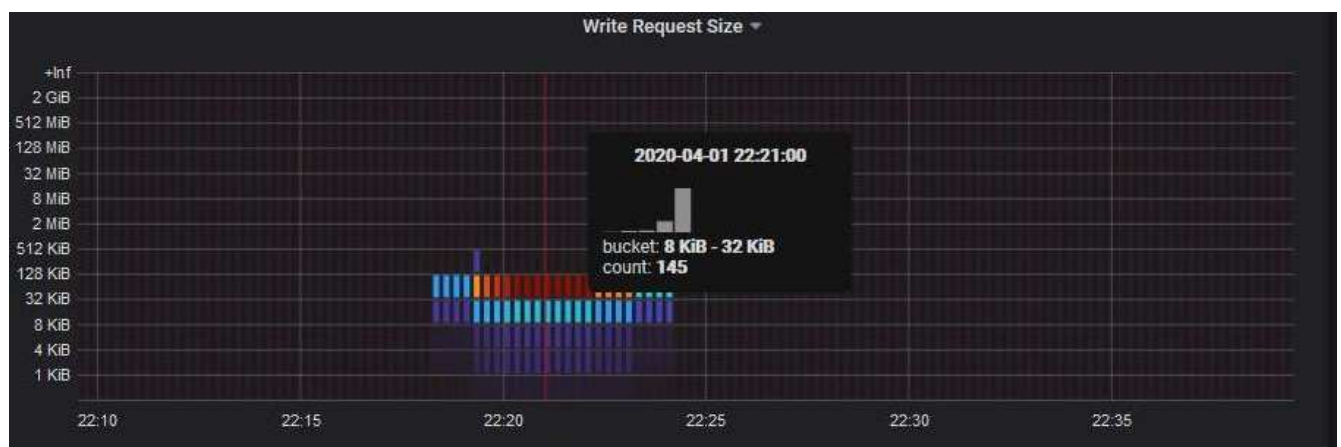
Os gráficos a seguir estão incluídos na página da Web.

- **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, acesse 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

[Monitorar e solucionar problemas](#)

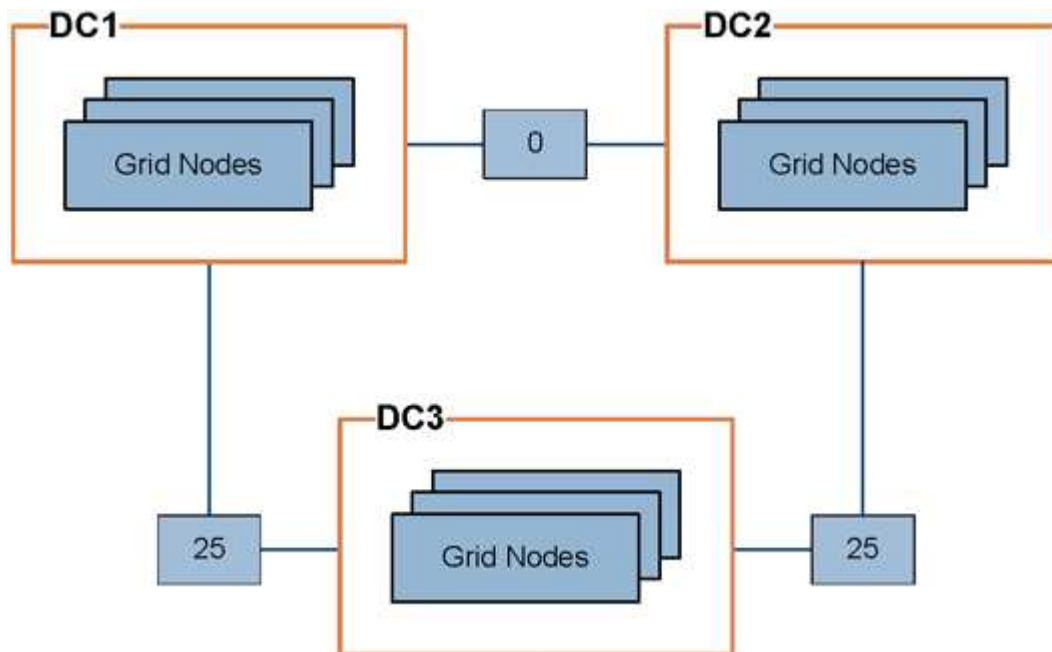
Gerenciar custos de link

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 (Connection Load Balancer) obsoleto nos nós do Gateway para direcionar as conexões do cliente. [Como funciona o balanceamento de carga - serviço CLB](#) Consulte .

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 DC2 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 conectados por uma LAN.

Atualizar custos de link

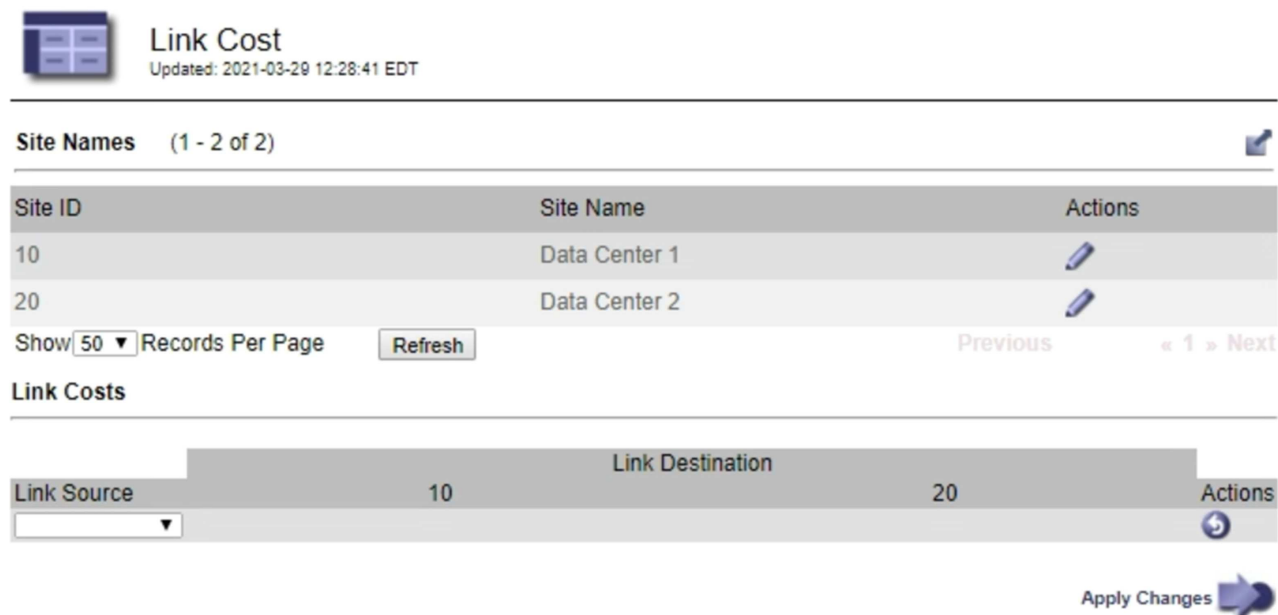
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de Configuração de Página de topologia de Grade.

Passos

1. Selecione **CONFIGURATION > Network > Link Cost**.



Link Cost
Updated: 2021-03-29 12:28:41 EDT

Site Names (1 - 2 of 2)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	

Show 50 Records Per Page Previous « 1 » Next

Link Costs

Link Source	Link Destination	Actions
<input type="text" value="10"/>	20	

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, selecione **Revert**.

3. Selecione **aplicar alterações**.

Use o AutoSupport

O que é 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
- 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 do Gerenciador de Grade. A mensagem inclui um link para a página de configuração do AutoSupport.

The AutoSupport feature is disabled. You should enable AutoSupport to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.



Se você fechar a mensagem, ela não aparecerá novamente até que o cache do navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

O que é o Digital Advisor?

O consultor digital é baseado na nuvem e aproveita as análises preditivas e o conhecimento da comunidade fornecidos pela 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 consultor digital no site de suporte da NetApp.

["Documentação do Digital Advisor"](#)

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"](#)

Configurar o AutoSupport

Você pode ativar o recurso AutoSupport e as opções individuais do AutoSupport quando instalar o StorageGRID pela primeira vez, ou ativá-los posteriormente.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root ou outra configuração de grade.
- Se você usar o protocolo HTTPS ou HTTP para enviar mensagens AutoSupport, você forneceu 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, [Configurado um servidor proxy Admin](#)tem o .

- Se utilizar SMTP como protocolo para mensagens AutoSupport, configurou um servidor de correio SMTP. A mesma configuração do servidor de e-mail é usada para notificações de e-mail de alarme (sistema legado).

Especifique o protocolo para mensagens AutoSupport

Você pode usar qualquer um dos seguintes protocolos para enviar mensagens AutoSupport:

- **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 (**SUPPORT > Alarmes (legacy) > 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 **SUPPORT > Tools > AutoSupport**.

A página AutoSupport é exibida e a guia **Configurações** é selecionada.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Protocol Details

Protocol ?

☒ HTTPS
☐ HTTP
☐ SMTP

NetApp Support Certificate Validation ?

Use NetApp support certificate ▼

AutoSupport Details

Enable Weekly AutoSupport ?

☒

Enable Event-Triggered AutoSupport ?

☒

Enable AutoSupport on Demand ?

☐

Software Updates

Check for software updates ?

☒

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

☐

Save

Send User-Triggered AutoSupport

- Selecione o protocolo que pretende utilizar para enviar mensagens AutoSupport.
- Se você selecionou **HTTPS**, selecione se deseja usar um certificado TLS para proteger a conexão com o servidor de suporte da 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 verifique o certificado**: Selecione esta opção somente quando tiver um bom motivo para não usar a validação do certificado, como quando houver um problema temporário com um certificado.
- Selecione **Guardar**.

Todas as mensagens semanais, acionadas pelo utilizador e acionadas por eventos são enviadas utilizando o protocolo selecionado.

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.

Para determinar quando a mensagem AutoSupport semanal será enviada, vá para a guia **AutoSupport > resultados**. Na seção **Weekly AutoSupport**, observe o valor para **Next Scheduled Time**.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Weekly AutoSupport

Next Scheduled Time ⓘ 2021-09-14 21:10:00 MDT

Most Recent Result ⓘ Idle (NetApp Support)

Last Successful Time ⓘ N/A (NetApp Support)

Pode desativar o envio automático de mensagens AutoSupport semanais a qualquer momento.

Passos

1. Selecione **SUPPORT > Tools > AutoSupport**.
2. Desmarque a caixa de seleção **Ativar AutoSupport semanal**.
3. Selecione **Guardar**.

Desative mensagens AutoSupport acionadas por evento

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.

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 **CONFIGURATION > System > Display OPTIONS**. Em seguida, selecione **notificação suprimir tudo**.)

Passos

1. Selecione **SUPPORT > Tools > AutoSupport**.
2. Desmarque a caixa de seleção **Ativar AutoSupport acionado por evento**.
3. Selecione **Guardar**.

Habilite o AutoSupport sob demanda

O AutoSupport On Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente.

Por padrão, o AutoSupport On Demand está desativado. A ativação deste recurso permite que o suporte técnico solicite que o sistema StorageGRID envie mensagens 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 **SUPPORT > Tools > AutoSupport**.
2. Selecione **HTTPS** para o protocolo.
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 verificações para atualizações de software

Por predefinição, o StorageGRID contacta o NetApp para determinar se estão disponíveis atualizações de software para o seu sistema. Se estiver disponível um hotfix do StorageGRID ou uma nova versão, a nova versão será exibida na página Atualização do StorageGRID.

Conforme necessário, você pode opcionalmente desativar a verificação de atualizações de software. Por exemplo, se o sistema não tiver acesso à WAN, desative a verificação para evitar erros de download.

Passos

1. Selecione **SUPPORT > Tools > AutoSupport**.
2. Desmarque a caixa de seleção **verificar atualizações de software**.
3. Selecione **Guardar**.

Adicione 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.

Para verificar ou alterar o protocolo usado para enviar mensagens AutoSupport, consulte as instruções para [Especifique o protocolo para mensagens AutoSupport](#).




Não é possível usar o protocolo SMTP para enviar mensagens AutoSupport para um destino adicional.


Passos


1. Selecione **SUPPORT > Tools > AutoSupport**.
2. Selecione **Ativar destino AutoSupport adicional**.


São apresentados os campos de destino AutoSupport adicional.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination  ☒

Hostname 

Port 

Certificate Validation 

You are not using a TLS certificate to secure the connection to the additional AutoSupport destination.

Save

Send User-Triggered AutoSupport


- Introduza o nome de anfitrião do servidor ou o endereço IP de um servidor de destino AutoSupport adicional.





Pode introduzir apenas um destino adicional.


- 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).
- 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.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination  ☒

Hostname 

Port 

Certificate Validation 

CA Bundle 

```
-----BEGIN CERTIFICATE-----
abcdefghijklmnopqrstuvwxyz
123456/7890ABCDEFabcdefghijklmnopqrstuvwxyz
-----END CERTIFICATE-----
```

Browse

- 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.

Acione 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root ou outra configuração de grade.

Passos

1. Selecione **SUPPORT > Tools > 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.

Solucionar 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. Pode verificar o estado das mensagens do AutoSupport selecionando **SUPPORT > Tools > AutoSupport > results**.



As mensagens AutoSupport acionadas por evento são suprimidas quando você suprime as notificações de e-mail em todo o sistema. (Selecione **CONFIGURATION > System > Display OPTIONS**. Em seguida, selecione **notificação suprimir tudo**.)

Quando a mensagem AutoSupport não é enviada, "Falha" aparece na guia **resultados** da página **AutoSupport**.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Weekly AutoSupport

Next Scheduled Time ? 2020-12-11 23:30:00 EST

Most Recent Result ? Idle (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

Event-Triggered AutoSupport

Most Recent Result ? N/A (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

User-Triggered AutoSupport

Most Recent Result ? Failed (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

AutoSupport On Demand

AutoSupport On Demand messages are only sent to NetApp Support.

Most Recent Result ? N/A (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

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 (**SUPPORT > Alarmes (legacy) > > 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 eletrônico no [monitorar e solucionar problemas de instruções](#).

Corrija uma falha de mensagem do 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.`

Envie mensagens AutoSupport do e-Series 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 conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão Administrador do dispositivo de armazenamento ou a permissão de acesso root.



Você deve ter o firmware SANtricity 8,70 (11,7) ou superior para acessar o Gerenciador de sistema 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 quiser configurar o servidor proxy Admin no Grid Manager, [Configure as configurações do proxy Admin](#) consulte .

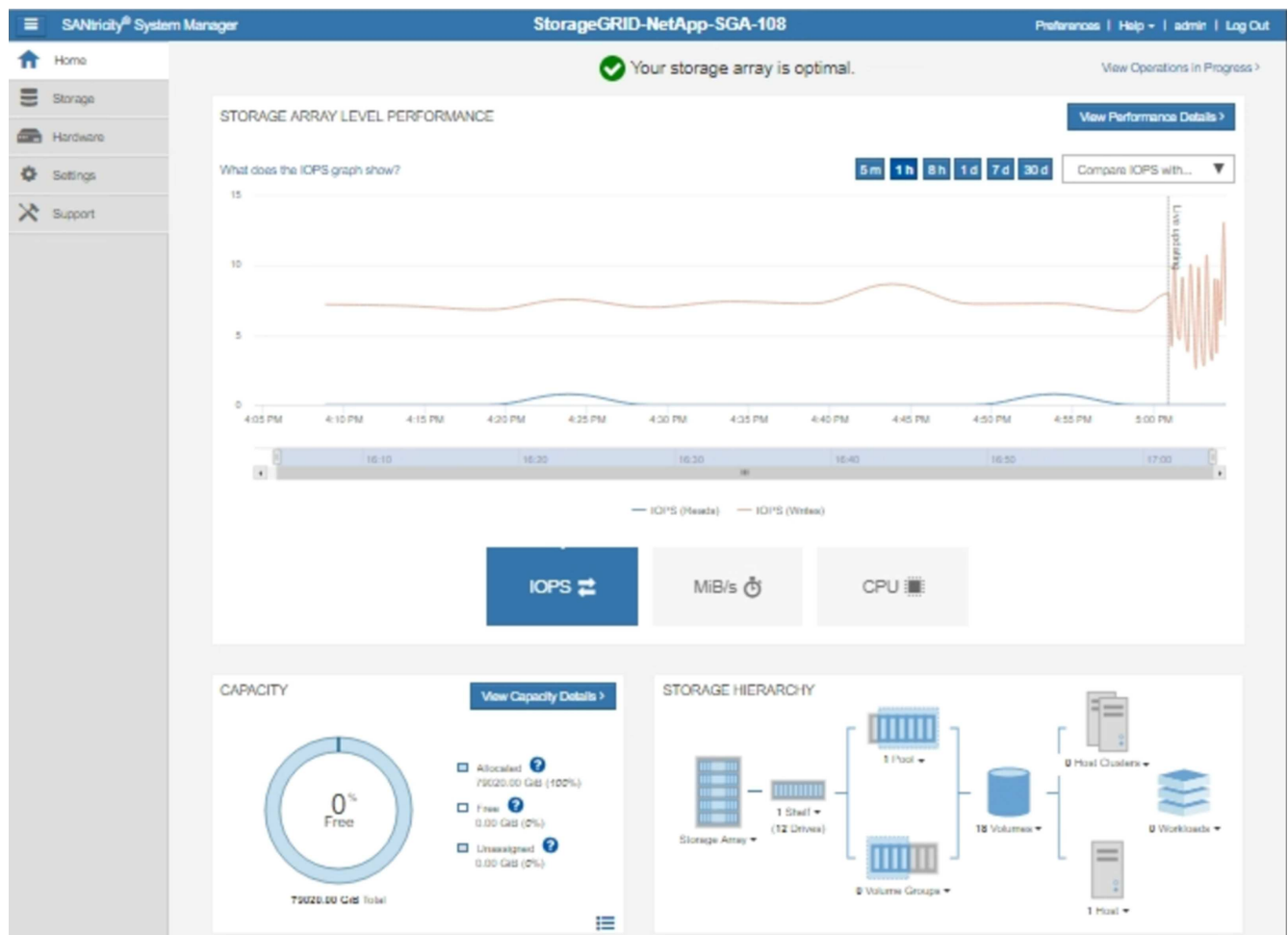


Este procedimento destina-se apenas à configuração de um servidor proxy StorageGRID para mensagens AutoSupport e-Series. Para obter detalhes adicionais sobre a configuração do e-Series AutoSupport, consulte "[Documentação do NetApp e-Series e do SANtricity](#)".

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 **SUPPORT > SUPPORT Center > AutoSupport**.

É apresentada a página operations (operações de AutoSupport).

Technical Support

Chassis serial number: 031517000693

 [NetApp My Support](#)

US/Canada 888.463.8277


[Other Contacts](#)

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: **Enabled** 

[Enable/Disable AutoSupport Features](#)

AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)

AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)

Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)

The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)

Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)

Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Seleccione **Configurar método de entrega AutoSupport**.

A página Configurar método de entrega AutoSupport é exibida.

Configure AutoSupport Delivery Method [X]

Select AutoSupport dispatch delivery method...

☒ **HTTPS**

☐ HTTP

☐ Email

HTTPS delivery settings [Show destination address](#)

Connect to support team...

☐ Directly ?

☒ **via Proxy server** ?

Host address ?

tunnel-host

Port number ?

10225

☐ My proxy server requires authentication

☐ via Proxy auto-configuration script (PAC) ?

Save **Test Configuration** Cancel

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 conectar 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."

Gerenciar nós de storage

Sobre o gerenciamento de nós de storage

Os nós de storage fornecem capacidade e serviços de storage em disco. O gerenciamento de nós de storage implica o seguinte:

- Gerenciamento de opções de armazenamento
- Compreender quais são as marcas d'água do volume de storage e como você pode usar substituições de marca d'água para controlar quando os nós de armazenamento se tornam somente leitura
- Monitoramento e gerenciamento do espaço usado para metadados de objetos
- Configuração de configurações globais para objetos armazenados
- Aplicando as configurações do nó de armazenamento
- 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 topologia de Grade (**SUPPORT > Grid topology**).

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 conectam, 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.

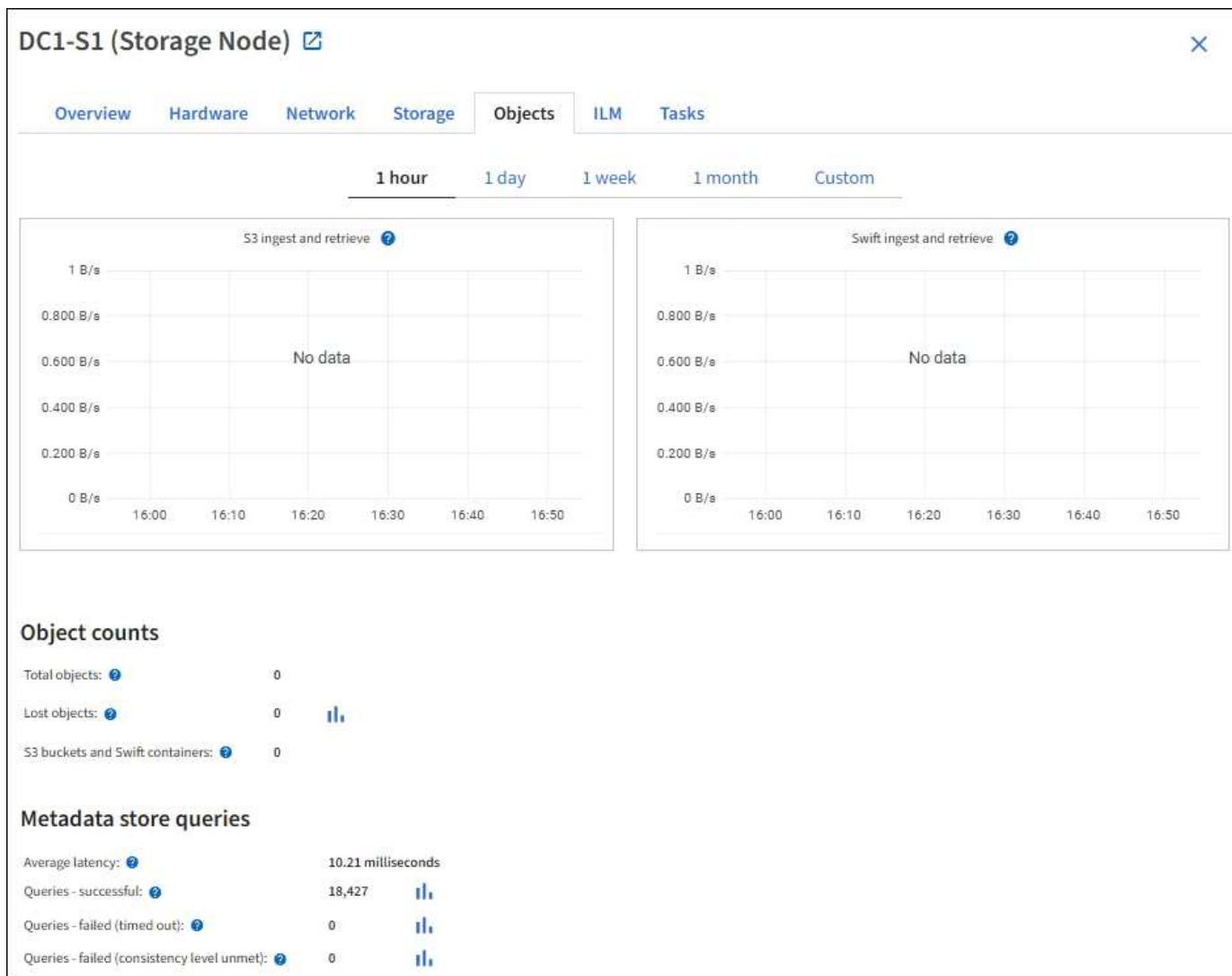
O que é o serviço DDS?

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. [Execute 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. [Execute 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 em **NODES > Storage Node > ILM**.

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	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	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.

[Gerenciar o storage de metadados de objetos](#)

Gerenciar opções de armazenamento


As opções de armazenamento incluem as definições de segmentação de objetos, os valores atuais para marcas d'água de volume de armazenamento e a definição espaço reservado de metadados. 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 .

Storage Options

Overview

Configuration



Storage Options Overview

Updated: 2021-11-23 11:01:41 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

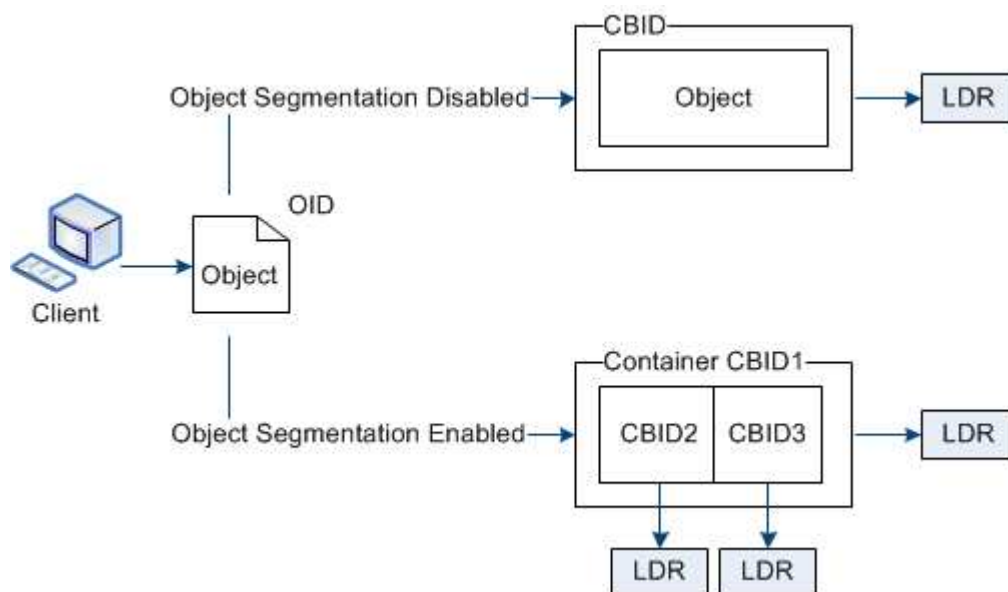
Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

O que é 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 contêiner de segmento que lista as informações do cabeçalho de todos os segmentos como conteúdo.



Ao recuperar um contêiner 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 dentro do conjunto de armazenamento especificado na regra ILM.

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:

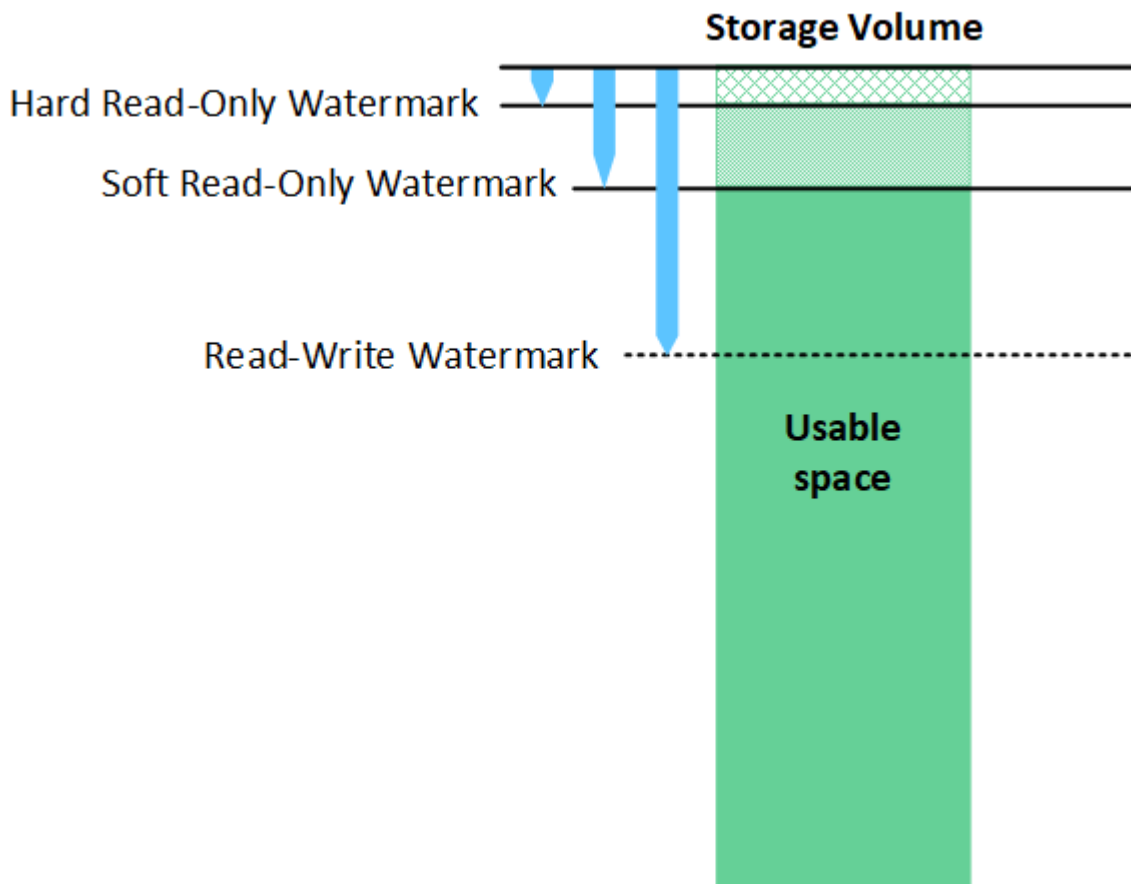
segmento de container e segmento 1 e segmento 2 são três objetos armazenados

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.

O que são marcas d'água de volume de armazenamento?

O StorageGRID usa três marcas d'água de volume de storage para garantir que os nós de storage sejam transferidos com segurança para um estado somente leitura antes que eles sejam executados com muito pouco espaço e para permitir que os nós de storage que foram transferidos para um estado somente leitura sejam novamente lidos.





As marcas d'água do volume de armazenamento aplicam-se apenas ao espaço utilizado para dados de objetos replicados e codificados por apagamento. Para saber mais sobre o espaço reservado para metadados de objetos no volume 0, vá para [Gerenciar o storage de metadados de objetos](#).

O que é o Soft Read-Only Watermark?

O **Storage volume Soft Read-Only Watermark** é a primeira marca d'água a indicar que o espaço utilizável de um nó de armazenamento para dados de objetos está se tornando cheio.

Se cada volume em um nó de armazenamento tiver menos espaço livre do que o Watermark Soft Read-Only desse volume, o nó de armazenamento muda para *read-only mode*. O modo somente leitura significa que o nó de storage anuncia serviços somente leitura para o resto do sistema StorageGRID, mas atende a todas as solicitações de gravação pendentes.

Por exemplo, suponha que cada volume em um nó de armazenamento tenha uma marca de água somente leitura suave de 10 GB. Assim que cada volume tiver menos de 10 GB de espaço livre, o nó de armazenamento passa para o modo somente leitura suave.

O que é a marca d'água Hard Read-Only?

O **Storage volume Hard Read-Only Watermark** é a próxima marca d'água para indicar que o espaço utilizável de um nó para dados de objeto está se tornando cheio.

Se o espaço livre em um volume for menor do que a marca de água Hard Read-Only desse volume, as gravações no volume falharão. As gravações em outros volumes podem continuar, no entanto, até que o espaço livre nesses volumes seja menor do que suas marcas de água somente leitura dura.

Por exemplo, suponha que cada volume em um nó de armazenamento tenha uma marca d'água somente leitura de 5 GB. Assim que cada volume tiver menos de 5 GB de espaço livre, o nó de armazenamento não aceita mais nenhuma solicitação de gravação.

A marca d'água Hard Read-Only é sempre inferior à marca d'água Soft Read-Only.

O que é a marca d'água Read-Write?

O **marca d'água de leitura e gravação de volume de armazenamento** aplica-se apenas a nós de armazenamento que tenham feito a transição para o modo somente leitura. Ele determina quando o nó pode se tornar leitura-gravação novamente. Quando o espaço livre em qualquer volume de armazenamento em um nó de armazenamento é maior do que a marca de água de leitura e gravação desse volume, o nó automaticamente faz a transição de volta para o estado de leitura e gravação.

Por exemplo, suponha que o nó de armazenamento tenha sido transferido para o modo somente leitura. Suponha também que cada volume tenha uma marca d'água de leitura-escrita de 30 GB. Assim que o espaço livre para qualquer volume aumentar para 30 GB, o nó torna-se leitura-gravação novamente.

A marca d'água de leitura-escrita é sempre maior do que a marca d'água Soft Read-Only e a marca d'água Hard Read-Only.

Ver marcas de água do volume de armazenamento

Você pode visualizar as configurações atuais da marca d'água e os valores otimizados pelo sistema. Se não estiverem a ser utilizadas marcas de água otimizadas, pode determinar se pode ou deve ajustar as definições.

O que você vai precisar

- Concluiu a atualização para o StorageGRID 11,6.
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem a permissão de acesso root.

Ver as definições atuais da marca d'água

Você pode exibir as configurações atuais de marca d'água de armazenamento no Gerenciador de Grade.


Passos

1. Selecione **CONFIGURATION > System > Storage options**.
2. Na seção marcas d'água de armazenamento, observe as configurações para as três substituições de marca d'água de volume de armazenamento.

Storage Options

Overview

Configuration



Storage Options Overview

Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

- Se as substituições da marca d'água forem **0**, todas as três marcas d'água são otimizadas para cada volume de armazenamento em cada nó de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Esta é a configuração padrão e recomendada. Você não deve atualizar esses valores. Conforme necessário, você pode opcionalmente [Ver marcas de água de armazenamento otimizadas](#).

- Se as substituições da marca d'água forem valores não 0, marcas d'água personalizadas (não otimizadas) estão sendo usadas. Não é recomendável usar configurações personalizadas de marca d'água. Use as instruções para [Solução de problemas de baixa substituição de marca d'água somente leitura alertas](#) determinar se você pode ou deve ajustar as configurações.

Ver marcas de água de armazenamento otimizadas

O StorageGRID usa duas métricas Prometheus para mostrar os valores otimizados que calculou para a marca d'água **volume de armazenamento Soft Read-Only**. Você pode visualizar os valores otimizados mínimo e

máximo para cada nó de storage em sua grade.

1. Selecione **SUPPORT > Tools > Metrics**.
2. Na seção Prometheus, selecione o link para acessar a interface do usuário Prometheus.
3. Para ver a marca d'água mínima de leitura suave recomendada, insira a seguinte métrica Prometheus e selecione **execute**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

A última coluna mostra o valor mínimo otimizado do Soft Read-Only Watermark para todos os volumes de armazenamento em cada nó de armazenamento. Se esse valor for maior que a configuração personalizada para o **Storage volume Soft Read-Only Watermark**, o alerta **Low read-only Watermark** (Sobreposição de marca d'água somente leitura baixa) será acionado para o Storage Node.

4. Para ver a marca d'água somente leitura suave recomendada, insira a seguinte métrica Prometheus e selecione **execute**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

A última coluna mostra o valor máximo otimizado do Soft Read-Only Watermark para todos os volumes de armazenamento em cada nó de armazenamento.

Gerenciar o 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.

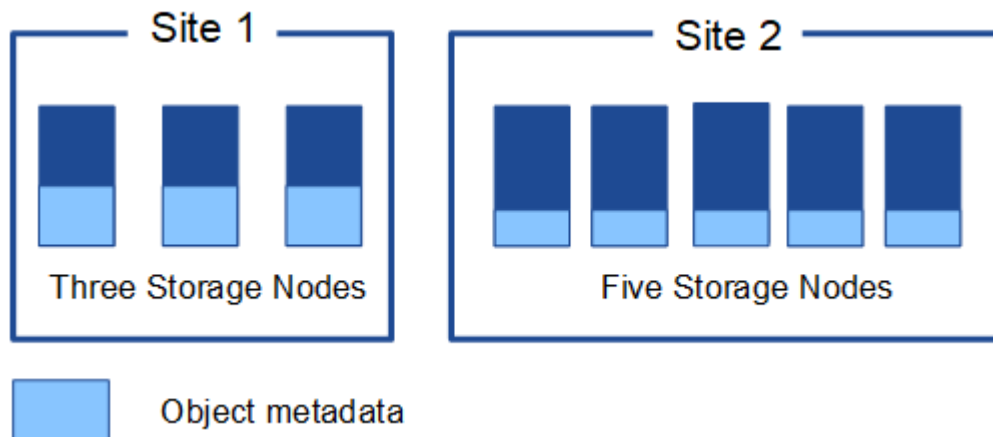
Para um objeto no StorageGRID, os metadados de objeto incluem os seguintes tipos de informações:

- 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?

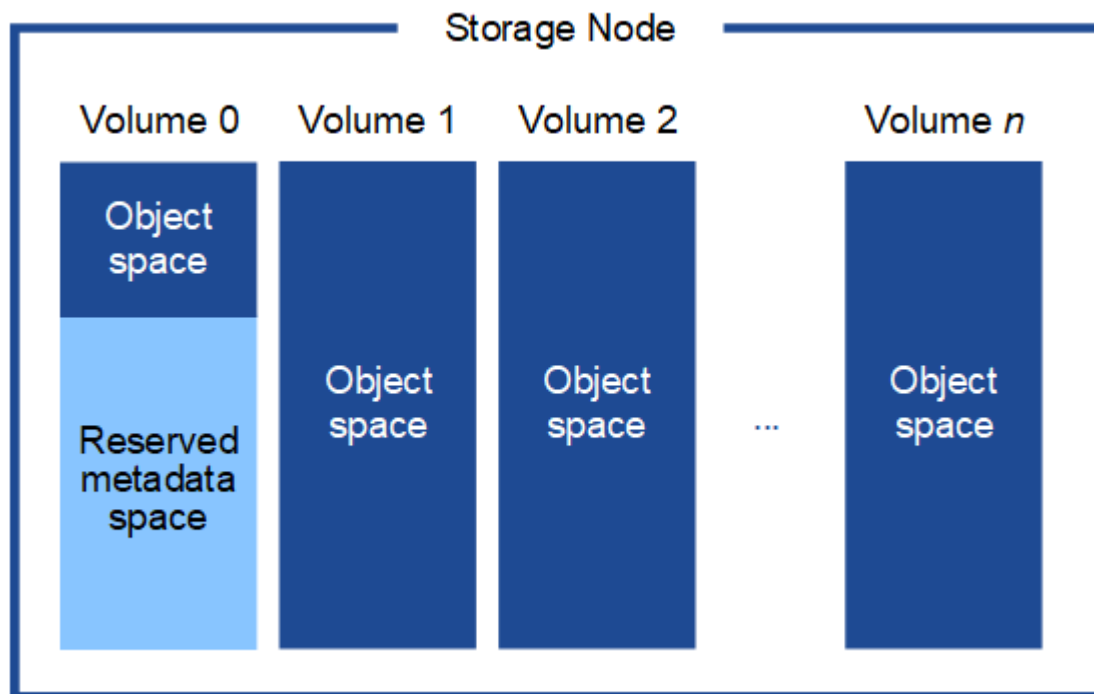
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados de objetos contra perda, o StorageGRID armazena três cópias dos metadados de todos os objetos no sistema em cada local. As 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 11,6 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 11,6
11,5/11,6	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)
	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 **CONFIGURATION > System > Storage options**.
2. Na tabela Storage Watermarks (marcas de água de armazenamento), localize **Metadata Reserved Space** (espaço reservado de metadados).



Storage Options Overview

Updated: 2021-12-10 13:53:01 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	8,000 GB

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 11,6 na qual cada nó de armazenamento tem 128 GB ou mais de RAM.

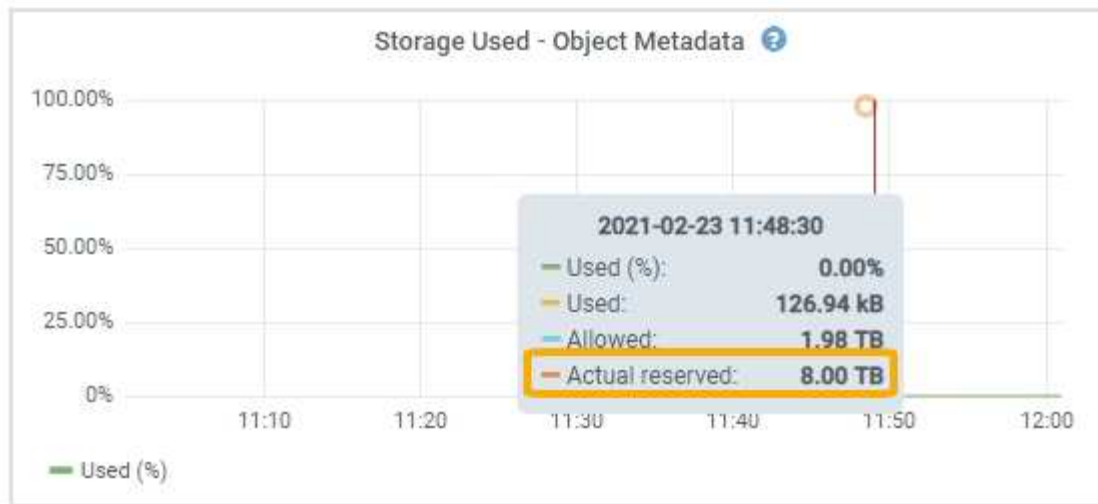
Espaço reservado real para metadados

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
500 GB ou mais	O menor desses valores: <ul style="list-style-type: none">• Volume 0• 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 11,6. 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.

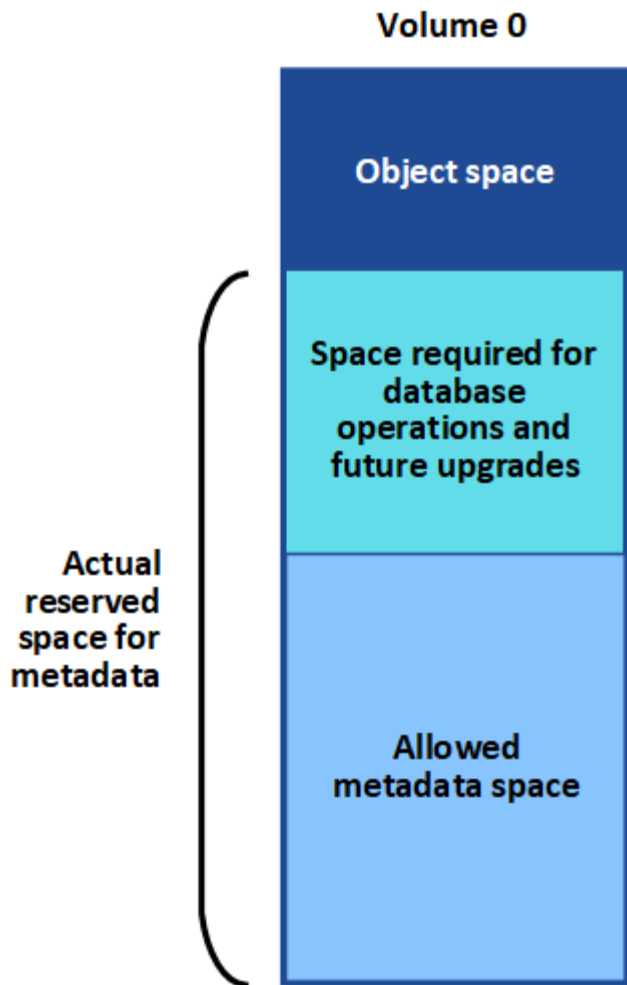
Exemplo de espaço reservado real de metadados

Suponha que você instale um novo sistema StorageGRID usando a versão 11,6. 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 11,6 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.



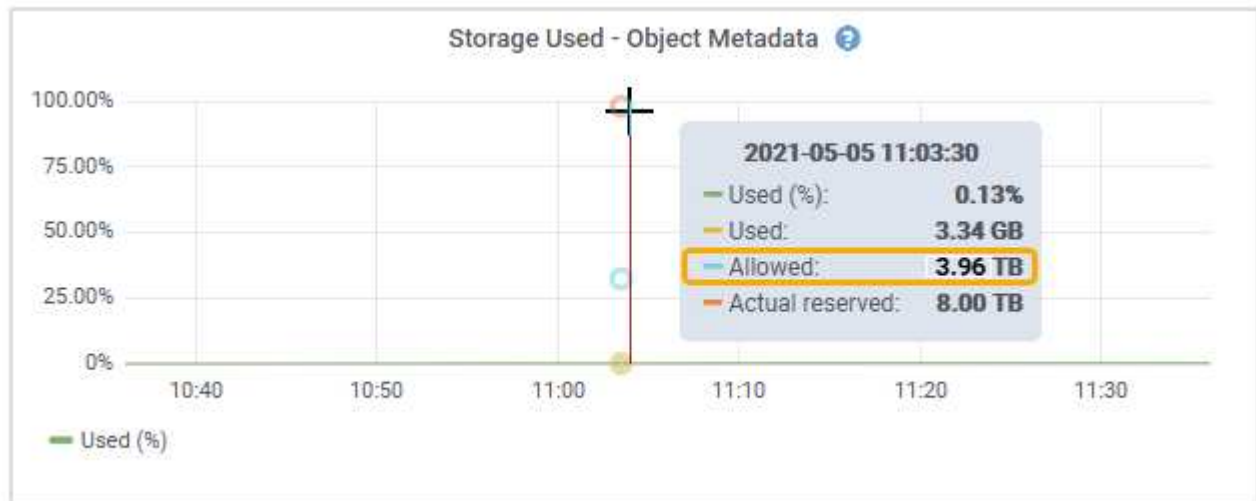
A tabela a seguir mostra como o StorageGRID calcula o espaço de metadados permitido* para diferentes nós de armazenamento, com base na quantidade de memória do nó e no espaço reservado real para metadados.

	Quantidade de memória no nó de armazenamento		
	≪ 128 GB	≫ 128 GB	Espaço reservado real para metadados
≪ 4 TB	60% do espaço reservado real para metadados, até um máximo de 1,32 TB	60% do espaço reservado real para metadados, até um máximo de 1,98 TB	≫ 4 TB

Para exibir o espaço de metadados permitido para um nó de storage:

1. No Gerenciador de Grade, selecione **NÓS**.
2. Selecione o nó de armazenamento.
3. Selecione a guia **armazenamento**.
4. 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 3,96 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 11,6. 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 11,6 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 3 TB, com base no cálculo mostrado no [tabela para espaço permitido para metadados](#): (espaço reservado real para metadados - 1 TB) x 60%, até um máximo de 3,96 TB.

Como os nós de storage de diferentes tamanhos afetam a capacidade do objeto

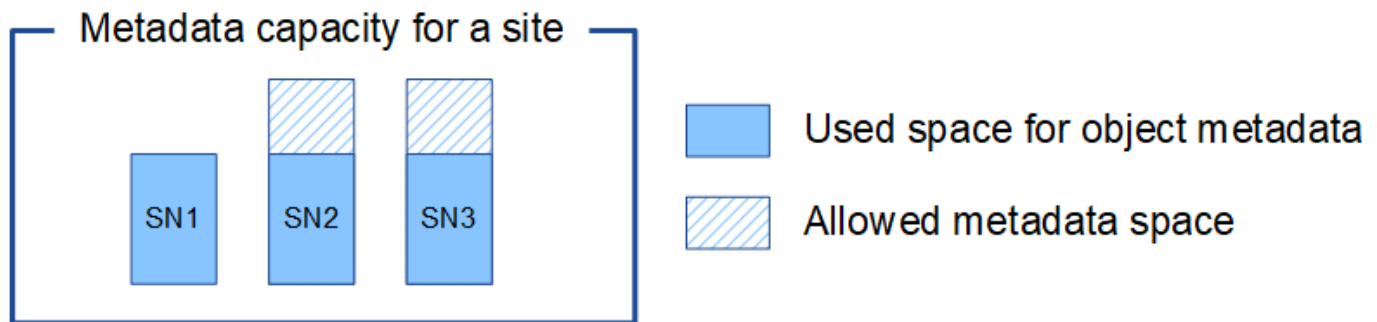
Como descrito acima, o StorageGRID distribui uniformemente os metadados de objetos nos nós de storage em cada local. Por esse motivo, se um site contiver nós de storage de tamanhos diferentes, o menor nó do local determinará a capacidade de metadados do local.

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, vá para [Monitorar e solucionar problemas](#).
- Para aumentar a capacidade dos metadados de objetos do seu sistema, adicione novos nós de storage. Vá para [Expanda sua grade](#).

Configure as configurações globais para objetos armazenados

Configurar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 compactados, 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 **CONFIGURATION > System > Grid options**.
2. Na seção **Opções de objetos armazenados**, marque a caixa de seleção **Compress Stored Objects**.

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing  ☒ SHA-1 ☐ SHA-256

3. Selecione **Guardar**.

Configurar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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-ingерidos 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 **CONFIGURATION > System > Grid options**.
2. Na seção Opções de objetos armazenados, altere criptografia de objetos armazenados para **nenhum** (padrão), **AES-128** ou **AES-256**.

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing  ☒ SHA-1 ☐ SHA-256

3. Selecione **Guardar**.

Configurar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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 **CONFIGURATION > System > Grid options**.
2. Na seção Opções de objetos armazenados, altere o hash de objetos armazenados para **SHA-1** (padrão) ou **SHA-256**.

Stored Object Options

Compress Stored Objects ? ☐

Stored Object Encryption ? ☒ None ☐ AES-128 ☐ AES-256

Stored Object Hashing ? ☒ SHA-1 ☐ SHA-256

3. Selecione **Guardar**.

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	<p>O estado atual do protocolo HTTP para S3, Swift e outro tráfego StorageGRID interno:</p> <ul style="list-style-type: none"> • 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. • Online: A operação continua normalmente
Auto-Iniciar HTTP	HTAS	<ul style="list-style-type: none"> • 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. • 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	<p>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.</p> <p>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.</p> <p>O atributo pode ter um dos seguintes valores:</p> <ul style="list-style-type: none"> • Offline: Quando o estado desejado é Offline, o serviço LDR coloca o componente LDR > Storage offline. • 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. • 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). Use somente depois que a verificação existência do objeto for concluída. Os dados de objeto replicado em falta são restaurados automaticamente pelo sistema StorageGRID.

Nome do atributo	Código	Descrição
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	<p>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.</p> <p>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.</p>

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.
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.

Nome do atributo	Código	Descrição
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. Use somente depois que a verificação existência do objeto for concluída.

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	<p>Selecione para desativar a replicação de entrada como parte de um procedimento de manutenção ou teste. Deixe desmarcado durante o funcionamento normal.</p> <p>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.</p>
Desativar replicação efetuada	DSOR	<p>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.</p> <p>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.</p>

Informações relacionadas

[Monitorar e solucionar problemas](#)

Gerencie 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.

Adicione 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 [Expandindo um sistema StorageGRID](#).

Adicione compartimentos 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 [Expandindo um sistema StorageGRID](#).

Adicionar 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 [Expandindo um sistema StorageGRID](#).

Gerenciar nós de administração

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 conectando a um nó Admin. Você pode se conectar 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. [Use a API de gerenciamento de grade](#) Consulte .

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 conectividade 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.

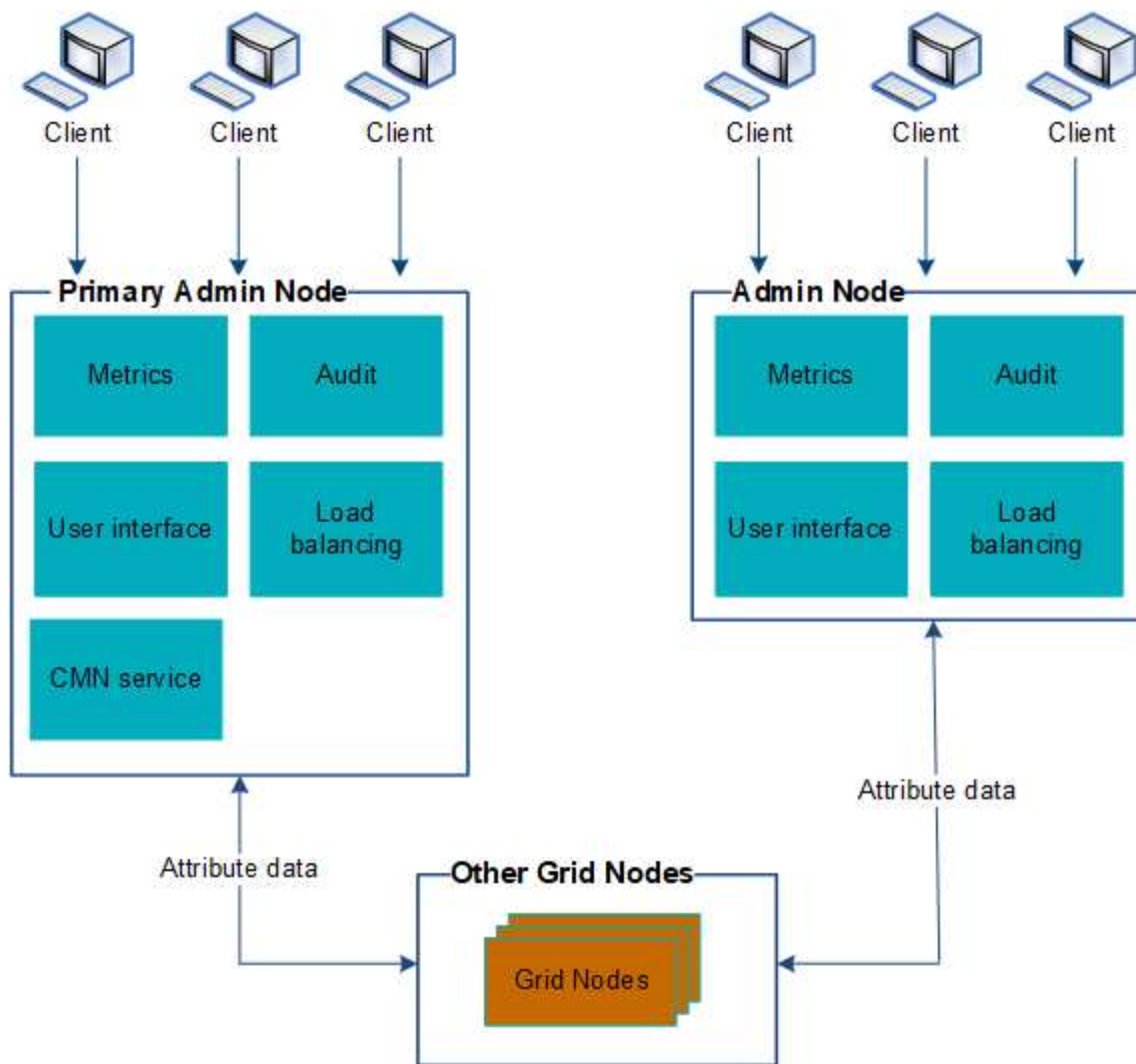
O que é o serviço Prometheus

O serviço Prometheus coleta métricas de séries temporais dos serviços em todos os nós.

Use 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 reconectar 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. [Gerenciar grupos de alta disponibilidade](#) Consulte .



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.


Identifique 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **site > Admin Node** e, em seguida,  selecione 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.

Selecione 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

Sobre esta tarefa

A página **CONFIGURATION > System > Display OPTIONS** mostra qual Admin Node está atualmente selecionado 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 detectado 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 detectar 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 detectar 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 conectividade.

Passos

1. Selecione **CONFIGURATION > System > Display OPTIONS**.
2. No menu Opções de exibição, selecione **Opções**.
3. Selecione o nó Admin que deseja definir como o remetente preferido na lista suspensa.



Display Options

Updated: 2017-08-30 16:31:10 MDT

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input type="checkbox"/>

Apply Changes

4. Selecione **aplicar alterações**.

O Admin Node é definido como o remetente preferido de notificações.


Exibir status de notificação e filas



O serviço do sistema de gerenciamento de rede (NMS) nos nós de administração 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 **SUPPORT > Tools > Grid topology**. Finalmente, selecione **site > Admin Node > NMS > Interface Engine**.



Overview
Alarms
Reports
Configuration

Main





Overview: NMS (170-176) - Interface Engine
Updated: 2009-03-09 10:12:17 PDT

NMS Interface Engine Status:	Connected	
Connected Services:	15	

E-mail Notification Events

E-mail Notifications Status:	No Errors	
E-mail Notifications Queued:	0	

Database Connection Pool

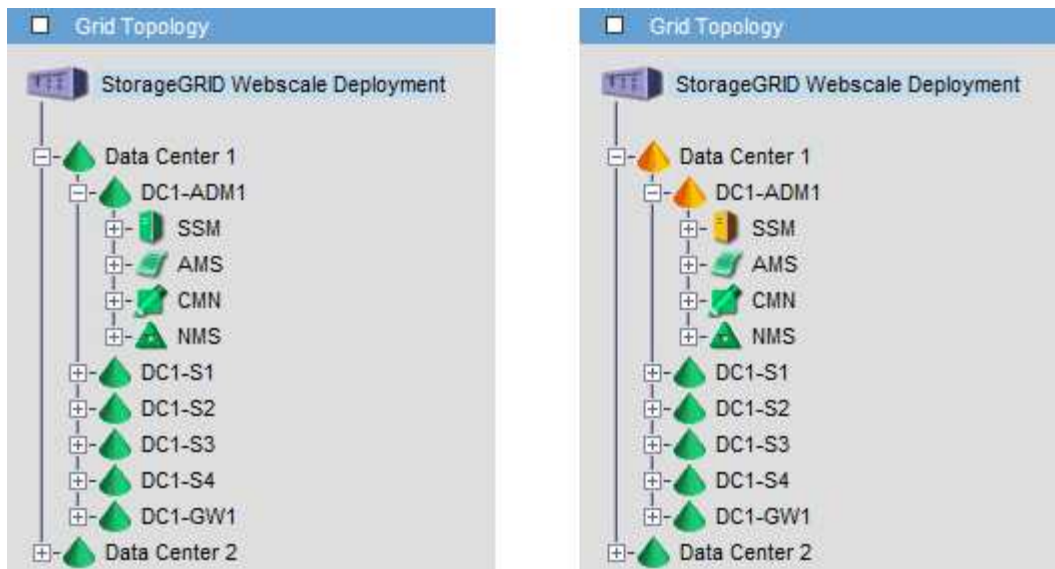
Maximum Supported Capacity:	100	
Remaining Capacity:	95 %	
Active Connections:	5	

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 conectar 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.

Configurar 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, [Rever registros de auditoria](#) consulte .



A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID. Se você tiver a opção de usar CIFS ou NFS, escolha NFS.

Configurar clientes de auditoria para CIFS

O procedimento usado para configurar um cliente de auditoria depende do método de autenticação: Windows Workgroup ou Windows active 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.

Configurar 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

- Tem o `Passwords.txt` ficheiro com a palavra-passe da conta root/admin (disponível no REFERIDO pacote).
- Você tem 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:

- Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- 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.

- Introduza: `set-authentication`
- Quando solicitado para a instalação do Windows Workgroup ou do active Directory, digite: `workgroup`
- 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 smb 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`

Configurar clientes de auditoria para o ativo 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

- Tem o `Passwords.txt` ficheiro com a palavra-passe da conta root/admin (disponível no REFERIDO pacote).
- Você tem o nome de usuário e a senha do CIFS ativo Directory.
- Você tem 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:

- Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- 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 ativo 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.

- Quando solicitado para a instalação do Workgroup ou do ativo Directory: `ad`
- Quando solicitado, insira o nome do domínio AD (nome de domínio curto).
- Quando solicitado, insira o endereço IP do controlador de domínio ou o nome de host DNS.
- Quando solicitado, insira o nome completo do domínio realm.

Use letras maiúsculas.

- 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 ativo 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 ativo 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`

Adicione 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

- Tem o `Passwords.txt` ficheiro com a palavra-passe da conta root/admin (disponível no REFERIDO pacote).
- Você tem 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:

- Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- 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`

Remover 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 tem o `Passwords.txt` arquivo com as senhas da conta root (disponível no REFERIDO pacote).
- Você tem 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`

Altere 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

- [Adicione um usuário ou grupo a um compartilhamento de auditoria CIFS](#)
- [Remover um usuário ou grupo de um compartilhamento de auditoria CIFS](#)

Verificar a 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.

Configurar o cliente de auditoria para NFS

O compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.

O que você vai precisar

- Tem o `Passwords.txt` ficheiro com a palavra-passe root/admin (disponível no REFERIDO pacote).
- Você tem o `Configuration.txt` arquivo (disponível no REFERIDO pacote).
- O cliente de auditoria está 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.

Adicione 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

- Tem o `Passwords.txt` ficheiro com a palavra-passe da conta root/admin (disponível no REFERIDO pacote).
- Você tem o `Configuration.txt` arquivo (disponível no REFERIDO pacote).
- O cliente de auditoria está 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`

Verificar a 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 conectividade (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 conectividade.

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

- Tem o `Passwords.txt` ficheiro com a palavra-passe da conta root/admin (disponível no REFERIDO pacote).
- Você tem 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`

Altere o endereço IP de um cliente de auditoria NFS

Conclua estas etapas se precisar alterar o endereço IP de um cliente de auditoria NFS.

Passos

1. Adicione um novo endereço IP a um compartilhamento de auditoria NFS existente.
2. Remova o endereço IP original.

Informações relacionadas

- [Adicione um cliente de auditoria NFS a um compartilhamento de auditoria](#)
- [Remover um cliente de auditoria NFS do compartilhamento de auditoria](#)

Gerenciar nós de arquivamento

O que é um nó de arquivo

Opcionalmente, cada local de data center do StorageGRID pode ser implantado com um nó de arquivo, que permite que você se conecte a um sistema de armazenamento de arquivamento externo direcionado, como o Gerenciador de armazenamento do Tivoli (TSM).

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.

The screenshot displays the StorageGRID Webconsole interface. On the left, the 'Grid Topology' pane shows a hierarchical view of the deployment. Under 'Data Center 1', several nodes are listed, including 'DC1-ADM1-98-160', 'DC1-G1-98-161', 'DC1-S1-98-162', 'DC1-S2-98-163', 'DC1-S3-98-164', and 'DC1-ARC1-98-165'. The 'DC1-ARC1-98-165' node is highlighted with a blue box, and its sub-nodes ('SSM', 'ARC', 'Replication', 'Store', 'Retrieve', 'Target', 'Events', 'Resources') are also visible. On the right, the 'Overview' tab is selected, showing the 'Main' page for the 'ARC (DC1-ARC1-98-165) - ARC' node. The page includes a status summary table and a 'Node Information' section.

Overview: ARC (DC1-ARC1-98-165) - ARC		
Updated: 2015-09-30 10:29:18 PDT		
ARC State:	Online	
ARC Status:	No Errors	
Tivoli Storage Manager State:	Online	
Tivoli Storage Manager Status:	No Errors	
Store State:	Online	
Store Status:	No Errors	
Retrieve State:	Online	
Retrieve Status:	No Errors	
Inbound Replication Status:	No Errors	
Outbound Replication Status:	No Errors	

Node Information	
Device Type:	Archive Node
Version:	10.2.0
Build:	20150928.2133.a27b3ab
Node ID:	19002524
Site ID:	10

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.

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 de arquivamento (ARC) em nós de arquivamento fornece a interface de gerenciamento que você pode usar para configurar conexões com armazenamento de arquivamento 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.

Archive para a nuvem por meio da API S3

Você pode configurar um nó de arquivo para se conectar 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 [Gerenciando objetos com ILM](#).

Configure as configurações de conexão para a API S3

Se você estiver se conectando 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. [Gerenciar objetos com ILM](#) Consulte .

O que você vai precisar


- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- Você criou um bucket no sistema de storage de arquivamento de destino:
 - O bucket é dedicado a um único nó de arquivo. Ele não pode ser usado por outros nós de arquivamento ou outras aplicações.
 - O balde tem a região apropriada selecionada para a sua localização.
 - O bucket deve ser configurado com o controle de versão suspenso.
- A Segmentação de objetos está ativada e o tamanho máximo do segmento é 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**.

OverviewAlarmsReportsConfiguration

MainAlarms



Configuration: ARC (98-127) - Target

Updated: 2015-09-24 15:48:22 PDT

Target Type:

Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name:

name

Region:

Virginia or Pacific Northwest (us-east-1)

Endpoint:

https://10.10.10.123:8082

☐ Use AWS

Endpoint Authentication:

☐

Access Key:

ABCD123EFG45AB

Secret Access Key:

••••••

Storage Class:

Standard (Default)

Apply Changes

- 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.

- 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. Selecione **aplicar alterações**.

As configurações especificadas são validadas e aplicadas ao seu sistema StorageGRID. Uma vez configurado, o destino não pode ser alterado.

Modifique as configurações de conexão para a API S3

Depois que o nó de arquivo é configurado para se conectar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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**.

Overview


Alarms

Reports

Configuration

Main

Alarms




Configuration: ARC (98-127) - Target

Updated: 2015-09-24 15:48:22 PDT

Target Type: Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name:	name		
Region:	Virginia or Pacific Northwest (us-east-1)		
Endpoint:	https://10.10.10.123:8082	<input type="checkbox"/>	Use AWS
Endpoint Authentication:	<input type="checkbox"/>		
Access Key:	ABCD123EFG45AB		
Secret Access Key:	••••••		
Storage Class:	Standard (Default)		

Apply Changes 

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. Selecione **aplicar alterações**.

Modifique o 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

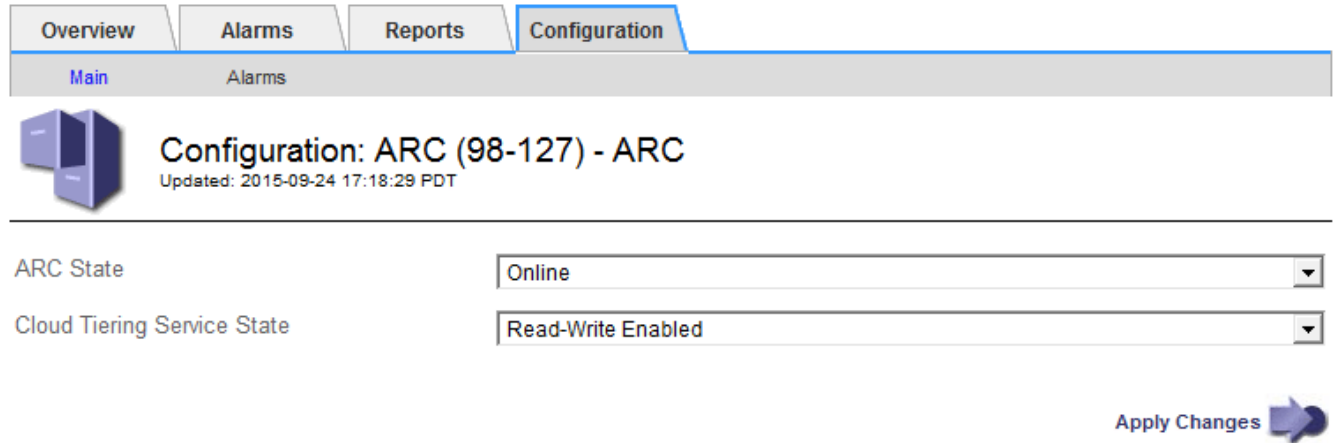
- Você deve estar conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você deve ter permissões de acesso específicas.
- O nó de arquivo deve ser configurado.

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**.




Overview Alarms Reports Configuration

Main Alarms

 Configuration: ARC (98-127) - ARC
Updated: 2015-09-24 17:18:29 PDT

ARC State Online

Cloud Tiering Service State Read-Write Enabled

Apply Changes 

4. Selecione um **Estado do Serviço de disposição em camadas na nuvem**.
5. Selecione **aplicar alterações**.

Redefina a contagem de falhas de armazenamento para conexão API S3

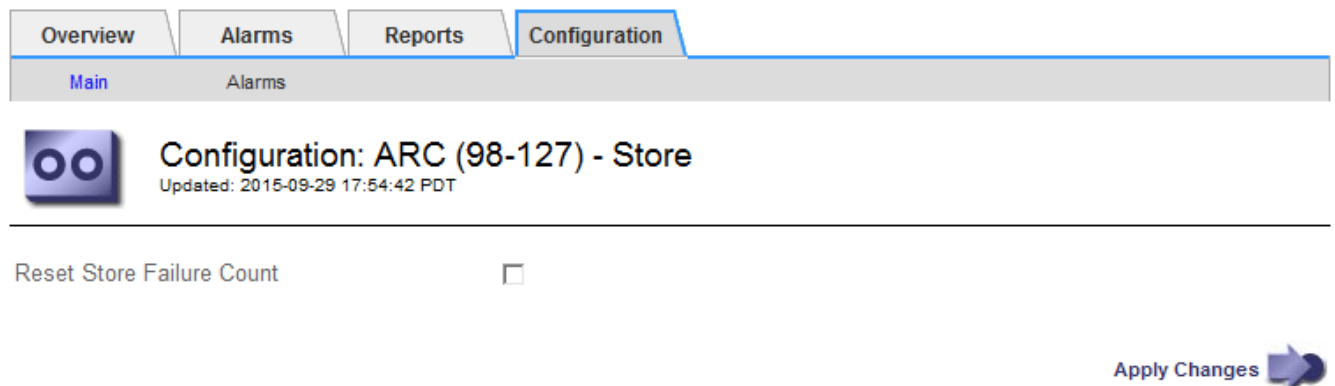
Se o seu nó de arquivo se conectar a um sistema de armazenamento de arquivos por meio da API S3, você poderá redefinir a contagem de falhas de armazenamento, que pode ser usada para limpar o alarme ARVF (falhas de armazenamento).

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.


Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Archive Node > ARC > Store**.
3. Selecione **Configuração > Principal**.




Overview Alarms Reports Configuration

Main Alarms

 Configuration: ARC (98-127) - Store
Updated: 2015-09-29 17:54:42 PDT

Reset Store Failure Count ☐

Apply Changes 

4. Selecione **Repor contagem de falhas de armazenamento**.

5. Selecione **aplicar alterações**.

O atributo Store Failures (falhas de armazenamento) é repostado a zero.

Migre 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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](#)

Archive para fita através do 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).

Configurar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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. Seleccione **SUPPORT > Tools > Grid topology**.
2. Seleccione **Archive Node > ARC > Target**.
3. Seleccione **Configuração > Principal**.

Overview Alarms Reports Configuration

Main Alarms

Configuration: ARC (DC1-ARC1-98-165) - Target
Updated: 2015-09-28 09:56:36 PDT

Target Type: Tivoli Storage Manager (TSM)

Tivoli Storage Manager State: Online

Target (TSM) Account

Server IP or Hostname: 10.10.10.123

Server Port: 1500

Node Name: ARC-USER

User Name: arc-user

Password: ••••••

Management Class: sg-mgmtclass

Number of Sessions: 2

Maximum Retrieve Sessions: 1

Maximum Store Sessions: 1

Apply Changes

4. Na lista suspensa **tipo de destino**, seleccione **Tivoli Storage Manager (TSM)**.
5. Para o **Tivoli Storage Manager State**, seleccione **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. Selecione **aplicar alterações**.

Otimize um nó de arquivo para sessões de middleware TSM

Você pode otimizar o desempenho de um nó de arquivo que se conecta ao Tivoli Server Manager (TSM) configurando as sessões do nó de arquivo.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem 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**.


Overview

Alarms

Reports

Configuration

MainAlarms


Configuration: ARC (DC1-ARC1-98-165) - Target
Updated: 2015-09-28 09:56:36 PDT

Target Type:

Tivoli Storage Manager (TSM)

Tivoli Storage Manager State:

Online

Target (TSM) Account

Server IP or Hostname:

10.10.10.123

Server Port:

1500

Node Name:

ARC-USER

User Name:

arc-user

Password:

••••••

Management Class:

sg-mgmtclass

Number of Sessions:


2

Maximum Retrieve Sessions:

2

Maximum Store Sessions:

1

Apply Changes 

5. Selecione **aplicar alterações**.

Configure o estado do arquivo e os contadores para o TSM

Se o seu Archive Node se conectar 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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Archive Node > ARC > Store**.
3. Selecione **Configuração > Principal**.

OverviewAlarmsReportsConfiguration

MainAlarms



Configuration: ARC (DC1-ARC1-98-165) - Store

Updated: 2015-09-29 17:10:12 PDT

Store State

Online


Archive Store Disabled on Startup

☐

Reset Store Failure Count

☐

Apply Changes



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. Selecione **aplicar alterações**.

Informações relacionadas

[Gerencie um nó de arquivo quando o servidor TSM atingir a capacidade](#)

Gerencie um nó de arquivo quando o servidor TSM atingir 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. Esta situação pode ser evitada através do monitoramento proativo do servidor TSM.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

Sobre esta tarefa

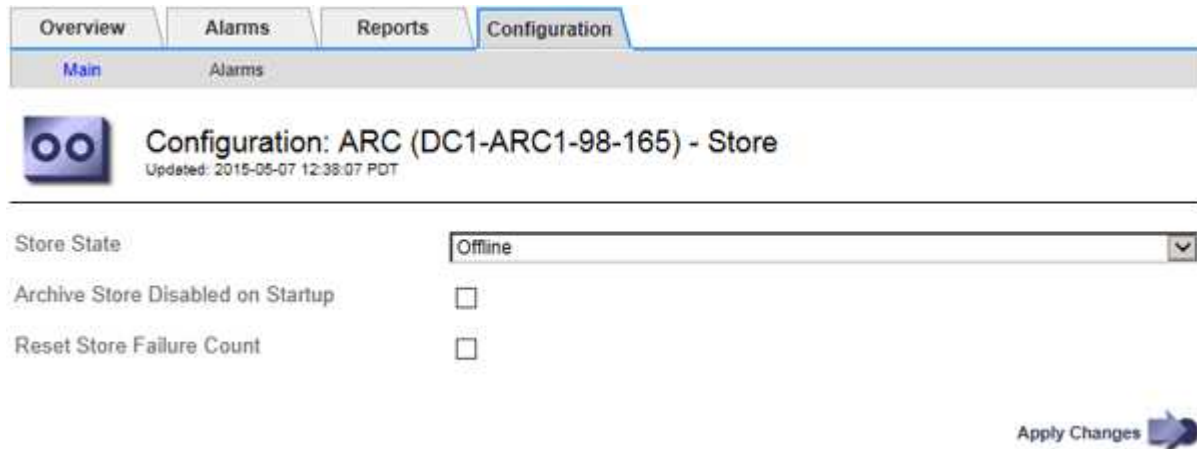
O nó de arquivo continua a aceitar dados de objeto para transferência para o servidor TSM depois que o servidor TSM parar de aceitar novo conteúdo. Este conteúdo não pode ser gravado em Mídia gerenciada pelo servidor TSM. Um alarme é acionado se isso acontecer.

Impedir que o serviço ARC envie conteúdo para o servidor TSM

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. Selecione **aplicar alterações**.

Defina Archive Node como 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.

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. Selecione **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 está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Archive Node > ARC > Retrieve**.
3. Selecione **Configuração > Principal**.

Configuration: ARC (DC1-ARC1-98-165) - Retrieve
Updated: 2015-05-07 12:24:45 PDT

Retrieve State	Online
Reset Request Failure Count	<input type="checkbox"/>
Reset Verification Failure Count	<input type="checkbox"/>

Apply Changes

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. Selecione **aplicar alterações**.

Configurar a replicação do nó de arquivo

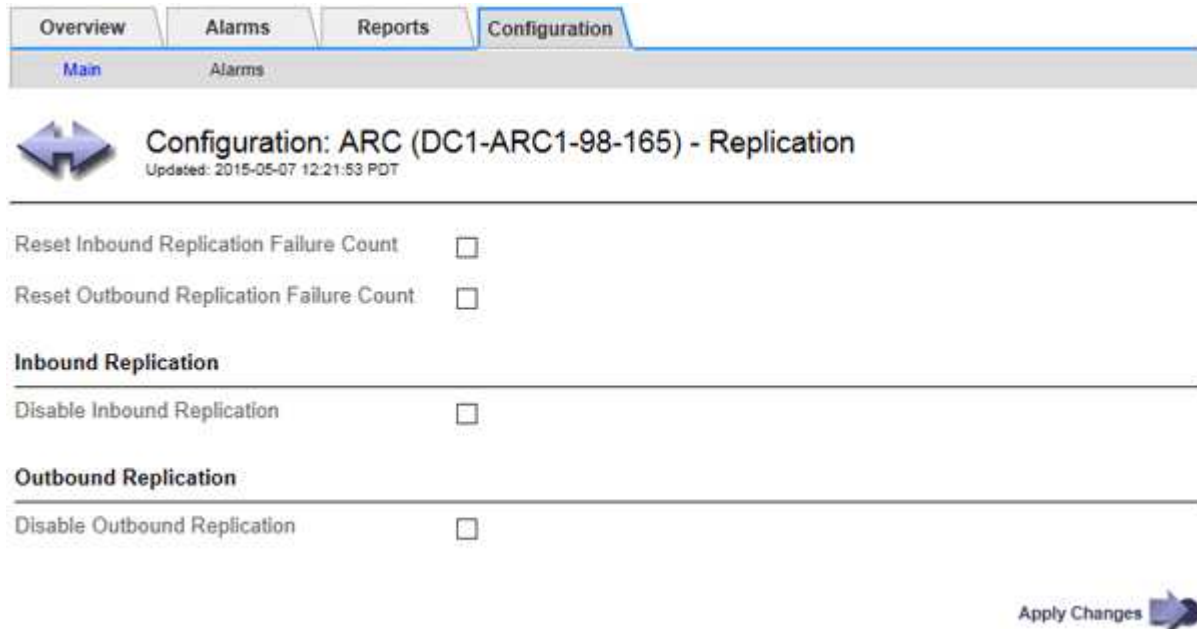
Você pode configurar as configurações de replicação para um nó de arquivo e desativar a replicação de entrada e saída ou redefinir as contagens de falha que estão sendo rastreadas para os alarmes associados.

O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.


Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **Archive Node > ARC > Replication**.
3. Selecione **Configuração > Principal**.



Overview Alarms Reports Configuration

Main Alarms

 Configuration: ARC (DC1-ARC1-98-165) - Replication
Updated: 2015-05-07 12:21:53 PDT

Reset Inbound Replication Failure Count ☐


Reset Outbound Replication Failure Count ☐

Inbound Replication

Disable Inbound Replication ☐

Outbound Replication

Disable Outbound Replication ☐

Apply Changes 

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. Selecione **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, monitore 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. [Monitorar e solucionar problemas](#) Consulte .

Integre o Tivoli Storage Manager

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.

Conclua 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.

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"](#)

Instale 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.

Configure 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 registrar 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.

Defina 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 login no servidor com Privileges administrativo e usar a ferramenta dsmadm 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 conectado 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 conectada 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 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).

Defina uma política de domínio e Registre 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 vaziar 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 "standard", 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 `dsmadm` para criar e ativar a diretiva de domínio.

Crie e ative 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.

Migrar 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.

Confirme 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 sistema StorageGRID, [Gerenciar nós de storage](#) consulte e [Monitorar e solucionar problemas](#).

Determine 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. [Gerenciar objetos com ILM](#) Consulte .



Uma política de ILM que foi incorretamente especificada pode causar perda de dados irreversível. Revise cuidadosamente todas as alterações feitas em uma política ILM antes de ativá-la para garantir que a política funcionará conforme pretendido.

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.

Agendar e monitorar a migração de dados

A migração de dados deve ser agendada e monitorada conforme necessário para garantir que os dados sejam colocados de acordo com a política de ILM dentro do prazo exigido.

Agendar a 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 monitore de perto os atributos relevantes e tome medidas se excederem os valores aceitáveis.

Monitorar a migração de dados

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	<ol style="list-style-type: none">1. Selecione SUPPORT > Tools > Grid topology.2. Selecione deployment > Overview > Main.3. Na seção ILM Activity, monitore o número de objetos mostrados para os seguintes atributos:<ul style="list-style-type: none">◦ Aguardando - todos (XQUZ): O número total de objetos aguardando avaliação ILM.◦ Aguardando - Cliente (XCQZ): O número total de objetos aguardando avaliação ILM das operações do cliente (por exemplo, ingest).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.

Informações sobre direitos autorais

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

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

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

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

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

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

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

Informações sobre marcas comerciais

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